On Group and Semigroup Algebras

Paula Murgel Veloso

'Would you tell me, please, which way I ought to go from here?'
'That depends a good deal on where you want to get to,' said the Cat.
'I don't much care where–' said Alice.
'Then it doesn't matter which way you go,' said the Cat.
'–so long as I get somewhere,' Alice added as an explanation.
'Oh, you're sure to do that,' said the Cat, 'if you only walk long enough.'
(Lewis Carroll, *Alice's Adventures in Wonderland*)

Agradecimentos

Ao Prof. Arnaldo Garcia, do IMPA, pela orientação do meu mestrado e do meu doutorado, e pelo incentivo.

Ao Prof. Guilherme Leal, da UFRJ, pela co-orientação do meu doutorado, por ter-me proposto o problema que resultou no segundo capítulo desta tese, e pelo apoio constante.

Aos Profs. Eduardo Esteves, do IMPA, Jairo Gonçalves, da USP, Pavel Zalesski, a UNB, e Amilcar Pacheco, da UFRJ, membros da banca de defesa de tese, pelos comentários e sugestões.

To Prof. Eric Jespers, from Vrije Universiteit Brussel, for having proposed the problem presented in the third chapter of this thesis, for the elucidative conversations, good advice and kind hospitality during my stay in Brussels.

À Prof. Luciane Quoos, da UFRJ, pelas discussões matemáticas sempre esclarecedoras e bem-humoradas, e pela colaboração no artigo no qual se baseia o segunto capítulo desta tese.

To Dr. Ann Dooms, from Vrije Universiteit Brussel, for the nice and fruitful discussions and friendly support, and for the collaboration on the article in which the third chapter of this thesis is based.

Aos Profs. Paulo Henrique Viana (*in memoriam*), Carlos Tomei e Pe. Paul Schweitzer, da PUC-Rio, por me mostrarem a beleza da Matemática e pela amizade.

Aos professores do IMPA, em especial aos Profs. Karl-Otto Stöhr, César Camacho, Paulo Sad e Manfredo do Carmo.

A todos os meus colegas do IMPA, principalmente aos meus amigos de turma do mestrado e aos amigos da Álgebra Juscelino Bezerra, Cleber Haubrichs, Juliana Coelho e André Contiero.

Aos professores e alunos grupo de Álgebra Não-Comutativa da UFRJ.

To the colleagues, professors and friends from Vrije Universiteit Brussel, especially Isabel Goffa, Julia Dony and Kris Janssen.

A todos os funcionários do IMPA, em especial àqueles da Comissão de Ensino, da xerox e da segurança.

Ao CNPq, pelo apoio financeiro e pela oportunidade de passar um ano

na Vrije Universiteit Brussel, Bruxelas, Bélgica, no programa de doutorado-sanduíche.

Aos amigos Leandro Pimentel, Lourena Rocha, Marcos Petrúcio Cavalcante, Cecília Salgado, José Cal Neto, Ricardo Bello, Taissa Abdalla, Kaká Boa Morte, Yolande Lisbona, Wanderley Pereira, Alexandre Toledo, Helder Gatti, Raul Tanaka, Eri Lou Nogueira, Paula Avellar, Sérgio Leiros, Karla Suite, Cristina Diaconu, Maria Agustina Cibran, pela amizade, pela companhia em todos os momentos, por enriquecerem e iluminarem minha vida.

À minha família, principalmente aos meus pais Paulo Augusto e Sheila Regina, e à minha irmã Flávia, pelo ambiente familiar sempre alegre e acolhedor, pelos constantes carinho, incentivo, paciência e exemplo.

Paula Murgel Veloso
Julho, 2006

Contents

Introduction

In this work, we are interested in Group Ring Theory. Although some issues in Semigroup Ring Theory are also presented, the main focus is group rings.

In CHAPTER 1, the basic theoretical foundations in group and semigroup rings are laid. These ideas will be used throughout the entire work.

We begin with a presentation of definitions and theorems from Ring Theory, establishing their particular instances in the context of group rings. We define group rings; the augmentation mapping; involutions; the Jacobson radical of a ring; idempotents; simple components; the character table of a group; trivial, bicyclic and unitary units; the upper central series, the FC center and the hypercenter of a group. Important results from Ring and Group Ring Theory are then recalled, such as Wedderburn-Malcev theorem, the decomposition of a semisimple ring in a direct sum of ideals, Wedderburn-Artin theorem, Maschke theorem. For the sake of completeness and because this may be elucidating in the sequel, some results are presented with their proofs (Perlis-Walker theorem, the character method for obtaining primitive central idempotents in group algebras over complex fields, Berman-Higman lemma and its corollaries).

As a prerequisite to the study of semigroup rings, we briefly present fundamental concepts from Semigroup Theory. We define semigroups and special kinds of semigroups (regular, inverse, completely 0-simple, Brandt); idempotents; principal factors and principal series of a semigroup; provide basic results concerning the structure of semigroups, and present elucidative and useful examples, such as Rees matrix semigroups and Malcev nilpotent semigroups. Fundamental notions from Semigroup Ring Theory are then exposed: we define semigroup and contracted semigroup rings, followed by some clarifying examples, and results concerning the structure of semisimple semigroup algebras, with special attention given to semigroup algebras over the rational field, matrix semigroup rings and Munn algebras.

The reader who is well acquainted with all these concepts can concentrate on the notation introduced.

CHAPTER 2 is part of a joint work ([33]) with Prof. Luciane Quoos, from the Institute of Mathematics, UFRJ. The main result in this chapter is an alternative procedure to compute the primitive central idempotents of a group algebra of a finite nilpotent group over the complex field, not relying on the character table of the group, following methods previously applied by Jespers and Leal to the rational case. As a partial result, we present a formula for the primitive idempotents of the group algebra of the finite abelian group over any field, which permits to build all cyclic codes over a given finite field.

At first, some notation is fixed, and we state and prove a theorem that yields a formula for the primitive idempotents in a semisimple group algebra of a finite abelian group over an algebraically closed field; though the result is extremely useful and new, the proof is quite easy and short. Next, the same result is extended to a semisimple group algebra of a finite abelian group over an any field, using the known method of Galois descent.

Then some technical definitions and facts, which appear in the literature specific to the study of primitive central idempotents, are stated. A few recent results on the subject are recalled, as they play an auxiliary role to our main result. Finally, a fully internal description of the primitive central idempotents of a group algebra of a finite nilpotent group over the complex field is presented. The classical method for computing primitive central idempotents in complex group algebras relies on the character table of the group, whose construction has complexity growing exponentially with the order of the group. Our tool depends only on a lattice of subgroups of the given group, satisfying some intrinsic conditions. Though the complexity of this new method is still unknown, it is a theoretic alternative to the classical character method that might turn out to be simpler and faster to use.

The material in CHAPTER 3 is based on a joint work ([9]) with Dr. Ann Dooms, from the Department of Mathematics, Vrije Universiteit Brussel, where I had the opportunity of spending one year of my Ph.D. under the support of CNPq, Brasil. We define the new concept of the normalizer of a semigroup in the unit group of its integral semigroup ring. Several known results and properties on the normalizer of the trivial units in the unit group of an integral group ring are shown to hold for the normalizer of a finite inverse semigroup. This indicates that our concept of normalizer of a semigroup behaves as desired, and might be suitable and helpful in investigations on the isomorphism problem in semigroup rings and partial group rings, as is analogously done with group rings. We also construct free groups in the unit group of the integral semigroup ring of an inverse semigroup, using a bicyclic unit and its image under an involution.

We start by giving the definition of the normalizer of a semigroup in the unit group of its integral semigroup ring. This definition coincides with the normalizer of the trivial units in the case of an integral group ring and behaves very much like it in inverse semigroups. These semigroups have a natural involution, and semigroup rings of inverse semigroups are a wide and interesting class containing, for instance, matrix rings and partial group rings. This natural involution allows us to extend Krempa's characterization of the normalizer in group rings to a very useful property of the normalizer of a semigroup. We will describe the torsion part of the normalizer and investigate the double normalizer. Just like in group rings, the normalizer of a semigroup contains the finite conjugacy center of the unit group of the integral semigroup ring and the second center. It remains open what the normalizer is in case the semigroup ring is not semisimple; we give an example that provides some clues of how the normalizer might behave in this case. This new concept of normalizer might be useful to tackle the isomorphism problem for semigroup rings and partial group rings, and this is an interesting path to follow in further studies.

The normalizer problem is then posed for integral semigroup rings, and solved for finite Malcev nilpotent semigroups having a semisimple rational semigroup ring. Like with integral group rings, we get that the normalizer of a finite semigroup is a finite extension of the center of the semigroup ring.

Borel and Harish-Chandra showed the existence of free groups contained in the unit group of an integral semigroup ring. As an additional consequence of the investigation of the natural involution in a Brandt semigroup, we investigate the problem of constructing free groups in the unit group of an integral semigroup ring using a bicyclic unit and its involuted image, following Marciniak and Sehgal.

These are, so far, my contributions to the investigation of group rings.

Chapter 1

Preliminaries

In this beginning chapter, we shall collect most of the needed background in group and semigroup ring theory. For a more comprehensive approach, we refer the reader to [25], [36], [4] and [30]. Those familiar with all the required concepts can concentrate on the notation.

1.1 Group Ring Theory

1.1.1 Basic Definitions

Definition 1.1.1. Let G be a (multiplicative) group, and R be a ring with identity 1. The *group ring* RG is the ring of all formal sums $\alpha = \sum_{g\in G} \alpha_g g$, $\alpha_g \in R$, with finite *support* $supp(\alpha) = \{g \in G; \alpha_g \neq 0\}$. We say that α_g is the *coefficient of* g *in* α. Two elements α and β in RG are equal if and only if they have the same coefficients. The zero element in RG is the element $0 := \sum_{g\in G} 0g$, and the identity in RG is the element $1 := 1e + \sum_{g\in G\setminus\{e\}} 0g$ (with e the identity in G, which shall be denoted henceforth by 1). The *sum* $\alpha + \beta$ is the element $\sum_{g\in G}(\alpha_g + \beta_g)g$. The *product* $\alpha\beta$ is the element $\sum_{g\in G} \gamma_g g$, where $\gamma_g = \sum_{\substack{x,y\in G \\ xy=g}} \alpha_x\beta_y$, for each $g \in G$. If R is a commutative ring, then RG is an R-algebra and is called a *group algebra*.

Definition 1.1.2. Let RG be a group ring. The *augmentation mapping* of RG is the ring homomorphism $\varepsilon : RG \to R$, $\sum_g \alpha_g g \mapsto \sum_g \alpha_g$. Its kernel, denoted by $\Delta(G)$, is the *augmentation ideal of* RG. We have that $\Delta(G) = \left\{\sum_{g\in G} \alpha_g(g-1); \alpha_g \in R\right\}$.

If N is a normal subgroup of G, then there exists a natural homomorphism $\varepsilon_N : RG \to R(G/N)$, $\sum_g \alpha_g g \mapsto \sum_g \alpha_g gN$. The kernel of this mapping, denoted by $\Delta_R(G, N)$, is the ideal of RG generated by $\{n-1; n \in N\}$.

We recall the definition of a ring with involution.

Definition 1.1.3. Let A be a commutative ring and R be an A-algebra. An *involution on* R is an A-module automorphism $\tau : R \to R$ such that, for all $x, y \in R$

$$\tau(xy) = \tau(y)\tau(x) \text{ and } \tau^2(x) = x.$$

Let G be a group. If R is a ring with an involution τ, we can define an involution $*$ on RG extending τ as

$$(\sum_{g\in G} \alpha_g g)* := \sum_{g\in G} \tau(\alpha_g)g^{-1}.$$

For instance, we can define an involution on $\mathbb{C}G$, known as the *classical involution* as $(\sum_{g\in G} \alpha_g g)* := \sum_{g\in G} \overline{\alpha_g} g^{-1}$, where $\overline{\alpha_g}$ denotes the complex conjugate of α_g.

Now we need some concepts and results from Ring Theory that are relevant in studying group rings.

Definition 1.1.4. Let R be a ring. The *Jacobson radical of* R, denoted by $Jac(R)$ or $\mathcal{J}(R)$, is defined as the intersection of all maximal left ideals in R if $R \neq 0$, or as (0) if $R = 0$.

Evidently, if $R \neq 0$, maximal ideals always exist by Zorn's Lemma.

In the definition above, we used left ideals; we could similarly define the right Jacobson radical of R. It turns out that both definitions coincide (see [17, §4]), so the Jacobson radical of a ring is a two-sided ideal.

The Jacobson radical of a ring has many important properties and shows up in a number of theorems in Group and Semigroup Ring Theory. We shall mention only the ones we need in this work.

Lemma 1.1.5. *[25, Lemma 2.7.5] Let R be a ring. Then $\mathcal{J}(R/\mathcal{J}(R)) = 0$.*

Definition 1.1.6. An element e in a ring R is said to be an *idempotent* if $e^2 = e$. If e is an idempotent, $e \neq 0$ and $e \neq 1$, then e is a *nontrivial idempotent*. Two distinct idempotents e and f in a ring R are said to be *orthogonal* if $ef = fe = 0$. An idempotent e is said to be *primitive* if it cannot be written as $e = e' + e''$, with e' and e'' nonzero orthogonal idempotents.

Definition 1.1.7. Let R be a ring, and M be a (left) R-module. M is called a *simple* (or *irreducible*) *(left) R-module* if M is nonzero and M has no (left) R-submodules other than (0) and M. A nonzero ring R is said to be a *simple ring* if (0) and R are the only two-sided ideals of R.

Definition 1.1.8. Let R be a ring, and M be a (left) R-module. M is called a *semisimple* (or *completely reducible*) *(left) R-module* if every (left) R-submodule of M is a direct summand of M (i.e., for every (left) R-submodule N of M, there is a (left) R-submodule N' such that $M = N \oplus N'$).

Evidently, an analogous definition makes sense for rings (an equivalent definition of semisimplicity for an Artinian ring R is $Jac(R) = 0$ [25, Theorem 2.7.16]) . It is worth observing that the notions of left and right semisimplicity are equivalent for rings (see, for instance, [17, Corollary 3.7]).

If R is a semisimple ring, then the inner structure of R determines all the simple R-modules, up to isomorphism.

Lemma 1.1.9. *[25, Lemma 2.5.13] Let R be a semisimple ring, L be a minimal left ideal of R and M be a simple R-module. We have that $LM \neq 0$ if and only if $L \simeq M$ as R-modules; in this case, $LM = M$.*

Certain rings can be decomposed as a direct sum of ideals. Recall that a field F is a *perfect field* if every algebraic extension of F is separable, or, equivalently, $char(F) = 0$ or $char(F) = p \neq 0$ and $F^p = F$.

Theorem 1.1.10 (Wedderburn–Malcev). *[35, Theorem 2.5.37] Let R be a finite dimensional algebra over a perfect field F. Then*

$$R = \mathcal{S}(R) \oplus \mathcal{J}(R) \text{ (as a vector space over } F),$$

where $\mathcal{J}(R)$ is the Jacobson radical of R, and $\mathcal{S}(R)$ is a subalgebra of R isomorphic to $R/\mathcal{J}(R)$.

In the Wedderburn–Malcev Theorem, notice that, since $\mathcal{S}(R) \simeq R/\mathcal{J}(R)$, we have that $\mathcal{S}(R)$ is a semisimple algebra by Lemma 1.1.5.

The decomposition of a ring as a direct sums of ideals has a very important particular case when the ring is semisimple.

Theorem 1.1.11. *[25, Theorem 2.5.11] Let $R = \bigoplus_{i=1}^{s} A_i$ be a decomposition of a semisimple ring R as a direct sum of minimal two-sided ideals. Then there exists a uniquely determined family $\{e_1, \ldots, e_s\}$ such that:*

1. *e_i is a nonzero central idempotent, for $i = 1, \ldots, s$;*
2. *$e_i e_j = \delta_{ij} e_i$, for $i, j = 1, \ldots, s$, where δ_{ij} is Kronecker's delta (in particular, e_i and e_j are orthogonal for $i \neq j$);*
3. *$1 = \sum_{i=1}^{s} e_i$;*

4. *e_i cannot be written as $e_i = e_i' + e_i''$, where e_i' and e_i'' are both nonzero central orthogonal idempotents, for $1 \leq i \leq s$.*

Conversely, if there exists a family of idempotents $\{e_1, \ldots, e_s\}$ satisfying the above conditions, then $A_i := Re_i$ are minimal two-sided ideals and $R = \bigoplus_{i=1}^{s} A_i$. The elements $\{e_1, \ldots, e_s\}$ are called the primitive central idempotents of R.

Definition 1.1.12. The unique two-sided ideals of a semisimple ring R are called the *simple components of R*

The following characterization of semisimple rings will be very important for us:

Theorem 1.1.13 (Wedderburn–Artin). *[17, Theorem 3.5] A ring R is semisimple if and only if it is a direct sum of matrix algebras over division rings, i.e., $R \simeq M_{n_1}(D_1) \oplus \ldots \oplus M_{n_s}(D_s)$, where $n_1, \ldots, n_s$ are positive integers and $D_1, \ldots, D_s$ are division rings. The number s and the pairs $(n_1, D_1), \ldots, (n_s, D_s)$ are uniquely determined (up to permutations).*

Now we can proceed to translate these ring theoretical concepts into valuable information about group rings.

Theorem 1.1.14 (Maschke). *[25, Corollary 3.4.8] Let K be field and G be a finite group. The group algebra KG is semisimple if and only if $char(K)$ does not divide $|G|$.*

The following special elements of a group ring play a major role both in Group Ring Theory and in the present work in particular.

Definition 1.1.15. Let R be a ring with identity and let H be a finite subset of a group G. Define the element $\widehat{H}$ of RG as $\widehat{H} := \sum_{h \in H} h$. If $H = \langle a \rangle$ is a cyclic subgroup of G of finite order, we shall sometimes write $\widehat{a}$ instead of $\widehat{\langle a \rangle}$. If $|H|$ is invertible in R, we may define the element $\widetilde{H}$ of RG as $\widetilde{H} := \frac{1}{|H|} \sum_{h \in H} h$. If $\{C_i\}_{i \in I}$ is the set of conjugacy classes of G which contain only a finite number of elements, then the elements $\widehat{C}_i$ in RG are called the *class sums of G over R.*

These constructions enable us to get, for instance, a basis for the center of a group ring and idempotent elements.

Theorem 1.1.16. *[25, Theorem 3.6.2] Let G be a group and R be a commutative ring. The set $\{\widehat{C}_i\}_{i \in I}$ of all class sums of G over R is a basis of $\mathcal{Z}(RG)$ over R.*

Lemma 1.1.17. *[25, Lemma 3.6.6] Let R be a ring with identity and let H be a finite subgroup of a group G. If $|H|$ is invertible in R, then $\widetilde{H}$ is an idempotent of RG. Moreover, $\widetilde{H}$ is central if and only if $H \lhd G$.*

Group Representation Theory is a very powerful means to obtain new results in Algebra. It is also a useful tool to "realize" an abstract group as a concrete one. Some knowledge of Group Representation Theory is vital to the understanding of group rings.

Definition 1.1.18. Let G be a group, R a commutative ring and V a free R-module of finite rank. A *representation of G over R, with representation space V* is a group homomorphism $T : G \to GL(V)$, where $GL(V)$ denotes the group of R-authomorphisms of V. The rank of V is called the *degree of T* and denoted by $deg(T)$. Fixing an R-basis of V, we can define an isomorphism between $GL(V)$ and $GL_n(R)$, with $n = deg(T)$, where $GL_n(R)$ denotes the group of $n \times n$ invertible matrices with coefficients in R. We can thus consider the induced group homomorphism $T : G \to GL_n(R)$, in which case we talk about a *matrix representation*.

Two representations $T : G \to GL(V)$ and $T' : G \to GL(W)$ of G over R are *equivalent representations* if there exists an isomorphism of R-modules $\phi : V \to W$ such that $T'(g) = \phi \circ T(g) \circ \phi^{-1}$, for all $g \in G$. A representation $T : G \to GL(V)$ is an *irreducible representation* if $V \neq 0$ and if V and 0 are the only invariant subspaces of V under T.

There is a strong connection between group representations and modules, in which group rings play a major role, as it may be seen in the following proposition:

Proposition 1.1.19. *[25, Propositions 4.2.1 and 4.2.2] Let G be a group and R be a commutative ring with identity. There is a bijection between the representations of G over R and the (left) RG-modules which are free of finite rank over R:*

- *given a representation $T : G \to GL(V)$ of G over R, associate to it the (left) RG-module M constructed from V by keeping the same additive structure and defining the product of $v \in V$ by $\alpha \in RG$ as $\alpha v := \sum_{g \in G} \alpha_g T(g)(v)$;*
- *if M is a (left) RG-module which is free of finite rank over R, define the representation $T : G \to GL(M)$; $T(g) : m \mapsto gm$.*

Two representations of G over R are equivalent if and only if the corresponding (left) RG-modules are isomorphic. Also, a representation is irreducible if and only if the corresponding (left) RG-module is simple.

The case when a group is represented over a field is of particular interest. Historically, this was the first case to be studied and, therefore, most applications were developed in this context.

The notion of character is of fundamental importance in Group Representation Theory and in Group Theory. It also shows up in the study of group rings; in particular, there is a well-known formula for computing idempotents of complex group algebras of finite groups that completely relies on characters.

Definition 1.1.20. Let $T : G \to GL(V)$ be a representation of a group G over a field K, with representation space V. The *character χ of G afforded by T* is the map $\chi : G \to K; g \mapsto tr(T(g))$, where $tr(T(g))$ is the trace of the matrix associated to $T(g)$ with respect to any basis of V over K. If T is an irreducible representation, then χ is called an *irreducible character*

Proposition 1.1.21. *[25, Proposition 5.1.3] Let G be a finite group and K be a field such that $char(K) \nmid |G|$. Consider $\chi_1, \ldots, \chi_r$ the characters afforded by a complete set $T_1, \ldots, T_r$ of inequivalent irreducible representations of G over K. Then the set of all characters of G over K is the set $\{\chi = \sum_{i=1}^{r} n_i\chi_i; n_i \in \mathbb{Z}, i = 1, \ldots, r\}$.*

Next, we give an example of a very special representation and the corresponding character, which will be useful in the sequel.

Example 1.1.22 (Regular Representation and Regular Character). Let G be a finite group of order n. Consider the representation $T : G \to GL(\mathbb{C}G)$ that associates to each $g \in G$ the linear map $T_g : x \mapsto gx$. This is called the *regular representation of G over $\mathbb{C}$*. Denote by ρ the character afforded by T, i.e., the *regular character*.

Regard T as the matrix representation obtained by taking the elements of G in some order as an R-basis of RG. It is clear that the image of each $g \in G$ is a permutation matrix. Notice that if $g \neq 1$, then $gx \neq x$, so all the elements on the diagonal of matrix $T(g)$ are equal to zero. Hence,

$$\rho(g) = \begin{cases} 0 & , \text{if } g \neq 1 \\ |G|, & , \text{if } g = 1. \end{cases}$$

We know that

$$\mathbb{C}G \simeq M_{n_1}(\mathbb{C}) \oplus \ldots \oplus M_{n_s}(\mathbb{C}) \simeq (\mathbb{C}G)e_1 \oplus \ldots \oplus (\mathbb{C}G)e_s$$

(Theorem 1.1.13 and Theorem 1.1.11), with $\{e_1, \ldots, e_s\}$ the primitive central idempotents of $\mathbb{C}G$, and that, for all $i = 1, \ldots, s$, $M_{n_i}(\mathbb{C}) \simeq (\mathbb{C}G)e_i \simeq$

$L_1^i \oplus \ldots \oplus L_{n_i}^i$, where L_j^i denotes the irreducible (left) $\mathbb{C}G$-module consisting of $n_i \times n_i$ matrices having complex elements on the j^{th} column and zeros elsewhere. Clearly, by Lemma 1.1.9, for all $j = 1, \ldots, n_i$, $L_j^i \simeq L_1^i$ (as $\mathbb{C}G$-modules), which has dimension n_i over $\mathbb{C}$. So, $\mathbb{C}G \simeq n_1 L_1^1 \oplus \ldots \oplus n_s L_1^s$.

If T_i denotes the irreducible representation of G over $\mathbb{C}$ corresponding to L_1^i and χ_i denotes the character T_i affords, then we have that $T = \bigoplus_{i=1}^s n_i T_i$ and $\rho = \sum_{i=1}^s n_i \chi_i$. Since $n_i = deg(T_i) = \chi_i(1)$ (because $\chi_i(1) = tr(T_i(1)) = tr(I_{n_i})$, where I_{n_i} is the $n_i \times n_i$ identity matrix), it follows that

$$\rho = \sum_{i=1}^{s} \chi_i(1)\chi_i \ (*).$$

In the isomorphism $\mathbb{C}G \simeq M_{n_1}(\mathbb{C}) \oplus \ldots \oplus M_{n_s}(\mathbb{C})$, each idempotent e_i corresponds to the element $(0, \ldots, 0, I_{n_i}, 0, \ldots, 0)$, with I_{n_i} the identity matrix in $M_{n_i}(\mathbb{C})$. It is clear that $T_i(e_i)$ is the linear function defined in L_1^i by multiplication by the identity element, i.e., it is the identity function on the simple component $M_{n_i}(\mathbb{C})$. Since $e_i e_j = \delta_{ij} e_i$, it follows that

$$T_i(e_j) = \begin{cases} 0 & , \text{if } i \neq j, \\ I_{n_i} & , \text{if } i = j; \end{cases}$$

and

$$\chi_i(e_j) = \begin{cases} 0 & , \text{if } i \neq j, \\ tr(I_{n_i}) = deg(T_i) & , \text{if } i = j. \end{cases}$$

Lemma 1.1.23. *Let G be a group and χ be a character afforded by a representation of G. Then χ is constant on each of the conjugacy classes of G.*

Thus, the following definition makes sense:

Definition 1.1.24. Let G be a group and $C_1, \ldots, C_r$ be its conjugacy classes. Choose, for each i, an arbitrary $x_i \in C_i$. The matrix $(\chi_i(x_j))$ is called the *character table of G*.

The case of group characters over the complex field will be extremely important for us. We would like to know the dimensions of the complex character table of a group. Notice that we learn, from example 1.1.22, that the number of irreducible characters of a group G is equal to s, the number of simple components in the Wedderburn–Artin decomposition of $\mathbb{C}G$. In fact, more is known:

Proposition 1.1.25. *[25, Proposition 3.6.3, Theorem 4.2.7] Let G be a finite group and K be an algebraically closed field such that $char(K) \nmid |G|$. Then the number of simple components of KG is equal to the number of conjugacy classes of G, which equals the number of irreducible nonequivalent representations of G over K.*

Remark 1.1.26. Actually, the above proposition is still true in a slightly more general setting: when K is a splitting field for G (see [25, Definition 3.6.4]).

Let A be a ring (with identity). We recall that we denote by $\mathcal{U}(A)$ the multiplicative group of units of A, i.e.,

$$\mathcal{U}(A) := \{x \in A; xy = yx = 1, \text{ for some } y \in A\}.$$

There are not many known methods for constructing units in group rings, most of them being either elementary or very old. Therefore, describing units in group rings is a very active and important field of research.

Definition 1.1.27. Let R be a ring with identity and G be a group. An element in the group ring RG of the form rg, where $r \in \mathcal{U}(R)$ and $g \in G$, is called a *trivial unit of RG*, its inverse being the element $r^{-1}g^{-1}$.

For instance, the trivial units in $\mathbb{Z}G$ are the elements of $\pm G$. Generally speaking, group rings do have nontrivial units, though these may be hard to find.

Let A be a ring with zero divisors. Take $x, y \in A \setminus \{0\}$ such that $xy = 0$. Then, for an arbitrary $t \in A$, $\eta := ytx$ is a square zero element. Thus, $1 + \eta$ is a unit, with inverse $1 - \eta$. A very special and important case occurs when A is an integral group ring.

Definition 1.1.28. Let G be a group. Consider $a, b \in G$, with a of finite order, and define

$$u_{a,b} := 1 + (1 - a)b\widehat{a}.$$

Since $(1 - a)\widehat{a} = 0$, $u_{a,b}$ is a unit in $\mathbb{Z}G$, called a *bicyclic unit*.

Notice that the definition of bicyclic units still makes sense for integral semigroup rings (see Section 1.2).

Proposition 1.1.29. *[25, Proposition 8.1.6] Let g, h be elements of a group G, with $o(g) < \infty$. Then, the bicyclic unit $u_{g,h}$ is trivial if and only if h normalizes $\langle g \rangle$ and, in this case $u_{g,h} = 1$.*

Next, we define a type of unit that is related to the classical involution on an integral group ring.

Definition 1.1.30. Let G be a group. An element $u \in \mathbb{Z}G$ is said to be a *unitary unit* if $uu^* = u^*u = 1$, where $*$ is the classical involution on $\mathbb{Z}G$ (see Definition 1.1.3).

Now we recall some definitions from Group Theory that will be helpful when studying the unit group of group rings and semigroup rings (see [34]).

Definition 1.1.31. Let G be a group. Consider the *upper central series of* G

$$\{1\} = \mathcal{Z}_0(G) \leq \mathcal{Z}_1(G) \leq \mathcal{Z}_2(G) \leq \ldots,$$

defined inductively as $\mathcal{Z}_1(G) := \mathcal{Z}(G)$ and $\mathcal{Z}_n(G)$, the n^{th} *center of* G, is the only subgroup of G such that

$$\mathcal{Z}_n(G)/\mathcal{Z}_{n-1}(G) = \mathcal{Z}(G/\mathcal{Z}_{n-1}(G)).$$

Notice that $u \in \mathcal{Z}_{n+1}(G)$ if and only if $(u, g) \in \mathcal{Z}_n(G)$, for all $g \in G$, where $(u, g) := u^{-1}g^{-1}ug$ is the *commutator of* u *and* g.

The union

$$\mathcal{Z}_\infty(G) := \bigcup_i \mathcal{Z}_i(G)$$

is called the *hypercenter of* G. If there exists $m \in \mathbb{N}$ such that $\mathcal{Z}_\infty(G) = \mathcal{Z}_m(G)$ and m is the smallest possible number with this property, then m is called the *central height of* G.

Let N and H be subsets of G. The *centralizer of* H *in* N is defined by

$$\mathcal{C}_N(H) := \{g \in N; gh = hg, \forall h \in H\}.$$

The *finite conjugacy center of* G (or *FC center of* G) $\Phi(G)$ is the set of all elements of G that have a finite number of conjugates in G, i.e.,

$$\Phi(G) := \{g \in G; |\mathcal{C}_g| < \infty\} = \{g \in G; (G : \mathcal{C}_G(g)) < \infty\},$$

where $\mathcal{C}_g$ denotes the G-conjugacy class of $g \in G$. It is well known ([25, Lemma 1.6.3]) that $\Phi(G)$ is a characteristic subgroup of G.

Let H be a subgroup of G and $g, h \in G$. We denote by H^g the conjugate of H by g, i.e.,

$$H^g = gHg^{-1},$$

and we denote by h^g the conjugate of h by g, i.e.,

$$h^g = ghg^{-1}.$$

1.1.2 Some Results

In this subsection, we recall some results that will be helpful in the sequel. Although these are basic facts from Group Ring Theory, we include their proofs for the sake of completeness.

The next theorem deals with the problem of finding the Wedderburn–Artin decomposition (according to Theorem 1.1.13) of a semisimple group algebra KG of a finite abelian group G.

Theorem 1.1.32. *[32, Perlis–Walker] Let G be a finite abelian group of order n, and K be a field such that $char(K) \nmid n$. Then*

$$KG \simeq \bigoplus_{d|n} a_d K(\zeta_d),$$

where $a_d K(\zeta_d)$ denotes the direct sum of a_d copies of $K(\zeta_d)$, ζ_d are primitive roots of unity of order d and $a_d = n_d/[K(\zeta_d) : K]$, with n_d denoting the number of elements of order d in G.

Proof. Let us first analyse the case when $G = \langle a; a^n = 1\rangle$ is a cyclic group of order n.

Consider the map $\phi : K[X] \to KG; f \mapsto f(a)$. We have that ϕ is a ring epimorphism with kernel $(X^n - 1)$; thus $KG \simeq \frac{K[X]}{(X^n-1)}$. Consider $X^n - 1 = \prod_{d|n} \Phi_d$, the decomposition of $X^n - 1$ in cyclotomic polynomialnomials Φ_d in $K[X]$, i.e., $\Phi_d = \prod_j (X - \zeta_j)$, where ζ_j runs over all the primitive roots of unity of order d, for all $d|n$. For each d, let $\Phi_d = \prod_{i=1}^{a_d} f_{d_i}$ be the decomposition of Φ_d in irreducible polynomials in $K[X]$. So,

$$X^n - 1 = \prod_{d|n} \prod_{i=1}^{a_d} f_{d_i}.$$

Since $char(K) \nmid n$, it follows that $X^n - 1$ is a separable polynomial, i.e., all the f_{d_i}'s are distinct irreducible polynomials. By the Chinese Remainder Theorem, it follows that

$$KG \simeq \bigoplus_{d|n} \bigoplus_{i=1}^{a_d} \frac{K[X]}{(f_{d_i})}.$$

Now, for each d_i, we have that $\frac{K[X]}{(f_{d_i})} \simeq K(\zeta_{d_i})$, with ζ_{d_i} a root of f_{d_i}. Thus,

$$KG \simeq \bigoplus_{d|n} \bigoplus_{i=1}^{a_d} K(\zeta_{d_i}),$$

and ζ_{d_i} are primitive roots of unity of orders d dividing n. So, for a fixed d, we have that $K(\zeta_{d_i}) = K(\zeta_{d_j})$, for any $i, j = 1, \ldots, a_d$, and we may write

$$KG \simeq \bigoplus_{d|n} a_d K(\zeta_d),$$

with ζ_d a primitive root of unity of order d. Also, $deg(f_{d_i}) = [K(\zeta_d) : K]$, for all $i = 1, \ldots, a_d$, so, taking degrees in the decomposition of Φ_d, we have that $\phi(d) = a_d[K(\zeta_d) : K]$, where ϕ denotes Euler's totient function. It is well known that, since G is a cyclic group of order n, for any divisor d of n, the number n_d of elements of order d in G is precisely $\phi(d)$. Hence, $a_d = n_d/[K(\zeta_d) : K]$.

Suppose now that G is a finite abelian noncyclic group. We proceed by induction on the order of G. So assume the result holds for any abelian group of order less than n.

Using the Structure Theorem of Finite Abelian Groups, we can write $G = G_1 \times H$, with H a cyclic group of order n_2 and $|G_1| = n_1 < n$. By the induction hypothesis, we can write $KG_1 \simeq \bigoplus_{d_1|n_1} a_{d_1} K(\zeta_{d_1})$, with $a_{d_1} = \frac{n_{d_1}}{[K(\zeta_{d_1}):K]}$ and n_{d_1} denoting the number of elements of order d_1 in G_1. Therefore,

$$KG \simeq K(G_1 \times H) \simeq (KG_1)H \simeq (\bigoplus_{d_1|n_1} a_{d_1} K(\zeta_{d_1}))H \simeq \bigoplus_{d_1|n_1} a_{d_1}(K(\zeta_{d_1})H)$$

(because, for any ring R and any groups G and H, it holds that $R(G \times H) \simeq (RG)H$, and, if $R = \oplus_{i\in I} R_i$, with $\{R_i\}_{i\in I}$ a family of rings, then $RG \simeq \oplus_{i\in I} R_i G$). Decomposing each direct summand, we get

$$KG \simeq \bigoplus_{d_1|n_1} \bigoplus_{d_2|n_2} a_{d_1} a_{d_2} K(\zeta_{d_1}, \zeta_{d_2}),$$

with $a_{d_2} = n_{d_2}/[K(\zeta_{d_1}, \zeta_{d_2}) : K(\zeta_{d_1})]$ and n_{d_2} denoting the number of elements of order d_2 in H. Taking $d := lcm(d_1, d_2)$, it follows that $K(\zeta_d) = K(\zeta_{d_1}, \zeta_{d_2})$. Set $a_d := \sum_{lcm(d_1,d_2)=d} a_{d_1} a_{d_2}$ and let us see that the result follows. In fact, since $[K(\zeta_d) : K] = [K(\zeta_{d_1}, \zeta_{d_2}) : K(\zeta_{d_1})][K(\zeta_{d_1}) : K]$, we have that

$$a_d[K(\zeta_d) : K] = \sum_{lcm(d_1,d_2)=d} a_{d_1} a_{d_2}[K(\zeta_{d_1}, \zeta_{d_2}) : K(\zeta_{d_1})][K(\zeta_{d_1}) : K] =$$

$$\sum_{lcm(d_1,d_2)=d} n_{d_1} n_{d_2}.$$

From $G = G_1 \times H$, each element in $g \in G$ may be written as $g = g_1 h$, with $g_1 \in G_1$ and $h \in H$ and, since G is abelian, $o(g) = lcm(o(g_1), o(h))$. Hence, $\sum_{lcm(d_1,d_2)=d} n_{d_1} n_{d_2} = n_d$, the number of elements of order d in G, and $a_d = n_d/[K(\zeta_d) : K]$. Therefore $KG \simeq \bigoplus_{d|n} a_d K(\zeta_d)$ □

If one knows the Wedderburn–Artin decomposition of a semisimple ring, it is only natural to search for its primitive central idempotents (Theorem 1.1.11). In Chapter 2, we develop methods to find primitive central idempotents of semisimple group algebras of finite abelian groups and of complex group algebras of finite nilpotent groups. In the latter case, there already exists a classical method to compute the primitive central idempotents that relies on the group's character table.

The character table of a group provides the primitive central idempotents of its complex group algebra by means of the following formula.

Theorem 1.1.33. *[25, Theorem 5.1.11] Let G be a finite group, and $\chi_1, \ldots, \chi_r$ be all the irreducible complex characters of G. For $i = 1, \ldots, r$, define*

$$e_i := \frac{\chi_i(1)}{|G|} \sum_{g \in G} \chi_i(g^{-1})g.$$

Then $e_1, \ldots, e_r$ are the primitive central idempotents of the complex group algebra $\mathbb{C}G$.

Proof. For each $i = 1, \ldots, r$, we may write $e_i = \sum_{g \in G} \alpha_g g$. Evaluating the regular character ρ on e_i, we get $\rho(e_i) = \sum_{g \in G} \alpha_g \rho(g) = \alpha_1 |G|$. Thus, for any $x \in G$, we have that $\rho(x^{-1}e_i) = \sum_{g \in G} \alpha_{xg} \rho(g) = \alpha_x |G|$. From Example 1.1.22, $(*)$ it follows that $\alpha_x |G| = \rho(x^{-1}e_i) = \sum_{j=1}^{r} \chi_j(1)\chi_j(x^{-1}e_i)$. Consider T_i the representation associated to the character χ_i. We get that

$$T_i(x^{-1}e_i) = T_i(x^{-1})T_i(e_i) = T_i(x^{-1}),$$

$$T_j(x^{-1}e_i) = T_j(x^{-1})T_j(e_i) = 0,$$

for $i \neq j$, and thus

$$\chi_i(x^{-1}e_i) = \chi_i(x^{-1}),$$

$$\chi_j(x^{-1}e_i) = 0,$$

for $i \neq j$. As a result,

$$\alpha_x = \frac{1}{|G|} \chi_i(1)\chi_i(x^{-1}),$$

for all $x \in G$. Hence, from $e_i = \sum_{g \in G} \alpha_g g$, the desired formula follows. □

Now we proceed to state some results about trivial units (see Definition 1.1.27) in integral group rings that will be very relevant in the study of the normalizer of integral semigroup rings in Chapter 3.

The next result states that the trivial units are the only unitary units (see Definition 1.1.30); it has an elementary proof and, nevertheless, is very useful in the study of units in group rings.

Proposition 1.1.34. *Let G be a group and $\gamma = \sum_{g\in G} \gamma_g g \in \mathbb{Z}G$. We have that $\gamma\gamma^* = 1$ if and only if $\gamma \in \pm G$.*

Proof. If $\gamma = \pm g$, for $g \in G$, then $\gamma^* = \pm g^{-1} = \gamma^{-1}$.

Conversely, if $\gamma\gamma^* = 1$, then we have that

$$1 = \sum_{g\in G} \gamma_g^2 1 + \sum_{\substack{g,h\in G \\ g\neq h}} \gamma_g\gamma_h gh^{-1}.$$

Thus, $1 = \sum_{g\in G} \gamma_g^2 1$ and $0 = \sum_{\substack{g,h\in G \\ g\neq h}} \gamma_g\gamma_h gh^{-1}$. Since $\gamma_g \in \mathbb{Z}$ for all $g \in G$, this implies that $\gamma_{g_0} = \pm 1$ for a unique $g_0 \in G$ and $\gamma_g = 0$ for all $g \neq g_0$. Hence, $\gamma = \pm g_0$. □

The next result, due to Berman and Higman, is also valid for infinite groups; however, we shall only need it for finite groups, and, in this case, there is an independent proof.

Lemma 1.1.35 (Berman–Higman). *Let $\gamma = \sum_{g\in G} \gamma_g g$ be a unit of finite order in the integral group ring $\mathbb{Z}G$ of a finite group G. If $\gamma_1 \neq 0$ then $\gamma = \gamma_1 = \pm 1$.*

Proof. Let $n = |G|$ and suppose $\gamma^m = 1$, for some positive integer m. Consider the regular representation T and the regular character ρ (see Example 1.1.22) on the group algebra $\mathbb{C}G$, and regard $\mathbb{Z}G$ as a subring of $\mathbb{C}G$. We have that

$$\rho(\gamma) = \sum_{g\in G} \gamma_g \rho(g) = \gamma_1 n.$$

Since $\gamma^m = 1$, we have that $T(\gamma)^m = T(\gamma^m) = T(1) = I$; thus $T(\gamma)$ is a root of the polynomial $X^m - 1 = 0$, which is separable. So there is a basis of $\mathbb{C}G$ such that $T(\gamma)$ is an $n \times n$ diagonal matrix, with m^{th} roots of unity ζ_i in the diagonal and zeros elsewhere.

Hence,

$$\rho(\gamma) = tr(T(\gamma)) = \sum_{i=1}^{n} \zeta_i = n\gamma_1,$$

and, taking absolute values,

$$n|\gamma_1| \leq \sum_{i=1}^{n} |\zeta_i| = n.$$

Now, $n|\gamma_1| \geq n$, for $\gamma_1 \in \mathbb{Z}$, then we must have $|\gamma_1| = 1$ and also $\sum_{i=1}^{n} |\zeta_i| = |\sum_{i=1}^{n} \zeta_i|$, which happens if and only if $\zeta_1 = \ldots = \zeta_n$.

Therefore, $n\gamma_1 = n\zeta_1$, and consequently $\gamma_1 = \zeta_1 = \pm 1$. So, $T(\gamma) = \pm I$ and $\gamma = \pm 1$. □

The following corollaries of the Berman–Higman Lemma will be extremely helpful for us.

Corollary 1.1.36. *Let A be a finite abelian group. Then the group of torsion units of the integral group ring $\mathbb{Z}A$ is the group of trivial units $\pm A$.*

Proof. Let $\gamma = \sum_{g\in A} \gamma_g g \in \mathbb{Z}A$ be a unit of finite order. Suppose that $\gamma_{g_0} \neq 0$, for some $g_0 \in A$. Then, due to the commutativity of A, γg_0^{-1} is also a unit of finite order in $\mathbb{Z}A$ and $(\gamma g_0^{-1})_1 = \gamma_{g_0} \neq 0$. By Lemma 1.1.35, we have that $\gamma g_0^{-1} = \pm 1$, i.e., $\gamma = \pm g_0$. □

Corollary 1.1.37. *Let G be a finite group. Then the group of all torsion central units of the integral group ring $\mathbb{Z}G$ is the group of the central trivial units $\pm\mathcal{Z}(G)$.*

1.2 Semigroup Ring Theory

Before getting to the topic of semigroup rings itself, we will need some theory about semigroups.

1.2.1 Prerequisite: Semigroup Theory

Some notions on Semigroup Theory are generalizations of concepts from Group Theory; however, most of them resemble Ring Theory.

Definition 1.2.1. A *semigroup* is a nonempty set with an associative binary operation, which will be denoted multiplicatively by juxtaposition of elements.

An element θ of a semigroup S is called a *zero element* if $s\theta = \theta s = \theta$, for all $s \in S$. A *null semigroup* is a semigroup with zero in which the product of any two elements is the zero element.

An element 1 of a semigroup S is called an *identity* if $s1 = 1s = s$, for all $s \in S$. A *monoid* is a semigroup that has an identity.

An element s in a monoid S is said to be an *invertible element* (or a *unit*) if there exists $s' \in S$ such that $ss' = s's = 1$; the element s' is called the *inverse element* of s and is denoted s^{-1}. The *unit group* of a monoid S is the group $\mathcal{U}(S) := \{s \in S; sr = rs = 1 \text{ , for some } r \in S\}$. A *group* S is a monoid in which every element is invertible, i.e., $S = \mathcal{U}(S)$. A group S is said to be an *abelian group* (or a *commutative group*) if $sr = rs$, for all $s, r \in S$.

A *semigroup homomorphism* is a function $f : S \longrightarrow T$ from a semigroup S to a semigroup T such that $f(rs) = f(r)f(s)$, for all $r, s \in S$.

If S is a semigroup, then we denote by S^1 the smallest monoid containing S. So

$$S^1 = \begin{cases} S & \text{, if S already has an identity element;} \\ S \cup \{1\} & \text{, if S does not have an identity element,} \end{cases}$$

with $s1 = 1s = s$, for all $s \in S^1$. Similarly, we denote by S^0 the smallest semigroup with a zero containing S. So

$$S^0 = \begin{cases} S & \text{, if S already has a zero element;} \\ S \cup \{\theta\} & \text{, if S does not have a zero element,} \end{cases}$$

with $s\theta = \theta s = \theta$, for all $s \in S^0$. In particular, for a group G, we say that G^0 is a *group with zero*.

Adjoining a zero normally simplifies arguments, while adjoining an identity is often useless, as the structure theory of semigroups relies on subsemigroups and ideals, which do not have an identity in general.

The following example describes a kind of matrix semigroup that is of utmost importance in the algebraic theory of semigroups.

Example 1.2.2 (Rees Matrix Semigroup). Let G be a group, $G^0 = G \cup \{\theta\}$ be the group with zero obtained from G by the adjunction of a zero element θ (as in Definition 1.2.1), and I and M be arbitrary nonempty sets. By an $I \times M$ *matrix over* G^0 we mean a mapping $A : I \times M \to G^0$, for which we use the notation $a_{i,m} := A(i, m)$, for $(i, m) \in I \times M$, and $(a_{i,m}) := A$.

By a *Rees* $I \times M$ *matrix over* G^0 we mean an $I \times M$ matrix over G^0 having at most one nonzero element. For $g \in G$, write $(g)_{i,m}$, with $i \in I$ and $m \in M$, for the $I \times M$ matrix having g in the (i, m)-entry, its remaining entries being θ. For any $i \in I$ and $m \in M$, the expression $(\theta)_{i,m}$ denotes the $I \times M$ *zero matrix*, which will be also be denoted by θ.

Now let P be a fixed arbitrary $M \times I$ matrix over G^0. We define a multiplication operation in the set of all Rees $I \times M$ matrices over G^0 as $AB := A \circ P \circ B$, where $\circ$ denotes the usual multiplication of matrices and, in performing this, we agree that, for $g \in G^0$, $\theta + g = g = g + \theta$. We call P the *sandwich matrix* with respect to this multiplication. Clearly, the set of all Rees $I \times M$ matrices over G^0 is closed under this operation, which is also associative. So, we can consider the *Rees* $I \times M$ *matrix semigroup over the group with zero* G^0 *with sandwich matrix* P and denote it by $\mathcal{M}^0(G, I, M, P)$. When the sets I and M are finite, say $|I| = n$ and $|M| = m$, we will write $\mathcal{M}^0(G, I, M, P)$ simply as $\mathcal{M}^0(G, n, m, P)$.

In fact, this type of semigroups is very natural, for instance:

1. In the ring of integral $n \times n$ matrices $M_n(\mathbb{Z})$, denote by $e_{i,j}$ the $n \times n$-matrix with 1 as the (i,j)-entry and zeros elsewhere. We call $e_{i,j}$ a *matrix unit* . We may multiply matrix units in the following way:

$$e_{i,j}e_{k,l} = \begin{cases} e_{i,l}, & \text{if } j = k, \\ 0, & \text{if } j \neq k. \end{cases}$$

   The matrix units in $M_n(\mathbb{Z})$ and the $n \times n$ zero matrix form, with this multiplication, the matrix semigroup $\mathcal{M}^0(\{1\}, n, n, I_n)$, where I_n denotes the $n \times n$-identity matrix.

2. Let G be a group with identity 1 and $P = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$. The matrix semigroup $\mathcal{M}^0(G, 1, 2, P)$ is isomorphic to the semigroup $G_1 \cup G_2 \cup \{\theta\}$, with G_1 and G_2 isomorphic copies of G such that $G_1G_2 \subseteq G_2$ and $G_2G_1 \subseteq G_1$.

Now we define some special subsets of semigroups having a certain algebraic structure.

Definition 1.2.3. A *subsemigroup* of a semigroup is a nonempty subset which is closed under multiplication. A *submonoid* of a semigroup is a subsemigroup with an identity. A *subgroup* of a semigroup is a subsemigroup that is a group.

If T is a nonempty subset of a semigroup S, we write $\langle T \rangle$ for the subsemigroup generated by T (if T is finite, say $T = \{t_1, \ldots, t_n\}$, we often write $\langle t_1, \ldots, t_n \rangle$ instead of $\langle T \rangle$). A semigroup S is said to be a *cyclic semigroup* if $S = \langle x \rangle$ for some $x \in S$. An element x of a semigroup S is a *periodic element* if $\langle x \rangle$ is finite. A semigroup is a *periodic semigroup* if every cyclic subsemigroup is finite.

Note that the identity of a subgroup G of a semigroup S need not to be the identity of S (actually, S may not have an identity at all). As as example, consider $S := \mathcal{M}^0(G, n, n, I_n)$, where I_n denotes the $n \times n$ identity matrix and G is any group; S has no identity element. But $M := \{s = ge_{1,1} \in \mathcal{M}^0(G, n, n, I_n); g \in G\}$ is a subgroup of S with identity $1e_{1,1}$.

Definition 1.2.4. An element e in a semigroup S is called an *idempotent* if $e = e^2$. We write $E(S)$ for the set of idempotent elements of a semigroup S. The set $E(S)$ has a natural partial order: $e \leq f \iff ef = fe = e$. An idempotent e in a semigroup S is said to be *primitive* if it is a nonzero idempotent and if it is minimal with respect to the partial order in $E(S)$.

Notice that the notion of primitive idempotent in a ring (Definition 1.1.6) is equivalent to the one given above.

Observe that a finite cyclic semigroup always contains an idempotent. In fact, let $\langle s\rangle$ be a finite cyclic semigroup. So there exist positive integers n and k so that $s^{n+k} = s^n$. Hence, $s^{n+vk} = s^n$, for any positive integer v. In particular, $s^{n(1+k)} = s^n$. So the semigroup $\langle s\rangle$ contains an element a so that $a^m = a$, for some integer $m \geq 2$. If $m = 2$, then a is an idempotent. Otherwise, $a^{m-1}, a^{m-2} \in \langle s\rangle$ and

$$(a^{m-1})^2 = a^{m-1}a^{m-1} = (a^{m-1}a)(a^{m-2}) = a^m a^{m-2} = aa^{m-2} = a^{m-1},$$

and then a^{m-1} is an idempotent.

Definition 1.2.5. Let I be a nonempty subset of a semigroup S. We say I is a *right ideal* of S if $xs \in I$, for all $s \in S$ and $x \in I$, i.e., $IS^1 \subseteq I$. A *left ideal* is defined analogously. We call I an *ideal* of S if it is a left and a right ideal of S.

For $a \in S$, the *ideal generated by* a is defined as $J_a := S^1aS^1 = SaS \cup Sa \cup aS \cup \{a\}$.

Definition 1.2.6. A semigroup S is said to be a *regular semigroup* if it satisfies the *Von Neumann regularity condition*, i.e., for every $s \in S$, there exists $x \in S$ such that $sxs = s$. A semigroup is said to be an *inverse semigroup* if it is regular and its idempotents commute; or, equivalently, every principal right ideal and every principal left ideal of S has a unique idempotent generator; or, also equivalently, if for every $s \in S$, there exists a unique $x \in S$ such that $sxs = s$ and $xsx = x$ ([4, Theorem 1.17]).

Let S be a semigroup. Define the the *center of* S as the subset $\mathcal{Z}(S) = \{x \in S; xs = sx, \forall s \in S\}$.

If a semigroup S has a minimal ideal K, then K is called a *kernel of* S. Clearly, any two distinct minimal ideals of S are disjoint. Since two ideals A and B of S always contain their set product AB, it follows that S can have at most one kernel K. Notice that S may not have a kernel at all (this is the case, for instance, if S is an infinite cyclic semigroup). If S has a kernel K, K may be characterized as the intersection of all ideals of S, because K is contained in every ideal of S.

Let e be an idempotent in a semigroup S. Then $eSe = \{ese; s \in S\}$ is a submonoid of S with identity element e. Now, eSe coincides with $\{x \in S; ex = xe = x\}$, the set of elements of S for which e is an identity. Consider $H_e := \mathcal{U}(eSe)$, the unit group of the monoid eSe. Then H_e is a subgroup of S and it is the largest subgroup of S for which e is the identity. Such subgroups are called the *maximal subgroups* of S. Notice that all the maximal

subgroups of S are isomorphic. There is a one-to-one correspondence between the idempotents e and maximal subgroups H_e of a semigroup S, since e is the unique idempotent element of H_e. H_e contains every subgroup of S that meets H_e. Thus, distinct maximal subgroups are disjoint.

Now, the Rees matrix semigroups defined in Example 1.2.2 are important in characterizing some special kinds of semigroups.

Lemma 1.2.7. *[4, Lemma 3.1] Let G be a group, I and M be arbitrary nonempty sets, and P be a $M \times I$ matrix over G^0. Then the Rees $I \times M$ matrix semigroup $\mathcal{M}^0(G, I, M, P)$ over G^0 with sandwich matrix P is a regular semigroup if and only if each row and each column of P contains a nonzero entry. In such a case, P is said to be a* regular matrix.

Proposition 1.2.8. *[30, Lemma 1.4] Let G be a group, I and M be arbitrary nonempty sets, and P be a $M \times I$ matrix over G^0. Then the nonzero idempotents of the Rees $I \times M$ matrix semigroup $\mathcal{M}^0(G, I, M, P)$ over G^0 with sandwich matrix P are precisely the elements $e = (p_{j,i}^{-1})_{i,j}$, with $p_{j,i} \neq \theta$. Define $S_{i,j} := \{(g)_{i,j}; g \in G^0,\ p_{j,i} \neq \theta\}$. Then all the $S_{i,j} \setminus \{\theta\}$ together with $\{\theta\}$ are the maximal subgroups of $\mathcal{M}^0(G, I, M, P)$. In fact, $e\mathcal{M}^0(G, I, M, P)e \simeq S_{i,j}$.*

Notice that, on the proposition above, all the $S_{i,j}$ are isomorphic to G^0.

Definition 1.2.9. Let S be a semigroup. An equivalence relation ρ on S is called a *right congruence relation* if, for all $a, b, c \in S$, it holds that $a\rho b$ implies $ac\rho bc$. An equivalence relation ρ on S is called a *left congruence relation* if, for all $a, b, c \in S$, it holds that $a\rho b$ implies $ca\rho cb$. An equivalence relation ρ on S is a *congruence relation* if it is both a right and a left congruence relation. We denote by S/ρ the set of the equivalence classes and by $\overline{a}$ the equivalence class containing the element $a \in S$. S/ρ becomes a semigroup with multiplication defined as $\overline{a}\overline{b} = \overline{ab}$. We call S/ρ the *factor semigroup* of S modulo ρ.

Let S be a semigroup and I be an ideal in S. Define ρ the *Rees congruence modulo I* on S as $a\rho b \iff a = b$ or $a, b \in I$. We write S/I for S/ρ and call this the *Rees factor semigroup of S modulo I*. As a convention, the Rees factor $S/\emptyset$ is defined to be S (even though the empty set $\emptyset$ is not an ideal).

Clearly, for a semigroup S and a congruence relation ρ, there is a natural semigroup homomorphism $S \to S/\rho; a \mapsto \overline{a}$. Congruence relations on groups yield the concept of normal subgroups.

Let S be a semigroup and I be an ideal in S. Notice that the equivalence classes of S/I are I itself and every one-element set $\{a\}$, with $a \in S \setminus I$. Thus, as a set, S/I may be identified with $S \setminus I$ with an element θ adjoined,

and such that $\overline{a}\theta = \theta\overline{a} = \theta$, so θ is actually a zero element. Intuitively, when we pass from S to S/I, we identify all the elements of I with θ and the nonzero elements of S/I correspond with $S \setminus I$; therefore, we will usually denote the nonzero elements of S/I as a (with $a \in S \setminus I$) instead of $\overline{a}$. There is a one-to-one correspondence between the ideals of S containing I and the ideals of S/I.

In analogy with what happens in groups and rings, we have the following lemma:

Lemma 1.2.10. *Let S be a semigroup and I, J be ideals of S such that $I \subseteq J$. Then J/I is an ideal of S/I and $(S/I)/(J/I) \simeq S/J$.*

We introduce, in analogy to simple rings, special kinds of semigroups that are "indecomposable" in some sense.

Definition 1.2.11. A semigroup is called a *simple semigroup* if it has no ideals other than itself.

A semigroup S with a zero θ is said to be a 0-*simple semigroup* if S has no ideals other than S and $\{\theta\}$, and $S^2 = S$, or, equivalently S has no proper ideals other than $\{\theta\}$, and S is not a null semigroup of cardinality two.

A semigroup is called a *completely* 0-*simple semigroup* if it is 0-simple and it contains a primitive idempotent (see Definition 1.2.4).

A semigroup is said to be a *Brandt semigroup* if it is a completely 0-simple inverse semigroup.

Notice that if S is a semigroup having zero element θ, then $\{\theta\}$ is always an ideal of S. Thus, the definition of simple semigroup is not very interesting. Completely 0-simple semigroups, on the other hand, will turn out to be the building blocks of the structure theory of semigroups.

Let us characterize 0-simple semigroups and completely 0-simple semigroups in more detail:

Lemma 1.2.12. *[4, Lemma 2.28] Let S be a semigroup with zero θ, and such that $S \neq \theta$. Then S is 0-simple if and only if $SaS = S$ for every $a \in S$, $a \neq \theta$.*

Lemma 1.2.13. *([4, §2.7, Exercise 11] A semigroup S with zero is completely 0-simple if and only if all of the following conditions are satisfied:*

1. *S is regular;*
2. *every nonzero idempotent of S is primitive;*
3. *if e and f are nonzero idempotents of S, then $eSf \neq \theta$.*

The next theorem characterizes completely 0-simple semigroups and also Brandt semigroups.

Theorem 1.2.14. *[4, Theorem 3.5, Theorem 3.9] A semigroup is completely 0-simple if and only if it is isomorphic to a regular Rees matrix semigroup over a group with zero.*

Furthermore, a semigroup is a Brandt semigroup if and only if it is isomorphic to a Rees matrix semigroup $\mathcal{M}^0(G, M, M, I_{|M|})$ over a group with zero G^0 with the $M \times M$ identity matrix $I_{|M|}$ as sandwich matrix.

Definition 1.2.15. Let S be a semigroup with zero. Define the equivalence relation $\mathcal{J}$ in S by $x\mathcal{J}y \iff J_x = J_y$ (see Definition 1.2.5), i.e., x and y generate the same ideal in S. We use the notation $J(x)$ for the *$\mathcal{J}$-class of S containing x*, i.e., $J(x)$ is the set of elements that generate the ideal J_x. Two elements are said to be *$\mathcal{J}$-equivalent* if they determine the same $\mathcal{J}$-class. Let I_x denote the set of elements of J_x that do not generate J_x, i.e., $I_x := \{y \in J_x; J_y \subsetneq J_x\}$. So I_x is an ideal of S and $J_x \setminus I_x = J(x)$. The quotient $S_x := J_x/I_x$ is called a *principal factor of S*

By a *principal series of S* we mean a strictly decreasing chain of ideals S_i of S, begining with S and ending with $\{\theta\}$, and such that there is no ideal of S strictly between S_i and S_{i+1}, for $i = 1, \ldots, m$. The *factors of a principal series of S* are the Rees factors S_i/S_{i+1}.

Remark 1.2.16. Notice that the definition of principal series with which we are working is slightly different from that of [4]. Our series ends with the zero ideal rather than the empty set; so we will always adjoin a zero to the semigroup before considering its principal series.

From the following lemma, it becomes clear why 0-simple and completely 0-simple semigroups are said to be "building blocks" for all semigroups.

Lemma 1.2.17. *[4, Lemma 2.39] Each principal factor of any semigroup (with zero) is either 0-simple or null.*

Theorem 1.2.18. *[4, Theorem 2.40] Let S be a semigroup (with zero), having principal series $S = S_1 \supset S_2 \supset \cdots \supset S_m \supset S_{m+1} = \{\theta\}$. Then its factors are isomorphic in some order to the principal factors of S. In particular, any two principal series of S have isomorphic factors.*

Corollary 1.2.19. *[4, Corollary 2.56] Any periodic (in particular, any finite) 0-simple semigroup is completely 0-simple.*

Theorem 1.2.20. *Every finite semigroup with zero has a principal series and the principal factors are either completely 0-simple or null semigroups.*

To end this section, we give an example of a well known class of semigroups.

Example 1.2.21 (Malcev Nilpotent Semigroups). [21, 26, 30] Let S be a semigroup. Consider, for x, y in S, and $w_1, w_2, \ldots, w_i, \ldots \in S^1$, the following sequence defined inductively:

$$x_0 = x,$$

$$y_0 = y,$$

and for $n \geq 0$

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

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

If $x_n = y_n$, for all $x_0, y_0 \in S$ and all w_i in S^1, and n is the least positive integer with this property, then S is said to be a *Malcev nilpotent semigroup of class n*.

Finite Malcev nilpotent semigroups have been classified by Okniński in [31]. It is interesting to observe that a group is Malcev nilpotent of class n if and only if it is nilpotent of class n in the classical sense [30, Theorem 7.2].

We have that a Brandt semigroup which is a matrix semigroup over a nilpotent group (Theorem 1.2.14) is Malcev nilpotent. Actually, these are the only Malcev nilpotent completely 0-simple semigroups [16, Lemma 2.1]. Hence, the completely 0-simple principal factors of a finite Malcev nilpotent semigroup are Brandt semigroups, which are of the form $\mathcal{M}^0(G, M, M, I_{|M|})$, where $I_{|M|}$ denotes the $M \times M$-identity matrix and G is a nilpotent group.

1.2.2 Basic Definitions and Some Important Results

Semigroup rings arise naturally as a generalization of group rings when we replace the group by a semigroup.

Definition 1.2.22. Let S be a semigroup, and R be a ring with identity 1. The *semigroup ring* RS is the ring of all formal sums $\alpha = \sum_{s \in S} \alpha_s s$, $\alpha_s \in R$, with finite *support* $supp(\alpha) = \{s \in S; \alpha_s \neq 0\}$. We say that α_s is the *coefficient of s in* α. Two elements α and β in RS are equal if and only if they have the same coefficients. The *sum* $\alpha + \beta$ is the element $\sum_{s \in S} (\alpha_s + \beta_s) s$. The *product* $\alpha\beta$ is the element $\sum_{s \in S} \gamma_s s$, where $\gamma_s = \sum_{\substack{x,y \in S \\ xy = s}} \alpha_x \beta_y$, for each $s \in S$. If R is a commutative ring, then RS is an R-algebra and is called a *semigroup algebra*.

Let S be a semigroup without zero element, and R be a ring. Notice that $RS^0 \simeq RS \times R\theta$. In order to "get rid of" the factor $R\theta$, we will need the notion of contracted semigroup ring.

Definition 1.2.23. Let S be a semigroup with a zero element θ, and R be a ring with identity 1. The *contracted semigroup ring* R_0S of S over R is the ring $RS/R\theta$, i.e., the elements of R_0S may be identified with the set of finite sums $\alpha = \sum_{s\in S} \alpha_s s$, $\alpha_s \in R$, $s \in S \setminus \{\theta\}$, with componentwise addition and multiplication defined on the R-basis $S \setminus \{\theta\}$ as

$$st = \begin{cases} st, & \text{if } st \neq \theta, \\ 0, & \text{if } st = \theta, \end{cases}$$

and then extended by distributivity to all elements. If S is a semigroup without zero element, we define the *contracted semigroup ring* of S over R as $R_0S := RS$.

Some natural classes of rings may be treated as contracted semigroup rings and not as (not contracted) semigroup rings.

Example 1.2.24.

1. Let R be a ring, $n > 1$ be an integer, and let S be the semigroup of $n \times n$ matrix units with zero (as in Example 1.2.2.1). Then $R_0S \simeq M_n(R)$. Notice that, if K is a field, then $M_n(K)$ is a simple ring. But a (not contracted) semigroup algebra of a nontrivial semigroup is never simple, as it contains the augmentation ideal, that is, the ideal of all elements of the semigroup algebra of which the sum of the coefficients is zero.

2. Let R be a ring, I and M be nonempty sets and $P = (p_{m,i})$ be an $M \times I$ matrix over R. Consider the set $\mathcal{M}(R, I, M, P)$ of all $I \times M$ matrices over R with finitely many nonzero entries. For any $A = (a_{i,m})$ and $B = (b_{i,m}) \in \mathcal{M}(R, I, M, P)$, addition is defined entrywise and multiplication is defined as follows:

   $$AB := A \circ P \circ B, \text{ with } \circ \text{ denoting the usual matrix multiplication.}$$

   With these operations $\mathcal{M}(R, I, M, P)$ becomes a ring, called a *ring of matrix type over R with sandwich matrix P*. If each row and column of P contains an invertible element of R, then we call $\mathcal{M}(R, I, M, P)$ a *Munn ring*. Note that if $i \in I$, $m \in M$ and $p_{m,i}$ is a unit of R then $e := (p_{m,i}^{-1})_{im}$ is an idempotent of $\mathcal{M}(R, I, M, P)$ such that $e\mathcal{M}(R, I, M, P)e \simeq R$. When the sets I and M are finite, say $|I| = n$ and $|M| = m$, we will denote $\mathcal{M}(R, I, M, P)$ simply as $\mathcal{M}(R, n, m, P)$.

Let G be a group. It is easily verified that $R_0\mathcal{M}^0(G^0, I, M, P) \simeq \mathcal{M}(RG, I, M, P)$ (see Example 1.2.2). If $R = \mathbb{Z}G$, $m = n$ and P is the $n \times n$ identity matrix, then $\mathcal{M}(R, n, m, P) = M_n(\mathbb{Z}G)$.

3. Let K be a field, Ω be any nonempty set, X be the free monoid on an alphabet $\{x_i; i \in \Omega\}$, and I be an ideal in KX generated by an ideal J of X. We call KX/I a *monomial algebra*. We have that KX/I is a K-space with basis the Rees factor semigroup X/J and, thus, $KX/I \simeq K_0(X/J)$ (see Lemma 1.2.25 below).

Lemma 1.2.25. *[4, Lemma 5.12] Let S be a semigroup and I be an ideal in S. Then RI is an ideal in RS and $RS/RI \simeq R_0(S/I)$.*

The analogue of Maschke Theorem (Theorem 1.1.14) for semigroup algebras is the following theorem:

Theorem 1.2.26. *[30, Theorem 14.24] Let K be a field and S a finite semigroup. The following conditions are equivalent:*

1. *KS is a semisimple algebra*
2. *S^0 has a series of ideals $S^0 = S_1 \supset S_2 \supset \ldots \supset S_n \supset S_{n+1} = \{\theta\}$, with each principal factor $S_i/S_{i+1} \simeq \mathcal{M}^0(G_i, n_i, n_i, P_i)$, a square completely 0-simple matrix semigroup, with G_i a finite group such that $char(K) \nmid |G_i|$ and P_i invertible in $M_{n_i}(KG_i)$, for all i.*

In the case of inverse semigroups, which are the most useful class of semigroups in the present work, we have the following special case, that resembles a lot Maschke Theorem:

Theorem 1.2.27. *[4, Theorem 5.26] Let K be a field and S a finite inverse semigroup. The semigroup algebra KS is semisimple if and only if $char(K)$ is zero or a prime not dividing the order of any subgroup of S.*

The following result shows that rings of matrix type (Example 1.2.24.2) arise naturally from matrix semigroup rings.

Theorem 1.2.28. *[30, Lemma 5.1] Let R be a ring and let S be a matrix semigroup $\mathcal{M}^0(G, I, M, P)$. Then we have that $R_0S \simeq \mathcal{M}(RG, I, M, P)$, where we consider the entries in P as elements of the group ring RG. If S is completely 0-simple, then $\mathcal{M}(RG, I, M, P)$ is a Munn ring.*

Munn rings are very important in the study of semigroup algebras over a finite semigroup, as is shown in the following corollary:

Corollary 1.2.29. *Let S be a finite semigroup with zero element θ and with a principal series $S = S_1 \supset S_2 \supset \ldots \supset S_n \supset S_{n+1} = \{\theta\}$. Then the semigroup ring RS has a series of ideals $RS = RS_1 \supset RS_2 \supset \ldots \supset RS_n \supset RS_{n+1} = R\theta$, where each factor $RS_i/RS_{i+1} \simeq R_0(S_i/S_{i+1})$ is either a nilpotent ring or a Munn ring over a group ring.*

Example 1.2.30. If $S := \{e_{1,1}, e_{1,2}, e_{2,2}, \theta\}$, then $\begin{pmatrix} \mathbb{Z} & \mathbb{Z} \\ 0 & \mathbb{Z} \end{pmatrix} \simeq \mathbb{Z}_0 S$. S has a principal series

$$S \supset \{e_{2,2}, e_{1,2}, \theta\} \supset \{e_{1,2}, \theta\} \supset \{\theta\},$$

with Rees factors $S/\{e_{2,2}, e_{1,2}, \theta\} \simeq \{e_{1,1}\}^0$, $\{e_{2,2}, e_{1,2}, \theta\}/\{e_{1,2}, \theta\} \simeq \{e_{2,2}\}^0$ and $\{e_{12}, \theta\}/\{\theta\} \simeq \{e_{1,2}, \theta\}$, a null semigroup.

In order to investigate units in semigroup algebras, it is elucidative to know when a Munn algebra over a group algebra contains an identity.

Theorem 1.2.31. *[30, Corollary 5.26] Let $S = \mathcal{M}^0(G, I, M, P)$ be a Rees matrix semigroup and K be a field. The following conditions are equivalent:*

1. *$K_0 S$ has an identity;*
2. *I and M are finite sets of the same cardinality n and P is an invertible matrix in $M_n(KG)$.*

Moreover, if both conditions hold, then $K_0 S \simeq M_n(KG)$ and S is completely 0-simple.

Chapter 2

Central Idempotents of Group Algebras of Finite Nilpotent Groups

In this chapter, the primitive central idempotents of a semisimple group algebra of a finite abelian group over an arbitrary field are exhibited. Afterwards, we determine the primitive central idempotents in a complex group algebra of a finite nilpotent group (without using group characters).

Let G be a finite abelian group of order n, and K be a field such that $char(K) \nmid n$. Consider the abelian group algebra KG. From Theorem 1.1.32, we know that $KG \simeq \bigoplus_i K(\zeta_i)$, where ζ_i are primitive roots of unity whose orders divide n. Clearly, the primitive idempotents of KG are the inverse images of each tuple of the form $(0, \ldots, 0, 1, 0, \ldots, 0)$ under this isomorphism. We shall describe the primitive idempotents of KG. In particular, we obtain a description for all cyclic codes (Definition 2.1.7) over finite fields.

For G an arbitrary finite group, the primitive central idempotents of the complex group algebra $\mathbb{C}G$ are given by the formula $\frac{\chi(1)}{|G|} \sum_{g \in G} \chi(g^{-1})g$, where χ is an irreducible complex character of G and 1 is the identity of G (Theorem 1.1.33). Though theoretically important, this description is not very useful in practical terms, because, with the known methods, the computational complexity of calculating the character table of a given finite group grows exponentially with respect to the order of the group.

Consider now G a finite nilpotent group. The primitive central idempotents in the rational group algebra $\mathbb{Q}G$ have been determined at [14], without making use of the character table of G. We are going to use a similar method and the abelian case in order to find out the primitive central idempotents in the complex group algebra $\mathbb{C}G$.

Our description allows the construction of the character table of G using a

lattice of subnormal subgroups of G. In particular, our description is helpful in studying counterexamples to the Isomorphism Problem in group rings ([25, Chapter 9]).

2.1 Primitive Idempotents of Semisimple Group Algebras of a Finite Abelian Group

Let $G \simeq C_1 \times \ldots \times C_s$ be a finite abelian group of order n, with $C_i = \langle g_i; g_i^{n_i} = 1 \rangle$ the cyclic group of order n_i generated by g_i (Structure Theorem of Finite Abelian Groups), and let K be a field such that $char(K) \nmid n$.

Define $m := lcm(n_1, \ldots, n_s)$. For $i = 1, \ldots, s$, consider ζ_{n_i} a primitive root of unity of order n_i in $\overline{K}$, an algebraic closure of K. Given an s-tuple of integers $\bar{l} = (l_1, \ldots, l_s)$, with $0 \leq l_i \leq n_i - 1$, define the polynomial $P_{\bar{l}} \in K(\zeta_m)[X_1, \ldots, X_s]$ as:

$$P_{\bar{l}} = \prod_{i=1}^{s} \prod_{\substack{k_i=0 \\ k_i \neq l_i}}^{n_i-1} (X_i - \zeta_{n_i}^{k_i}),$$

where ζ_m is a primitive root of unity of order m. Notice that $P_{\bar{l}}(\zeta_{n_1}^{k_1}, \ldots, \zeta_{n_s}^{k_s}) \neq 0$ if and only if $\bar{k} = \bar{l}$. This polynomial will be useful to describe the primitive idempotents of KG.

Suppose K is an algebraically closed field such that $char(K) \nmid n$. From Theorem 1.1.32, it follows that $KG \simeq K \oplus \ldots \oplus K$, with n copies of K on the right side (indeed, in this case, for each divisor d of n, we have that $K(\zeta_d) = K$ and, thus, $[K(\zeta_d) : K] = 1$, $a_d = \frac{n_d}{[K(\zeta_d):K]} = n_d$ and $\sum_{d|n} n_d = n$). The n components of the direct sum $K \oplus \ldots \oplus K$ will be indexed by the s-tuple of integers $\bar{l} = (l_1, \ldots, l_s)$, with $0 \leq l_i \leq n_i - 1$, in the following manner: the first n_s coordinates are the ones having $l_i = 0$, for $i \neq s$, and l_s varying from 0 to $n_s - 1$; the next n_s coordinates are the ones having $l_i = 0$, for $i \neq s, s-1$, $l_{s-1} = 1$ and l_s varying from 0 to $n_s - 1$; the next n_s coordinates are the ones having $l_i = 0$, for $i \neq s, s-1$, $l_{s-1} = 2$ and l_s varying from 0 to $n_s - 1$; and so on.

Lemma 2.1.1. *Let $G \simeq C_1 \times \ldots \times C_s$ be the finite abelian group of order n, with $C_i = \langle g_i; g_i^{n_i} = 1 \rangle$ a cyclic group of order n_i generated by g_i, and let K be an algebraically closed field such that $char(K) \nmid n$. The isomorphism $KG \simeq K \oplus \ldots \oplus K$ maps*

$$g_1^{x_1} \ldots g_s^{x_s} \mapsto (\ldots, \zeta_{n_1}^{x_1 k_1} \ldots \zeta_{n_s}^{x_s k_s}, \ldots)_{0 \leq k_i \leq n_i - 1},$$

where $\zeta_{n_i} \in K$ is a primitive root of unity of order n_i, for each $i = 1, \ldots, s$.

Proof. We proceed by induction on s, the number of cyclic components of G.

When $s = 1$, then $G = \langle g; g^n = 1 \rangle$ is a cyclic group of order n. Define $\zeta := \zeta_n$, a primitive root of the unity of order n. Consider $v^i := (1, \zeta^i, \zeta^{2i}, \ldots, \zeta^{(n-1)i}) \in K \oplus \ldots \oplus K$, for $i = 1, \ldots, n$. We shall see that $\{v^i; i = 1, \ldots, n\}$ is a K-basis for $K \oplus \ldots \oplus K$.

Notice that the $n \times n$ matrix having vector v^i as its i^{th} line is an invertible Vandermonde matrix. Thus, the n vectors in the set $\{v^i; i = 1, \ldots, n\}$ are linearly independent. Since the K-dimension of $K \oplus \ldots \oplus K$ is n, we conclude that $\{v^i; i = 1, \ldots, n\}$ is a K-basis for $K \oplus \ldots \oplus K$.

Consider the K-linear mapping

$$\phi : KG \longrightarrow K \oplus \ldots \oplus K,$$

$$g \mapsto (1, \zeta, \zeta^2, \ldots, \zeta^{n-1}).$$

Notice that $\{g^i; i = 1, \ldots, n\}$ is a K-basis of KG and that $\phi(g^i) = v^i$. So, $KG \overset{\phi}{\simeq} K \oplus \ldots \oplus K$ as K-vector spaces. Clearly, ϕ is a ring homomorphism, and hence $KG \overset{\phi}{\simeq} K \oplus \ldots \oplus K$ as rings too.

Now we consider the case where $G \simeq C_1 \times \ldots \times C_s$, with $s > 1$. Assume the result holds for any abelian group having $s - 1$ cyclic components.

Define $G_1 := C_1 \times \ldots \times C_{s-1}$. We know that

$$KG \simeq K(G_1 \times C_s) \simeq (KG_1)C_s,$$

the isomorphisms being

$$\sum \alpha_{\overline{x}} g_1^{x_1} \ldots g_{s-1}^{x_{s-1}} g_s^{x_s} \mapsto \sum \alpha_{\overline{x}} (g_1^{x_1} \ldots g_{s-1}^{x_{s-1}}, g_s^{x_s}),$$

$$\sum \alpha_{\overline{x}} (g_1^{x_1} \ldots g_{s-1}^{x_{s-1}}, g_s^{x_s}) \mapsto \sum_{x_s} \Big(\sum_{x_1, \ldots, x_{s-1}} \alpha_{\overline{x}} g_1^{x_1} \ldots g_{s-1}^{x_{s-1}} \Big) g_s^{x_s},$$

where $\overline{x} := (x_1, \ldots, x_{s-1}, x_s)$, with $0 \leq x_i \leq n_i - 1$, for each i. By the induction hypothesis, we have that

$$KG_1 \simeq K \oplus \ldots \oplus K,$$

$$g_1^{x_1} \ldots g_{s-1}^{x_{s-1}} \mapsto (\ldots, \zeta_{n_1}^{x_1 k_1} \ldots \zeta_{n_{s-1}}^{x_{s-1} k_{s-1}}, \ldots)_{0 \leq k_i \leq n_i - 1}.$$

So, it follows that

$$(KG_1)C_s \simeq (K \oplus \ldots \oplus K)C_s \simeq KC_s \oplus \ldots \oplus KC_s,$$

where the last isomorphism is

$$\sum_{x_s}(\sum_{x_1,\ldots,x_{s-1}} \alpha_{\overline{x}}(\ldots,\zeta_{n_1}^{x_1k_1}\ldots\zeta_{n_{s-1}}^{x_{s-1}k_{s-1}},\ldots),g_s^{x_s}) \mapsto$$

$$(\ldots,\sum \alpha_{\overline{x}}\zeta_{n_1}^{x_1k_1}\ldots\zeta_{n_{s-1}}^{x_{s-1}k_{s-1}}g_s^{x_s},\ldots)_{0\leq k_i\leq n_i-1}.$$

Using the cyclic group case, we have that

$$KC_s \oplus \ldots \oplus KC_s \simeq K \oplus \ldots \oplus K,$$

$$(\ldots,\sum \alpha_{\overline{x}}\zeta_{n_1}^{x_1k_1}\ldots\zeta_{n_{s-1}}^{x_{s-1}k_{s-1}}g_s^{x_s},\ldots) \mapsto$$

$$(\ldots,\sum \alpha_{\overline{x}}\zeta_{n_1}^{x_1k_1}\ldots\zeta_{n_{s-1}}^{x_{s-1}k_{s-1}}\zeta_s^{x_sk_s},\ldots)_{0\leq k_i\leq n_i-1},$$

which is the desired result. □

Now we describe the primitive idempotents of a semisimple group algebra of a finite abelian group over an algebraically closed field.

Theorem 2.1.2. *Let $G \simeq C_1 \times \ldots \times C_s$ be a finite abelian group of order n, with $C_i = \langle g_i; g_i^{n_i} = 1\rangle$ the cyclic group of order n_i generated by g_i, and let K be an algebraically closed field such that $char(K) \nmid n$. Then the primitive idempotents of the abelian group algebra KG are the elements:*

$$e_{\overline{l}} := \frac{P_{\overline{l}}(g_1,\ldots,g_s)}{P_{\overline{l}}(\zeta_1^{l_1},\ldots,\zeta_s^{l_s})},$$

where $0 \leq l_i \leq n_i - 1$, for $i = 1,\ldots,s$.

Proof. The image of $e_{\overline{l}} = \frac{P_{\overline{l}}(g_1,\ldots,g_s)}{P_{\overline{l}}(\zeta_1^{l_1},\ldots,\zeta_s^{l_s})}$ under the isomorfism $KG \overset{\phi}{\simeq} K\oplus\ldots\oplus K$ specified in Lemma 2.1.1 is

$$\phi(e_{\overline{l}}) = (\ldots,\frac{P_{\overline{l}}(\zeta_1^{k_1},\ldots,\zeta_s^{k_s})}{P_{\overline{l}}(\zeta_1^{l_1},\ldots,\zeta_s^{l_s})},\ldots)_{0\leq k_i\leq n_i-1}.$$

Since $P_{\overline{l}}(\zeta_1^{k_1},\ldots,\zeta_s^{k_s}) \neq 0$ if and only if $\overline{k} = \overline{l}$, we have that all the coordinates of $\phi(e_{\overline{l}})$ are zero, except the one in the position indexed by $\overline{l}$, which equals

$$\frac{P_{\overline{l}}(\zeta_1^{l_1},\ldots,\zeta_s^{l_s})}{P_{\overline{l}}(\zeta_1^{l_1},\ldots,\zeta_s^{l_s}))} = 1.$$

Thus, $\phi(e_{\overline{l}}) = (0,\ldots,0,1,0,\ldots,0)$, with 1 in the position $(l_1,\ldots,l_s)$, and hence $e_{\overline{l}}$ is a primitive idempotent of KG. □

Corollary 2.1.3. *With the same notation as in Theorem 2.1.2, suppose that* $G = \langle g; g^n = 1\rangle$ *is the cyclic group of order* n *generated by* g*. Let* ζ *be a primitive root of unity of order* n*. Then the primitive idempotents in* KG *are:*

$$e_l := \frac{\zeta^{n-l}}{n} \prod_{i=0, i\neq l}^{n-1} (g - \zeta^i),$$

where $0 \leq l \leq n-1$*.*

Proof. Notice that

$$P_l(\zeta^l) = \prod_{\substack{i=0 \\ i\neq l}}^{n-1} (\zeta^l - \zeta^i) = \zeta^l \prod_{i=1}^{n-1} (1 - \zeta^i) = \zeta^l n.$$

Now, since $P_l(g) = \prod_{\substack{i=0 \\ i\neq l}}^{n-1} (g - \zeta^i)$, the result follows directly from Theorem 2.1.2. □

When the field K is not algebraically closed, exhibiting the isomorphism $KG \simeq \bigoplus_i K(\zeta_i)$, with ζ_i primitive roots of unity, is more complicated. In order to avoid this, we adopt an alternative method and use the algebraically closed case to get the primitive idempotents:

Theorem 2.1.4. *Let* $G \simeq C_1 \times \ldots \times C_s$ *be a finite abelian group of order* n*, with* $C_i = \langle g_i; g_i^{n_i} = 1\rangle$ *the cyclic group of order* n_i *generated by* g_i*, and let* K *be a field such that* $char(K) \nmid n$*. Define* $m := lcm(n_1, \ldots, n_s)$*. Consider* $\mathcal{A} := Aut(K(\zeta_m)|K)$*, the Galois group of the field extension* $K(\zeta_m)|K$*. Then, for a fixed* s*-tuple of integers* $\bar{l} = (l_1, \ldots, l_s)$*, with* $0 \leq l_i \leq n_i - 1$*, the element* $e_{\bar{l}}$ *defined below is a primitive idempotent of the abelian group algebra* KG*:*

$$e_{\bar{l}} := \sum_{\sigma \in A} \frac{P_{\bar{l}}^{\sigma}(g_1, \ldots, g_s)}{\sigma(P_{\bar{l}}(\zeta_{n_1}^{l_1}, \ldots, \zeta_{n_s}^{l_s}))},$$

the sum of all Galois conjugates of $P_{\bar{l}}(g_1, \ldots, g_s)/P_{\bar{l}}(\zeta_{n_1}^{l_1}, \ldots, \zeta_{n_s}^{l_s})$*, where* $P_{\bar{l}}^{\sigma}$ *denotes the polynomial in* $K(\zeta_m)[X_1, \ldots, X_s]$ *obtained by applying* σ *to the coefficients of* $P_{\bar{l}}$*. Furthermore, these are all the primitive idempotents of* KG*.*

Proof. From the Theorem 2.1.2, it follows that

$$f_{\bar{l}} := \frac{P_{\bar{l}}(g_1, \ldots, g_s)}{P_{\bar{l}}(\zeta_{n_1}^{l_1}, \ldots, \zeta_{n_s}^{l_s})}$$

is a primitive idempotent of $\overline{K}G$, where $\overline{K}$ is an algebraic closure of K. Therefore, $f_{\bar{l}}$ is also a primitive idempotent in $K(\zeta_m)G$. Notice that $K(\zeta_m)$ is the minimal field extension K_1 of K such that all the $f_{\bar{l}}$'s belong to K_1G. Each $\sigma \in \mathcal{A}$ induces a unique automorphism σ^* of $K(\zeta_m)G$, i.e., for $\alpha = \sum_{g\in G} \alpha_g g \in K(\zeta_m)G$, define $\sigma^*(\alpha) := \sum_{g\in G} \sigma(\alpha_g)g$. Thus, $\sigma^*(f_{\bar{l}})$ is still a primitive idempotent of $K(\zeta_m)G$ and of $\overline{K}G$.

Let e be a primitive idempotent in KG. We may write $e = f_1 + \ldots + f_t$, where f_i are primitive idempotents in $\overline{K}G$. Let K_2 be the minimal field such that, for each $i = 1, \ldots, t$, f_i belongs to K_2G. Take $\tau \in Aut(K_2|K)$. Applying τ^* to e, we get $e = \tau^*(e) = \tau^*(f_1) + \ldots + \tau^*(f_t)$ and, by the unique representation in K_2G (Theorem 1.1.11), we have that, for each $i = 1, \ldots, t$, there exists a $j = 1, \ldots, t$, such that $\tau^*(f_i) = f_j$. Thus, all the f_i are Galois-conjugates of one another. In fact, suppose that (after reordering) $f_1, \ldots, f_s$ are all conjugates of f_1 and that $f_{s+1}, \ldots, f_t$, for some $1 < s < t$. Then, defining $e' := f_1 + \ldots + f_s$ and $e'' := f_{s+1} + \ldots + f_t$, we have that $e = e' + e''$, with e' and e'' orthogonal nonzero idempotents in KG, which contradicts the primitivity of e. So e is exactly the sum of the distinct Galois-conjugates of a primitive idempotent in $\overline{K}G$, and thus, by definition, $e = e_{\bar{l}}$ for some $\bar{l}$.

Notice that the primitive idempotents e in KG and the set of distinct $e_{\bar{l}}$'s defined exist in equal number. We conclude that each $e_{\bar{l}}$ is a primitive idempotent in KG.

□

Corollary 2.1.5. *With the same notation as in Theorem 2.1.4, suppose that $G = \langle g; g^n = 1\rangle$ is the cyclic group of order n generated by g. Let ζ be a primitive root of unity of order n. Fix $0 \leq l \leq n-1$. Consider $\mathcal{A} := Aut(K(\zeta)|K)$, the Galois group of the field extension $K(\zeta)|K$. Then the element e_l defined below is a primitive idempotent of the abelian group algebra KG:*

$$e_l := \sum_{\sigma\in\mathcal{A}} \frac{\sigma(\zeta^{n-l})}{n} \prod_{\substack{i=0 \\ i\neq l}}^{n-1} (g - \sigma(\zeta^i)),$$

Furthermore, these are all the primitive idempotents of KG.

Proof. The proof is a direct application of Theorem 2.1.4 to Corollary 2.1.3. □

Example 2.1.6 (Cyclic Codes). In order to make connections between cyclic codes and the computation of primitive idempotents for semisimple group algebras of finite abelian groups, we need some very basic concepts o coding theory, for which the reference is [37].

Let $\mathbb{F}_q$ denote the finite field of q elements, with q a power of a prime integer p. Consider the n-dimensional vector space $\mathbb{F}_q^n$, whose elements are n-tuples $a = (a_0, \ldots, a_{n-1})$.

Definition 2.1.7. A *code* C is a linear subspace of $\mathbb{F}_q^n$. We call n the *length of* C and $dim C$ (as a $\mathbb{F}_q$-vector space) the *dimension of* C. A code C is said to be a *cyclic code* if its automophism group $Aut(C)$ contains the *cyclic shift*, i.e., $(c_0, c_1, \ldots, c_{n-1}) \in C \Longrightarrow (c_1, \ldots, c_{n-1}, c_0) \in C$.

It is common in coding theory to identify $\mathbb{F}_q^n$ with the vector space P_n of polynomials of degree less than n over $\mathbb{F}_q$ via the correspondence

$$a = (a_0, \ldots, a_{n-1}) \longleftrightarrow a(x) = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} \in \mathbb{F}_q[x].$$

Clearly, a cyclic code C of length n may be identified with the corresponding ideal in $\frac{\mathbb{F}_q[x]}{(x^n-1)}$.

Let $G = \langle g; g^n = 1\rangle$ be the cyclic group of order n generated by g. We have that $\mathbb{F}_q G \simeq \frac{\mathbb{F}_q[x]}{(x^n-1)}$ as rings, by taking the morphism $g \mapsto \overline{x}$. Thus, we have an immediate connection between group rings and coding theory.

Determining a cyclic code of length n over a finite field $K = \mathbb{F}_q$ such that $char(K) = p \nmid n$ corresponds to determining an ideal in the semisimple group algebra KG, where G is a cyclic group of order n. In this case, all the ideals of KG are direct summands $\oplus_{k=1}^{l}(KG)e_{i_k}$, where $l \leq n$ and $e_1, \ldots, e_n$ are the primitive idempotents of KG as determined in Corollary 2.1.5.

2.2 Primitive Central Idempotents of Complex Group Algebras of a Finite Nilpotent Group

We shall first state some definitions and results needed on this section.

Definition 2.2.1. Let R be a ring with identity and let G be a group. For e a primitive central idempotent of RG, define the subset G_e of G as $G_e := \{g \in G; eg = e\}$.

Definition 2.2.2. Let G be a finite group and K be a field. Define the element $\varepsilon(G)$ in KG by

$$\varepsilon(G) := \begin{cases} 1 & \text{, if } G = \{1\}; \\ \prod_{M \in \mathcal{M}(G)}(1 - \widetilde{M}) & \text{, if } G \neq \{1\}, \end{cases}$$

where $\mathcal{M}(G)$ denotes the set of all minimal nontrivial normal subgroups of G.

Remark 2.2.3. Notice that if A and B are subgroups of a group G, with $A \subseteq B$, then $\widetilde{A}\widetilde{B} = \widetilde{B}$ and $(1-\widetilde{A})(1-\widetilde{B}) = (1-\widetilde{A})$. So we can redefine $\varepsilon(G)$ as

$$\varepsilon(G) := \prod_{\substack{N \lhd G \\ N \neq \{1\}}} (1-\widetilde{N}),$$

when G is a nontrivial group. Notice, in particular, that if N is a nontrivial normal subgroup of G, then $(1-\widetilde{N})\varepsilon(G) = \varepsilon(G)$.

The following lemma is elementary, but extremely useful.

Lemma 2.2.4. *Let G be a finite group, K be a field such that $char(K) \nmid |G|$, and e be a primitive central idempotent of KG. Then:*

1. *G_e is a normal subgroup of G and $e\widetilde{G_e} = e$. Thus, e is also a primitive central idempotent of $(KG)\widetilde{G_e}$, and, since $(KG)\widetilde{G_e} \simeq K(G/G_e)$, the image $\overline{e}$ of e in $K(G/G_e)$ is a primitive central idempotent of $K(G/G_e)$;*
2. *if N is a normal subgroup of G, then $e\widetilde{N} = e$ if and only if $N \subseteq G_e$;*
3. *$G_e = \{1\}$ if and only if $\varepsilon(G)e = e$;*
4. *if $H := G_e$ and N is a normal subgroup of G contained in H, then $(G/N)_{\overline{e}} = H/N$, where $\overline{e}$ denotes the image of e in $K(G/N)$(we call attention to this special case: if N is a normal subgroup of G and $\overline{e}$ is a primitive central idempotent in $K(G/N)$, then: $(G/N)_{\overline{e}} = \{1\}$ if and only if $G_e = N$, where e denotes the image of $\overline{e}$ in KG).*

Proof. 1. To see that G_e is a normal subgroup of G, take $h \in G$ and $g \in G_e$. Since e is central, we have that $hgh^{-1}e = hgeh^{-1} = e$. So $hgh^{-1} \in G_e$, and thus G_e is normal in G.

By Definition 2.2.1, we have that

$$e\widetilde{G_e} = \frac{e\sum_{g\in G_e} g}{|G_e|} = \frac{\sum_{g\in G_e} eg}{|G_e|} = \frac{\sum_{g\in G_e} e}{|G_e|} = \frac{|G_e|e}{|G_e|} = e.$$

So e is a primitive central idempotent of $(KG)\widetilde{G_e}$ and $\overline{e}$, the image of e in $K(G/G_e)$, is a primitive central idempotent of $K(G/G_e)$.

2. Consider N a normal subgroup of G. Then $\widetilde{N}$ is a central idempotent of KG. Since e is a primitive central idempotent of KG, we have that $e\widetilde{N}$ is either equal to zero or to e.

Suppose $e\widetilde{N} = e$. We have that

$$(KG)e = (KG)\widehat{N}e \simeq K(G/N)e.$$

Thus we have the following diagram

$$KG \longrightarrow K(G/N) \xrightarrow{\times e} K(G/N)e \xrightarrow{\simeq} (KG)e,$$

the maps beign

$$g \mapsto \overline{g},$$
$$\overline{g} \mapsto \overline{g}e,$$
$$\overline{g}e \mapsto g\widehat{N}e = ge.$$

From the diagram, it follows that the $ker(KG \xrightarrow{\times e} (KG)e) = G_e$ and that $N \subseteq ker(KG \xrightarrow{\times e} (KG)e)$.

If $N \subseteq G_e$, then

$$e\widetilde{N} = \frac{e\sum_{g\in N} g}{|N|} = \frac{\sum_{g\in N} eg}{|N|} = \frac{\sum_{g\in N} e}{|N|} = \frac{|N|e}{|N|} = e.$$

3. Suppose $G_e = \{1\}$. If N is a nontrivial normal subgroup of G, then, by *2.*, we have that $e\widetilde{N} = 0$. So, from Definition 2.2.2, it follows that

$$\varepsilon(G)e = \prod_{M\in\mathcal{M}(G)} (1-\widetilde{M})e = \prod_{M\in\mathcal{M}(G)} (e-\widetilde{M}e) = \prod e = e.$$

Suppose $G_e \neq \{1\}$. Then, by Remark 2.2.3, we have that $\varepsilon(G) = (1-\widetilde{G_e})\varepsilon(G)$ and $e\varepsilon(G) = e(1-\widetilde{G_e})\varepsilon(G) = 0$.

4. This part of the Lemma follows directly from Definition 2.2.1.

□

The definitions and notations needed in the following lemma and theorem are stated in Definition 1.1.31.

We need the following technical lemma ([14, Lemma 2.3]):

Lemma 2.2.5. *Let G be a finite group, K be a field such that $char(K) \nmid |G|$, and $g \in G$. If $g^{-1}\mathcal{C}_g \cap \mathcal{Z}(G) \neq \{1\}$, then G contains a central element z of prime order so that $\widetilde{\mathcal{C}_g} = \widetilde{\mathcal{C}_g\langle z\rangle}$.*

Proof. By assumption there exist $h \in G$ and $1 \neq z \in \mathcal{Z}(G)$ so that $h^{-1}gh = zg$. Hence, for any positive integer n we get, by induction, that $h^{-n}gh^n = z^n g$. Replacing z by some power of z, if necessary, we may assume that z has prime order. It then follows that $\langle z\rangle \mathcal{C}_g \subseteq \mathcal{C}_g$. So $\langle z\rangle \mathcal{C}_g = \mathcal{C}_g$ and therefore $\widetilde{\mathcal{C}_g} = \widetilde{\mathcal{C}_g}\widetilde{\langle z\rangle}$. □

Before actually using the lemma, let us just observe that $g \notin \mathcal{C}_G(\mathcal{Z}_2(G))$ implies $g^{-1}\mathcal{C}_g \cap \mathcal{Z}(G) \neq \{1\}$. In fact, suppose that, for $g \in G$, it holds that $g^{-1}\mathcal{C}_g \cap \mathcal{Z}(G) = \{1\}$. Take $l \in \mathcal{Z}_2(G)$. We have that $\overline{g^{-1}l^{-1}gl} = \overline{1}$ in $G/\mathcal{Z}(G)$ (because $\mathcal{Z}_2(G)/\mathcal{Z}(G) = \mathcal{Z}(G/\mathcal{Z}(G))$, an abelian group); in other words, there exists $z_1 \in \mathcal{Z}(G)$ such that $g^{-1}l^{-1}gl = z_1$, so, by hypothesis, $z_1 = 1$. Hence, $g \in \mathcal{C}_G(\mathcal{Z}_2(G))$.

We need a result from Jespers-Leal-Paques ([14, Proposition 2.1]). This result is stated in the reference for the group algebra $\mathbb{Q}G$, where G is a finite nilpotent group. We observe that the proof given in the article is still valid for the case $\mathbb{C}G$ and we include it here for the sake of completeness.

Proposition 2.2.6. *Let G be a finite nilpotent group, $e \in \mathbb{C}G$ and $G_1 := \mathcal{C}_G(\mathcal{Z}_2(G))$, the centralizer in G of the second center of G. e is a primitive central idempotent of $\mathbb{C}G$ with G_e trivial if and only if $e = \sum_{g\in G} e_1^g$, the sum of all distinct G-conjugates of e_1, with e_1 a primitive central idempotent of $\mathbb{C}G_1$ satisfying $\bigcap_{g\in G}((G_1)_{e_1})^g = \{1\}$.*

Proof. Suppose $e \in \mathbb{C}G$ is a primitive central idempotent with $G_e = \{1\}$. By Theorem 1.1.16, we may write $e = \sum_{g\in G} \alpha_g \widetilde{\mathcal{C}_g}$, with each $\alpha_g \in \mathbb{C}$.

For any $g \in G$ with $g \notin \mathcal{C}_G(\mathcal{Z}_2(G))$, by Lemma 2.2.5, there exists a nontrivial central element $w_g \in G$ of prime order such that $\widetilde{\mathcal{C}_g} = \widetilde{\mathcal{C}_g}\ \widetilde{\langle w_g\rangle}$. Hence,

$$e = \sum_{g\in \mathcal{C}_G(\mathcal{Z}_2(G))} \alpha_g \widetilde{\mathcal{C}_g} + \sum_{g\notin \mathcal{C}_G(\mathcal{Z}_2(G))} \alpha_g \widetilde{\mathcal{C}_g}\ \widetilde{\langle w_g\rangle}.$$

Because $G_e = \{1\}$, Lemma 2.2.4 yields that $e = e\varepsilon(G)$. Notice that $\varepsilon(G)\widetilde{\langle w_g\rangle} = 0$, for, since w_g has prime order and is central, $\langle w_g\rangle \in \mathcal{M}(G)$ and, by Definition 2.2.2,

$$\begin{aligned}
&\varepsilon(G)\widetilde{\langle w_g\rangle} = \textstyle\prod_{M\in\mathcal{M}(G)}(1-\widetilde{M})\widetilde{\langle w_g\rangle} = \\
&(\textstyle\prod_{M\in\mathcal{M}(G)\setminus\{\langle w_g\rangle\}}(1-\widetilde{M}))(1-\widetilde{\langle w_g\rangle})\widetilde{\langle w_g\rangle} = \\
&(\textstyle\prod_{M\in\mathcal{M}(G)\setminus\{\langle w_g\rangle\}}(1-\widetilde{M}))(\widetilde{\langle w_g\rangle}-\widetilde{\langle w_g\rangle}) = 0,
\end{aligned}$$

i.e., $\varepsilon(G) \in \langle \widetilde{\mathcal{C}_g}; g \in \mathcal{C}_G(\mathcal{Z}_2(G))\rangle_{\mathbb{C}}$, the $\mathbb{C}$-subspace of $\mathbb{C}G$ generated by $\{\widetilde{\mathcal{C}_g}; g \in \mathcal{C}_G(\mathcal{Z}_2(G))\}$.

So we get that

$$e = e\varepsilon(G) = \sum_{g \in \mathcal{C}_G(\mathcal{Z}_2(G))} \alpha_g \widetilde{\mathcal{C}_g} \cdot \varepsilon(G),$$

and thus $e \in \langle \widetilde{\mathcal{C}_g}; g \in \mathcal{C}_G(\mathcal{Z}_2(G)) \rangle_{\mathbb{C}}$ too.

Notice that $G_1 = \mathcal{C}_G(\mathcal{Z}_2(G))$ is normal in G; so if $g \in G_1$ and $h \in \mathcal{C}_g$, then $h \in G_1$. In fact, we have that $h = l^{-1}gl$, for some $l \in G$. Take $x \in \mathcal{Z}_2(G)$. So $x^{-1}h^{-1}xh = z \in \mathcal{Z}(G)$ and $lx^{-1}l^{-1}g^{-1}lxl^{-1}gl = lz$. Since $\mathcal{Z}_2(G)$ is normal in G, we have that $y = lx^{-1}l^{-1} \in \mathcal{Z}_2(G)$, and thus $y^{-1}g^{-1}yg = z = 1$ (because $g \in G_1 = \mathcal{C}_G(\mathcal{Z}_2(G))$). Hence, $x^{-1}h^{-1}xh = 1$ and $h \in G_1$, as desired.

Thus, we have shown that $supp(e) \subseteq G_1 = \mathcal{C}_G(\mathcal{Z}_2(G))$. Notice that e is not necessarily a primitive central idempotent of $\mathbb{C}G_1$. However, it is possible to write

$$e = e_1^{g_1} + \ldots + e_1^{g_n},$$

the sum of all G-conjugates of a primitive central idempotent $e_1 \in \mathbb{C}G_1$.

In fact, since $e \in \mathbb{C}G_1$ we may write, by Theorem 1.1.11, $e = a_1e_1 + \ldots + a_me_m$, with $\{e_1, \ldots, e_m\}$ all the primitive central idempotens of $\mathbb{C}G_1$ and $a_i \in \mathbb{C}G_1$. We have, for $i = 1, \ldots, m$, that ee_i is either equal to 0 or to e_i, because ee_i is an idempotent and e_i is a primitive idempotent. Hence, after possibly reordering the e_i's, we have that $e = e_1 + \ldots + e_k$, for some $k \leq m$. Now we only have to check that every e_i is a G-conjugate of e_1. For $g \in G$, we have that $e = e^g = e_1^g + \ldots + e_k^g$, and by the unique representation in $\mathbb{C}G_1$ (Theorem 1.1.13), we have that, for each $i = 1, \ldots, k$, there exists a $j = 1, \ldots, k$, such that $e_i^g = e_j$. Thus, all the e_i are G-conjugate of one another. So e is exactly the sum of the distinct G-conjugates of e_1.

Observe that $((G_1)_{e_1})^{g_i} = (G_1)_{e_1^{g_i}}$ (for $g \in (G_1)_{e_1^{g_i}} \iff ge_1^{g_i} = e_1^{g_i} \iff g^{g_i^{-1}}e_1 = e_1 \iff g^{g_i^{-1}} \in (G_1)_{e_1} \iff g \in ((G_1)_{e_1})^{g_i}$). Hence, it easily follows that $\cap_{i=1}^n((G_1)_{e_1})^{g_i} = G_e = \{1\}$. This proves the necessity of the conditions.

Conversely, suppose that G is a finite nilpotent group, that e_1 is a primitive central idempotent of $\mathbb{C}G_1$, where $G_1 := \mathcal{C}_G(\mathcal{Z}_2(G))$, and that $\cap_{g \in G}((G_1)_{e_1})^g = \{1\}$. Let $e := e_1^{g_1} + \ldots + e_1^{g_n}$ be the sum of all distinct G-conjugates of e_1. Clearly, e is a central idempotent of $\mathbb{C}G$ and $G_e = \cap_{g \in G}((G_1)_{e_1})^g = \{1\}$.

To see that e is primitive, write $e = f_1 + \ldots + f_k$, a sum of primitive central idempotents of $\mathbb{C}G$. For any nontrivial central subroup N of G, by Lemma 1.1.17, $\widetilde{N}$ is a central idempotent of $\mathbb{C}G_1$ (for $N \subseteq \mathcal{Z}(G) \subseteq \mathcal{C}_G(\mathcal{Z}_2(G)) = G_1$), so either $\widetilde{N}e_1 = 0$ or $\widetilde{N}e_1 = e_1$. However, the latter is impossible, as it implies, by Lemma 2.2.4, that $N \subseteq (G_1)_{e_1}$ and thus $N \subseteq \cap_{g \in G}((G_1)_{e_1})^g = \{1\}$. So we get that $\widetilde{N}e_1 = 0$. Recall that, for a nilpotent group, every

minimal normal subgroup is central ([25, Corollary 1.5.19]). Thus

$$\varepsilon(G)e_1 = \prod_{M\in\mathcal{M}(G)}(1-\widetilde{M})e_1 = \prod_{M\in\mathcal{M}(G)}(e_1-\widetilde{M}e_1) = e_1.$$

The same argument used above to see that $\widetilde{N}e_1 = 0$ works to show that $\widetilde{N}e_1^{g_i} = 0$, for any G-conjugate $e_1^{g_i}$ of e_1. Consequently, $\varepsilon(G)e = e$, and hence, by the unique representation in $\mathbb{C}G$ (Theorem 1.1.13), $\varepsilon(G)f_1 = f_1$. Therefore, by Lemma 2.2.4 again, $G_{f_1} = \{1\}$, and, by the first part of the proof, $f_1 \in \mathbb{C}G_1$. In the first part of the proof, we saw that a primitive central idempotent f_1, having $G_{f_1} = \{1\}$, may be written as the sum of all the distinct G-conjugates of e_1. So, by the definition of e, it follows that $e = f_1$ is a primitive central idempotent of $\mathbb{C}G$. □

The following theorem yields an explicit formula for the primitive central idempotents in $\mathbb{C}G$ when G is a finite nilpotent group.

Theorem 2.2.7. *Let G be a finite nilpotent group. The primitive central idempotents of the group algebra $\mathbb{C}G$ are precisely all elements of the form*

$$\sum_{g\in G}(e\widetilde{H_m})^g,$$

the sum of all distinct G-conjugates of e, where e is an element of $\mathbb{C}G_m$ such that $\overline{e}$ (the image of e in $\mathbb{C}(G_m/H_m)$) is a primitive central idempotent in $\mathbb{C}(G_m/H_m)$, having $(G_m/H_m)_{\overline{e}} = \{1\}$. The groups H_m and G_m are subgroups of G satisfying the following properties:

1. *$H_0 \subseteq H_1 \subseteq \ldots \subseteq H_m \subseteq G_m \subseteq \ldots \subseteq G_1 \subseteq G_0 = G$,*
2. *for $0 \leq i \leq m$, H_i is a normal subgroup of G_i, G_i/H_i is not abelian for $0 \leq i < m$, and G_m/H_m is abelian,*
3. *for $0 \leq i \leq m-1$, $G_{i+1}/H_i = \mathcal{C}_{G_i/H_i}(\mathcal{Z}_2(G_i/H_i))$,*
4. *for $1 \leq i \leq m$, $\bigcap_{x\in G_{i-1}/H_{i-1}} H_i^x = H_{i-1}$.*

Proof. Let us first show that the element defined above, satisfying the listed conditions, is in fact a primitive central idempotent of $\mathbb{C}G$. By condition 2, G_m/H_m is an abelian group. Let $\overline{f_m} := \overline{e}$, a primitive central idempotent in $\mathbb{C}(G_m/H_m)$, having $(G_m/H_m)_{\overline{e}} = \{1\}$. Since $\mathbb{C}(G_m/H_m) \simeq (\mathbb{C}G_m)\widetilde{H_m}$, we have that $f_m := e\widetilde{H_m}$ is a primitive central idempotent of $(\mathbb{C}G_m)\widetilde{H_m}$ and, thus, it is also a primitive central idempotent of $\mathbb{C}G_m$. From $(G_m/H_m)_{\overline{e}} = \{1\}$, we have, by Lemma 2.2.4, that $(G_m)_{f_m} = H_m$; so $(G_m/H_{m-1})_{\overline{f_m}'} =$

H_m/H_{m-1} (where $\overline{f_m}'$ is any preimage of $\overline{f_m}$ in G_m/H_{m-1}). Define $\overline{f_{m-1}} := \sum_{\overline{g}\in G_{m-1}/H_{m-1}} \overline{f_m}'^{\overline{g}}$, the sum of all distinct G_{m-1}/H_{m-1}-conjugates of $\overline{f_m}'$. Then it is a central idempotent of $\mathbb{C}(G_{m-1}/H_{m-1})$. From condition 4,

$$\bigcap_{g\in G_{m-1}/H_{m-1}} \left((G_m/H_{m-1})_{\overline{f_m}'}\right)^g = \bigcap_{g\in G_{m-1}/H_{m-1}} (H_m/H_{m-1})^g = \{1\}.$$

Conditions 3 and 4 provide the hypotheses for the Proposition 2.2.6, which yields that $\overline{f_{m-1}}$ is primitive in $\mathbb{C}(G_{m-1}/H_{m-1}) \simeq \widetilde{(\mathbb{C}G_{m-1})H_{m-1}}$. Thus, $f_{m-1} := (\sum_{g\in G_{m-1}} f_m^g)\widetilde{H_{m-1}}$, the image of $\overline{f_{m-1}}$ in $\widetilde{(\mathbb{C}G_{m-1})H_{m-1}}$, is a primitive central idempotent of $\mathbb{C}G_{m-1}$. We also have, by condition 2, that:

$$f_{m-1} = (\textstyle\sum_{g\in G_{m-1}} f_m^g)\widetilde{H_{m-1}} = \sum_{g\in G_{m-1}} (f_m\widetilde{H_{m-1}})^g =$$

$$\textstyle\sum_{g\in G_{m-1}} (e\widetilde{H_m}\widetilde{H_{m-1}})^g = \sum_{g\in G_{m-1}} (e\widetilde{H_m})^g,$$

By induction, we obtain that $f_0 = \sum_{g\in G}(e\widetilde{H_m})^g$ is a primitive central idempotent of $\mathbb{C}G$.

Now, let $f_0 := d$ be a primitive central idempotent of $\mathbb{C}G$, where G is a finite nilpotent group with nilpotency class c. Then $H_0 := G_d$ is a normal subgroup of $G_0 := G$ by Lemma 2.2.4, and, since $f_0\widetilde{H_0} = f_0$, we have that f_0 is a primitive central idempotent of $(\mathbb{C}G_0)\widetilde{H_0}$. From $(\mathbb{C}G)\widetilde{H_0} \simeq \mathbb{C}(G_0/H_0)$, we get that $\overline{f_0}$, the image of f_0 in $\mathbb{C}(G_0/H_0)$, is a a primitive central idempotent of $\mathbb{C}(G_0/H_0)$. Clearly, $(G_0/H_0)_{\overline{f_0}} = \{1\}$.

If G_0/H_0 is an abelian group, we know $\overline{f_0}$ from Theorem 2.1.2 and, trivially, $d = f_0 = \sum_{g\in G}(f_0\widetilde{H_0})^g$, because $f_0\widetilde{H_0} = f_0$ and f_0 is central.

If G_0/H_0 is not an abelian group, let G_1 be the unique subgroup of G_0 such that $G_1/H_0 = \mathcal{C}_{G_0/H_0}(\mathcal{Z}_2(G_0/H_0)) \neq G_0/H_0$. Then, by Proposition 2.2.6, we get:

$$\overline{f_0} = \sum_{\overline{g}\in G_0/H_0} \overline{f_1}^{\overline{g}},$$

where $\overline{f_1}$ is a primitive central idempotent of $\mathbb{C}(G_1/H_0)$, and

$$\bigcap_{x\in G_0/H_0} (H_1/H_0)^x = \{1\},$$

with H_1 the unique subgroup of G_0 containing H_0 such that $H_1/H_0 = (G_1/H_0)_{\overline{f_1}}$. So H_1 is a normal subgroup of G_1. Notice that, from the definition of G_1/H_0, its nilpotency class is at most $c-1$. Since $\mathbb{C}(G_1/H_1) \simeq$

$(\mathbb{C}(G_1/H_0)(\widetilde{H_1/H_0})$, we have that $\overline{\overline{f_1}}$, the image of $\overline{f_1}$ in $\mathbb{C}(G_1/H_1)$, is a primitive central idempotent of $\mathbb{C}(G_1/H_1)$, having $(G_1/H_1)_{\overline{\overline{f_1}}} = \{1\}$. If G_1/H_1 is an abelian group, then we know $\overline{\overline{f_1}}$ from Theorem 2.1.2. If G_1/H_1 is not an abelian group, the result follows by induction on the nilpotency class c of G. □

Remark 2.2.8. Notice that the statement and the proof of Theorem 2.2.7 are still valid if we replace $\mathbb{C}$ by any algebraically closed field K provided that $char(K)$ does not divide the order of the group. However, historically, the complex case is of particular interest. So, we decided to state the theorem in this context.

Remark 2.2.9. Given a finite nilpotent group G, we know the primitive central idempotents e_i of $\mathbb{C}G$ from Theorem 2.2.7. We can then readily compute the irreducible complex characters χ_i of G from the formula (Theorem 1.1.33)

$$e_i = \frac{\chi_i(1)}{|G|} \sum_{g \in G} \chi_i(g^{-1})g,$$

obtaining the character table of G.

It is known that if two finite groups G and H have the same character table, then $\mathbb{C}G \simeq \mathbb{C}H$ ([25, Theorem 5.22]). Thus our description of the primitive central idempotents of $\mathbb{C}G$ is useful in studying counterexamples to the Isomorphism Problem in group rings ([25, Chapter 9]).

2.3 Some Questions for Further Investigation

The results of [14], in which we base our method, were extended and simplified in [29], providing an algorithm using only elementary methods for calculating the primitive central idempotents of $\mathbb{Q}G$, when G is a finite nilpotent group, among other cases, but not of $\mathbb{C}G$. These improvements were implemented in a package ([27]) of programs for GAP System, version 4. An experimental comparison of the speed of the algorithm in [27] and the character method (computing primitive central idempotents from the character table of the group) was presented in [28] and showed that the first is usually faster. These improvements, however, do not carry on automatically to the complex case.

Notice that the computational complexity of the method proposed in Theorem 2.2.7 is still not known. It provides, however, a theoretic alternative to the usual character method that might be simpler.

Hence, calculating the computational complexity of the proposed method and trying to adapt the ideas in [29] to the complex case may be natural directions to follow in further studies of the subject.

Chapter 3

The Normalizer of a Finite Semigroup and Free Groups in the Unit Group of an Integral Semigroup Ring

Given a group G and a commutative ring R, one of the central problems in Group Ring Theory is deciding to which extent the group ring RG reflects the properties of the group G. More precisely, one might wonder: is it true that if $RG \simeq RH$ as R-algebras, then $G \simeq H$? This problem was stated for the first time in Higman's Ph.D. Thesis [13] and is known as the Isomorphism Problem ([25, Chapter 9]). The answer strongly depends on the ring R (for instance, from Theorem 1.1.32, it is known that if K is an algebraicaly closed field, G and H are both finite abelian groups having the same order, and $|G| = |H| \nmid char(K)$, then $KG \simeq KH$) and early results seemed to suggest that, for a given family of groups, it might be possible to obtain an adequate field for which the isomorphism problem would have a positive answer. However, Dade gave an example in [5] of two nonisomorphic groups such that their respective group algebras over any field are isomorphic.

Of primary importance is the case when $R = \mathbb{Z}$, for if $\mathbb{Z}G \simeq \mathbb{Z}H$, then $RG \simeq RH$ as R-algebras, for any commutative ring R.

The normalizer of the trivial units $\pm G$ in the unit group of an integral group ring $\mathbb{Z}G$ of a finite group G has turned out to be very useful ([15], [24]) in tackling the isomorphism problem for integral group rings. In particular, Hertweck's investigations in [12] have led to a counterexample to the isomorphism problem.

Quite naturally, the same problem also makes sense for semigroup rings ([25, Chapter 9]). Studying the normalizer for semigroup rings might be

helpful in investigating the isomorphism problem for semigroup rings themselves, or for group rings, via the connection between these two subjects provided by partial group rings ([6]). However, in the context of semigroup rings, very little is known. When we want to investigate this problem for semigroup rings in a similar way as was done for group rings, we need a suitable concept of normalizer, as we can no longer speak of trivial units.

In this chapter, we introduce a concept of normalizer of a semigroup S in the unit group of the integral semigroup ring $\mathbb{Z}S$. We show that this definition coincides with the normalizer of a group in case of integral group rings and behaves very much like it in the class of semigroups that are the most related with groups, namely inverse semigroups. These semigroups have a natural involution with which we can extend Krempa's characterization of the normalizer of the trivial units using the classical involution ([36, Proposition 9.4]). We will describe the torsion part of the normalizer and study the double normalizer. Just like in group rings ([8]), the normalizer of a semigroup contains the finite conjugacy center and the second center of the unit group of the integral semigroup ring. We will pose the normalizer problem for integral semigroup rings and solve it for finite Malcev nilpotent semigroups such that the rational semigroup ring is semisimple. Furthermore, just like in integral group rings ([36, Proposition 9.5]), we get that the normalizer of a semigroup is a finite extension of the center of the semigroup ring. All of this indicates that our concept of normalizer of a semigroup behaves as desired.

Also, using the natural involution on inverse semigroups, we will construct free groups in the unit group of the integral semigroup ring, following Marciniak and Sehgal [23], using a bicyclic unit and its image under the involution.

Semigroup rings of inverse semigroups are a wide and interesting class containing for example matrix rings and partial group rings, for which the isomorphism problem recently has been investigated (see [6] and [7]).

3.1 The Normalizer of a Semigroup

We start by giving the definition of the normalizer of a semigroup in the unit group of its integral semigroup ring. This definition coincides with the normalizer of the trivial units in the case of an integral group ring and behaves very much like it for some semigroups. Many results that hold for the normalizer of the trivial units in the unit group of an integral group ring will be extended to the context of integral semigroup rings by means of this definition.

Let S be a semigroup. Consider the contracted integral semigroup ring

with identity $(\mathbb{Z}_0 S)^1$. We denote by $\mathcal{U}((\mathbb{Z}_0 S)^1)$ the group of units of $(\mathbb{Z}_0 S)^1$. Define the normalizer of $\pm S$ as

$$N(\pm S) := \{u \in \mathcal{U}((\mathbb{Z}_0 S)^1); usu^{-1} \in \pm S, \text{ for all } \ s \in \pm S\},$$

which is clearly a semigroup.

Let M^0 be the subsemigroup of S which is the union of all the maximal subgroups of S (see Definition 1.2.6) with a zero θ adjoined, i.e.,

$$M^0 := (\cup_i \mathcal{U}(E_{i,i} S E_{i,i})) \cup \{\theta\},$$

where the $E_{i,i}$ are the idempotents of S. We can hence consider $N(\pm M^0)$

$$N(\pm M^0) := \{u \in \mathcal{U}((\mathbb{Z}_0 S)^1); usu^{-1} \in \pm M^0, \text{ for all } \ s \in \pm M^0\}.$$

More generally, let H be a subset of $\mathcal{U}((\mathbb{Z}_0 S)^1)$. Define the normalizer of $\pm H$ in $\mathcal{U}((\mathbb{Z}_0 S)^1)$ as

$$N(\pm H) := \{v \in \mathcal{U}((\mathbb{Z}_0 S)^1); v^{-1} uv \in \pm H \text{ , for all } \ u \in \pm H\}.$$

As a special case of this definition, we call attention to $N(N(S)$.

Given a group G, denote by $*$ the classical involution in the integral group ring $\mathbb{Z}G$ (Definition 1.1.3), i.e., for $\alpha = \sum_{g \in G} \alpha_g g \in \mathbb{Z}G$, with $\alpha_g \in \mathbb{Z}$, we have that $\alpha^* := \sum_{g \in G} \alpha_g g^{-1}$. Denote by $\mathcal{U}(\mathbb{Z}G)$ the group of units in $\mathbb{Z}G$ and by $N_{\mathcal{U}(\mathbb{Z}G)}(\pm G)$ the normalizer of the trivial units $\pm G$ in $\mathcal{U}(\mathbb{Z}G)$, i.e.,

$$N_{\mathcal{U}(\mathbb{Z}G)}(\pm G) := \{u \in \mathcal{U}(\mathbb{Z}G); ugu^{-1} \in \pm G, \text{ for all } \ g \in \pm G\}.$$

Krempa's characterization of the normalizer in group rings ([36, Proposition 9.4]) states that an element $u \in \mathcal{U}(\mathbb{Z}G)$ belongs to the normalizer $N_{\mathcal{U}(\mathbb{Z}G)}(\pm G)$ if and only if uu^* is a central element in $\mathcal{U}(\mathbb{Z}G)$. So, there is a close connection between the normalizer and the classical involution. Therefore, inverse semigroups (Definition 1.2.6) are the most interesting and suitable class of semigroups for investigating normalizers in semigroup rings.

For an inverse semigroup S (Definition 1.2.6), we can define the morphism

$$\diamond : S \to S; s \mapsto s',$$

where s' is the unique element in S such that $ss's = s$ and $s'ss' = s'$ (as in Definition 1.2.6). Clearly, $\diamond$ is an involution in S (see [4, Lemma 1.18]) and can be extended linearly to an involution in $(\mathbb{Z}_0 S)^1$, with $\diamond(1) := 1$. We will often denote $\diamond(a)$ by $a^\diamond$, for $a \in (\mathbb{Z}_0 S)^1$. Notice that, if $a \in (\mathbb{Z}_0 S)^1$ and $supp(a) \in G$, a subgroup of S, then $a^\diamond = a^*$. Also, if $u \in \mathcal{U}((\mathbb{Z}_0 S)^1)$, then it is easy to see that $(u^\diamond)^{-1} = (u^{-1})^\diamond$.

Let S be a finite inverse semigroup. It is well known ([4, §3.3, Exercise 3]) that every principal factor of S is a Brandt semigroup (i.e., a matrix semigroup of the form $\mathcal{M}^0(G, n, n, I_n)$, where I_n is the $n \times n$ identity matrix and G is a maximal subgroup of S, according to Theorem 1.2.14 and Proposition 1.2.8). Moreover, the rational semigroup algebra $\mathbb{Q}S$ is semisimple (Theorem 1.2.27). By Corollary 1.2.29, $\mathbb{Q}S$ has a series of ideals $\mathbb{Q}S = \mathbb{Q}S_1 \supset \mathbb{Q}S_2 \supset \ldots \supset \mathbb{Q}S_s \supset \mathbb{Q}S_{s+1} = \mathbb{Q}\theta$, where S_i are ideals in a principal series of S and $S_i/S_{i+1} \simeq \mathcal{M}^0(G_i, n, n, I_n)$ and $\mathbb{Q}S_i/\mathbb{Q}S_{i+1} \simeq \mathbb{Q}_0(S_i/S_{i+1}) \simeq M_{n_i}(\mathbb{Q}G_i)$, with $G_1, \ldots, G_s$ the maximal subgroups of S (up to isomorphism). We have that

$$\mathbb{Q}_0 S = \mathbb{Q}_0 S_1 \simeq \frac{\mathbb{Q}_0 S_1}{\mathbb{Q}_0 S_s} \times \mathbb{Q}_0 S_s \simeq \frac{\mathbb{Q}_0 S_1}{\mathbb{Q}_0 S_s} \times M_{n_s}(\mathbb{Q}G_s),$$

and

$$\frac{\mathbb{Q}_0 S_1}{\mathbb{Q}_0 S_{i+1}} \simeq \frac{\mathbb{Q}_0 S_1}{\mathbb{Q}_0 S_i} \times \frac{\mathbb{Q}_0 S_i}{\mathbb{Q}_0 S_{i+1}} \simeq \frac{\mathbb{Q}_0 S_1}{\mathbb{Q}_0 S_i} \times \mathbb{Q}_0(S_i/S_{i+1}) \simeq \frac{\mathbb{Q}_0 S_1}{\mathbb{Q}_0 S_i} \times M_{n_i}(\mathbb{Q}G_i),$$

for $i = 1, \ldots, s-1$. Thus, $(\mathbb{Q}_0 S)^1 \simeq M_{n_1}(\mathbb{Q}G_1) \oplus \ldots \oplus M_{n_s}(\mathbb{Q}G_s)$. Repeating the same argument for $\mathbb{Z}$, we have that $(\mathbb{Z}_0 S)^1 \simeq M_{n_1}(\mathbb{Z}G_1) \oplus \ldots \oplus M_{n_s}(\mathbb{Z}G_s)$. Therefore $\mathcal{U}((\mathbb{Z}_0 S)^1) \simeq GL_{n_1}(\mathbb{Z}G_1) \oplus \ldots \oplus GL_{n_s}(\mathbb{Z}G_s)$. Hence, we can work "coordinatewise" and we will therefore make the reduction to S a finite Brandt semigroup and G a maximal subgroup of S. In this case, $(\mathbb{Z}_0 S)^1 \simeq M_n(\mathbb{Z}G)$ and, for $a = (a_{i,j}) \in (\mathbb{Z}_0 S)^1$, we have that $(a_{i,j})^\diamond = (a^*_{j,i})$.

Given a group G, we denote by $Mon(\pm G)$ the group of monomial matrices over $\pm G$. Notice that for $a \in Mon(\pm G)$ we have that

$$(a^\diamond)_{i,j} = \begin{cases} a_{j,i}^{-1}, & \text{if } a_{j,i} \neq 0; \\ 0, & \text{if } a_{j,i} = 0. \end{cases}$$

Denote by $Diag(\pm G)$ the subgroup of $Mon(\pm G)$ consisting of matrices over $\pm G$ having nonzero elements only on the diagonal, and denote by $Scal(\pm G)$ the matrices of $Diag(\pm G)$ having the same element on the diagonal.

Remark 3.1.1 (Partial Group Rings). We recall the definition of partial group rings and some properties, which will make it possible to relate these objects with the present work.

Definition 3.1.2. Given a group G and a ring R with identity, we consider the semigroup S_G generated by the set of symbols $\{[g]; g \in G\}$, with the following relations:

1. $[s^{-1}][s][t] = [s^{-1}][st]$;
2. $[s][t][t^{-1}] = [st][t^{-1}]$;

3. $[s][e] = [s]$;

4. $[e][s] = [s]$;

for all $s, t \in G$. The *partial group ring* $R_{par}G$ is the semigroup ring of S_G over R, i.e.

$$R_{par}G := RS_G.$$

(Notice that relation *(4)* follows from the previous ones, and thus could be removed from the list.)

Given a group G, the semigroup S_G is an inverse semigroup ([10, Theorem 3.4]) and does not contain a zero element.

Remark 3.1.3. Let S be a finite semigroup. If all principal factors of S are of the form $\mathcal{M}^0(G, n, n, P)$, with P invertible in $M_n(\mathbb{Z}G)$, then, by Theorem 1.2.26, $(\mathbb{Q}_0 S)^1$ is a semisimple semigroup algebra and $(\mathbb{Q}_0 S)^1 \simeq M_{n_1}(\mathbb{Q}G_1) \oplus \ldots \oplus M_{n_s}(\mathbb{Q}G_s)$, where $G_1, \ldots, G_s$ are the maximal subgroups of S (up to isomorphism). Again, $(\mathbb{Z}_0 S)^1 \simeq M_{n_1}(\mathbb{Z}G_1) \oplus \ldots \oplus M_{n_s}(\mathbb{Z}G_s)$. By considering the ring isomorphism

$$f : \mathbb{Z}\mathcal{M}^0(G, n, n, I_n) \longrightarrow \mathbb{Z}\mathcal{M}^0(G, n, n, P) \text{ defined by } A \mapsto f(A) := AP^{-1},$$

we can work "coordinatewise", and transport all the results obtained on inverse semigroups to such a semigroup S.

3.1.1 Characterization of $N(\pm S)$ and Some Results

Recall that, for any semigroup , all maximal subgroups are ismomorphic (see Definition 1.2.6). In case S is a Rees matrix semigroup over a group G, then all the maximal semigroups are isomorphic to G (see Proposition 1.2.8).

We shall now characterize the normalizer of a semigroup and prove several interesting properties.

Theorem 3.1.4. *Let S be a finite Brandt semigroup, let M denote the union of all maximal subgroups of S, and let G be a maximal subgroup of S. We have that:*

1. $N(\pm S) = Scal(N_{\mathcal{U}(\mathbb{Z}G)}(\pm G))Mon(\pm G)$ *and* $N(\pm S) \subseteq N(\pm M^0)$;

2. $N(\pm M^0) = Mon(N_{\mathcal{U}(\mathbb{Z}G)}(\pm G))$;

3. *if* $u \in N(\pm M^0)$ *then* $uu^\diamond \in Diag(\mathcal{Z}(\mathcal{U}(\mathbb{Z}G)))$;

4. *if* $u \in N(\pm S)$ *then* $uu^\diamond \in \mathcal{Z}(\mathcal{U}(\mathbb{Z}_0 S)^1))$.

Proof. Being a Brandt semigroup, we have that (see Theorem 1.2.14) $S \simeq \mathcal{M}^0(G, n, n, I_n)$ and $M^0 \simeq \{s = ge_{i,i} \in \mathcal{M}^0(G, n, n, I_n); g \in G, i = 1, \ldots, n\}$, where I_n is the $n \times n$ identity matrix and $e_{i,j}$ are matrix units (Example 1.2.2.1). Let $u = \sum_{i,j=1}^{n} u_{i,j}e_{i,j} \in \mathcal{U}((\mathbb{Z}_0 S)^1)$.

1. For u to be in $N(\pm S)$, we need that for all $s \in \pm S$, there exists a $t \in \pm S$, such that $us = tu$. Now, $s = ge_{k,l}$ and $t = he_{m,p}$, for some $g, h \in \pm G$ and then $us = \sum_i u_{i,k}ge_{i,l}$ and $tu = \sum_j hu_{p,j}e_{m,j}$.

Thus, $us = tu$ means that

$$\begin{cases} u_{m,k}g &= hu_{p,l}; \\ u_{i,k} &= 0, \text{ for all } i \neq m; \\ u_{p,j} &= 0, \text{ for all } j \neq l. \end{cases}$$

When we take $k = l$ (i.e., $s = ge_{k,k} \in \pm M^0$), we deduce that

$$\begin{cases} u_{m,k}g &= hu_{p,k}; \\ u_{i,k} &= 0, \text{ for all } i \neq m; \ (*) \\ u_{p,j} &= 0, \text{ for all } j \neq k. \end{cases}$$

Suppose that $m \neq p$. Then we get that $u_{p,k} = 0$; hence, $u_{p,j} = 0$ for $1 \leq j \leq n$, which contradicts that u is a unit.

Therefore, $m = p$ (i.e., $t = he_{m,m} \in \pm M^0$) and $(*)$ becomes

$$\begin{cases} u_{m,k}g &= hu_{m,k}; \\ u_{i,k} &= 0, \text{ for all } i \neq m; \\ u_{m,j} &= 0, \text{ for all } j \neq k. \end{cases}$$

Since g and k are arbitrary, we get that u is a monomial matrix $\sum_k u_{m_k,k}e_{m_k,k}$, with $u_{m_k,k} \in N_{\mathcal{U}(\mathbb{Z}G)}(\pm G)$.

Now, consider $s = ge_{k,l} \in \pm S$, with $k \neq l$ (i.e., $s \in \pm S \setminus \pm M^0$). So $u \in N(\pm S)$, if

$$uge_{k,l}u^{-1} = u_{m_k,k}gu^{-1}_{m_l,l}e_{m_k,m_l} \in \pm S$$

(since $u^{-1} = \sum_i u^{-1}_{m_i,i}e_{i,m_i}$). As $u_{m_k,k} \in N_{\mathcal{U}(\mathbb{Z}G)}(\pm G)$, we have $u_{m_k,k}gu^{-1}_{m_l,l} = hu_{m_k,k}u^{-1}_{m_l,l} \in \pm G$, for some $h \in \pm G$; so $u_{m_k,k}u^{-1}_{m_l,l}$ must be in $\pm G$. Hence, all entries in u differ up to trivial units. Thus $u \in Scal(N_{\mathcal{U}(\mathbb{Z}G)}(\pm G))Mon(\pm G)$. So, $N(\pm S)) \subseteq Scal(N_{\mathcal{U}(\mathbb{Z}G)}(\pm G))Mon(\pm G)$.

Now, to see that $Scal(N_{\mathcal{U}(\mathbb{Z}G)}(\pm G))Mon(\pm G) \subseteq N(\pm S)$, consider $u \in Scal(N_{\mathcal{U}(\mathbb{Z}G)}(\pm G))Mon(\pm G)$, i.e., $u = \sum_{i,j=1}^{n} va_{i,j}e_{i,j}$ monomial, with $v \in N_{\mathcal{U}(\mathbb{Z}G)}(\pm G)$ and $a_{i,j} = 0$ or $a_{i,j} \in \pm G$. For $s = ge_{k,l} \in \pm S$, with $g \in \pm G$, we have that $us = \sum_i va_{i,k}ge_{i,l} = va_{i_k,k}ge_{i_k,l}$, where $a_{i_k,k}$ is the only nonzero element in the k^{th} column of u. Since $v \in N_{\mathcal{U}(\mathbb{Z}G)}(\pm G)$, we have

that $us = va_{i_k,k}ge_{i_k,l} = hva_{j_l,l}e_{i_k,l}$, where $a_{j_l,l}$ is the only nonzero element in the l^{th} column of u, for $h := va_{i_k,k}ga_{j_l,l}^{-1}v^{-1} \in \pm G$. So, $us = tu$, with $t = he_{i_k,j_l} \in \pm S$.

2. Notice that the proof that $N(\pm M^0) \subseteq Mon(N_{\mathcal{U}(\mathbb{Z}G)}(\pm G))$ is contained in the proof of *1.*, as we have seen that for $u = \sum_{i,j=1}^{n} u_{i,j}e_{i,j} \in \mathcal{U}((\mathbb{Z}_0 S)^1)$ and $s = ge_{k,k} \in \pm M^0$, $us = tu$ automatically implies that $t = he_{m,m} \in \pm M^0$ (hence, $u \in N(\pm M^0)$) and $u \in Mon(N_{\mathcal{U}(\mathbb{Z}G)}(\pm G))$.

To see that $Mon(N_{\mathcal{U}(\mathbb{Z}G)}(\pm G)) \subseteq N(\pm M^0)$, take $u \in Mon(N_{\mathcal{U}(\mathbb{Z}G)}(\pm G))$, i.e., $u = \sum_{i,j=1}^{n} u_{i,j}e_{i,j}$ monomial, with $u_{i,j} = 0$ or $u_{i,j} \in N_{\mathcal{U}(\mathbb{Z}G)}(\pm G)$, and $s = ge_{k,k} \in \pm M^0$, with $g \in \pm G$. We have that $us = \sum_i u_{i,k}ge_{i,k} = u_{i_k,k}ge_{i_k,k}$, where $u_{i_k,k}$ is the only nonzero element in the k^{th} column of u. Since $u_{i_k,k} \in N_{\mathcal{U}(\mathbb{Z}G)}(\pm G)$, we have that $us = u_{i_k,k}ge_{i_k,l} = hu_{i_k,k}e_{i_k,k}$, for some $h \in \pm G$. So, $us = tu$, with $t = he_{i_k,i_k} \in \pm M^0$.

3. Take $u \in N(\pm M^0)$. From the first part of the proof, we know that $u \in Mon(N_{\mathcal{U}(\mathbb{Z}G)}(\pm G))$, i.e., $u = (u_{i,j})$ monomial, with $u_{i,j} = 0$ or $u_{i,j} \in N_{\mathcal{U}(\mathbb{Z}G)}(\pm G)$. So $u^\diamond = (u_{j,i}^*)$. By computing $uu^\diamond$, we get a diagonal matrix with $u_{i,j}u_{i,j}^*$ in the (i,i) position, when $u_{i,j} \neq 0$. From [36, Proposition 9.4], we know that $u_{i,j}u_{i,j}^* \in \mathcal{Z}(\mathcal{U}(\mathbb{Z}G))$. So, we have the desired result.

4. Following the same lines of *3.*, we get the analogue result for $N(\pm S)$. □

We get, as an easy but important consequence, that an element of the normalizer commutes with its image under the involution $\diamond$.

Corollary 3.1.5. *Let S be a finite Brandt semigroup, let M denote the union of all maximal subgroups of S, and let G be a maximal subgroup of S. If $u \in N(\pm M^0)$, then $uu^\diamond = u^\diamond u$.*

Proof. Take $u \in N(\pm M^0)$, say $u = (u_{i,j})$ monomial, with $u_{i,j} = 0$ or $u_{i,j} \in N_{\mathcal{U}(\mathbb{Z}G)}(\pm G)$. From Theorem 3.1.4, (3), $uu^\diamond \in Diag(\mathcal{Z}(\mathcal{U}(\mathbb{Z}G)))$, i.e., for each i,j such that $u_{i,j} \neq 0$, we have that $u_{i,j}u_{i,j}^* \in \mathcal{Z}(\mathcal{U}(\mathbb{Z}G))$. So, for all i,j,

$$(u_{i,j}u_{i,j}^*)u_{i,j}^{-1}(u_{i,j}^*)^{-1} = u_{i,j}^{-1}(u_{i,j}u_{i,j}^*)(u_{i,j}^*)^{-1} = 1.$$

Thus $u_{i,j}u_{i,j}^* = u_{i,j}^*u_{i,j}$, for all i,j, and we have that $uu^\diamond = u^\diamond u$. □

For group rings, we know that the only unitary units (Definition 1.1.30) for the classical involution are the trivial units (Proposition 1.1.34). We now describe the analogous "$\diamond$-unitary elements".

Theorem 3.1.6. *Let S be a finite Brandt semigroup and G a maximal subgroup of S. For $v \in (\mathbb{Z}_0 S)^1$, $vv^\diamond = 1$ if and only if $v \in Mon(\pm G)$.*

Proof. This proof is very similar to the proof of Proposition 1.1.34.

Being a Brandt semigroup, we have that (see Theorem 1.2.14) $S \simeq \mathcal{M}^0(G, n, n, I_n)$ and $(\mathbb{Z}_0 S)^1 \simeq M_n(\mathbb{Z}G)$ (see Example 1.2.24).

Let $v = (v_{i,j}) \in (\mathbb{Z}_0 S)^1$, with $v_{i,j} = \sum_{g \in G} v_{i,j}(g)g \in \mathbb{Z}G$. From $vv^\diamond = 1 = I_n$, we get in particular that, for all i, $\sum_j v_{i,j} v_{i,j}^* = \sum_j (\sum_{g \in G} v_{i,j}(g)^2) = 1$. Hence, for each i, exactly one $v_{i,j}(g) = 1$, i.e., for each i, exactly one $v_{i,j}$ is a trivial unit and all the other ones are zero. Again, from $vv^\diamond = I_n$, we can deduce relations between the rows and columns from which it follows that $v \in Mon(\pm G)$.

Cleary, if $v \in Mon(\pm G)$, then $v^\diamond = v^{-1}$. □

Next, we prove some results for the normalizer in semigroup rings, that were proved for group rings in [18], [22] , [24].

The following Lemma is, in a certain sense, the semigroup ring analogue of a famous corollary of Berman–Higman Lemma for group rings (Corollary 1.1.36). It will be very helpful on many of the results to be proved, and it has an interesting immediate Corollary.

Lemma 3.1.7. *Let S be a finite Brandt semigroup and G a maximal subgroup of S. If $c \in Diag(\mathcal{Z}(\mathcal{U}(\mathbb{Z}G)))$ and c is a torsion unit, then $c \in Diag(\pm\mathcal{Z}(G))$.*

Proof. Take $c \in Diag(\mathcal{Z}(\mathcal{U}(\mathbb{Z}G)))$ a torsion unit, say $c = (c_{i,j})$, with $c_{i,j} = 0$, if $i \neq j$, and $c_{i,i} \in \mathcal{Z}(\mathcal{U}(\mathbb{Z}G))$ torsion units in $\mathbb{Z}G$. We have from Corollary 1.1.37, that, for all i, $c_{i,i} \in \pm\mathcal{Z}(G)$, i.e., $c \in Diag(\pm\mathcal{Z}(G))$. □

Corollary 3.1.8. *Let S be a finite Brandt semigroup, let M denote the union of all maximal subgroups of S, and let G be a maximal subgroup of S. If $u \in N(\pm M^0)$, then either $uu^\diamond$ has infinite order, or $uu^\diamond = 1$ and, in this case, $u \in Mon(\pm G)$.*

Proof. Take $u \in N(\pm M^0)$, say $u = (u_{i,j})$ monomial, with $u_{i,j} = 0$ or $u_{i,j} = \sum_{g \in G} u_{i,j}(g)g \in N_{\mathcal{U}(\mathbb{Z}G)}(\pm G)$. From Theorem 3.1.4, (3), we know that $uu^\diamond = c \in Diag(\mathcal{Z}(\mathcal{U}(\mathbb{Z}G)))$. Suppose c is a torsion unit. We have, from Lemma 3.1.7, that $c = (c_{i,j}) \in Diag(\pm\mathcal{Z}(G))$.

For each i, $c_{i,i} = u_{i,j} u_{i,j}^*$ is a trivial unit with $c_{i,i}(1) = \sum_{g \in G} u_{i,j}(g)^2 \neq 0$. It follows that, for each i, $c_{i,i} = 1$, i.e., $uu^\diamond = 1$. From Theorem 3.1.6, it now follows that $u \in Mon(\pm G)$. □

Denote by $T(N(\pm M^0))$ the set of torsion units in $N(\pm M^0)$. We can prove that the elements in $Mon(\pm G)$ are the only torsion elements in $N(\pm M^0)$ and in $N(\pm S)$.

Proposition 3.1.9. *Let S be a finite Brandt semigroup, let M denote the union of all maximal subgroups of S, and let G be a maximal subgroup of S. We have that $T(N(\pm M^0)) = Mon(\pm G) = T(N(\pm S))$.*

Proof. Take $u \in T(N(\pm M^0))$. From Corollary 3.1.5, we know that $uu^\diamond$ is a torsion unit and, from Corollary 3.1.8, we get $uu^\diamond = 1$, and thus $u \in Mon(\pm G)$.

The other inclusion is obvious.

The proof is similar for $T(N(\pm S))$. □

We can now characterize when the normalizer coincides with the torsion units.

Proposition 3.1.10. *Let S be a finite Brandt semigroup, let M denote the union of all maximal subgroups of S, and let G be a maximal subgroup of S. The following are equivalent:*

1. $N(\pm M^0) = T(N(\pm M^0))$;
2. $N(\pm S) = T(N(\pm S))$;
3. $\mathcal{Z}(\mathcal{U}(\mathbb{Z}G)) = \pm\mathcal{Z}(G)$.

Proof. From *1.* to *2.*, it is obvious, using that $N(\pm S) \subseteq N(\pm M^0)$ and Proposition 3.1.9.

Now, suppose *2.* is true. Since $\mathcal{Z}(\mathcal{U}(\mathbb{Z}_0 S)^1)) \simeq Scal(\mathcal{Z}(\mathcal{U}(\mathbb{Z}G)))$ is contained in $N(\pm S) = T(N(\pm S))$, we have by Lemma 3.1.7 that $\mathcal{Z}(\mathcal{U}(\mathbb{Z}G)) = \pm\mathcal{Z}(G)$.

If *3.* holds, then from Theorem 3.1.4, (3) it follows that for all $u \in N(\pm M^0)$, $uu^\diamond \in Diag(\pm\mathcal{Z}(G))$; in particular, $uu^\diamond$ has finite order. Thus, from Corollary 3.1.8, $u \in Mon(\pm G) \subseteq T(N(\pm M^0))$. The other inclusion is always true. □

For a finite group G, a well known result due to Krempa [36, Proposition 9.4] states that: for $u \in \mathcal{U}(\mathbb{Z}G)$, we have that $u \in N_{\mathcal{U}(\mathbb{Z}G)}(\pm G) \iff uu^* \in \mathcal{Z}(\mathcal{U}(\mathbb{Z}G))$. We will prove a similar result for $N(\pm Mon(G))$, but first we need the following lemma.

Lemma 3.1.11. *Let S be a finite Brandt semigroup, $S \neq \mathcal{M}(\{1\}, 2, 2, I_2)$ and G a maximal subgroup of S. If $t \in \mathcal{U}((\mathbb{Z}_0 S)^1)$ is such that $ta = at$, for all $a \in Mon(\pm G)$, then $t \in \mathcal{Z}(\mathcal{U}(\mathbb{Z}_0 S)^1))$.*

Proof. We have that $S \simeq \mathcal{M}^0(G, n, n, I_n)$, with I_n the $n \times n$ identity matrix. We divide the proof in two parts.

Part 1: If $t \in (\mathbb{Z}_0 S)^1$ and $ta = at$, for all $a \in Mon(\pm G)$, then there exist $\alpha \in \mathcal{Z}(\mathbb{Z}G)$ and $\beta \in \mathbb{Z}\widehat{G}$ such that $t = (t_{i,j})$, with $t_{i,j} = \begin{cases} \alpha, & \text{if } i = j \\ \beta, & \text{if } i \neq j \end{cases}$

We prove this by induction on n.

For $n = 1$ the result is obvious.

So, assume the result is valid for $n-1$ and we will verify it for n. Take $t \in (\mathbb{Z}_0 S)^1 \simeq M_n(\mathbb{Z}G)$ such that $ta = at$, for all $a \in Mon_n(\pm G)$ (i.e., the monomial $n \times n$ matrices over $\pm G$). So, $t = \begin{pmatrix} t_{1,1} & \dots & t_{1,n} \\ \vdots & t' & \\ t_{n,1} & & \end{pmatrix}$, where $t' \in M_{n-1}(\mathbb{Z}G)$ and it is easy to see that $t'b = bt'$, for all $b \in Mon_{n-1}(\pm G)$, as $e_{1,1} + b \in Mon_n(\pm G)$. Hence by the induction hypothesis, there exist $\alpha \in \mathcal{Z}(\mathbb{Z}G)$ and $\beta \in \mathbb{Z}\widehat{G}$ such that $t'_{i,j} = \begin{cases} \alpha, & \text{if } i = j \\ \beta, & \text{if } i \neq j \end{cases}$

Take $a = \sum g_i e_{i,i} \in Mon(\pm G)$. We have that $ta = \sum t_{i,j} g_j e_{i,j}$ and $at = \sum g_i t_{i,j} e_{i,j}$. Thus, for every i and j,

$$t_{i,j} g_j = g_i t_{i,j}. (**)$$

This means, in particular, that $t_{i,i} g_i = g_i t_{i,i}$ and, since this is valid for an arbitrary $g_i \in G$, we have that $t_{i,i} \in \mathcal{Z}(\mathbb{Z}G)$, for every i. For $i \neq j$, we get that $t_{i,j} \in \mathbb{Z}\widehat{G}$.

Now, take $a = \sum g_i e_{i,n+1-i} \in Mon(\pm G)$. Then $ta = \sum t_{i,n+1-j} g_{n+1-j} e_{i,j}$ and $at = \sum g_i t_{n+1-i,j} e_{i,j}$. Thus, for every i and j, $t_{i,n+1-j} g_{n+1-j} = g_i t_{n+1-i,j}$. So, for all j, $g_1 t_{n,j} = t_{1,n+1-j} g_{n+1-j} = g_1 t_{1,n+1-j}$, the last equality following from $(**)$. Hence, for all j, $t_{1,n+1-j} = t_{n,j}$, and, by the induction hypothesis, for $j \neq 1, n$, we have that $t_{1,j} = t_{n,n+1-j} = \beta$. Similarly, for all i, $g_i t_{n+1-i,1} = t_{i,n} g_n = g_i t_{i,n}$, the last equality following from $(**)$. Hence, for all i, $t_{(n+1-i),1} = t_{i,n}$, and, by the induction hypothesis, for $i \neq 1, n$, we have that $t_{i,1} = t_{(n+1-i),n} = \beta$. Also, we get $t_{1,1} = t_{n,n} = t_{i,i} = \alpha$, by the induction hypothesis again.

So, the only entries in t that are still unknown are $t_{1,n}$ and $t_{n,1}$.

Consider $a = g_1 e_{1,1} + \sum_{i=2}^{n} g_i e_{i,n+2-i} \in Mon(\pm G)$. Then we have that $ta = \sum_{i=1}^{n} (t_{i,1} g_1 e_{i,1} + \sum_{j=2}^{n} t_{i,n+2-j} g_{n+2-j} e_{i,j})$ and $at = \sum_{j=1}^{n} (g_1 t_{1,j} e_{1,j} + \sum_{i=2}^{n} g_i t_{n+2-i,j} e_{i,j})$. Thus, $g_1 t_{1,n} = t_{1,2} g_2 = g_2 t_{1,2}$, the last equality following from $(**)$. Hence, $t_{1,n} = t_{1,2} = \beta$, by the induction hypothesis.

Finally, consider $a = g_n e_{n,n} + \sum_{i=1}^{n-1} g_i ei, n-i \in Mon(\pm G)$. We have that $ta = \sum_{i=1}^{n} (t_{i,n} g_n e_{i,n} + \sum_{j=1}^{n-1} t_{i,n-j} g_{n-j} e_{i,j})$ and $at = \sum_{j=1}^{n} (g_n t_{n,j} e_{n,j} +$

$\sum_{i=1}^{n-1} g_i t_{n-i,j} e_{i,j}$). Thus, $g_n t_{n,1} = t_{n,n-1} g_{n-1} = g_n t_{n,n-1}$, the last equality following from $(**)$. Hence, $t_{n,1} = t_{n,n-1} = \beta$, by the induction hypothesis. And this concludes the proof of the first part of the Lemma.

Part 2: If $t \in \mathcal{U}((\mathbb{Z}_0 S)^1)$ is such that $t = (t_{i,j})$, with $t_{i,j} = \begin{cases} \alpha, & \text{if } i = j \\ \beta, & \text{if } i \neq j \end{cases}$, for some $\alpha \in \mathcal{Z}(\mathbb{Z}G)$ and $\beta = b\widehat{G} \in \mathbb{Z}\widehat{G}$, then $t \in \mathcal{Z}(\mathcal{U}((\mathbb{Z}_0 S)^1))$.

The case $n = 1$ is trivial.

For the rest of the proof, we assume $n > 2$ or $|G| > 1$.

Take t as in the statement above. Notice that, by performing elementary operations on t, $det(t)$ is multiplied by ± 1 (since we are working on integral matrices). Then, by bringing t to its row-echelon form, it is easy to see that $det(t) = \pm(\alpha - \beta)^{n-1}(\alpha + (n-1)\beta)$. Since t is a unit, we have that $det(t) \in \mathcal{U}(\mathbb{Z}G)$. Consider ε the augmentation mapping in $\mathbb{Z}G$. If we take $\varepsilon(det(t))$, we get that it is in $\mathbb{Z}$ and it is a unit; so

$$\varepsilon(det(t)) = \pm(\varepsilon(\alpha) - b|G|)^{n-1}(\varepsilon(\alpha) + (n-1)b|G|) = \pm 1.$$

We claim that the only integer solutions to these equations are $\varepsilon(\alpha) = \pm 1$ and $b = 0$.

Let us first take a look at $(\varepsilon(\alpha) - b|G|)^{n-1}(\varepsilon(\alpha) + (n-1)b|G|) = 1$. So, either $(\varepsilon(\alpha) - b|G|)^{n-1} = 1$ and $(\varepsilon(\alpha) + (n-1)b|G|) = 1$, or $(\varepsilon(\alpha) - b|G|)^{n-1} = -1$ and $(\varepsilon(\alpha) + (n-1)b|G|) = -1$. If n is odd, the second option can never occur, and the only possible integer solutions for the first case are $\varepsilon(\alpha) = \pm 1$ and $b = 0$ (since the case $n = 1$ has already been dealt with and is excluded). If n is even, we have the desired result immediately.

Analyzing equation $(\varepsilon(\alpha) - b|G|)^{n-1}(\varepsilon(\alpha) + (n-1)b|G|) = -1$, we get either $(\varepsilon(\alpha) - b|G|)^{n-1} = -1$ and $(\varepsilon(\alpha) + (n-1)b|G|) = 1$, or $(\varepsilon(\alpha) - b|G|)^{n-1} = 1$ and $(\varepsilon(\alpha) + (n-1)b|G|) = -1$. If n is odd, the first option is not possible, and the only existing integer solutions for the second case are $\varepsilon(\alpha) = \pm 1$ and $b = 0$. If n is even, then the only possible integer solutions are the desired ones (since we have already dealt with the cases $n = 2$ and G trivial, and $n = 1$) .

Because t is a unit and a diagonal matrix with α on all nonzero entries, we have that $\alpha \in \mathcal{Z}(\mathcal{U}(\mathbb{Z}G))$, which finishes the proof. □

Theorem 3.1.12. *Let S be a finite Brandt semigroup, let G be a maximal subgroup, and let $u \in \mathcal{U}((\mathbb{Z}_0 S)^1)$. We have that $u \in N(Mon(\pm G))$ if and only if $uu^{\diamond} \in \mathcal{Z}(\mathcal{U}((\mathbb{Z}_0 S)^1))$.*

Proof. We examine separately the case where $S = \mathcal{M}(\{1\}, 2, 2, I)$, with I the 2×2 identity matrix. We have that $(\mathbb{Z}_0 S)^1 = M_2(\mathbb{Z})$ and $\mathcal{Z}(\mathcal{U}((\mathbb{Z}_0 S)^1)) =$

$\pm I_2$. By means of elementary matrix computations, we see that

$$N(Mon(\pm\{1\})) = \{\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}, \begin{pmatrix} 0 & \pm 1 \\ \pm 1 & 0 \end{pmatrix}\},$$

and $u \in N(Mon(\pm G))$ implies $uu^\diamond = I_2$. Now, if $uu^\diamond = \pm I_2$, for $u \in \mathcal{U}(M_2(\mathbb{Z}))$, then, making elementary matrix computations, we get that $u = \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$ or $u = \begin{pmatrix} 0 & \pm 1 \\ \pm 1 & 0 \end{pmatrix}$. In either case, $u \in N(Mon(\{\pm 1\}))$.

For the rest of the proof, we assume $S \neq \mathcal{M}(\{1\}, 2, 2, I)$.

Take $u \in \mathcal{U}((\mathbb{Z}_0 S)^1)$ and $a \in Mon(\pm G)$. Assume $u \in N(Mon(\pm G))$. Then $b := uau^{-1} \in Mon(\pm G)$. Hence, applying $\diamond$ to both sides, $b^\diamond = b^{-1} = (u^{-1})^\diamond a^{-1} u^\diamond$. Taking inverses in this equality, $b = (u^\diamond)^{-1} a u^\diamond$. Thus,

$$a = u^\diamond b (u^\diamond)^{-1}.$$

So,

$$u^\diamond ua(u^\diamond u)^{-1} = u^\diamond uau^{-1}(u^\diamond)^{-1} = u^\diamond b(u^\diamond)^{-1} = u^\diamond (u^\diamond)^{-1} a u^\diamond (u^\diamond)^{-1} = a.$$

We have proved that $u^\diamond u$ commutes with elements from $Mon(\pm G)$. By Lemma 3.1.11, it follows that $u^\diamond u \in \mathcal{Z}(\mathcal{U}(\mathbb{Z}_0 S)^1))$. So $u^\diamond u = (u^\diamond)^{-1} u^\diamond uu^\diamond = uu^\diamond \in \mathcal{Z}(\mathcal{U}(\mathbb{Z}_0 S)^1))$.

Now, suppose $uu^\diamond \in \mathcal{Z}(\mathcal{U}((\mathbb{Z}_0 S)^1))$. Then $uu^\diamond = u^\diamond u$ and $(u^\diamond u)^{-1} = u^{-1}(u^{-1})^\diamond \in \mathcal{Z}(\mathcal{U}((\mathbb{Z}_0 S)^1))$. We want to show that $uau^{-1} \in Mon(\pm G)$, for all $a \in Mon(\pm G)$. We have that

$$(uau^{-1})(uau^{-1})^\diamond = ua(u^{-1}(u^{-1})^\diamond)a^{-1}u^\diamond = uu^{-1}(u^{-1})^\diamond u^\diamond = 1.$$

So, by Theorem 3.1.6, $uau^{-1} \in Mon(\pm G)$, as desired. □

By Theorem 3.1.4, (4) we get the following Corollary:

Corollary 3.1.13. *Let S be a finite Brandt semigroup and let G be a maximal subgroup of S. Then $N(\pm S) \subseteq N(Mon(\pm G))$.*

The reverse inclusion remains an open and interesting problem.

When the central units of $\mathbb{Z}G$ are trivial, the problem is solved.

Proposition 3.1.14. *Let S be a finite Brandt semigroup and let G be a maximal subgroup of S. We have that $N(\pm S) = Mon(\pm G) = N(Mon(\pm G))$ if and only if $\mathcal{Z}(\mathcal{U}(\mathbb{Z}G)) = \pm\mathcal{Z}(G)$.*

Proof. Suppose $N(\pm S) = Mon(\pm G) = N(Mon(\pm G))$. As $\mathcal{Z}(\mathcal{U}(\mathbb{Z}_0 S)^1)) \simeq Scal(\mathcal{Z}(\mathcal{U}(\mathbb{Z}G)))$ is contained in $N(\pm S) = Mon(\pm G)$, we have by Lemma 3.1.7 that $\mathcal{Z}(\mathcal{U}(\mathbb{Z}G)) = \pm\mathcal{Z}(G)$.

In case $\mathcal{Z}(\mathcal{U}(\mathbb{Z}G)) = \pm\mathcal{Z}(G)$, then from Theorem 3.1.4, (4) it follows that for all $u \in N(\pm S)$, $uu^\diamond \in Scal(\pm\mathcal{Z}(G))$; in particular, $uu^\diamond$ has finite order. Thus, from Corollary 3.1.8, $u \in Mon(\pm G)$. The other inclusion is always true. Take $u = (u_{i,j}) \in N(Mon(\pm G))$ with $u_{i,j} = \sum_{g\in G} u_{i,j}(g)g \in \mathbb{Z}G$. We have, by Theorem 3.1.12, that $uu^\diamond = (c_{i,j}) \in \mathcal{Z}(\mathcal{U}((\mathbb{Z}_0 S)^1)) = Scal(\pm\mathcal{Z}(G))$. For each i, $c_{i,i} = \sum_j u_{i,j}u^*_{i,j}$ is a trivial unit with $c_{i,i}(1) = \sum_j(\sum_{g\in G} u_{i,j}(g)^2) \neq 0$. It follows that, for each i, $c_{i,i} = 1$, i.e., $uu^\diamond = 1$, and thus $u \in Mon(\pm G)$ by Theorem 3.1.6. The other inclusion is obvious. □

Next, we prove a result for the double normalizer in semigroup rings, that was shown for group rings by Li in [18].

Theorem 3.1.15. *Let G be a finite group. Then $N(N(Mon(\pm G))) = N(Mon(\pm G))$.*

Proof. Take $v \in N(N(Mon(\pm G))$ and $a \in Mon(\pm G)$. Clearly, $Mon(\pm G) \subseteq N(Mon(\pm G))$. So, from Theorem 3.1.12, $v^{-1}av(v^{-1}av)^\diamond \in \mathcal{Z}(\mathcal{U}(\mathbb{Z}_0 S)^1)) \simeq Scal(\mathcal{Z}(\mathcal{U}(\mathbb{Z}G)))$. Since $u := v^{-1}av$ and $u^\diamond = (v^{-1}av)^\diamond$ are commuting torsion units, their product is also a torsion unit. Thus, by Lemma 3.1.7 we have that $c := uu^\diamond \in Scal(\pm\mathcal{Z}(G))$.

Now let $u = (u_{i,j})$, with $u_{i,j} = \sum_{g\in G} u_{i,j}(g)g \in \mathbb{Z}G$. For each i, $c_{i,i} = \sum_j u_{i,j}u^*_{i,j}$ is a trivial unit, with $c_{i,i}(1) = \sum_j(\sum_{g\in G} u_{i,j}(g)^2) \neq 0$. So, it follows that, for each i, $c_{i,i} = 1$, i.e., $uu^\diamond = 1$. Thus $a(vv^\diamond) = (vv^\diamond)a$, for $a^\diamond = a^{-1}$. From Lemma 3.1.11, this means that $vv^\diamond \in \mathcal{Z}(\mathcal{U}(\mathbb{Z}_0 S)))$. Hence, $v \in N(Mon(\pm G))$, as desired.

The other inclusion is obvious. □

Remark 3.1.16. The definitions of the hypercenter $\mathcal{Z}_\infty(G)$ and the finite conjugacy center $\Phi(G)$ of a group G are stated in Definition 1.1.31.

The hypercenter and the finite conjugacy center of the unit group of an integral group ring and of an integral semigroup ring have been given special attention in recent years.

It is a well known result that, if G is a finite group, then $\mathcal{Z}_\infty(\mathcal{U}_1(\mathbb{Z}G)) = \mathcal{Z}_2(\mathcal{U}_1(\mathbb{Z}G))$ (see [1]) and that $\mathcal{Z}_\infty(\mathcal{U}_1(\mathbb{Z}G)) \subseteq N_{\mathcal{U}_1(\mathbb{Z}G)}(G)$ (see [20] and [19]), where $\mathcal{U}_1(\mathbb{Z}G)$ stands for the *normalized units of* $\mathbb{Z}G$, i.e., the units in $\mathbb{Z}G$ having augmentation 1.

In Corollary 5.2 and 5.3 in [8], a description is given for the finite conjugacy center $\Phi(\mathcal{U}((\mathbb{Z}_0 S)^1))$ and second center $\mathcal{Z}_2(\mathcal{U}((\mathbb{Z}_0 S)^1))$ of the unit group

of an integral semigroup ring of a finite semigroup S such that $\mathbb{Q}S$ is semisimple. The result shows that both groups equal the hypercenter $\mathcal{Z}_\infty(\mathcal{U}((\mathbb{Z}_0S)^1))$ and are central if and only if S has no principal factors which are so called $\mathcal{Q}^*$-groups. A torsion group G is said to be a *$\mathcal{Q}^*$-group* if G has an abelian normal subgroup A of index 2 which has an element a of order 4 such that, for all $h \in A$ and all $g \in G \setminus A$, $g^2 = a^2$ and $g^{-1}hg = h^{-1}$; or, equivalently, $\mathcal{U}(\mathbb{Z}G)$ contains an abelian periodic normal subgroup $H \subseteq G$ such that $H \not\subseteq \mathcal{Z}(G)$ (see [2], [3]).

From the description of $N(\pm S)$ we gave, it follows that the finite conjugacy center $\Phi(\mathcal{U}((\mathbb{Z}_0S)^1))$ and the second center $\mathcal{Z}_2(\mathcal{U}((\mathbb{Z}_0S)^1))$ (hypercenter) are always contained in $N(\pm S)$, similarly to the group ring case, i.e.,

$$\mathcal{Z}_2(\mathcal{U}((\mathbb{Z}_0S)^1)) = \mathcal{Z}_\infty(\mathcal{U}((\mathbb{Z}_0S)^1)) = \Phi(\mathcal{U}((\mathbb{Z}_0S)^1)) \subseteq N(\pm S).$$

3.1.2 The Normalizer Problem for Semigroup Rings

The normalizer problem for group rings [36, Problem 43] asks whether

$$N_{\mathcal{U}(\mathbb{Z}G)}(\pm G) = \mathcal{Z}(\mathcal{U}(\mathbb{Z}G))(\pm G),$$

where G is a group. It has a positive answer for many classes of finite groups, among which finite nilpotent groups [36, Corollary 9.2]. One can now state this problem in the setting of semigroup rings: is it true that

$$N(\pm S) = \mathcal{Z}(\mathcal{U}((\mathbb{Z}_0S)^1))Mon(\pm G)?$$

In the case of a Malcev nilpotent semigroup S such that $\mathbb{Q}S$ is semisimple we have a positive answer to the analogous problem in semigroup rings. The only Malcev nilpotent completely 0-simple semigroups are the Brandt semigroups over a nilpotent group ([16, Lemma 2.1]). As observed before, we can assume that the principal series of S has only one Rees factor.

Theorem 3.1.17. *Let S be a finite Brandt semigroup over a finite nilpotent group G and let M denote the union of all maximal subgroups of S. Then*

$$N(\pm M^0) = Mon(\mathcal{Z}(\mathcal{U}(\mathbb{Z}G))(\pm G)) \text{ and } N(\pm S) = \mathcal{Z}(\mathcal{U}(\mathbb{Z}_0S)^1)Mon(\pm G).$$

Proof. From Theorem 3.1.4, (2), $N(\pm M^0) = Mon(N_{\mathcal{U}(\mathbb{Z}G)}(\pm G))$. Because S is Malcev nilpotent, we have that G is a finite nilpotent group (see Example 1.2.21). Thus, the normalizer problem for $\mathbb{Z}G$ has a positive answer and $N_{\mathcal{U}(\mathbb{Z}G)}(\pm G) = \mathcal{Z}(\mathcal{U}(\mathbb{Z}G))(\pm G)$. So,

$$N(\pm M^0) = Mon(N_{\mathcal{U}(\mathbb{Z}G)}(\pm G)) = Mon(\mathcal{Z}(\mathcal{U}(\mathbb{Z}G))(\pm G)).$$

Following the same lines, we get the result for $N(\pm S)$. □

In general, the normalizer problem does not hold for group rings, though the normalizer is known up to finite index [36, Proposition 9.5]. We get the same result in semigroup rings.

Proposition 3.1.18. *Let S be a finite Brandt semigroup, let M denote the union of all maximal subgroups of S, and let G be a maximal subgroup of S. If $u \in N(\pm M^0)$, then $u^2 \in Diag(\mathcal{Z}(\mathcal{U}(\mathbb{Z}G)))Mon(\pm G)$, and if $u \in N(\pm S)$, then $u^2 \in \mathcal{Z}(\mathcal{U}(\mathbb{Z}_0S)^1))Mon(\pm G)$.*

Proof. Take $u \in N(\pm M^0)$. Define $v := u^\diamond u^{-1}$, then $vv^\diamond = u^\diamond u^{-1}(u^{-1})^\diamond u = u^\diamond(u^\diamond u)^{-1}u$. From Corollary 3.1.5, we have $vv^\diamond = u^\diamond(uu^\diamond)^{-1}u = 1$. Hence by Theorem 3.1.6 we have that $v \in Mon(\pm G)$. So, $u^\diamond = vu$ and $uu^\diamond = u^\diamond u = vu^2 \in Diag(\mathcal{Z}(\mathcal{U}(\mathbb{Z}G)))$ by Theorem 3.1.4, (3).

The same reasoning gives the result for $u \in N(\pm S)$. □

Corollary 3.1.19. *Let S be a finite Brandt semigroup and G a maximal subgroup of S. Then*

$$\frac{N(\pm S)}{\mathcal{Z}((\mathcal{U}(\mathbb{Z}_0S)^1))Mon(\pm G)}$$

is an elementary abelian 2-group.

3.2 Free Groups generated by Bicyclic Units

By Hartley and Pickel [11], we know that there are free groups contained in the unit group of an integral semigroup ring. Marciniak and Sehgal [23] constructed a free group of rank 2 in the unit group of an integral group ring using a nontrivial bicyclic unit (Definition 1.1.28) and its image under the classical involution (Definition 1.1.3).

Since a Brandt semigroup S has the involution $\diamond$ (see Section 3.1 and Definition 1.2.11), we can investigate the same problem for a nontrivial bicyclic unit of $(\mathbb{Z}_0S)^1$.

Theorem 3.2.1. *Let S be a Brandt semigroup. Take $s \in S$ such that the cyclic semigroup $\langle s\rangle$ is a group of order n, and $t \in S$ such that $u_{s,t} = 1 + (1-s)t\widehat{s}$ is a nontrivial bicyclic unit in $(\mathbb{Z}_0S)^1$. Then:*

1. *if st is in a maximal subgroup G of S and if $\langle s\rangle$ is not normal in $\langle t\rangle$, then $\langle u_{s,t}, (u_{s,t})^\diamond\rangle$ is a free subgroup of $\mathcal{U}((\mathbb{Z}_0S)^1)$;*
2. *if $st = 0$ and $o(s) \geq 2$, then $\langle u_{s,t}, (u_{s,t})^\diamond\rangle$ is a free subgroup of $\mathcal{U}((\mathbb{Z}_0S)^1)$;*

3. if $st = 0$ and $o(s) = 1$, then $\langle u_{s,t}, (u_{s,t})^\diamond \rangle$ is not a free subgroup of $\mathcal{U}((\mathbb{Z}_0 S)^1)$.

Proof. Recall that, being a Brandt semigroup, we have that (see Theorem 1.2.14) $S \simeq \mathcal{M}^0(G, n, n, I_n)$ and $M^0 \simeq \{s = ge_{i,i} \in \mathcal{M}^0(G, n, n, I_n); g \in G, i = 1, \ldots, n\}$, where I_n is the $n \times n$ identity matrix and $e_{i,j}$ are matrix units (Example 1.2.2.1).

Since s generates a subgroup of order n in S, it is of the form $s = ge_{i,i}$, for $g \in G$, $i = 1, \ldots, n$. Notice that in order for $u_{s,t}$ to be nontrivial we must have $t = he_{j,i}$, for $h \in G$, $j = 1, \ldots, n$.

1. If st is in a maximal subgroup G of S, then we must have $j = i$. So $u_{s,t} = u_{g,h}e_{i,i}$ and, since $\langle s \rangle$ is not normal in $\langle t \rangle$ (i.e., $h \notin N_G(\langle g \rangle)$, $u_{s,t}$ is a nontrivial bicyclic unit in $(\mathbb{Z}_0 S)^1$ and $u_{g,h}$ is a nontrivial bicyclic unit in $\mathbb{Z}G$. So $(u_{s,t})^\diamond = u^*_{g,h}e_{i,i}$. Thus, Marciniak and Sehgal's main result in [23] gives us that $\langle u_{s,t}, (u_{s,t})^\diamond \rangle$ is a free subgroup of $\mathcal{U}((\mathbb{Z}_0 S)^1)$.

2. If $st = 0$, this means that $j \neq i$. Then $u_{s,t} = 1 + h\widehat{g}e_{j,i}$ and $(u_{s,t})^\diamond = 1 + \widehat{g}h^{-1}e_{i,j}$.

When $o(g) \geq 2$, consider the ring homomorphism

$$\phi : (\mathbb{Z}_0 S)^1 \longrightarrow M_n(\mathbb{Z}) \text{ given by } \alpha = (\alpha_{i,j}) \in (\mathbb{Z}_0 S)^1 \mapsto (\varepsilon(\alpha_{i,j})) \in M_n(\mathbb{Z}),$$

where ε is the augmentation mapping in $\mathbb{Z}G$. By Sanov's Theorem ([25, Theorem 10.1.3]) applied to the 2×2 nonzero submatrix of $\phi(u_{s,t})$ and $\phi(u_{s,t})^\diamond)$, we obtain the result.

3. Since $st = 0$, we have that $j \neq i$ and $u_{s,t} = 1 + h\widehat{g}e_{j,i}$, $(u_{s,t})^\diamond = 1 + \widehat{g}h^{-1}e_{i,j}$.

When $g = 1$, then $u_{s,t} = 1 + he_{j,i}$, $(u_{s,t})^\diamond = 1 + h^{-1}e_{i,j}$ and $((u_{s,t})^\diamond)^{-1} = 1 - h^{-1}e_{i,j}$. Thus, by performing elementary matrix computations, $u_{s,t}((u_{s,t})^\diamond)^{-1}$ is of order 6. Hence, $\langle u_{s,t}, (u_{s,t})^\diamond \rangle$ is not a free group. □

3.3 Some Questions for Further Investigation

So far, in this chapter, we have always considered semigroups for which the rational semigroup algebra is semisimple. It remains open what $N(\pm S)$ is in case there is a Jacobson radical (see Definition 1.1.4 and Theorem 1.1.10). The following example indicates that $N(\pm S)$ might always be central.

Example 3.3.1. Let G be a finite group. Define $S := \{Ge_{1,2}, Ge_{1,3}, G_{2,3}\}$, where $e_{i,j}$ are 3×3 matrix units (Example 1.2.2.1). Then $T := (S^0)^1$ is a

finite semigroup with zero element and identity and

$$\Gamma := (\mathbb{Z}_0 T)^1 = \mathbb{Z}_0 T = \left\{ \begin{pmatrix} z & \mathbb{Z}G & \mathbb{Z}G \\ 0 & z & \mathbb{Z}G \\ 0 & 0 & z \end{pmatrix} ; z \in \mathbb{Z} \right\}$$

is an integral semigroup ring, having Jacobson radical $\mathcal{J}(\Gamma) = \mathbb{Z}Ge_{1,2} + \mathbb{Z}Ge_{1,3} + \mathbb{Z}Ge_{2,3}$. Observe that $\mathcal{U}(\Gamma) = 1 + \mathcal{J}(\Gamma)$.

Let us now compute $N(\pm T)$. Take $u = \pm(\sum_{i=1}^{3} e_{i,i}) + te_{1,2} + ve_{1,3} + xe_{2,3}$, where $t, v, x \in \mathbb{Z}G$. In order to normalize $ge_{1,2}$, with $g \in \pm G$, it follows that $x = 0$. Note that u already normalizes $ge_{1,3}$, and that $ge_{2,3}$ is normalized by u if and only if $t = 0$.

Hence,

$$N(\pm T) = \{\pm(\sum_{i=1}^{3} e_{i,i}) + ve_{1,3}; v \in \mathbb{Z}G\} = \mathcal{Z}(\mathcal{U}(\Gamma)).$$

As it has been said in the beginning of this chapter, the study of the normalizer for semigroup rings, in analogy to what happens in group rings, might be elucidative in tackling the isomorphism problem. However, this connection still has to be made in the context of semigroup rings, and this is a natural direction for further studies on the subject.

It should also be interesting to investigate the usefulness of the results obtained to the isomorphism problem for partial group rings, for which it may be necessary to further explore the structure of the semigroup S_G associated to a given group G.

Bibliography

[1] Satya R. Arora, A. W. Hales and I. B. S. Passi, *Jordan Decomposition and Hypercentral Units in Integral Group Rings*, Commun. in Algebra 21 (1993), 25–35.

[2] A. A. Bovdi, *The Periodic Normal Divisors of the Multiplicative Group of a Group Ring I*, Sibirsk Mat. Z. 9 (1968), 495–498.

[3] A. A. Bovdi, *The Periodic Normal Divisors of the Multiplicative Group of a Group Ring II*, Sibirsk Mat. Z. 11 (1970), 492–511.

[4] A. H. Clifford and G. B. Preston, *The Algebraic Theory of Semigroups. Volume I*, Mathematical Surveys, no. 7, American Mathematical Society, Providence, R.I., 1961.

[5] E. C. Dade, *Deux Groupes Finis Distincts ayant la même Algèbre de Groupe sur tout Corps*, Math. Z. 119 (1971), 345–348.

[6] M. A. Dokuchaev, R. Exel and P. Piccione, *Partial Representations and Partial Group Algebras*, Journal of Algebra 226 (2000) 505–532.

[7] M. A. Dokuchaev and C. Polcino Milies, *Isomorphisms of Partial Group Rings*, Glasgow Math. J. 46 (2004), 161–168.

[8] A. Dooms, E. Jespers and S. O. Juriaans, *Units in Orders and Integral Semigroup Rings*, J. Algebra 265 (2003), No. 2, 675–689.

[9] A. Dooms and P. M. Veloso, *The Normalizer of a Semigroup and Free Groups in the Unit Group of an Integral Semigroup Ring*, Journal of Algebra and Applications (submitted)

[10] R. Exel, *Partial Actions of Groups and Actions of Inverse Semigroups*, Proc. Amer. Math. Soc. 126 (1998), No. 12, 3481–3494.

[11] B. Hartley and P. F. Pickel, *Free Groups in Unit Groups of Integral Group Rings*, Canad. J. Math. 32 (1980), 1342–1352.

[12] M. Hertweck, *A Counterexample to the Isomorphism Problem for Integral Group Rings*, Ann. of Math., 154 (2001), No. 1, 115–138.

[13] G. Higman, *Units in Group Rings*, D.Ph. Thesis, University of Oxford, Oxford, 1940.

[14] E. Jespers, G. Leal and A. Paques, *Idempotents in Rational Abelian Group Algebras*, Journal of Algebra and Its Applications, Vol. 2, No. 1 (2003), 57–62.

[15] E. Jespers and S. O. Juriaans, *Isomorphisms of Integral Group Rings of Infinite Groups*, J. Algebra 223 (2000), No. 1, 171–189.

[16] E. Jespers and J. Okniński, *Nilpotent Semigroups and Semigroup Algebras*, J. Algebra 169 (1994), No. 3, 984–1011.

[17] T. Y. Lam, *A First Course in Noncommutative Rings*, Springer-Verlag New York (2001).

[18] Y. Li, *On the Normalizers of the Unitary Subgroup in an Integral Group Ring*, Communications in Algebra 25 (1997), No. 10, 3267-3282.

[19] Y. Li and M.M. Parmenter, *Hypercentral Units n Integral Group Rings*, Proc. Amer. Math. Soc. 129 (2001), No. 8, 2235–2238.

[20] Y. Li, M. M. Parmenter and S. K. Sehgal, *On the Normalizer Property for Integral Group Rings*, Commun. in Algebra 27 (1999), 4217–4223.

[21] A. I. Malcev, *Nilpotent Semigroups*, Uc. Zap. Ivanovsk. Ped. Inst. 4 (1953), 107–111(in Russian).

[22] Z. S. Marciniak and K. W. Roggenkamp, *The Normalizer of a Finite Group in its Integral Group Ring and Čech Cohomology*, Algebra—representation theory (Constanta, 2000), 159–188, NATO Sci. Ser. II Math. Phys. Chem., 28, Kluwer Acad. Publ., Dordrecht (2001).

[23] Z. S. Marciniak and S. K. Sehgal, *Constructing Free Subgroups of Integral Group Ring Units*, Proc. Amer. Math. Soc. 125 (1997), No. 4, 1005–1009

[24] M. Mazur, *The Normalizer of a Group in the Unit Group of its Group Ring*, J. Algebra 212 (1999), No. 1, 175–189.

[25] C. P. Milies and S. K. Sehgal, *An Introduction to Group Rings*, Kluwer Academic Publishers, 2002.

[26] B. H. Neumann and Tekla Taylor, *Subsemigroups of Nilpotent Groups*, Proc. Roy. Soc, Ser. A 274 (1963), 1–4.

[27] A. Olivieri and Á del Río, *wedderga. A GAP 4 Package for Computing Central Idempotents and Simple Components of Rational Group Algebras* (2003)

[28] A. Olivieri and Á del Río, *An Algorithm to Compute the Primitive Central Idempotents and the Wedderburn Decomposition of Rational Group Algebras*, J. Symbolic Comput., 35(6) (2003), 673–687.

[29] A. Olivieri, Á del Río and J. J. Simón, *On Monomial Characters and Central Idempotents of Rational Group Algebras*, Comm. Algebra, Vol. 32, No. 4 (2004), 1531–1550.

[30] J. Okniński, *Semigroup Algebras*, Marcel Dekker, 1991.

[31] J. Okniński, *Nilpotent Semigroup Of Matrices*, Math. Proc. Camb. Phil. Soc. 120 (1996), No. 4, 617–630.

[32] S. Perlis and G. Walker, *Abelian Group Algebras of Finite Order*, Trans. Amer. Math. Soc. 68 (1950), 420–426.

[33] L. Quoos and P. M. Veloso, *The Primitive Central Idempotents of Abelian Group Algebras and of Complex Nilpotent Algebras*, Proceedings of the Edinburgh Mathematical Society (submitted)

[34] D. J. S. Robinson, *A Course in the Theory of Groups*, Springer-Verlag, New York, 1982.

[35] L. Rowen, *Ring Theory. Volume I*, Academic Press, London, 1988.

[36] S. K. Sehgal, *Units in Integral Group Rings*, Longman Scientific & Technical Press, Harlow, 1993.

[37] H. Stichtenoth, *Algebraic function fields and codes*, Springer-Verlag New York, 1993.

Index