The Austraian National University

Group Representations, Nilpotent Algebras and Finite Algebra Groups

Maximillian K. Wakefield

A THESIS

in

Mathematics

Presented to the Faculties of the Australian National University in Algebra for the Degree of Masters of Mathematical Sciences

2018

Supervisor of Thesis

Masters Covenor

Dedicated to Lindsay and Sabina.

Abstract

The purpose of this thesis is introduce the reader to representations of finite algebra groups and summarise some key results concerning such representations.

The work that follows begins by reviewing key properties of finite group representations and nilpotent algebras. The representations studied are for the most part complex representations, however much of the theory applies equally to many other Fields. We follow this discussion with an introduction to finite algebra groups by exploring the relationship that exists between these groups and the Jacobson Radical of algebras over finite fields.

Then we consider the work of Zoltan Halasi in significant detail and attempt to clarify some of the ambiguites a reader may face in reading his paper. In addition, we prove and state many of the excluded facts and results on which his arguments rely.

Finally, we conclude by analysing the irreducible representations of a specific class of finite algebra groups. This is our working example. In doing so, we highlight how the work of Halasi simplifies the search for irreducible representations. We end the final section by introducing a non-finite algebra group that shares many similarities to the class of groups considered in our working example. Determining whether or not an analagous theorem to the one proved by Halasi holds for these groups is an open problem. It is the belief of the author that a person who is interested in exploring the irreducible representations of such groups may find this thesis a solid introduction.

Contents

1 Introduction

In Algebra, to perform good mathematics one must often work from the ground up. To appreciate the work of Halasi and to consider representations of finite algebra groups (both to be defined later) is no different. The introduction chapter summarises the general topics that the author researched and studied in completing this Thesis. At the commencement of the project most of the studied topics were relatively foreign to the author and thus he has considered it of great importance to outline many of the results and definitions on which understanding the work of Halasi relies. In addition, since the work of Halasi sits in the crossfire of Group Theory, Representation Theory and Nilpotent Ring Theory, the required background knowledge is relatively vast for such a concise paper and justifies the lengthy introduction. A mature, or adult mathematician (in the words of Alex Isaev) will be able to skip most of the introduction and simply use it as a reference where required. A final aim of the introduction chapter is to ensure the thesis is as self-contained as possible.

For the most part, the author has written this thesis as if he were writing to a student (perhaps himself) attempting to learn this interesting and challenging area of mathematics.

Finally, the author takes great pleasure in thanking his supervisor Uri Onn for introducing him to many new topics in algebra and for providing patient and persistent guidance and feedback. Thanks must also be given to the following people for teaching the author mathematics at the Australian National University and inspiring him to take on greater challenges in the field. In some but no particular order they are : Idione Meneghal, John Stachurski, Joan Licata, Alex Isaev, James Borger, David Smyth, John Urbas, Michael Barnsley, Timothy Trudgian and Bryan Wang.

1.1 An introduction to Representation Theory

We now give a brief summary of the established results regarding the beautiful interplay between characters, representations and group theory that will be relied on in this text.

Definition 1.1. *Let F be a field, V a vector space over F and G a group. Then an F-representation (or simply representation) of G is a group homomorphism $\rho : G \to GL(V)$. If n is the dimension of V as vector space over F, then n is also the dimension, or degree, of the representation.*

From here on we will only consider finite-dimensional vector spaces V and finite groups. If V is vector space of dimension n, choosing a basis $\mathbf{B}$ gives an isomorphism from $GL(V)$ to $GL_n(F)$. It is then common to identify ρ with a group homomorphism, or matrix representation, $R : G \to GL_n(F)$, by the rule

$$\rho_g \rightsquigarrow \text{its matrix} = R_g.$$

Since the image of an elememt $g \in G$ under ρ is an invertible linear operator, denoted by ρ_g, such a homomorphism explicitly requires that

$$\rho_{gh}(v) = \rho_g(\rho_h(v)),$$

for all $g, h \in G$ and $v \in V$. In matrix notation,

$$R_{gh} = R_g R_h.$$

If ρ and ρ' are two representations of a group G in V and V' respectively, then $\rho \approx \rho'$ (isomorphic) if there exists an isomorphism of vector spaces $T : V \to V'$, such that

$$T(\rho_g(v)) = \rho'_g(T(v))$$

for all $g \in G, v \in V$. The compatibility with the operations of G leads T to be referred to as a G-isomorphism. Note that the condition of T being a G-isomorphism can be reconsidered as requiring that

$$\rho_g(v) = T^{-1}(\rho'_g(T(v))),$$

for all $g \in G$ and all $v \in V$. When ρ and ρ' correspond to matrix representations R and R' respectively, then $\rho \approx \rho'$, or equivalently, $R \approx R'$, if there exists an invertible matrix P such that

$$R_g = P^{-1} R'_g P$$

for all $g \in G$.

An equivalent and at times appealing way to think of a representation of a group G on a vector space V is by viewing G as acting by linear operators on the underlying set V. That is, a representation is a map $G \times V \to V$ that satisfies the follwoing axioms of a group action (sometimes refrerred to as group operation) by linear operator:

1. $(1, v) = v$ for all $v \in V$, where 1 is the identity in G.
2. $(gg', v) = (g, (g'v))$ for all $g.g' \in G$ and $v \in V$.
3. $(g, (v + v')) = (g, v) + (g, v')$ for all $g \in G$ and $v, v' \in V$.
4. $(g, (cv)) = c(g, v)$ for all $g \in G, v \in V$ and $c \in F$, where F is the scalar field.

It is a pedantic exercise to see that operation by linear operators on the vector spave V is equivalent to a representation on V. If G is a group and S is a set, any map $G \times S \to S$ that satisfies the first two conditions in the above list is a group action. Throughout this thesis we will employ group actions in multiple settings (e.g. the induced representation covered in section 1.2).

To simplify our efforts, when discussing representations of finite groups G in this paper, we will be referring to group homomorphisms

$$\rho : G \to GL_n(\mathbb{C}).$$

As a result, from here on all representations are $\mathbb{C}$-representations.

Definition 1.2. *Let ρ be a representation of G. Then the character χ associated with ρ is the $\mathbb{C}$ valued function whose domain is the group G, defined by*

$$\chi(g) = \text{trace } \rho_g.$$

In general the character of a representation is not a homomorphism - for instance $\chi(1) = 1$ if and only if the representation is one-dimensional. When $\chi : G \to \mathbb{C}\backslash\{0\}$ is a group homomorphism, we say that χ is a linear character.

Lemma 1.3. *Let χ be the character of a representation ρ of a finite group G.*

1. *Isomorphic representations have the same character.*
2. *Characters are constant on conjugacy classes.*

Proof. 1) When P is an invertible matrix and A is a $n \times n$ matrix, then $\text{trace}(PAP^{-1}) = \text{trace}(A)$. Conjugate matrices have the same trace.

2) If g and g' are conjugate, then there exists $h \in G$ such that $g' = hgh^{-1}$. Then since R is a homomorphism, $R_{g'} = R_h R_g R_h^{-1}$. That is, $R_{g'}$ and R_g are conjugate matrices. The result follows. □

We have the following properties of characters, the third of which was just discussed:

Proposition 1.4. *If χ is the character of a representation ρ of degree n, then:*

(a) $\chi(1) = n$,

(b) $\chi(g^{-1}) = \overline{\chi(g)}$,

(c) $\chi(hgh^{-1}) = \chi(g)$.

where $\bar{z}$ denotes the complex conjugate.

The **group algebra** $\mathbb{C}[G]$ is the set of all formal linear combinations

$$\alpha = \sum_{x \in G} a_x x,$$

with $a_x \in \mathbb{C}$. Addition is then given by the rule

$$\sum_{x \in G} a_x x + \sum_{x \in G} b_x x = \sum_{x \in G} (a_x + b_x) x.$$

Multiplication is then given by the convolution product

$$\left(\sum_{x \in G} a_x x \right) \left(\sum_{x \in G} b_x x \right) = \sum_{z \in G} \left(\sum_{xy = z} a_x b_y \right) z.$$

As a ring, $\mathbb{C}[G]$ is commutative if and only if G is commutative. We also observe that as an algebra over $\mathbb{C}$, the elements of G form a basis.

Now suppose that V is a $\mathbb{C}$-vector space and $\rho : G \to GL(V)$ a representation of G. Given an element $g \in G$ and $v \in V$, by setting

$$gv = \rho_g(v),$$

and extending linearly, V becomes a "left" $\mathbb{C}[G]$ module. Conversely, every algebra-homorphism

$$\mathbb{C}[G] \to \mathrm{End}_{\mathbb{C}}(V)$$

induces a group-homomorphism

$$G \to GL(V).$$

Thus the theory of representations is often intertwined with the theory of modules. Many texts do not discriminate between the terminology "linear representation" and "module". We will for the most part refer to representations, however the alternative module approach is very useful in the application of Wedderburn and Maschke's theorem.

In addition, we encourage all readers to consider proving key theorems concerning representations by analysing the action of the group algebra $\mathbb{C}[G]$ on left-modules. An obvious example is when we encounter the Regular representation (see Artin [2].) The Regular representation corresponds to treating $\mathbb{C}[G]$ as a left-module over itself and is perhaps the most important representation of a group that one encounters in representation theory.

If $\rho : G \to GL(V)$ is a representation and W a vector subspace of V such that $\rho_g(w) \in W$ for all $g \in G$ and $w \in W$, then W is G-invariant. Since ρ_g is an invertible map and W is a finite-dimensional subspace, this is equivalent to stating that $\rho_g W = W$ for all $g \in G$. By restricting ρ to W, we obtain a subrepresentation of V, namely

$$\rho_W : G \to GL(W).$$

In the language of modules, this corresponds to W being a sub-$\mathbb{C}[G]$-module of V. When V is the direct sum of G-invariant subspaces, say $V = W_1 \bigoplus W_2$, we say that ρ is the direct sum of its restriction to W_1 and W_2 and we identify this by writing

$$\rho = \rho_1 \oplus \rho_2,$$

where ρ_1 and ρ_2 are the restrictions of ρ to W_1 and W_2, respectively.

Definition 1.5. *Let $\rho : G \to GL(V)$ be a representation. Then ρ (or for convenience V) is irreducible if V has no proper G-invariant subspace. If V has a proper G-invariant subspace, then ρ (or V) is reducible.*

In module terminology, an irreducible representation V is a simple $\mathbb{C}[G]$-module.

Theorem 1.6 (Schur's Lemma)**.** *Let A be a ring and V and W simple A-modules. If $\phi : V \to W$ is a non-zero module homomorphism, then ϕ is an isomorphism.*

Proof. The kernal and image of a module homomorphism are sub-modules. The result follows. □

Corollary 1.1. *Let ρ and ρ' be irreducible representations on V and V' respectively. If $T : V \to V'$ is a non-zero G-invariant, $\mathbb{C}$-homomorphism, i.e. $T(\rho_g) = \rho'_g(T)$ for all $g \in G$, then $\rho \approx \rho'$.*

Proof. We note that by extending the action of G linearly, V and V' are simple $\mathbb{C}[G]$-modules. Since T is a homomorphism of $\mathbb{C}$-vector spaces that is G-invariant, it is a $\mathbb{C}[G]$-module homomorphism. By Schur's lemma it is an isomorphism. □

The next two theorems are powerful foundational results in Algebra. For this reason we state them without limiting the base field to the complex numbers.

Theorem 1.7 (Maschke's Theorem)**.** *Every representation of a finite group G over a field F with characteristic not dividing $|G|$ is a direct sum of irreducible representations.*

For a representation theoretic proof of this theorem one can review the text by Artin [2]. Alternatively, one can find a proof in Lang [3] that the group algebra $F[G]$ is semi-simple, i.e., every $F[G]$-module E is the direct sum of simple submodules.

Theorem 1.8 (Wedderburn)**.** *Let G be a finite group and F a field such that the characteristic of F does not divide $|G|$. Up to isomorphism, there are finitely many simple $F[G]$- modules.*

A proof of this result can be found in almost any graduate text on algebra. From here on we now assume that V is a vector space over $\mathbb{C}$ unless otherwise specified.

Theorem 1.9 (Wedderburn)**.** *Let $\rho_i : G \to GL_{n_i}(V_i)$, $1 \leq i \leq h$, be the distinct irreducible representations of G where $n_i = \dim V_i$. Then the algebra $\mathbb{C}[G]$ is a product of matrix algebras $M_{n_i}(\mathbb{C})$. That is*

$$\mathbb{C}[G] \approx \prod_{i=1}^{h} M_{n_i}(\mathbb{C}).$$

Proof. See Serre [4]. □

An immediate consequence of these results is the first two parts of the following corollary. The third item is proved in Artin [2] using facts about characters which we discuss next.

Corollary 1.2. *Let G be a finite group.*

1. *There are finitely many isomorphism classes of irreducible representations.*
2. *Let $\rho_1, ..., \rho_h$ represent the isomorphism classes of irreducible represntations of G, and let $\chi_1, ..., \chi_h$ be the characters they afford. The dimension d_i of ρ_i (or of χ_i) divides the order of G and $|G| = d_1^2 + ... + d_h^2$.*
3. *The number of irreducible represntations is the same number as the number of conjugacy classes in the group.*

A useful consequence of this result is the following theorem.

Theorem 1.10. *Let G be a finite abelian group.*

1. *Every irreducible character of G is one-dimensional. The number of irreducible characters is equal to the order of the group.*

2. *Every matrix representation R of G is diagonalizable. That is, every matrix R_g is similar (conjugate) to a diagonal matrix.*

For each irreducible representation ρ we likewise have an *irreducible* character χ. Let $\mathrm{Irr}(G)$ denote the set of irreducible characters of a finite group G.

Any function from a group G into $\mathbb{C}$ that is constant on conjugacy classes is called a **class function.** It follows from lemma 1.3 that characters are class functions. The set of complex-valued class functions is a complex vector space, which we denote as $\mathcal{C}$. It is turned into a Hermitian space by the form

$$\langle \varphi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \varphi(g)\overline{\psi(g)}. \tag{1.1}$$

We confirm it is a Hermitian form $\mathcal{C} \times \mathcal{C} \to \mathbb{C}$. To do so obeserve that viewing each $\chi \in \mathcal{C}$ as vectors, we have

$$\chi = \big(\chi(g_1), ..., \chi(g_n)\big)_{g_i \in G},$$

where $n = |G|$. Then 1.1 is simply the standard form on $\mathbb{C}^n$ scaled by a factor. It is thus a Hermitian form.

Some of the key results one learns in their early studies of representation theory are the following theorems. We present the theorems when $F = \mathbb{C}$, however many of the results can be extended to other fields.

Theorem 1.11 (Orthogonality Relations)**.** *The irreducible characters of G form an orthonormal basis of the space $\mathcal{C}$. If χ_i is the character of an irreducible representation ρ_i, then $\langle \chi_i, \chi_i \rangle = 1$. If χ_i and χ_j are the characters of non-isomorphic irreducible representations ρ_i and ρ_j, then $\langle \chi_i, \chi_j \rangle = 0$.*

Theorem 1.12. *Every complex-valued class function φ on a group G can be uniquely expressed in the form*

$$\varphi = \sum_{\chi \in Irr(G)} a_\chi \chi,$$

where $a_\chi \in \mathbb{C}$.

1.2 Induced Representations.

Let H be a subgroup of a finite group G. Suppose for some vector space W over $\mathbb{C}$ we have a representation

$$\sigma : H \to GL(W).$$

For simplicity, let $\sigma_h(w) = hw$. Where $[G : H] = n$, let $\Lambda = \{\lambda_1, ..., \lambda_n\}$ be a system of representatives of the left cosets of H in G, i.e. each $g \in G$ can be wriiten uniquely as $\lambda_i h$ for some $\lambda_i \in \Lambda, h \in H$. Denote the set of cosets of H in G by G/H. The Group Action

$$G \times G/H \to G/H$$

given by the rule

$$(g, \lambda_1 H) \rightsquigarrow (g\lambda_1)H = \lambda_j H \quad \text{for some } 1 \leq j \leq n,$$

is a well defined group action - a permutation of the cosets G/H - with the following elementary properties.

1. The Operation of G on G/H is transitive.
2. The stabilizer of the coset H is the subgroup H.

Returning our focus to vector spaces, for each λ_i we have a vector space $\lambda_i W$ over $\mathbb{C}$ if we identify scalar multiplication $\mathbb{C} \times \lambda_i W \to \lambda_i W$ by the rule

$$(c, \lambda_i w) \rightsquigarrow \lambda_i(cw).$$

It is easy to see that $\lambda_i W \approx W$ as $\mathbb{C}$-vector spaces. Let

$$V = \bigoplus_{i=1}^{n} \lambda_i W.$$

If $\lambda_i w \in \lambda_i W$, then multiplication by an element $g \in G$ can be defined in a very natural way. Since $g\lambda_i = \lambda_j h$ for some $1 \leq j \leq n$ and $h \in H$, let $g(\lambda_i w) = \lambda_j(hw) = \lambda_j \tilde{w}$ since $hW = W$. We extend using linearity and have G act on the vector space V as follows

$$g \sum_{i=1}^{n} \lambda_i w_i = \sum_{i=1}^{n} (g\lambda_i) w_i = \sum_{\substack{i=1 \\ g\lambda_i = \lambda_j h_j}}^{n} \lambda_j(h_j w_i).$$

This defines the induced representation

$$\rho_H^G : G \to GL(V).$$

We turn this into a formal definition for referencing purposes.

Definition 1.13. *Let $\rho : G \to GL(V)$ and $\sigma : H \to GL(W)$ be representations where G acts on V as decsribed above. Then the representation ρ is induced by the representation σ.*

Observe that

$$\dim(V) = n \dim(W) = [G : H] \dim(W). \tag{1.2}$$

It is common to write ρ as σ_H^G, or simply σ^G when H is clear.

Theorem 1.14 (Characters of induced representations)**.** *If $\rho : G \to GL(V)$ is induced from $\sigma : H \to GL(W)$ and χ_ρ and χ_σ are the corresponding characters, then for each $g \in G$*

$$\chi_\rho(g) = \sum_{\substack{\lambda \in \Lambda \\ \lambda^{-1} g \lambda \in H}} \chi_\sigma(\lambda^{-1} g \lambda) = \frac{1}{|H|} \sum_{\substack{s \in G \\ s^{-1} g s \in H}} \chi_\sigma(s^{-1} g s).$$

Proof. We aim to compute $\chi_\rho(g) = \mathrm{trace}_V(\rho_g)$. For a basis for V, we consider a union of bases of $\rho_{\lambda_i} W$. Clearly the only non-zero diagonal terms of ρ_g will correspond to the subspaces $\rho_{\lambda_i} W$ such that $\rho_g \rho_{\lambda_i} W = \rho_{g\lambda_i} W = \rho_{\lambda_i} W$. This implies that $g\lambda_i = \lambda_i h$ for some $h \in H$. The first formula follows from this.

The second formula follows from two observations. Firstly, suppose that for $s \in G$ we have $sH = \lambda_i H$. Then $g\lambda_i H = \lambda_i H$ implies $s^{-1} g s H = H$. Secondly, since $s = \lambda_i h$ for some $h \in H$ and applying the fact that characters are constant on conjugacy classes, we have

$$\chi_\sigma(s^{-1} g s) = \chi_\sigma((h^{-1}\lambda_i^{-1}) g (\lambda_i h)) = \chi_\sigma(h^{-1}(\lambda_i^{-1} g \lambda_i) h) = \chi_\sigma(\lambda_i^{-1} g \lambda_i).$$

□

The character of the induced representation is called the induced character. If $\rho = \sigma^G$ and χ_σ is the character of σ, then we often write the induced character as χ_H^G, or simply χ_σ^G.

We conclude our brief introduction to representation theory with the following fact that induction is transitive.

Fact 1.15. *Suppose that $H \leq G \leq K$ are groups. Then:*

$$(\sigma_H^G)_G^K = \sigma_H^K.$$

1.3 Nilpotent Algebras.

Much of this thesis will be focused on the study of algebras A over finite fields $\mathbb{F}_q$. We recall that an algebra A over a field F is a F-vector space equipped with an F- bilinear product $A \times A \to A$. In many areas of mathematics, we consider an algebra over a field F to be a ring A together with a ring homomorphism

$$\varphi : F \to Z(A),$$

where $Z(A)$ is the center of A. Then scalar multiplication $F \times A \to A$ is given by the rule

$$(f, a) \rightsquigarrow \varphi(f)a.$$

For our purposes this latter description of an algebra is quite limiting as we now see.

Definition 1.16. *An associative algebra A over a field F is said to be a* ***nilpotent algebra*** *if there exists a positive integer n such that $A^n = 0$. The nilpotency class of A is the smallest natural number k such that $A^k = 0$.*

Fact 1.17. *A non-zero nilpotent algebra A over a field F with nilpotency class k does not have a multiplicative identity.*

Proof. Per absurdum, suppose A has a multiplicative identity which we denote as 1. Then $0 = 1^k = (1^{k-1})1 = 1^{k-1} = ... = 1$. Hence $1 = 0$ and A is the zero vector space. Contradiction. □

Thus the "ring-homomorphism" definition of an algebra over a field F is limiting because it clashes with the definition of a nilpotent algebra, because there is no way to map the multilplicative identity of F into A. Thus all we require is A to be an F-vector space with an F-bilinear map.

Example 1.1. *A simple example of a nilpotent algebra over $\mathbb{Q}$ is the algebra E of strictly upper triangular matrices in $M_4(\mathbb{Q})$ with equal elements next to the main diagonal.*

$$E = \begin{bmatrix} 0 & a & * & * \\ 0 & 0 & a & * \\ 0 & 0 & 0 & a \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Importantly, we note that since E is nilpotent, and thus contains no multiplicative identity, we cannot identify the algebra structure of E over $\mathbb{Q}$ via an injective ring homomorphism. Instead we consider the action of $\mathbb{Q}$ on E to be "inherited" from the

algebra $M_4(\mathbb{Q})$. Whenever it is clear that the nilpotent algebra we are working with is a sub-algebra of a larger unital algebra, then it will be assumed that the scalar multiplication is "inherited." An important example of this is when we work with the Jacobson Radical of a finite dimensional algebra over a field.

Definition 1.18. *Let A be a finite dimensional algebra over a field F. The **Jacobson Radical** of A is the ideal $J(A) = J$ which is the intersection of all maximal ideals of A.*

Theorem 1.19. *The Jacobson radical of a finite dimensional algebra A over a field F is a nilpotent algebra over F.*

Before proving this theorem we state and prove some propositions. All of these propositions can be found as exercises in Lang [3]. Unless stated otherwise, all ideals are left ideals and the ring A is not assumed to be commutative.

Proposition 1.20. *Let A be a unital ring. There exists a bijection between maximal (left) ideals of A and simple A modules (up to isomorphism).*

Proof. The bijection is given by the rule

$$M \in \{\text{set of maximal ideals of } A\} \longleftrightarrow A/M.$$

Suppose M is a maximal ideal of A. Then A/M is a A-module. By the Correspondence Theorem for A-modules, A/M is simple. Conversely, let E be a simple A-module. Then by definition, E is not the zero module. Choose $x \in E$ such that $x \neq 0$. Then $f : A \to E$ given by the rule $a \rightsquigarrow ax$ is module homomorphism, with non-trivial image. Since the image of a module homomorphism is a sub-module, f is surjective with kernal M. By the Isomorphism Theorem for modules, $A/M \approx E$. By the correspondence theorem, M must be maximal. □

Proposition 1.21. *For every simple A-module E we have $JE = 0$, where $J = J(A)$.*

Proof. Choose $x \in E$ such that $x \neq 0$. Then $a \rightsquigarrow ax$ is a surjective module homomorphism with kernal M. By 1.15 we know that M is maximal. Clearly J being the intersection of all maximal ideals implies that $J \subset M$. Hence $Jx = 0$. Since x was an arbitrary non-zero element of E, the result follows. □

Proposition 1.22. *The Jacobson radical of (A/J) is 0.*

Proof. We know that A/J is a ring. Let $\pi : A \twoheadrightarrow A/J$ be the canonical ring-homomorphism. Suppose M' is a maximal ideal in A/J. By the correspondence theorem $\pi^{-1}(M')$ is a maximal ideal in A that contains J. Hence maximal ideals in A/J correspond to maximal ideals in A that contain J. Let $J' = J(A/J)$. If $J' \neq 0$, then there exists $x \notin J$ such that $\pi(x) \in J'$. But then x is in all maximal ideals that contain J. Since every maximal ideal of A has J as a subset, x is in all maximal ideals. Hence x is in J. Contradiction. □

Proposition 1.23. *The Jacobson radical is a two-sided ideal.*

Proof. Let $\bigoplus_i E_i$ be the direct sum of all simple A-modules E_i. Then we have the obvious ring homomorphism

$$A \to \mathrm{End}_{\mathbb{Z}} \bigoplus_i E_i$$

given by $a \rightsquigarrow \bigoplus aE_i$. By 1.15 the Jacobson radical is the kernal of this map, which is a two-sided ideal by the definition of a module. □

Theorem 1.24 (Nakayama's Lemma)**.** *Let A be any ring and E a finitely generated A-module. Let $J = J(A)$. If $JE = E$ then $E = 0$.*

Proof. We prove the theorem when A is a local ring with unique maximal ideal M. Supose E is finitely generated by $(e_1, ..., e_n)$. Since $JE = E$, we see that there exists $j_1, ..., j_n \in M$ such that

$$j_1 e_1 + ... + j_n e_n = e_n.$$

Hence $(1 - j_n)e_n = j_1 e_1 + ... + j_{n-1} e_{n-1}$. Since $j_n \in M$, we must have $(1 - j_n)$ as a unit. If it was not a unit, then it would be contained in a maximal ideal. Since A is local it would be contained in M. But then $1 \in M$, which is absurd. Thus e_n is contained in the module generated by the $n - 1$ generators. Applying induction shows that the generating set must be empty. □

The general case is more complex and we omit it.
In the preceding proof we actually touch on a more general description of the Jacobson Radical.

Proposition 1.25. *Let J be the Jacobson Radical of a ring A. Then $x \in J$ if and only if for all $a, b \in A$, $1 + axb$ is a unit.*

Proof. We choose to work with left ideals. Suppose $x \in J$ and for contradiction suppose $1 + axb$ is not a unit. Then the principal ideal $A(1 + axb)$ is contained in some maximal ideal M. Since J is two-sided, $xb \in J$ and thus $xb \in M$. Hence $-axb \in M$. This would imply that $1 \in M$, which is our contradiction. Conversely, suppose that for all $a, b \in A$ we have that $1 + axb$ is a unit. For contradiction, suppose that $x \notin J$. Then there exists a maximal ideal M' such that $x \notin M'$. Then $M \cup Ax = A$. Hence there exists $m \in M, y \in A$ such that $m - yx = 1$. Hence $1 + yx \in M$ and thus not a unit. Contradiction. □

Proposition 1.26. *The Jacobson radical J contains all Nilpotent ideals of a ring A.*

Proof. Let N be a (left) nilpotent ideal of class n. Suppose $x \in N$. Then for any $a \in A$, we have $ax \in N$. Then

$$(1+ax)(1-(ax)+(ax)^2-(ax)^3+....\pm(ax)^{n-1}) = 1.$$

By 1.25, $x \in J$. □

Before we prove theorem 1.19 we still need another definition.

Definition 1.27. *A Ring A is **Artinian** if every descending sequence of left ideals $J_1 \supset J_2...$ with $J_i \neq J_{i+1}$ is finite.*

With this definition and the following lemma we prove 1.14. We won't prove the lemma.

Lemma 1.28. *A finite dimensional algebra A over a field F is Artinian.*

Proof of Theorem 1.19. Let $J(A) = J$ be the Jacobson radical of A. We immediately have a descending sequence $J \supset J^2... \supset J^m$, which stabilizes for some integer m because A is artinian. Suppose for contradiction that $J^m \neq 0$. Consider the set of left ideals $\{\mathcal{K}\}$ such that $K \subset J^m$ and $J^m K \neq 0$ for all $K \in \mathcal{K}$. This set is non-empty because $J^m \in \mathcal{K}$. Because A is artinian, there exists a minimal principal ideal $X \in \mathcal{K}$. Choose some $x \in X$ such that $J^m x \neq 0$. Since $J^m x$ is an ideal and $J^m x \subset Ax$, by X being minimal, we have $X = J^m x$. Then $JX = JJ^m X = J^m X = X$. By Nakayama's lemma, $X = 0$, which is absurd. Thus our original assumption that $J^m \neq 0$ must be false.

□

At times, it will be convenient to consider a nilpotent algebra N over a field F without reference to a unital algebra A containing N. In this case, if necessary, we will be clear in describing the action of F on N.

1.4 Free Algebras

Let R be a commutative ring and $X = \{X_1, ..., X_n\}$ be a set of variables. Let $R[X]$ be the free R-module with basis consisting of all possible words in the alphabet X. $R[X]$ can naturally be made into an R-algebra by defining multiplication as R-billinear concantenation. The R-algebra arising from these operations is **free algebra** over R generated by the set X. We denote it as $F_R(X)$.

The free algebra $F_R(X)$ is well described on wikipedia [15] as the non-commutative analogue of the polynomial ring over R in X.

For any algebra A we define A^n to be the set of all sums

$$x_1 \cdots x_n + ... + y_1 \cdots y_n$$

where $x_i, y_i \in A$. It is an ideal of A. We then define $F_R(n, X)$, the **free nilpotet algebra** over R with nilpotency class n, to be

$$F_R(X)/F_R(X)^n.$$

A frequentely used and easy fact (that seems to at times confuse people) is that for any algebra A and any integer n, $A^n \subset A^k$ for all $1 \leq k \leq n$.

1.5 Algebra Groups

For much of this paper we study algebras over finite fields. For clarity, for some prime p, the field $\mathbb{F}_q$ is the finite field of $q = p^f$ elements where $f \geq 1$. The order of 1 in $\mathbb{F}_q$, which is referred to as the *characteristic* of the field, is clearly p.

Suppose that A is a finite dimensional unital $\mathbb{F}_q$-algebra. If $J = J(A)$ is the Jacobson radical of A, then from our work above we have a group

$$G = 1 + J = \{1 + j | j \in J\}.$$

This is called an **$\mathbb{F}_q$-algebra group** or more generally, a finite algebra group. The group operation is given by the rule

$$(1 + j_1)(1 + j_2) = 1 + j_1 + j_2 + j_1 j_2.$$

Conversely, if J is a finite dimensional nilpotent algebra over $\mathbb{F}_q$, we can define an algebra A in such a way that J is the Jacobson radical of A. We do this be letting $A = \mathbb{F}_q \cdot 1 + J$. Since this algebra only contains one maximal ideal (J), we immediately have that $J(A) = J$. This allows us to establish a bijection between finite nilpotent algebras J and algebra groups.

When F is a field of prime charcateristic p and A is an algebra over F, e.g. $F = \mathbb{F}_q$, then the group $G = 1 + J$ is a p-subgroup of the group of units of A (see Isaacs [5]). Since we can consider J as a vector space over $\mathbb{F}_q$, we can deduce further that the group G has q-power order.

A subgroup H of G is an $\mathbb{F}_q$-algebra subgroup if $H = 1 + U$, for some U that is a sub-algebra of J. Hence H is itself an $\mathbb{F}_q$- algebra subgroup and thus must have q-power index in G. This fact combined with the dimension formula for induced representations (equation 1.2) will provide the key link between Theorem 2.1 and Theorem 2.2 discussed in section 2. The following lemma is also useful:

Lemma 1.29. *Let $G = 1+J$ be a finite algebra group. Then $1+J^k$ is a normal subgroup for all $k \geq 1$.*

Proof. Obvious. □

1.6 Commutators in Groups and Rings:

Much of what we study later on involves exploiting relationships that exist between various subgroups of $G = 1 + J$. Thus we now outline some notation that will be employed. For any two subgroups H_1, H_2 of G, the subgroup generated by the set of elements $h_1 h_2 h_1^{-1} h_2^{-1}$, where $h_1 \in H_1$ and $h_2 \in H_2$, will be denoted by $[H_1, H_2]$.

When A is an algebra, the **Lie bracket** is the commutator $[x, y] = xy - yx$ for $x, y \in A$. When dealing with an algebra A and sub-algebras B_1 and B_2, the notation $[B_1, B_2]$ will denote the sub-algebra generated by elements of the form $b_1 b_2 - b_2 b_1$ where $b_1 \in B_1$ and $b_2 \in B_2$. It will be referred to as the Lie commutator for obvious reasons.

It is somewhat frustrating that we use the same notation, $[\cdot, \cdot]$, for two different things. Nevertheless, we do so because it matches the notation used by Halasi.

This concludes our introduction chapter.

2 An introduction to the work of Halasi.

The work of Zoltan Halasi in 2003 concerned nilpotent algebras over finite fields and representations of the corresponding algebra groups. Specifically, the theorem proved by Halasi settled an open problem regarding the nature of such representations. This theorem had originally been asserted by Gutkin, in [12], however he provided a defective proof. Halasi remedies this situation. The therom first stated by Gutkin and later correctly proved by Halasi is:

Theorem 2.1 (Halasi [1])**.** *Let G be an $\mathbb{F}_q$- algebra group and $\chi \in Irr(G)$. Then there exists an $\mathbb{F}_q$-algebra subgroup $H \leq G$ and a linear character λ of H such that $\chi = \lambda^G$.*

The bijection established in 1.5 allows us to state this in simpler terms. Namely, if A is a finite dimensional unital algebra over $\mathbb{F}_q$, where $q = p^r$ and J the Jacobson radical of A, then every irreducible character of $G = 1 + J$ is induced from a one-dimensional character of some subgroup of the form $H = 1 + U$, where U is a subalgebra of J, i.e. $U \subset J$.

In 1994 Isaacs (in [5]) provided an analysis of the failings of Gutkin's original argument, as well as a counter-example involving upper-triangular matrices. In addition, in the same paper Isaacs proved his Theorem A, which we now state as our Theorem 2.2:

Theorem 2.2 (Isaacs[5])**.** *Let G be an $\mathbb{F}_q$-algebra group. Then all irreducible complex characters of G have $q-$ power degree.*

It is clear now that by the arguments in section 1.5 concerning the index of finite algebra subgroups, that Theorem 2.2 is a direct consequence of Theorem 2.1. We note that the following Corollary given by Isaacs in [5] is a direct consequece of Theorem 2.1.

Corollary 2.1. *Let q be a power of a prime p and let T be a Sylow p-subgroup of $GL(n, q)$. Then T is such that all of its irreducible characters have degrees that are powers of q.*

Proof. The proof provided by Isaacs in [5] deduces that T can be taken to have the form $1 + J$ where J is the Jacobson radical of an $\mathbb{F}_q$-algebra A. The result follows from Theorem 2.1. □

It is also appropriate to recognise that in proving Theorem 2.1, Halasi relies heavily on texts, exercises and papers recorded by Isaacs that are included in the references. In researching the work of Halasi, [5] and [8] proved to be invaluable references for the author of this thesis. Throughout the review of the paper, we note many of the instances where these works provide key insights.

We also make mention that Halasi was not the first to make progress on the proof of Theorem 2.1. Of note is the work of Andre in [13] where he provided a proof of Theorem 2.2 for the case $J^p = 0$, where $p = \text{char}\mathbb{F}_q$. To do so he relied on the exp map described after Lemma 3.2. Moreover, Kazhdan in [14] provided a proof for a specific group that was in turn applicable to a range of other similar groups. However in the words of Isaacs, "for each type of group he imposes some restriction on the characteristic" [5]. Halasi's work thus rids the field of such limitations and allows mathematicians to analyse characters of finite algebra groups without restriction. The brilliance of Halasi was in his ability to pass the results of such authors to any free nilpotent algebra over the integers, which will be explained later on as the key breakthrough required to prove Theorem 2.1.

Halasi proves Theorem 2.1 by utilising relationships that exist between commutators of subgroups and their corresponding sub-algebras. The key theorem proven and used is the following:

Theorem 2.3 (Halasi)**.** *Let J be an arbitrary nilpotent ring and let $1 + J$ be the group associated to J. Then for all $m, n \in \mathbb{N}$:*

$$[1 + J^m, 1 + J^n] \subseteq [1 + J, 1 + J^{m+n-1}]. \tag{2.1}$$

To prove Theorem 2.1 Halasi also applies the following observation:

Theorem 2.4. *Let $G = 1 + J$ be an $\mathbb{F}_q$-algebra group and $\varphi \in Irr(1 + J^2)$. If φ is a G-invariant character, then φ is linear.*

We now provide a comprehensive treatement of Halasi's paper. In doing so we re-write his results, expanding on details omitted from the paper. It is our hope that this clarifies some ambiguities that a reader may encounter when first examining Halasi's paper.

3 Review of Halasi's work.

Before beginning we provide a quick roadmap of the approach taken by Halasi. The following diagram summarises the order in which the theorems are proved. The arrows indicate that the preceeding theorem is the key ingredient in the proof of the succeeding theorem. The diagram is:

$$\text{Theorem 2.3} \dashrightarrow \text{Theorem 2.4} \dashrightarrow \text{Theorem 2.1} \dashrightarrow \text{Theorem 2.2},$$

where the final arrow can be replaced by an implication arrow by our previous observation concerning the order of finite algebra groups. Thus Halasi establishes useful and interesting relationships between subgroups generated by commutators and applies these relationships to prove the theorems that concern character theory. The creativity of the paper in this sense is quite extraordinary.

The bulk of Halasi's paper is devoted to proving Theorem 2.3 and thus this is where we begin. To prove Theorem 2.3 Halasi initially asserts the following lemma. We do the same.

Lemma 3.1. *If* $[1 + A^k, 1 + A^l] \subseteq [1 + A, 1 + A^{k+l-1}]$ *for a nilpotent ring* A*, then* $[1 + B^k, 1 + B^l] \subseteq [1 + B, 1 + B^{k+l-1}]$ *for every quotient ring* B *of* A*.*

Proof. Let $\pi : A \to B$ be the canonical ring-homomorphism. Then it is trivial to see that $\hat{\pi} : 1 + A \to 1 + B$ given by extending π, i.e. $\hat{\pi}(1 + x) = 1 + \pi(x)$ is a well-defined group homomorphism. Moreover, $\hat{\pi}(1 + A^k) = 1 + B^k$. Now suppose H and K are subgroups of $1 + A$. Then we have that $\hat{\pi}[H, K] = [\hat{\pi}(H), \hat{\pi}(K)]$. Thus $[1+A^k, 1+A^l] \subseteq [1+A, 1+A^{k+l-1}]$ implies that $\hat{\pi}[1+A^k, 1+A^l] \subseteq \hat{\pi}[1+A, 1+A^{k+l-1}]$. Passing $\hat{\pi}$ inside the commutator brackets completes the proof.

□

The following lemma greatly simplifies the proof of Theorem 2.3. This proof is not included in the paper.

Lemma 3.2. *Let* N *be a nilpotent ring of nilpotency class* n*. Then* N *is a quotient of* $F_{\mathbb{Z}}(n, X)$ *for some* X*.*

Proof. Any ring is a $\mathbb{Z}$-algebra in exactly one way. We are free to choose X, so we choose sufficiently many elements from N and mod out by all relations. Since the nilpotency class of N is n, it is clear that $F_{\mathbb{Z}}(X)^n$ vanishes in this process. □

It follows that to prove Theorem 2.3 it is enough to show that formula (2.1) holds in the case that J is a free nilpotent algebra over $\mathbb{Z}$. However, to do so Halasi first turns his

attention to free nilpotent algebras over $\mathbb{Q}$ and a bijection between Lie commutators and group commutators. We alert the reader to the fact that the proof provided by Andre in [13] was limited precisely because it depended on the following bijection. Halasi is able to sidestep this limitation, but before exploring this we first outline the usefulness of the bijection. The following is extracted from Halasi [1].

If J is a nilpotent algebra over the **field** R such that either char $R = 0$ (e.g. $R = \mathbb{Q}$) or char $R = p$ and $x^p = 0$ for all $x \in J$ then we can define the map $\exp : J \to 1 + J$ and the inverse of this map $\ln : 1 + J \to J$ by the power series:

$$\exp(x) = 1 + x + \frac{x^2}{2} + ... + \frac{x^k}{k!} + \cdots,$$

$$\ln(1 + x) = x - \frac{x^2}{2} + ... + (-1)^{k+1}\frac{x^k}{k} + \cdots.$$

The Campbell-Hausdorff (found in [6]) formula says that for all $a, b \in J$:

$$\exp(a)\exp(b) = \exp(a + b + z(a, b)), \tag{3.1}$$

where $z(a, b)$ is an element in the Lie subalgebra generated by a and b.

Lemma 3.3. *Let J be a nilpotent algebra over $\mathbb{Q}$. Then the* exp *map establishes a bijection between J^k and $1 + J^k$ for all k. Furthermore,* exp *is a bijection between the Lie commutator $[J^k, J^l]$ and the group commutator $[1 + J^k, 1 + J^l]$.*

Proof. First part of lemma: The exp and ln are formally mutual inverses to eachother, and give rise to well-defined maps. It is clear that $\exp(J^k) \subset 1+J^k$ and that $\ln(1+J^k) \subset J^k$. The first bijection is established.

Second part of lemma: To begin we aim to show that $[1 + J^k, 1 + J^l] \subset \exp[J^k, J^l]$. Note that $[J^k, J^l]$ is a subalgebra of J and thus by the construction of algebra groups and (3.1), $\exp[J^k, J^l]$ is a subgroup of $1 + J$. Choose $x \in J^k$ and $y \in J^l$. Then $[\exp(x), \exp(y)] = \exp([x, y] + \omega(x, y))$ by [7, Lemma 9.15], where $\omega(x, y) \in [J^k, J^l]$. Thus $[1 + J^k, 1 + J^l] \subset \exp[J^k, J^l]$.

We now show that $\exp[J^k, J^l] \subset [1 + J^k, 1 + J^l]$. To do so we assume that $k \geq l$ and use reverse induction on the size of k, noting that for k greater then the nilpotency class of J the result is true. Suppose that $u \in [J^k, J^l]$. Then we write u as

$$u = \sum_{i=1}^{n} [u_i, v_i],$$

where $u_i \in J^k$ and $v_i \in J^l$. By the lemma mentioned before and by the Campbell-Hausdorff formula (3.1),

$$\exp(u)\left(\prod_{i=1}^{n}[\exp(u_i)\exp(v_i)]\right)^{-1} = \exp(u)\prod_{i=n}^{1}\exp(-[u_i,v_i]-w(u_i,v_i)) = \exp(\omega),$$

where ω is a rational linear combination of commutators in the elements u_i, v_i of weight ≥ 3. Thus $\omega \in [J^{k+l}, J^l]$ and $\exp(\omega) \in [1+J^{k+l}, 1+J^l] \subseteq [1+J^k, 1+J^l]$ by reverse induction on k. Therefore $\exp(u) \in [1+J^k, 1+J^l]$ and we are done. □

This ends the extraction from Halasi [1]. From here we follow Halasi but allow ourselves the liberty to divert where necessary.

We continue with our focus on free nilpotent algebras over $\mathbb{Q}$ and with Lemma 3.3 prove the following useful equation:

Lemma 3.4. *If J is a free nilpotent algebra over $\mathbb{Q}$, then for all $k \geq 2$,*

$$[1+J, 1+J] \cap (1+J^k) = [1+J, 1+J^{k-1}]. \tag{3.2}$$

Proof. Utilising the bijection just established, showing

$$[J,J] \cap J^k = [J, J^{k-1}]$$

is equivalent to (3.2). That $[J, J^{k-1}] \subset [J,J] \cap J^k$ is clear from the definition of the Lie commutator (see 1.6). To prove $[J, J^{k-1}] \supset [J,J] \cap J^k$ we let n be the nilpotency class of J and X to be a free generator set of J. Then a basis for J is all words in the alphabet X of length less than n. Halasi denotes this basis B as

$$B = \bigcup_{i=1}^{n-1} X^i,$$

where $X^i = \{u_1u_2\cdots u_i | u_j \in X, 1 \leq j \leq i\}$. Then $[J,J] \cap J^k$ is generated as a vector space over $\mathbb{Q}$ by the set

$$Y = \{[a,b] | a \in X^l, b \in X^m, l+m \geq k\},$$

where we utilised the fact that the Lie bracket $[a,b]$ is $\mathbb{Q}$- bilinear. We then let $a = x_1x_2\cdots x_l \in X^l$ and $b = y_1y_2\cdots y_m \in Y^m$ such that $l+m \geq k$. Then

$$[a,b] = x_1\cdots x_l y_1\cdots y_m - y_1\cdots y_m x_1\cdots x_l$$

$$= (x_1)(x_2\cdots x_l y_1\cdots y_m) - (x_2\cdots x_l y_1\cdots y_m)(x_1) + (x_2)(x_3\cdots x_l y_1\cdots y_m x_1) - (x_3\cdots x_l y_1\cdots y_m x_1)(x_2)$$

$$\cdots + (x_l)(y_1\cdots y_m x_1\cdots x_{l-1}) - (y_1\cdots y_m x_1\cdots x_{l-1})(x_l) \in [J, J^{k-1}].$$

This shows that $Y \subset [J, J^{k-1}]$ and thus $[J,J] \cap J^k \subset [J, J^{k-1}]$. □

This is an important result, however its application is limited because it pertains only to free nilpotent algebras over $\mathbb{Q}$. Moreover, as discussed above, the use of the exp map immediately limits any work that relies on the approach taken so far to a restricted class of finite algebra groups. This is exactly why the work of Andre in [13] only proved lemma 2.1 for the case that $J^p = 0$, where $p = \text{char}\mathbb{F}_q$.

Fortunately, Halasi is able to show (3.2) holds for free nilpotent algebras over $\mathbb{Z}$, but to do so requires the following lemma. The proof of the following lemma provided by Halasi caused the author unnecessary confusion. Perhaps this can be attributed to the brevity of Halasi's argument. We have provided a modified proof of the one given by Halasi in the next section, which is hopefully clearer.

3.1 Revised proof of Lemma 2.4 in Halasi.

Lemma 3.5. *Let V be a vector space over $\mathbb{Q}$ and let $B = \{b_1, ..., b_j, ...\} \subseteq V$ be a basis of V. For any subset Y we denote $\langle Y\rangle_{\mathbb{Z}}$ the set of all linear combinations of elements from Y with integer coefficients. If $Y \subseteq \{b_i - b_j | b_i, b_j \in B\}$, then $\langle Y\rangle_{\mathbb{Q}} \cap \langle B\rangle_{\mathbb{Z}} = \langle Y\rangle_{\mathbb{Z}}$.*

Proof. We choose $z \in \langle Y\rangle_{\mathbb{Q}} \cap \langle B\rangle_{\mathbb{Z}}$ with $z \neq 0$. Write $z = \alpha_1 y_1 + ... + \alpha_s y_s$ such that

1. $\alpha_i \in \mathbb{Q}^{\times}$,
2. $y_i = b_t - b_k$ for some $t = t(i), k = k(i)$ and $t \neq k$, for $1 \leq i \leq s$,
3. The set $\{y_1, ..., y_s\} \subseteq Y$ is a linearly independent subset of V.

This can always be done for any $z \in \langle Y\rangle_{\mathbb{Q}} \cap \langle B\rangle_{\mathbb{Z}}$ by re-arranging and factoring. We prove the lemma using induction on s.

If $s = 1$, then $z = \alpha_1 y_1 = \alpha_1(b_t - b_k)$ for $b_t, b_k \in B$, $b_t \neq b_k$. It is clear that for $z \in \langle B\rangle_{\mathbb{Z}}$ it must be that $\alpha_1 \in \mathbb{Z}$.

Now suppose the result holds for dim $\leq s - 1$. Since $\dim\langle y_1, ...y_s\rangle_{\mathbb{Q}} = s$, then there is a $b_j \in B$ such that there exists exactly one y_k, $1 \leq k \leq s$, with non-zero coordinate in b_j. If not then condition 3 would be violated. Since B is a basis, the coefficient α on b_j, which is the coefficient on y_k, must lie in $\mathbb{Z}$. Then by assumption

$$z \pm \alpha y_k = \sum_{i \neq k} \alpha_i y_i \in \langle Y\rangle_{\mathbb{Z}}.$$

Thus $z \in \langle Y\rangle_{\mathbb{Z}}$. This completes the proof.

□

3.2 Equation (3.2) for free nilpotent algebras over $\mathbb{Z}$.

We now establish equation (3.2) for free nilpotent algebras over $\mathbb{Z}$ and to use this to prove Theorem 2.3. To prove that equation 3.2 holds for for free nilpotent algebras over $\mathbb{Z}$ we adopt the following notation used by Halasi. A free nilpotent algebra over $\mathbb{Q}$ of unspecified nilpotency class will be denoted by $N(\mathbb{Q})$ and a free nilpotent algebra over $\mathbb{Z}$ of unspecified nilpotency class will be denoted by $N(\mathbb{Z})$. The following lemma is exactly what we require. We provide the proof produced by Halasi [1] verbatim.

Lemma 3.6. *For all $k \geq 2$,*

$$[1 + N(\mathbb{Z}), 1 + N(\mathbb{Z})] \cap (1 + N(\mathbb{Z})^k) = [1 + N(\mathbb{Z}), 1 + N(\mathbb{Z})^{k-1}].$$

Proof. Firstly, that $[1 + N(\mathbb{Z}), 1 + N(\mathbb{Z})^{k-1}] \subset [1 + N(\mathbb{Z}), 1 + N(\mathbb{Z})] \cap (1 + N(\mathbb{Z})^k)$ is a simple consequence of the commutator subgroup. To see this, note that for $a \in N(\mathbb{Z})$ and $b \in N(\mathbb{Z})^{k-1}$ any commutator $(1 + a)(1 + b)(1 + a)^{-1}(1 + b)^{-1} = (1 + a)(1 + b)(1 - a + a^2 \cdots)(1 - b + b^2 \cdots) = (1 \pm ab(P)))$, where P is a polynomial in a and b. The reverse inclusion is much harder.

Observe that $1 + N(\mathbb{Z})^k \leq 1 + N(\mathbb{Q})^k$ and thus

$$\begin{aligned}[1 + N(\mathbb{Z}), 1 + N(\mathbb{Z})] \cap (1 + N(\mathbb{Z})^k) &\leq [1 + N(\mathbb{Q}), 1 + N(\mathbb{Q})] \cap (1 + N(\mathbb{Q})^k) \\ &= [1 + N(\mathbb{Q}), 1 + N(\mathbb{Q})^{k-1}]\end{aligned}$$

by applying Lemma 2.8. Let X be a free generating set of $N(\mathbb{Q})$ and n the nilpotency class of $N(\mathbb{Q})$. Then we can write all elements of $N(\mathbb{Q})$ as polynomials in X with coefficients in $\mathbb{Q}$ such that all terms of the polynomial have total degree $< n$. Then $N(\mathbb{Z})$ is simply the set of polynomials with integer coefficients. Hence it is enough to show that the elements of $[1 + N(\mathbb{Q}), 1 + N(\mathbb{Q})^{k-1}]$ with integer coefficients belong to $[1 + N(\mathbb{Z}), 1 + N(\mathbb{Z})^{k-1}]$. Define the degree of an element of $N(\mathbb{Z})$ to be the smallest total degree of its terms. Let $1 + z \in [1 + N(\mathbb{Q}), 1 + N(\mathbb{Q})^{k-1}] \cap (1 + N(\mathbb{Z}))$ be an arbitrary element of interest. Suppose z has degree $l > k-1$, then $1+z \in [1+N(\mathbb{Q}), 1+N(\mathbb{Q})^{l-1}]$, by Lemma 2.8. To show that $1 + z \in [1 + N(\mathbb{Z}), 1 + N(\mathbb{Z})^{k-1}]$ we use reverse induction using that fact that when $l \geq n$ the result is true.

Let $X^l = \{u_1 u_2 \cdots u_l | u_j \in X, 1 \leq j \leq l\}$ and $[X, X^{l-1}] = \{[u, v] | u \in X, v \in X^{l-1}\}$. Since $1 + z \in [1 + N(\mathbb{Q}), 1 + N(\mathbb{Q})^{l-1}]$, write

$$1 + z = \prod [1 + x_i, 1 + y_i]^{\pm 1},$$

where $x_i \in N(\mathbb{Q})$ and $y_i \in N(\mathbb{Q})^{l-1}$. Then $[x_i, y_i] \in \langle [X, X^{l-1}] \rangle_{\mathbb{Q}} + N(\mathbb{Q})^{l+1}$. Thus

$$1 + z = \prod [1 + x_i, 1 + y_i]^{\pm 1} \in \left(1 + \sum \pm [x_i, y_i] + N(\mathbb{Q})^{l+1}\right) \cap (1 + N(\mathbb{Z}))$$

$$\subset 1 + \left(\left\langle [X, X^{l-1}] \right\rangle_{\mathbb{Q}} \cap N(\mathbb{Z})\right) + N(\mathbb{Q})^{l+1}.$$

Applying our Lemma 3.5 we see that $\langle [X, X^{l-1}] \rangle_{\mathbb{Q}} \cap N(\mathbb{Z}) = \langle [X, X^{l-1}] \rangle_{\mathbb{Z}}$, and thus

$$1 + z \in 1 + \langle [X, X^{l-1}] \rangle_{\mathbb{Z}} + N(\mathbb{Q})^{l+1}.$$

It follows that $z \in \sum_{j=1}^{m} \alpha_j [a_j, b_j] + N(\mathbb{Q})^{l+1}$, where $\alpha_j \in \mathbb{Z}, a_j \in X$ and $b_j \in X^{l-1}$. Consider

$$1 + z' = (1 + z)\left(\prod [1 + \alpha_j a_j, 1 + b_j] \right)^{-1},$$

which is an element of $[1 + N(\mathbb{Q}), 1 + N(\mathbb{Q})^{k-1}] \cap (1 + N(\mathbb{Z}))$. Moreover z' has degree greater than l since we eliminated all such terms with total degree l. Thus by induction, $1 + z' \in [1 + N(\mathbb{Z}), 1 + N(\mathbb{Z})^{k-1}]$. Since $\left(\prod [1 + \alpha_j a_j, 1 + b_j]\right)^{-1}$ is also clearly in $[1 + N(\mathbb{Z}), 1 + N(\mathbb{Z})^{k-1}]$, we conclude that $1 + z \in [1 + N(\mathbb{Z}), 1 + N(\mathbb{Z})^{k-1}]$. □

Proof of Theorem 2.3 . By Lemma 3.1 it is enough to show that equation 2.1 holds for $J = N(\mathbb{Z})$. From our work we know that

$$[1 + N(\mathbb{Z})^m, 1 + N(\mathbb{Z})^n] \subset [1 + N(\mathbb{Z}), 1 + N(\mathbb{Z})] \cap (1 + N(\mathbb{Z})^{m+n})$$

$$= [1 + N(\mathbb{Z}), 1 + N(\mathbb{Z})^{m+n-1}]$$

by Lemma 3.2. □

3.3 Characters of Algebra Groups

We now turn our attention to the characters of algebra groups and prove the main Theorems of Halasi.

Let J be a nilpotent algebra over a finite field $\mathbb{F}_q$ where $q = p^f$ for some prime p. Let $G = 1 + J$ be the finite algebra group associated to J. The main results of Halasi concerning character theory, namely Theorems 2.1 and 2.4, are proven using the following lemma.

Lemma 3.7. *Let $G = 1 + J$ be a finite algebra group of $\mathbb{F}_q$ and $\chi \in Irr(G)$. Then the following properties are equivalent:*

1. *There exist a proper algebra subgroup $H < G$ and $\varphi \in Irr(H)$ such that $\chi = \varphi^G$.*
2. *χ_{1+J^2} is not irreducible.*

To prove this lemma we require some definitions and a fact.

Definition 3.8. *Let $H \lhd G$. If ϑ is a class function on H and $g \in G$, then $\vartheta^g(h) = \vartheta(ghg^{-1})$ is a conjugate class function.*

In fact it is shown in Isaacs [8] that this process of conjugating class functions defines a group operation of G on $\mathrm{Irr}(H)$: by $g * \varphi \rightsquigarrow \varphi^g$. Since any element in H acts trivially on the set of class functions, we can re-phrase this by stating that G/H acts on $\mathrm{Irr}(H)$: by $\bar{g} * \varphi \rightsquigarrow \varphi^g$.

Definition 3.9. *Let $H \lhd G$ and let $\varphi \in Irr(H)$. Then*

$$I_G(\varphi) = \{g \in G | \varphi^g = \varphi, \}$$

is the Inertia group of φ in G.

It is a subgroup precisely because it is the stabilizer of the character φ. Of course $H \subset I_G(\varphi)$ and $|G|/|I_G(\varphi)|$ is the order of the orbit.

Fact 3.10 (Isaacs [8])**.** *Let $H \lhd G$ and let $\varphi \in Irr(H)$. Then $\varphi^G \in Irr(G)$ if and only if $I_G(\varphi) = H$.*

Definition 3.11. *Let χ be a character of a group G. Then $Z(\chi) = \{g \in G : |\chi(g)| = \chi(1)\}$.*

For instance, if χ is a linear character of a group G then $Z(\chi) = G$.

Lemma 3.12. *Let χ be a character of G and let $R : G \to GL_n(\mathbb{C})$ be a representation that affords χ. Then $Z(\chi) = \{g \in G | R_g = \alpha I for some\ \alpha \in \mathbb{C}\}$.*

Proof. Firstly, we must show that R_g is similar (conjugate) to a diagonal matrix $\text{diag}(\alpha_1, ..., \alpha_n)$. Observe that we can restrict the representation R to the abelian subgroup $\langle g \rangle$. Then by applying Maschke's theorem, we see that R_g is similar to a representation in block diagonal form - i.e. a direct sum of irreducible representations. But $\langle g \rangle$ is abelian and thus all irreducible representations are one-dimensional. Hence R_g is similar to a diagonal representation. Moreover, clearly $|\alpha_i| = 1$.

To prove the lemma observe that R_g is similar to $\text{diag}(\alpha_1, ..., \alpha_n)$ where $|\alpha_i| = 1$ and $|\sum \alpha_i| = n$. But $|\sum \alpha_i| = n$ if and only if all α_i's are the same. Say $\alpha_i = \alpha$ for all i. Then R_g is similar to αI, which commutes with all matrices. Hence $R_g = \alpha I$. □

Definition 3.13. *Let χ be a character of G. Then ker $(\chi) = \{g \in G | \chi(g) = \chi(1)\}$.*

A simple lemma that can be found in Isaacs [8] is the following:

Lemma 3.14. *Let R be a representation of G into $GL_n(\mathbb{C})$ which affords the character χ. Then $g \in ker(R)$ if and only if $\chi(g) = \chi(1)$.*

We also require the following lemma, which concerns the Jacobson radical.

Lemma 3.15 (Isaacs [5])**.** *Let $J = J(R)$, where R is a finite dimensional $\mathbb{F}_q$-algebra and suppose $U \subset J$ is a multiplicatively closed subspace. If $J = U + J^2$, then $U = J$.*

Proof. See Isaacs [5]. □

Proof of Lemma 3.3. (1) $\implies$ (2). Suppose $H = 1 + U \neq G$ is an alegbar subgroup and $\varphi \in \text{Irr}(H)$ such that $\chi = \varphi^G$. Let $K = H(1 + J^2) = 1 + U + J^2$. Since $U \neq J$, we have that $1 + J^2 \leq K \neq G$ by Lemma 3.7. By the transitivity of induction (Serre [4]), $\chi = (\varphi^K)^G$ and trivially χ_K is not irreducible. Since $1 + J^2 \leq K$, we must have that χ_{1+J^2} is also not irreducible.
(2) $\implies$ (1). We assume that χ_{1+J^2} is not irreducible and we let ψ be a constituent of χ_{1+J^2}. Let $H = 1 + U \geq 1 + J^2$ be a maximal $\mathbb{F}_q$-algebra subgroup such that ψ is extendible to H. Then $H \neq G$ because $\chi \in \text{Irr}(G)$. Choose $\varphi \in \text{Irr}(H)$ such that φ is an extension of ψ and φ is a constituent of χ_H. Now choose $x \in J - U$ and note that the subgroup $N_x = 1 + \mathbb{F}_q x + U$ is an $\mathbb{F}_q$-algebra subgroup. Moreover, $[N_x : H] = q$. Let $\vartheta \in \text{Irr}(N_x)$ be a such that φ is a constituent of ϑ_H. By Isaacs' Theorem 2.2, $\vartheta(1)$ and $\varphi(1)$ are both q powers. Then either $\vartheta_H = \varphi$ or $\vartheta_H = \varphi^{N_x}$. Clearly if the first were true, then H would not be maximal because $N_X \gneq H$. Thus $\vartheta = \varphi^{N_x}$. Since ϑ is irreducible, by Fact 3.6, $I_{N_x}(\varphi) = H$. Since x was arbitrary, $I_G(\varphi) = H$. Hence by another application of Fact 3.6, this time in the reverse direction, $\varphi^G \in \text{Irr}(G)$. By the **Frobenius reciprocity** formula we have that $\chi = \varphi^G$. □

We now have the required tools to prove Theorem 2.4.

3.4 Proof of Theorem 2.4

Proof of Theorem 2.4. Let $G = 1 + J$ be an algebra group and $\varphi \in \mathrm{Irr}(1 + J^2)$ be a G- invariant character. That is, $I_G(\varphi) = G$. By reverse-induction, we show that $[1 + J^2, 1 + J^k] \leq \ker\varphi$ for all $k \geq 2$. Clearly when k exceeds the nilpotency class of J the result holds. So suppose that $[1 + J^2, 1 + J^{k+1}] \leq \ker\varphi$. Thus $1 + J^{k+1} \leq Z(\varphi)$. Therefore, by [Isaacs,2 lemma 2.27] we have $\varphi_{1+J^{k+1}} = \lambda \cdot \varphi(1)$, where λ is a $G-$ invariant linear character of $1 + J^{k+1}$. Hence $[1 + J, 1 + J^{k+1}] \leq \ker\,\varphi$. Now we can apply Theorem 2.4, which states that $[1 + J^2, 1 + J^k] \leq [1 + J, 1 + J^{k+1}]$ and thus $[1 + J^2, 1 + J^k] \leq \ker\,\varphi$. Thus $[1 + J^2, 1 + J^2]$ is contained in the kernal of the representation. Hence the representation factors through the commutator subgroup and to be irreducible must therefore be linear. □

Proof of Theorem 2.1. Choose $\chi \in \mathrm{irr}(G)$. If χ is linear we are done. Suppose χ is not linear. Then χ_{1+J^2} is clearly G-invariant - because any character is constant on conjugacy classes. Hence it must be that $\chi \notin \mathrm{Irr}(1 + J^2)$. Hence by lemma 3.11 there exists a proper algebra subgroup $H \lneq G$ and $\varphi \in \mathrm{Irr}(H)$ such that $\chi = \varphi^G$. If φ is linear we stop. Otherwise we continue with this process and using the fact that $|G|$ is finite, we eventually arrive at an algebra subgroup $L \lneq H \lneq G$ such that λ is linear and $\lambda \in \mathrm{Irr}(L)$ and $\varphi = \lambda^H$. Applying the transitivity of induction (Fact 1.15) completes the proof. □

This concludes our review of Halasi's article.

4 A Working Example.

We consider the matrix ring $M_n(\mathbb{F}_p[t]/t^k)$, where $\mathbb{F}_p[t]/t^k$ is the truncated polynomial algebra with coefficients in $\mathbb{F}_p$. We see that $M_n(\mathbb{F}_p[t]/t^k)$ is an $\mathbb{F}_p$-algebra by the map $\mathbb{F}_p \rightsquigarrow \mathbb{F}_p I$. Throughout this section, we let $\omega_p = e^{2\pi i/p}$, where p is any prime. Since the choice of p is immaterial to our work, we will often just write ω_p as ω.

We reduce it to a nilpotent algebra over $\mathbb{F}_p$ by considering the ideal

$$J = t \cdot M_n(\mathbb{F}_p[t]/t^k)$$

Its nilpotency class is clearly k as $(tX)^k = 0$ for all $X \in M_n(\mathbb{F}_p[t]/t^k)$. Then as discussed above, we have the $\mathbb{F}_p$-algebra group

$$G = I + t \cdot M_n(\mathbb{F}_p[t]/t^k) = I + J.$$

Since this is a $p-$group we know that all irreducible complex characters of G have p power degree. Moreover, by Halasi [1] if χ is an irreducible complex character of G, then there exists an $\mathbb{F}_p$-algebra subgroup $H \leq G$ and a linear character λ of H such that $\chi = \lambda^G$.

For this section we attempt to follow the proof of Halasi to accurately describe the situation when $J = t \cdot M_2(\mathbb{F}_p[t]/t^k)$. Specifically, we aim to find the sub-algebras $U \subset J$ and linear characters of $I + U$ that induce the irreducible characters of $I + J$. To be clear J is the $\mathbb{F}_p$-algebra consisting of elements of the form

$$\begin{bmatrix} a_1 t + ... + a_{k-1}t^{k-1} & b_1 t + ... + b_{k-1}t^{k-1} \\ c_1 t + ...c_{k-1}t^{k-1} & d_1 t + ... + d_{k-1}t^{k-1} \end{bmatrix},$$

for $a_i, b_i, c_i, d_i \in \mathbb{F}_p$. Hence the group $G = I + J$ is elements of the form:

$$\begin{bmatrix} 1 + a_1 t + ... + a_{k-1}t^{k-1} & b_1 t + ... + b_{k-1}t^{k-1} \\ c_1 t + ...c_{k-1}t^{k-1} & 1 + d_1 t + ... + d_{k-1}t^{k-1} \end{bmatrix},$$

We directly see that $|I + J| = |J| = p^{4(k-1)}$.

4.1 $k = 2$

We start with the case when $k = 2$.

Proposition 4.1. *The finite algebra group $G = I + t \cdot M_2(\mathbb{F}_p[t]/t^2)$ is an abelian group of order p^4.*

The proof is simple and we do it for clarity as well as the fact that it provides greater insight into the group structure.

Proof. Let a, b, c, d, e, f, g, h be arbitrary elements in $\mathbb{F}_p$.

Let

$$A = \begin{bmatrix} 1+at & bt \\ ct & 1+dt \end{bmatrix},$$

and

$$B = \begin{bmatrix} 1+et & ft \\ gt & 1+ht \end{bmatrix}.$$

Then since $t^2 = 0$ in $\mathbb{F}_p[t]/t^2$, we have

$$AB = \begin{bmatrix} 1+(a+e)t & (b+f)t \\ (c+g)t & 1+(d+h)t \end{bmatrix} = BA$$

□

Thus by Theorem 1.10 every irreducible character of G is one-dimensional and there are p^4 of them. The sub-algebras described by Halasi are just J itself. Furthermore, we notice an interesting property of the multiplication of elements in $I + J$. To see this, let us write $A = I + tX$ and $B = I + tY$ for

$$X = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{F}_p)$$

and

$$Y = \begin{bmatrix} e & f \\ g & h \end{bmatrix} \in M_2(\mathbb{F}_p),$$

then

$$AB = (I + tX)(I + tY) = I + t(X + Y).$$

Thus we have a group isomorphism

$$\varphi : I + J \to M_2(\mathbb{F}_p)^+$$

defined by

$$I + tX \rightsquigarrow X.$$

Since

$$M_2(\mathbb{F}_p)^+ \approx \mathbb{F}_p^4, \tag{4.1}$$

we can apply the established results concerning representations of cyclic groups and representations of product groups to determine the irreducible characters. The major result required is the following proposition:

Proposition 4.2. *Let G be an abelian group that is the direct product of abelian subgroups G_1 and G_2, i.e. $G = G_1 \times G_2$.*

1. *If ρ^1 and ρ^2 are irreducible representations of G_1 and G_2 respectively, then $\rho : G \to \mathbb{C}^\times$ defined by $\rho(g_1, g_2) = \rho^1(g_1) \cdot \rho^2(g_2)$ is an irreducible representation of G.*

2. *Each irreducible representation of G is isomorphic to a representation $\rho^1 \cdot \rho^2$, where ρ^i is an irreducible representation of G_i.*

Proof. See Serre [4] for the more general result when G is not abelian. The proposition is a consequence. □

There is another way to view the irreducible representations of $M_2(\mathbb{F}_p)^+$ that is particularly illuminating for our purposes. To see this, observe that the character table of $\mathbb{F}_p$ is completely determined by where we map 1. Moreover, since $(1 + 1 + ... + 1)$ (p times) $= 0$, we have the following summary of the p irreducible characters of $\mathbb{F}_p$:

	0	1
χ_0	1	1
χ_1	1	ω
χ_2	1	ω^2
...	...	...
χ_{p-1}	1	ω^{p-1}

.

Then consider arbitrary $\chi_i \in \mathrm{Irr}(\mathbb{F}_p), \chi_i \neq \chi_0$. For each $X \in M_2(\mathbb{F}_p)$ we define a one-dimensional character $\psi_X : M_2(\mathbb{F}_p) \to \mathbb{C}^\times$ by the following rule:

$$\psi_X(A) = \chi_i(\mathrm{tr}XA).$$

We verify it is indeed a homomorphism from $M_2(\mathbb{F}_p)^+ \to \mathbb{C}^\times$.

Choose arbitrary $X, A, B \in M_2(\mathbb{F}_p)$. Then using the fact that $\chi_i : \mathbb{F}_p \to \mathbb{C}^\times$ is a group homomorphism we have:

$$\psi_X(A + B) = \chi_i(\mathrm{tr}X(A + B)) = \chi_i(\mathrm{tr}(XA + XB)) = \chi_i(\mathrm{tr}XA + \mathrm{tr}XB)$$

$$= \chi_i(\mathrm{tr}XA) \cdot \chi_i(\mathrm{tr}XB) = \psi_X(A) \cdot \psi_X(B).$$

The following lemma is simple:

Lemma 4.3. *Let $\psi_X : M_2(\mathbb{F}_p) \to \mathbb{C}^\times$ be defined as above. Then $\psi_X = \psi_Y$ if and only if $X = Y$.*

Proof. The $\Leftarrow$ direction is obvious. For $\Rightarrow$ by letting

$$X = \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix}$$

and

$$A = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix},$$

we see that $\mathrm{tr}(XA) = x_1a_1 + x_2a_3 + x_3a_2 + x_4a_4$. The result follows by choosing the a_i in the obvious way. □

Thus we immediately have p^4 distinct one-dimensional characters of $M_2(\mathbb{F}_p)$ and by our earlier work, this must be the set $\mathrm{Irr}(M_2(\mathbb{F}_p)^+)$.

4.2 A Digression on Symplectic Forms

To progress to higher values of k, we introduce some concepts that at first glance appear to be unrelated, however prove to be quite useful.

Definition 4.4. *Let V be a vector space over a field F. An anti-symmetric bilinear form on V is a bilinear form $B : V \times V \to F$, which satisfies the following properties for all $v, w \in V$:*

1. $B(v, w) = -B(w, v)$,
2. $B(v, v) = 0$,

We say that two vectors $v, w \in V$ are orthogonal if $B(v, w) = 0$. The Radical of the form B, denoted by $\mathrm{Rad}(B)$ is described as the orthogonal space to the whole space V:

$$\mathrm{Rad}(B) = \{v \in V | B(v, w) = 0 \text{ for all } w \in V\}.$$

It is clear that $\mathrm{Rad}(B)$ is a subspace of V. An anti-symmetric bilinear form B is non-degenerate if $\mathrm{Rad}(B) = \{0\}$. This is equivalent to the stating that for all $v \in V, v \neq 0$, there exists $w \in V$ such that

$$B(v, w) \neq 0.$$

When a form B is both anti-symmetric and non-degenerate, we say that B is a **symplectic** bilinear form on the vector space V.

Definition 4.5. *If V is a vector space over F and B is a symplectic form on V, then a subspace W is **isotropic** if $B(x, y) = 0$ for all $x, y \in W$.*

We also require the following Theorem:

Theorem 4.6. *Let V be a vector space of positive dimension m over a field F, and let $B : V \times V \to F$ be a symplectic bilinear form.*

1. *The dimension of V is even.*

2. *Every maximal isotropic subspace has dimension equal to* $\dim(V)/2$.

Proof. For (1) see Artin [2]. For (2) see Viterbo [17]. □

To illustrate the relevance of these definitions, we state the following powerful Theorem from Bushnell and Frohlich [19].

Theorem 4.7. *Let G be a finite group and N a normal subgroup, such that G/N is an elementary abelian $p-$group. Thus G/N has the structure of a $\mathbb{F}_p$ vector space. Let χ be a one-dimesnional character of N, which is stabilized by G. Define an anti-symmetric bilinear form on G/N by*

$$B_\chi : G/N \times G/N \to \mathbb{C}^\times, B(\bar{g}, \bar{h}) = \chi(ghg^{-1}h^{-1}).$$

Moreover, assume that the form is non-degenerate. Then there exists a unique up to isomorphism irreducible representation ρ_χ of G such that $\rho_{\chi_{|N}}$ contains χ.

Proof. See Bushnell and Frohlich [19]. □

this is an important result that highlights the relationship between symplectic forms and representation theory. We now turn our attention to the case when $k = 3$.

4.3 k=3

We make two identifications. Firstly,

$$I + J/I + J^2 \approx M_2(\mathbb{F}_p)^+.$$

Secondly, by including scalar multiplication $(c, X) \rightsquigarrow cIX$ for $c \in \mathbb{F}_p$ and $X \in M_2(\mathbb{F}_p)$, $M_2(\mathbb{F}_p)$ has the structure of a vector space over $\mathbb{F}_p$. Pulling our results back, we have that

$$I + J/I + J^2 \text{ is a vector space over } \mathbb{F}_p$$

where for $X, Y \in M_2(\mathbb{F}_p), c \in \mathbb{F}_p$:

1. **Addition** is given by the group operation, i.e. $(\overline{(I + tX)}, \overline{(I + tY)}) \rightsquigarrow \overline{(I + tX)(I + tY)} = \overline{I + t(X + Y)}$.

2. **Scalar multiplication** is given by the rule $(c, \overline{I + tX}) \rightsquigarrow \overline{I + t(cX)}$.

Although this supplies some rigour, it is for the most part easiest to just identify $I + J/I + J^2$ as a vector space over $\mathbb{F}_p$ by treating the space as the vector space $M_2(\mathbb{F}_p)$.

Secondly, we can embed the group $\mathbb{F}_p^+$ in $\mathbb{C}^\times$ by the map χ_1 defined in the preceeding section. For reminder, $\chi_1 : \mathbb{F}_p^+ \to \mathbb{C}^\times$ is a group homomorphism completely determined by the fact that

$$\chi_1(1) = e^{2\pi i/p} = \omega.$$

Thus we can identify $\mathbb{F}_p$ with points on the unit circle in the complex plane. Although χ_1 is a homomorphism defined on the additive group $\mathbb{F}_p^+$, the map is also well behaved (to some extent) with respect to the multiplicative structure of $\mathbb{F}_p$. Since $\chi_1(1) = \omega$ and $\chi_1(\alpha) = \omega^\alpha$ for all $0 \leq \alpha < p$, we have for $0 \leq \alpha \leq \beta < p$

$$\chi_1(\alpha\beta) = \omega^{\alpha\beta} = \chi_1(\alpha)^\beta = \chi_1(\beta)^\alpha.$$

It is worth noting that $\chi_1(\alpha\beta) \neq \chi_1(\alpha)\chi_1(\beta)$ in general and thus it is not a group homomorphism into $\mathbb{C}^\times$.

With these two identifications in place, we can now define a bilinear form on the vector space $I + J/I + J^2$ into the embedding of $\mathbb{F}_p$ in the complex plane. As above, $\pi : I + J \to I + J/I + J^2$ is the canonical homomorphism that sends $g \rightsquigarrow \overline{g}$.

Our anti-symmetric bilinear form: Choose θ_X a non-trivial character of $I + J^2$. For $g, h \in I + J$ we define

$$B_X(\overline{g}, \overline{h}) = \theta_X(ghg^{-1}h^{-1}).$$

Proposition 4.8. *The function B_X defined above is an anti-symmetric bilinear form - a map $I + J/I + J^2 \times I + J/I + J^2 \to \mathbb{C}^\times$ that satisfies the conditions given in Definition 4.4.*

Proof. For simplicity let $B_X = B$. Firstly since θ_X is a character of $I + J^2$ we have to show that the function defined even makes sense. However, this is simple since $I + J/I + J^2$ is an abelian group, it must be that $I + J^2$ contains the commutator subgroup and hence all commutators.

Now we verify that the map is bilinear in the first variable only. Choose arbitrary Y and $Z \in M_2(\mathbb{F}_p)$ and observe that

$$(I + tY)(I + tZ)(I - tY + (tY)^2)(I - tZ + (tZ)^2)$$

$$= I + t^2(YZ - ZY).$$

Thus

$$B(\overline{I+tY}, \overline{I+tZ}) = \theta_X(I + t^2(YZ - ZY)).$$

Then for $Y_1, Y_2, Z \in M_2(\mathbb{F}_p)$ and by an abuse of notation we have

$$B(Y_1 + Y_2, Z) = \theta_X((Y_1 + Y_2)Z - Z(Y_1 + Y_2)) = \theta_X(Y_1Z + Y_2Z - ZY_1 - ZY_2)$$

$$= \theta_X(Y_1Z - ZY_1) \cdot \theta_X(Y_2Z - ZY_2) = B(Y_1, Z) \cdot B(Y_2, Z),$$

where we used the fact that θ_X is one-dimensional and thus a homomorphism.

Continuing with the same shorthand notation, to verify scalar multiplication we are required to show that for $\alpha \in \mathbb{F}_p$ we have

$$B(\alpha Y, Z) = \theta_X(YZ - ZY)^\alpha.$$

Working through we see that

$$B(\alpha Y, Z) = \theta_X(\alpha YZ - Z\alpha Y) = \chi_1(\mathrm{tr}(\alpha X(YZ - ZY)))$$

$$= \chi_1(\alpha \cdot \mathrm{tr}(X(YZ - ZY))) = \chi_1(\mathrm{tr}(X(YZ - ZY)))^\alpha = B(Y, Z)^\alpha.$$

To show the map is bilinear in the second variable is a symmetrical argument and we omit it.

Finally we verify that the map is anti-symmetric. To do so requires showing that

$$B(\overline{g}, \overline{h}) = B(\overline{h}, \overline{g})^{-1}.$$

This is straightforward since

$$\theta_X(ghg^{-1}h^{-1}) = \theta_X((hgh^{-1}g^{-1})^{-1}) = \theta_X(hgh^{-1}g^{-1})^{-1}.$$

□

We compute the radical of B_X.

$$\mathrm{Rad}(B_X) = \left\{ \overline{g} \in I + J/I + J^2 | B(\overline{g}, \overline{h}) = 1 \text{ for all } \overline{h} \in I + J/I + J^2 \right\}.$$

Suppose without loss of generality that $\overline{g} = \overline{I + tY}$ for some $Y \in M_2(\mathbb{F}_p)$. Then we have the following fact:

Fact 4.9. *The element $\overline{g}$ is contained in Rad (B_X) if and only if $[X, Y] = 0$.*

Proof. Firstly we show the $\Leftarrow$ direction. Suppose $[X,Y] = XY - YX = 0$. Then for any $Z \in M_2(\mathbb{F}_p)$:

$$\theta_X(I + t^2(YZ - ZY)) = \chi_1(\mathrm{tr}(X(YZ - ZY))) = \chi_1(\mathrm{tr}(XYZ)) \cdot \chi_1(\mathrm{tr}(XZY))^{-1}$$

$$= \chi_1(\mathrm{tr}(XYZ)) \cdot \chi_1(\mathrm{tr}(YXZ))^{-1} = \chi_1(\mathrm{tr}(XY - YX)Z) = \chi_1(0) = 1$$

For the $\Rightarrow$ direction, suppose $\overline{g} \in \mathrm{Rad}\ (B_X)$ but $[X,Y] \neq 0$. Then some entry of

$$XY - YX = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix},$$

is non-zero. Wlog suppose $a_{11} \neq 0$. Then there exists a matrix $Z \in M_2(\mathbb{F}_p)$ such that $\mathrm{tr}((XY - YX)Z) = a_{11}$, which contradicts our assumption that $\overline{g} \in \mathrm{Rad}\ (B_X)$. This completes the proof. □

Thus we can describe the radical of the form as follows:

$$\mathrm{Rad}(B_X) = \left\{ \overline{I + tY} \in I + J/I + J^2 \middle| [X,Y] = 0 \right\},$$

for $Y \in M_2\mathbb{F}_p$. The following lemma is straightforward:

Proposition 4.10. *The Radical of the form B_X is a subgroup of $I + J/I + J^2$.*

Proof. The only condition worth verifying is that inverses are contained in $\mathrm{Rad}(B_X)$. Suppose $\overline{I + tY} \in \mathrm{Rad}(B_X)$. Then $\overline{I + tY}^{-1} = \overline{I - tY}$ and the result follows from Fact 4.9. □

Then the Correspondence Theorem states that $\pi^{-1}(\ \mathrm{Rad}(B_X))$ is a normal subgroup of $I + J$ because $\mathrm{Rad}(B_X)$ is a subgroup of the abelian group $I + J/I + J^2$. Moreover, if we let $H = \pi^{-1}(\ \mathrm{Rad}(B_X))$, then again by the Correspondence Theorem we have the following diagram

$$I + J^2 \subset H \subset I + J.$$

We now consider the conditions on X which determine $\mathrm{Rad}(B_X)$. It is clear from Fact 4.8 that we need to determine the centralizer of X in $M_2(\mathbb{F}_p)$. We denote the centralizer of X by the notation $C(X)$. We start with the simple case when X is a scalar matrix. If

$$X = \begin{bmatrix} \alpha & 0 \\ 0 & \alpha \end{bmatrix}$$

for some $\alpha \in \mathbb{F}_p$, then $C(X) = M_2(\mathbb{F}_p)$ and $\mathrm{Rad}(B_X)$ is the entire group $I + J/I + J^2$. This amounts to saying that

$$\mathrm{Rad}(B_X) \approx M_2(\mathbb{F}_p)^+ \text{ if } X \text{ is a scalar matrix,}$$

which is a 4-dimensional vector space ove $\mathbb{F}_p$.

Now suppose that X is not a scalar matrix. Then we have the following:

Proposition 4.11. *Let $X \in M_2(\mathbb{F}_p)$ and X not a scalar matrix. Then $C(X)$ is a 2-dimensional vector space over $\mathbb{F}_p$ with basis $\{I, X\}$. In other words*

$$C(X) = \{c_0 I + c_1 X | c_i \in \mathbb{F}_p\}.$$

Corollary 4.1. *If $X \in M_2(\mathbb{F}_p)$ is not a scalar matrix, then $|Rad(B_x)| = p^2$ and $|\pi^{-1}(Rad(B_x))| = p^6$.*

Proof of Proposition 4.11. We let $\mathbb{F}_p = F$. Let $f(t)$ be the characteristic polynomial of the matrix X. Of course f is of degree 2.

Firstly, suppose the roots of the characteristic polynomial are not contained in F. Hence f is irreducible. Then we have

$$K = F[X] \approx F[t]/\langle f(t) \rangle,$$

a degree 2 field extension of F with basis $\{I, X\}$. As a vector space over F, we know that $K \approx (F)^2$. Let V be the underlying vector space structure of K over F. Then V has dimension 2 over F and dimension 1 over K. Hence any matrix in $M_2(F)$ naturally acts on V. Now observe that for any $B \in C(X)$, $k \in K$ and $v \in V$, we have

$$B(kv) = k(Bv),$$

which implies that $C(X)$ is the endomorphism ring of the vector space V over K. Hence $C(X) = K$ and the result follows.

If the charateristic polynomial f of X splits over F, then we reduce X to Jordan form by conjugating X by some invertible element P. Then $B \in C(X)$ if and only if $PBP^{-1} \in C(PXP^{-1})$. There are two cases;

1. The roots of f are distinct, or
2. The roots coincide.

.
When the roots are distinct then by direct computation it is simple to see that $C(X)$ must be diagonal and hence dim $C(X) = 2$.

If the roots of f coincide then after reducing to Jordan form we have

$$X = \begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix}$$

for $\lambda \in F$. Then letting

$$X' = X - \lambda I = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

we see that $C(X') = C(X)$. Now suppose

$$B = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, B \in C(X').$$

Then by direct computation wee see that this occurs if $a = d$ and $c = 0$. That is, $B = c_0 I + c_1 X'$ for $c_i \in F$. Replacing X' with $X - \lambda I$ completes the proof.

□

Since the aim is to understand representations of $I + J$, we now outline how to extend characters of $I + J^2$ to larger subgroups of $I + J$ by using the radical of our form. For some $X \in M_2(\mathbb{F}_p)$, let B_X be the form described above and let θ_X be the linear character of $I + J^2$ that corresponds to this form. Moreover, let $H = \pi^{-1}(\mathrm{Rad}(B_X))$. Then we have $I + J^2 \lneq H \leq I + J$ and:

Proposition 4.12. *The character θ_X extends as a linear character to the subgroup H.*

To prove this proposition we rely on the following well-established result:

Proposition 4.13. *Let G be a finite abelian group and let G_1 be a subgroup of G. If χ is a linear character of G_1 then χ can be extended to a linear character of G.*

Proof of Proposition 4.12. Let $[H, H]$ be the commutator subgroup of H. Then by the definition of the Radical of B_X we have that $[H, H] \leq \ker(\theta_X)$. Let $\hat{\theta}_X$ be the character on $I + J^2/[H, H]$ defined by $\hat{\theta}_X(\bar{g}) = \theta_X(g)$. Since $I + J^2/[H, H] \leq H/[H, H]$ we can extend $\hat{\theta}_X$ to $H/[H, H]$ by proposition 4.13. This naturally defines a character on H, which by construction agrees with θ_X on $I + J^2$. □

With this in hand, we seperate our work to deal with the following two cases:

1. X is a scalar matrix,
2. X is not a scalar matrix.

4.3.1 X is a scalar matrix.

From our work above we know that $\pi^{-1}(\mathrm{Rad}(B_X)) = I + J$. Hence by Proposition 4.13 the character associated to this form, θ_X, extends to $I + J$. Any such extension is a linear character of $I + J$. There are p scalar matrices and for each matrix we can choose $|I + J/I + J^2| = p^4$ unique extensions. This gives us p^5 unique linear characters of G.

4.3.2 X is not a scalar matrix.

Suppose X is not a scalar matrix and let $H = \pi^{-1}(\mathrm{Rad}(B_X))$. We know that $|H| = p^6$. By proposition 4.13 each θ_X extends to H in p^2 unique ways. Let $\hat{\theta}_{X_i}$ denote an arbitrary extension of θ_X. Then let

$$\hat{B}_X : I + J/H \times I + J/H \to \mathbb{C}^\times$$

be given by

$$B(\bar{g}, \bar{h}) = \hat{\theta}_{X_i}(ghg^{-1}h^{-1}).$$

The $\mathbb{F}_p$-vector space $I + J/H$, containing p^2 elements, has dimension 2. We choose a maximal isotropic subspace M', which by Theorem 4.6 has dimension 1. We extend $\hat{\theta}_X$ to $\pi^{-1}(M') = M$ and denote this linear character by $\tilde{\theta}_X$. The induced representation $\tilde{\theta}_X^{I+J}$ has dimension p and is irreducible. Since we could choose $p^4 - p$ non-scalar X and extend these in p^2 unique ways, we have identified $p^2(p^4 - p)$ unique p degree representations of $I + J$. Combining our results from 4.3.1 and 4.3.2 and applying the counting formula we see that

$$|I + J| = p^8 = p^5(1) + p^2(p^4 - p)(p^2).$$

Thus we have all irreducible represntations. This concludes our discussion of $I + tM_2(\mathbb{F}_p[t]/t^k)$.

5 Future work

In researching this paper Uri Onn provided the author with a nilpotent ring that closely resembles the the algebra just considered. It was posed as a problem to see if we could conclude a similar result to Halasi and/or understand its representations to the extent just discussed in the preceeding section. We briefly explain this problem now.

Consider the matrix ring $M_n(\mathbb{Z}/p^k)$ for some integer $k \geq 2$. The order of $M_n(\mathbb{Z}/p^k)$ is equal to the order of $M_n(\mathbb{F}_p[t]/t^k)$ and the two rings exhibit many similarities. Similarly, we reduce the ring $M_n(\mathbb{Z}/p^k)$ to a nilpotent ring by considering the ideal

$$p \cdot M_n(\mathbb{Z}/p^k).$$

It is nilpotent because for any $X \in p \cdot M_n(\mathbb{Z}/p^k)$, we have

$$X^k = 0.$$

However, unlike above, the original ring $M_n(\mathbb{Z}/p^k)$ is not an $\mathbb{F}_p$-algebra. If it was an $\mathbb{F}_p$-algebra then there would exist an injective ring homomorphism $\phi : \mathbb{F}_p \to M_n(\mathbb{Z}/p^k)$. But $\phi(0) = p \cdot \phi(1) = pI \neq 0$ since $k \geq 2$. Thus no such homomorphism is possible. It follows that the nilpotent ring $p \cdot M_n(\mathbb{Z}/p^k)$ is also not an $\mathbb{F}_p$-algebra for $k > 2$.

We now consider the group

$$G = I + pM_n(\mathbb{Z}/p^k)$$

with the law of composition given by the rule $(I+pX)(I+pY) = I+p(X+Y)+p^2(XY)$. Since the nilpotency class of $pM_n(\mathbb{Z}/p^k)$ is k, we see that for all $pX \in pM_n(\mathbb{Z}/p^k)$ we have that

$$(I + pX)(I - pX + (pX)^2 - (pX)^3 + ... \pm (pX)^{k-1}) = I.$$

Since G is not a finite algebra group, we are unable to directly apply the results of Halasi. Nevertheless, we can do a similar study to the one conducted of the groups $I + tM_2(\mathbb{F}_p[t]/t^k)$ and compare results.

5.1 The case when $n = 2$.

Here we briefly introduce some of the properties of the above group and its representations when $G = I + pM_2(\mathbb{Z}/p^k)$ and $k \geq 2$. In particular, we observe that there are noticable similarities between these groups and the ones studied in the previous section.

The exercises conducted above could be followed with these groups to gain further insights. We briefly do the simplest of cases.

5.2 $k = 2$

When $k = 2$, then every $g \in I + pM_2(\mathbb{Z}/p^2)$ can be uniquely written in the form

$$g = \begin{bmatrix} 1 + pa & pb \\ pc & 1 + pd \end{bmatrix},$$

for $a, b, c, d \in \mathbb{Z}/p$. Since $\mathbb{Z}/p = \mathbb{F}_p$, by letting

$$X = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{F}_p),$$

re-write g as

$$g = I + pX.$$

Clearly, the choice of X defines each element in G. Moreover, for $h = I + pY$ it follows that

$$gh = I + p(X + Y) = hg.$$

Recalling our work from Section 4.2 leads us to conclude that

$$I + pM_2(\mathbb{Z}/p^2) \approx M_2(\mathbb{F}_p)^+ \approx I + tM_2(\mathbb{F}_\text{ı}[t]/t^2). \tag{5.1}$$

This allows us to accurately decsribe all characters of G: They are the characters outlined in Section 4.2.

This concludes our work. Hopefully the interested reader is keen to pursue the study of such groups and provide a more comprehensive treatment of their characters.

References

[1] Z. Halasi. On the characters and commutators of finite algebra groups. *Journal of Algebra*, 275: 481-487, 2004.

[2] M. Artin. *Algebra*. Pearson Education,Inc. 2011.

[3] S. Lang. *Algebra* (Third Edition) Addison-Wesley, 1993

[4] J.-P. Serre. *Linear Representations of Finite Groups* Springer-Verlag, 1977.

[5] I.M. Isaacs. Characters of groups associated with finite algebras. *Journal of Algebra*, 177: 708-730, 1995.

[6] N. Jacobson *Lie Algebras*. Interscience, New York 1962.

[7] E.I. Khukhro *p-Automorphisms of Finite p-Groups.* Cambridge University Press, Cambridge, 1997.

[8] I.M. Isaacs. *Character Theory of Finite Groups* Dover, New York, 1994.

[9] The Jacobson Radical. https://sites.math.washington.edu/ mitchell/Algh/jac.pdf. Accessed: 2017-12-24.

[10] Semisimple algebras and Wedderburn's Theorem. http://web.mat.bham.ac.uk/A.Evseev/pdf /wedderburn.pdf. Accessed: 2017-12-24.

[11] M. Sahai. On the Jacobson Radical and Unit Groups of Group Algebras *Publicacions Matematiques,* (Vol 42): 339-346, 1998.

[12] E.A. Gutkin. Representations of algebraic unipotent groups over a self-dual field, *Funkts. Analiz Ego Prilozheniya* 7, 80, 1973.

[13] C.A.M. Andre. Irreducible characters of finite algebra groups, in: *Matrices and Group Representations,* Coimbra, 1998, in: Textos Mat. Ser. B, vol 19, Univ. Coimbra, Coimbra, pg 65-80, 1999.

[14] D. Kazhdan. Proof of Springer's Hypothesis, *Israel Journal of Mathematics* 28,272-286, 1977.

[15] Free Algebras - Wikipedia https://en.wikipedia.org/wiki/Freealgebra. Accessed: 2017:01:10

[16] Symplectic Vector Spaces http://dornsife.usc.edu/assets/sites/618/docs/SymplecticVectorSpaces -2.pdf. Accessed 2017:01:16

[17] C. Viterbo. *Introduction to Symplectic Topology:* (http://www.math.polytechnique.fr/cmat/viterbo/B1.pdf), Accessed 2018:01:18

[18] A. Caranti. (https://math.stackexchange.com/users/58401/andreas-caranti) *Find dimension of Commuting matrices over field of prime elements*, URL (version: 2017-02-12): https://math.stackexchange.com/q/2140845, Accessed 2018:01:24

[19] C.J Bushnell and A. Frohlich . Gauss Sums and P-adic Division Algebras, *Lecture Notes in Mathematics*, Vol. 987, Springer-Varleg, Berlin, 1983.