Computational Aspects of Representation Theory

Nikhil Kumar

A dissertation submitted for the partial fulfilment of
BS-MS dual degree in Science

Indian Institute of Science Education and Research Mohali
April 2013

To my parents
for their unending support and encouragement

Certificate of Examination

This is to certify that the dissertation titled "Computational Aspects of Representation Theory" submitted by Mr. Nikhil Kumar (Reg. No. MS08035) for the partial fulfillment of BS-MS dual degree programme of the Institute, has been examined by the thesis committee duly appointed by the Institute. The committee finds the work done by the candidate satisfactory and recommends that the report be accepted.

Professor S.K. Khanduja	Dr. Varadharaj R. Srinivasan	Dr. Amit Kulshrestha
		(Supervisor)

Declaration

The work presented in this dissertation has been carried out by me under the guidance of Dr. Amit Kulshreshtha at the Indian Institute of Science Education and Research Mohali.

This work has not been submitted in part or in full for a degree, a diploma, or a fellowship to any other university or institute. Whenever contributions of others are involved, every effort is made to indicate this clearly, with due acknowledgement of collaborative research and discussions. This thesis is a bonafide record of original work done by me and all sources listed within have been detailed in the bibliography.

Nikhil Kumar

(Candidate)

Dated: April 26, 2013

In my capacity as the supervisor of the candidate's project work, I certify that the above statements by the candidate are true to the best of my knowledge.

Dr. Amit Kulshreshtha

(Supervisor)

Acknowledgment

I would like to take this opportunity to extend my special gratitude to Dr. Amit Kulshreshtha, who helped me to explore the computational aspects of representation theory and mentored me through all impediments encountered on the path. I am grateful to him for allowing me follow my passion for the subject and delve deeper into this captivating research area.

I would also like to thank his doctoral student Ms. Dilpreet Kaur for her valuable inputs and keen interest in my advancements of the project. She has indeed put in a lot of effort in editing my thesis and without her this work would not have been completed.

This project would not have been possible without the unconditional and unwavering support and belief of my family in me and my abilities.

I would like to take a moment and thank my batch mates who made my stay and learning at IISER a fun and meaningful.

Finally, I am thankful to IISER Mohali for providing me such a pleasant environment to work and Department of Science and Technology, India for giving me the INSPIRE fellowship.

Nikhil Kumar

Notations

- G : is a finite group with order $|G|$.
- F: a field such that $\text{Char}(F) \nmid |G|$.
- $GL(n, F)$: group of invertible $n \times n$ matrices with entries in F.
- e : exponent of the group G.
- Let $\mathcal{C}_1, \cdots, \mathcal{C}_k$ be the k distinct conjugacy classes of G with representatives $g_1, \cdots, g_k$ respectively, then:

  $h_r = |\mathcal{C}_r|$, be the size of the conjugacy class $\mathcal{C}_r$.

  $\rho^1, \cdots, \rho^k$ be the k irreducible representations of G.

  χ^i , be the character of the irreducible representation ρ^i.

  $d_i = \chi^i(1)$, be the degree of the character (or representation) of χ_i (or ρ^i).

  $\chi^i_r = \chi^i(C_r)$, the value attained χ^i over the conjugacy class C_r.

- $\mathcal{M}(G)$: the set of all minimal normal subgroups of G.

Contents

Notations i

Introduction 1

I Computing the character table 3

1 Representation and Character theory of finite groups 5

1.1 Character Tables 10

1.1.1 Orthogonality relations 10

2 Burnside's algorithm 13

2.1 The Algorithm 17

3 Dixon's Modification of Burnside's algorithm 19

3.1 Remarks about Burnside's algorithm 19

3.1.1 Implications of Dixon's modification 19

3.2 Transposing the problem to $\mathbb{Z}_p$ 20

3.3 Details of Dixon's method 20

3.3.1 Recovering the complex characters 21

3.4 The Burnside-Dixon algorithm 22

II Group Ring and central idempotents 25

4 Group Rings 27

4.1 Augmentation Ideals 29

4.2 Semisimplicity of Group Rings 32

5 Primitive central idempotents of rational group algebras 35

5.1 Idempotents of RG 35

5.2 Idempotents in the rational group algebra of finite nilpotent groups 37

III Appendix **45**

A GAP implementation of Burnside's algorithm **47**

B GAP implementation of Burnside-Dixon algorithm **53**

C GAP implementation for finding the primitive central idempotents **59**

D Graphs and Trees **67**

D.1 Representing Graphs 67

D.2 Graph Transversal- Depth First Search 68

Bibliography **70**

Introduction

In this expository report, the objects of our interest are algorithms for the computation of character table and the primitive central idempotents in the rational group algebra of nilpotent groups. The report consists of five chapters. The first chapter contains notions of representation theory that are required for the subsequent chapters. Chapters two and three discuss algorithms available for the computation of the character table, namely, the Burnside's algorithm and Dixon's modification of Burnside's method. In chapter four we introduce the concept of group rings and use their properties to compute the idempotents in the rational group algebra.

Nowadays, there are many algorithms for the computation for the character tables. The first algorithm discussed in the report was given by by Burnside in 1911[Bur04]. Appendix A gives the program for the `GAP` implementation of the Burnside's algorithm. Although, the method is extremely tedious, but for groups of higher order ($|G| \approx 500$) the complexity involved in the computation is too great. Dixon's modification[Dix67] helped reduce the complexity by performing the computations involved in Burnside's algorithm in a finite field $\mathbb{F}_p$ (for some suitable p) instead of the complex field. This modification helps avoid the round-off error encountered in case of complex field, makes the computation faster. Appendix B gives the `GAP` implementation of Burnside-Dixon algorithm.

The algorithms discussed above give us the complex characters of a group, but the rational characters or representations of a group cannot be computed in a straight forward way. In case of the rational group algebras, the primitive central idempotents can be used to find the decomposition of semisimple group algebras into simple algebras, which in turn give us the rational representation of the group, thereby giving the rational characters of the group. In the second part of this report, we first discuss about group rings and their semisimplicity and use these notions to study the idempotents in the rational group algebras. We finally discuss the primitive central idempotents of the rational group algebras of nilpotent groups as described in [EJ03]. The primitive central idempotents of $\mathbb{Q}G$, where G is a nilpotent group can be obtained from the subgroups of G which satisfy certain conditions as mentioned in the theorem below.

Theorem 5.1 *Let G be a finite nilpotent group. The primitive central idempotents of $\mathbb{Q}G$ are precisely all elements of the form*

$$\sum_g (\varepsilon(G_m, H_m))^g,$$

(the sum of all G-conjugates of $\varepsilon(G_m, H_m)$), where H_m and G_M are subgroups of G that satisfy all of the following properties:

1. $H_0 \subseteq H_1 \subseteq \cdots \subseteq H_m \subseteq G_m \subseteq \cdots \subseteq G_1 \subset G_0 = G$,

2. *for* $0 \leq i \leq m$, H_i *is a normal subgroup of* G_i *and* $\mathcal{Z}(G_i/H_i)$ *is cyclic,*

3. *for* $0 \leq i < m$, G_i/H_i *is not abelian, and* G_m/H_m *is abelian,*

4. *for* $0 \leq i < m$, $G_{i+1}/H_i = C_{G_i/H_i}(\mathcal{Z}_2(G_i/H_i))$,

5. *for* $1 \leq i \leq m$, $\cap_{x \in G_{i-1}/H_{i-1}} H_i^x = H_{i-1}$.

For the computation of the primitive central idempotents using `GAP`, many algorithms are available, most using the package *wedderga*. We have made an attempt to use the above mentioned theorem to compute the primitive central idempotents of $\mathbb{Q}G$, when G is a finite nilpotent group. Appendix C gives the code for computing the primitive central idempotents in `GAP`.

Part I

Computing the character table

Chapter 1

Representation and Character theory of finite groups

Characters of finite abelian groups have been used since the time of Gauss, but it was only after Frobenius that the use of characters was extended to finite non-abelian groups. In this chapter we record the basics of representation theory and the associated group characters.

Let G be a finite group and F a field, such that $\mathrm{Char}\,(F) \nmid |G|$. Also, let $GL(n, F)$ be the group of invertible $n \times n$ matrices with entries in F.

Definition 1.1. *A representation of a group G over a field F is a homomorphism*

$$\rho : G \to GL(n, F),$$

for some n. The degree of representation ρ is given by the integer n.

A representation ρ of G is said to be faithful, if $\mathrm{Ker}\,\rho = \{1\}$. Representations can also be viewed in terms of FG-modules which are defined below.

Definition 1.2. *Let V be a vector space over F and let G be a group. Then V is called an FG-module if a multiplication vg $(v \in V,\ g \in G)$ is defined, satisfying the following conditions for all $u,\ v\ \in V,\ \lambda \in F$ and $g,\ h \in G$:*

1. *$vg \in V$;*
2. *$v(gh) = (vg)h$;*
3. *$v1 = v$;*
4. *$(\lambda v)g = \lambda(vg)$;*

5. $(u+v)g \;=\; ug \,+\, vg.$

Note that for a fixed $g \in G$ the function $v \;\to\; vg \;\; (v \in v)$ is an F-endomorphism of V.

Definition 1.3. *Let V be an FG-module and let β be a basis of V. For each $g \in G$, we denote by $[g]_\beta$ the matrix of the F-endomorphism $v \;\to\; vg \;\; (v \in v)$, with respect to the basis β.*

Definition 1.4. *Let V be an FG-module. A subset W of V is said to be an FG-submodule of V if W is a F-subspace of V and $wg \in W$ for all $w \in W$ and all $g \in G$.*

Thus an FG-submodule of V is a subspace of V which is also an FG-module.

Definition 1.5. *An FG-module V is said to be irreducible if it is non-zero and it has no FG-submodule apart from $\{0\}$ and V.*

Definition 1.6. *Let V and W be FG-modules. A function $\theta : V \to W$ is said to be an FG-homomorphism if θ is a linear transformation and*

$$\theta(vg) \;=\; (\theta v)g \textit{ for all } v \in V,\; g \in G.$$

Thus, if θ sends v to w then it sends vg to wg.
Next we discuss two important results on irreducible FG-modules, namely the *Maschke's theorem* and *Schur's lemma.*

Theorem 1.1. *Maschke's Theorem*
Let G be a finite group, let F be $\mathbb{R}$ or $\mathbb{C}$, and let V be an FG-module. If U is an FG-submodule of V, then there is an FG-submodule W of V such that

$$V = U \oplus W.$$

Proof. We already have that U is an FG-submodule of V and choose a F-subspace W_o of V such that

$$V = U \oplus W_o.$$

To get W_o take a basis $v_1, \cdots, v_m$ of U and extend it a basis $v_1, \cdots, v_m, v_{m+1}, \cdots, v_n$ of V and let W_o be the span of $v_{m+1}, \cdots, v_n$. For $v \in V$, we have $v = u + w$, for unique $u \in U$ and $w \in W_o$. Define $\phi : V \to V$ setting $\phi(v) = u$. Clearly, ϕ is a projection of V with kernel W_o and image U. We modify ϕ to get an FG-homomorphism from V to V with image U. Define $\psi : V \to V$ by

$$\psi(v) = \frac{1}{|G|} \sum_{g \in G} \phi(vg)g^{-1} \quad (v \in V).$$

It clear that ψ is an endomorphism of V and $\operatorname{Im}(\psi) \subseteq U$. Take $v \in V$ and $x \in G$, then

$$\begin{aligned}\psi(vx) &= \frac{1}{|G|}\sum_{g\in G}\phi(vxg)g^{-1}\\ &= \frac{1}{|G|}\sum_{h\in G}\phi(vh)h^{-1}x\\ &= \left(\frac{1}{|G|}\sum_{h\in G}\phi(vh)h^{-1}\right)x\\ &= \psi(v)x.\end{aligned}$$

Thus, ψ is an FG-homomorphism. Next, we need to show that $\psi^2 = \psi$. For $u \in U$, $g \in G$, we have $ug \in U$, so $\phi(ug) = ug$. This gives us,

$$\psi(u) = \frac{1}{|G|}\sum_{g\in G}\phi(ug)g^{-1} = \frac{1}{|G|}\sum_{g\in G}(ug)g^{-1} = \frac{1}{|G|}\sum_{g\in G}u = u.$$

Now, let $v \in V$, then $\psi(v) \in U$, so by the above equation $\psi(\psi(v)) = \psi(v)$. Therefore, $\psi^2 = \psi$, thus $\psi : V \to V$ is a projection and an FG-homomorphism. Moreover, the above equation gives us $\operatorname{Im}\psi = U$. Let $W = \operatorname{Ker}\psi$, then W is an FG-submodule of V and $V = U \oplus W$, which completes the proof. □

Theorem 1.2. *Schur's Lemma*
Let V and W be irreducible $\mathbb{C}G$-modules.

1. *If $\theta : V \to W$ is a $\mathbb{C}G$-homomorphism, then either θ is a $\mathbb{C}G$-isomorphism, or $\theta(v) = 0$ for all $v \in V$.*
2. *If $\theta : V \to V$ is a $\mathbb{C}G$-isomorphism, then θ is a scalar multiple of the identity endomorphism 1_V.*

Proof. (1) Suppose that $\theta(v) \neq 0$ for some $v \in V$. Then $\operatorname{Im}\theta \neq \{0\}$. As $\operatorname{Im}\theta$ is a $\mathbb{C}G$-submodule of W, and W is irreducible, so we have $\operatorname{Im}\theta = W$. Also $\operatorname{Ker}\theta$ is a $\mathbb{C}G$-submodule of V and V is irreducible, so $\operatorname{Ker}\theta = \{0\}$. Thus θ is invertible, and hence is a $\mathbb{C}G$-isomorphism.

(2) Let $\lambda \in \mathbb{C}$ be an eigenvalue of the endomorphism θ, so $\operatorname{Ker}(\theta - \lambda 1_V) \neq \{0\}$. Thus $\operatorname{Ker}(\theta - \lambda 1_V)$ is a non-zero $\mathbb{C}G$-submodule of V, V being irreducible give us that $\operatorname{Ker}(\theta - \lambda 1_V) = V$. Therefore

$$v(\theta - \lambda 1_V) = 0 \quad ,\forall\, v \in V.$$

Thus, $\theta = \lambda 1_V$, as required. □

We now begin the discussion about the character theory of finite groups.

Definition 1.7. *Let V be a $\mathbb{C}G$-module and β be a basis of V. Then the character of V is the function $\chi : G \to \mathbb{C}$ defined by*

$$\chi(g) \;=\; tr[g]_\beta \;\; (g \in G).$$

Remark 1.1. *It should be noted that if β and β' are two bases of V, then there is an invertible matrix T, such that $[g]_{\beta'} = T^{-1}[g]_\beta T$. Therefore, the character χ is independent of the choice of basis of V.*

Definition 1.8. *If χ is the character of a $\mathbb{C}G$-module V, then the dimension of V is called the* degree *of χ.*

We now discuss some elementary results about groups characters.

Proposition 1.1. *If x and y are conjugate elements of the group G, then $\chi(x) \;=\; \chi(y)$, for all characters χ of G.*

Proof. Assume that x and y are conjugate elements of G, so $x \;=\; g^{-1}yg$, for some $g \in G$. Let V be a $\mathbb{C}G$-module with basis β, then

$$[x]_\beta \;=\; [g^{-1}yg]_\beta \;=\; [g^{-1}]_\beta[y]_\beta[g]_\beta.$$

Hence, we have $tr[x]_\beta \;=\; tr[y]_\beta$. Therefore $\chi(x) \;=\; \chi(y)$, where χ is the character of V. □

Proposition 1.2. *Let χ be the character of a $\mathbb{C}G$-module V. Suppose that $g \in G$ and g has order m. Then*

1. $\chi(1) \;=\; dim\, V$,
2. *$\chi(g)$ is a sum of m^{th} roots of unity,*
3. $\chi(g^{-1}) \;=\; \overline{\chi(g)}$,
4. *$\chi(g)$ is a real number if g is conjugate to g^{-1}.*

Proof. See Proposition 13.9 of [JL93]. □

Definition 1.9. *We define the* inner product *of two functions χ and ψ from $G \times G$ to $\mathbb{C}$ as,*

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

Let $C_G(g_i)$ denote the set of all centralizers of g_i in G, i.e.

$$C_G(g_i) = \{y \in G : \; yg_i = g_i y\}.$$

Proposition 1.3. *Assume that G has exactly k distinct conjugacy classes, with representatives $g_1, g_2, \cdots, g_k$. Let χ and ψ be characters of G. Then*

$$\langle \chi, \; \psi \rangle = \sum_{i=1}^{k} \frac{1}{|C_G(g_i)|} \chi(g_i)\overline{\psi(g_i)}.$$

Proof. Let $\mathcal{C}_i$ be the conjugacy class of G containing g_i. Since characters are constant on conjugacy classes we get,

$$\sum_{g \in {g_i}^G} \chi(g)\overline{\psi(g)} \;=\; |\mathcal{C}_i| \chi(g_i)\psi(g_i).$$

Also $G \;=\; \bigcup_{i=1}^{k} \mathcal{C}_i$ and $|\mathcal{C}_i| \;=\; |G|/|C_G(g_i)|$. Therefore,

$$\begin{aligned}
\langle \chi, \; \psi \rangle &= \frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\psi(g)} \\
&= \frac{1}{|G|} \sum_{i=1}^{k} \sum_{g \in \mathcal{C}_i} \chi(g)\overline{\psi(g)} \\
&= \sum_{i=1}^{k} \frac{|\mathcal{C}_i|}{|G|} \chi(g_i)\overline{\psi(g_i)} \\
&= \sum_{i=1}^{k} \frac{1}{|C_G(g_i)|} \chi(g_i)\overline{\psi(g_i)}.
\end{aligned}$$

□

For irreducible characters of a group G, we have the following results (for proofs refer [JL93], Ch-14):

Theorem 1.3.

1. *Let U and V be non-isomorphic irreducible $\mathbb{C}G$-modules, with characters χ and ψ, respectively. Then*

$$\langle \chi, \; \psi \rangle = 0.$$

2. *Suppose that V and W are $\mathbb{C}G$-modules, with characters χ and ψ, respectively. Then V and W are isomorphic if and only if $\chi \;=\; \psi$.*

3. *Let $\chi^1, \cdots, \chi^k$ be the irreducible characters of G. Then $\chi^1, \cdots, \chi^k$ are linearly independent vectors in the vector space of all functions from G to $\mathbb{C}$.*

We next state an important theorem giving us the number of irreducible characters of a group G.

Theorem 1.4. *The number of irreducible characters of G is equal to the number of conjugacy classes of G.*

Proof. Refer Theorem 15.3 of [JL93]. □

1.1 Character Tables

Definition 1.10. *Let $\chi^1, \cdots, \chi^k$ be the irreducible characters of G and let $g_1, \cdots, g_k$ be representatives of the conjugacy classes of G. The $k \times k$ matrix whose ij^{th}-entry is $\chi^i(g_j)$ (for all i, j with $1 \leq i, j \leq k$), is called the character table of G.*

We set $\chi^1 = 1_G$, the trivial character and $g_1 = 1$, the identity element of the group G. In the character table, the rows are indexed by irreducible character of G and the columns by the conjugacy classes. Since the irreducible characters of G and hence the rows of the character table are linearly independent, we get that:

Proposition 1.4. *The character table of G is an invertible matrix.*

1.1.1 Orthogonality relations

Theorem 1.5. *Let $\chi^1, \cdots, \chi^k$ be the irreducible characters of G, and let $g_1, \cdots, g_k$ be representatives of the conjugacy classes of G. Then the following relations hold for any r, $s \in \{1, \cdots, k\}$.*

1. *The row orthogonality relations:*

$$\langle \chi^r,\ \chi^s \rangle = \sum_{i=1}^{k} \frac{\chi^r(g_i)\overline{\chi^s(g_i)}}{|C_G(g_i)|} = \delta_{rs}.$$

2. *The column orthogonality relations:*

$$\sum_{i=1}^{k} \chi^i(g_r)\overline{\chi^i(g_s)} = \delta_{rs}|C_G(g_r)|.$$

Proof. Row orthogonality relation. We already have established that, $\langle \chi^r,\ \chi^s \rangle = \delta_{rs}$, for χ^r and χ^s in $\{\chi^1, \cdots, \chi^k\}$, the irreducible characters of G. This can be written in terms of rows of character table as

$$\sum_{i=1}^{k} \frac{\chi^r(g_i)\overline{\chi^s(g_i)}}{|C_G(g_i)|} = \delta_{rs}.$$

Column orthogonality relation. Now for $1 \leq s \leq k$ let ψ^s be a class function satisfying $\psi^s(g_r) = \delta_{rs} \quad (1 \leq r \leq k)$. We have $\psi^s = \sum_{i=1}^{k} \lambda_i \chi^i$, where $\lambda_i = \langle \psi^s, \chi^i \rangle = \frac{1}{|G|} \sum_{g \in G} \chi^s(g) \overline{\chi^i(g)}$. Also $\chi^s(g) = 1$ if g is conjugate to g_s and $\psi^s(g) = 0$ otherwise. Since there are $|G|/C_G(g_s)$ elements of G which are conjugate to g_s, so

$$\lambda_i = \frac{1}{|G|} \sum_{g \in G} \psi^s(g) \overline{\chi^i(g)} = \frac{\chi^i(g_s)}{|C_G(g_s)|}.$$

Therefore,

$$\delta_{rs} = \psi^s(g_r) = \sum_{i=1}^{k} \lambda_i \chi^i(g_r) = \sum_{i=1}^{k} \frac{\chi^i(g_r) \overline{\chi^i(g_s)}}{|C_G(g_s)|},$$

and the column relation holds. □

Chapter 2

Burnside's algorithm

In this chapter we will discuss the computation of the character table of a group G in a completely deterministic process, using the *Burnside's algorithm.*

The very first method to systematically compute the character table was given by Burnside in 1911 in his book titled *"Theory of Groups of Finite Order"*[Bur04]. Even though the method is extremely tedious to do in practice, but for groups of large order (say 500) the complexity involved is often too great.

Lemma 2.1. *If ρ is any irreducible representation of G and $\mathcal{C}$ is a conjugacy class in G, then*

$$\sum_{g \in \mathcal{C}} \rho(g)$$

is a scalar multiple of identity.

Proof. For all $g \in G$, we have

$$\rho(g).\left(\sum_{y \in \mathcal{C}} \rho(y)\right) = \left(\sum_{y \in \mathcal{C}} \rho(gyg^{-1})\right).\rho(g) = \left(\sum_{y \in \mathcal{C}} \rho(y)\right).\rho(g).$$

Hence, by Schur's lemma 1.2 we that $\sum_{y \in \mathcal{C}} \rho(y)$ is a scalar. □

By the above lemma we get that $\sum_{g \in \mathcal{C}} \rho(g) = \lambda I$, where λ is a scalar. Taking trace on both sides we get,

$$Tr\left[\sum_{y \in \mathcal{C}} \rho(y)\right] = \sum_{y \in \mathcal{C}} Tr[\rho(y)] = |\mathcal{C}|\chi(y) = \lambda\chi(1).$$

Therefore,

$$\lambda = \frac{|\mathcal{C}_r|\chi^i(g)}{\chi^i(1)} \quad (g \in G). \tag{2.1}$$

From now onwards, let $\mathcal{C}_1, \cdots, \mathcal{C}_k$ be the k conjugacy classes of G with representatives $g_1, \cdots, g_k$ respectively. Also, let $\rho^1, \cdots, \rho^k$ be the irreducible representations of G with $\chi^1, \cdots, \chi^k$ being their associated complex characters and let χ^i_j be the value attained by character χ^i over the conjugacy class C_j, $\quad (i, j = 1, 2, \cdots, r)$. With the notation defined above, Equation 2.1 ca be re-written as:

$$\lambda = \frac{|C_j|\chi^i_j}{\chi^i(1)} = \frac{h_j\chi^i_j}{d_i}.$$

Definition 2.1. *We define the class sum $\mathcal{C}_r^+$ for a conjugacy class $\mathcal{C}_r$ $(r = 1, \cdots, k)$ as the formal sum $\sum_{x \in \mathcal{C}_r} x$.*

Definition 2.2. *We define the class multiplication coefficients of G as integers c_{rst}, where*

$$c_{rst} = |\{(g_r, g_s) \in \mathcal{C}_r \times \mathcal{C}_s : \; g_r g_s = g_t, \; \textit{for any fixed} \; g_t \in \mathcal{C}_t\}|.$$

It should be noted that c_{rst} is independent of the choice of $g_t \in \mathcal{C}_t$.

Proposition 2.1. *For the class sums $\mathcal{C}_r^+$ and $\mathcal{C}_s^+$ of the conjugacy classes $\mathcal{C}_r$ and $\mathcal{C}_s$, respectively, we have*

$$\mathcal{C}_r^+\mathcal{C}_s^+ = \sum_{t=1}^{k} c_{rst}\mathcal{C}_t^+ \tag{2.2}$$

where each c_{rst} is a non-negative integer[CR62].

Proof. In the left hand of the above equation, we know that both $\mathcal{C}_r^+$ and $\mathcal{C}_s^+$ are formal sums of elements of G, so $\mathcal{C}_r^+\mathcal{C}_s^+$ is also formal a sum of elements of G, each occurring a non-negative integral number of times. So, each c_{rst} is a non-negative constant. We interpret $\{c_{rst}\}$ as the structure constants connecting the conjugacy classes of G. If we let $\mathcal{C}_r\mathcal{C}_s$ denote the collection of products $\{xy : x \in \mathcal{C}_r, y \in \mathcal{C}_s\}$ counted according to multiplicities, then each element of $\mathcal{C}_t$ occurs exactly c_{rst} times in $\mathcal{C}_r\mathcal{C}_s$.
In other words, if we fix an element $g_t \in \mathcal{C}_t$, then c_{rst} is the number of solutions (g_r, g_s) of

$$g_r g_s = g_t, \quad g_r \in \mathcal{C}_r, g_s \in \mathcal{C}_s.$$

□

We have for $1 \leq i \leq k$,

$$\chi^i(\mathcal{C}_r^+) = \sum_{g_r \in \mathcal{C}_r} \chi^i(g_r) = h_r\chi^i_r.$$

Since $\mathcal{C}_r^+$ lies in the center of the group algebra FG ([LP10], Proposition 12.22), we have that $\rho^i(\mathcal{C}_r^+)$ commutes with $\{\rho^i(x) : x \in FG\}$. From Lemma 2.1 we deduce that $\rho^i(\mathcal{C}_r^+)$ is a scalar matrix, say,

$$\rho^i(\mathcal{C}_r^+) = \omega_r^i I, \quad \omega_r^i \in F, 1 \leq i, r \leq k.$$

Taking the traces gives

$$h_r \chi_r^i = d_i \omega_r^i,$$

so that

$$\omega_r^i = \frac{h_r \chi_r^i}{d_i}, \quad 1 \leq i, r \leq k. \tag{2.3}$$

Now applying ρ^i to both sides of Equation 2.2

$$\rho^i(\mathcal{C}_r)^+ \rho^i(\mathcal{C}_s^+) = \sum_{t=1}^{k} c_{rst} \rho^i(\mathcal{C}_t^+)$$

which yields

$$\omega_r^i \omega_s^i = \sum_{t=1}^{k} c_{rst} \omega_t^i. \tag{2.4}$$

From Equation 2.3 and Equation 2.4 we get the following result.

Lemma 2.2. *For any two conjugacy classes $\mathcal{C}_r$ and $\mathcal{C}_s$ of G, we have*

$$\left(\frac{h_r \chi_r^i}{d_i}\right)\left(\frac{h_s \chi_s^i}{d_i}\right) = \sum_{t=1}^{k} c_{rst} \frac{h_t \chi_t^i}{d_i}$$

where c_{rst} is as defined above.

Definition 2.3. *For $r = 1, \cdots, k$, let M_r be the $k \times k$ integer matrix with $(s,\, t)^{th}$ entry c_{rst}. The matrix M_r is known as the class multiplication matrix.*

Observe that, from Lemma 2.2, we get that the k column vectors

$$(h_1 \chi_1^i / d_i,\ h_2 \chi_2^i / d_i, \cdots, h_k \chi_k^i / d_i) \quad (i = 1, \cdots, k) \tag{2.5}$$

are the common eigenvectors for the matrices M_i $(i = 1, \cdots, k)$. From the orthogonality relations of characters we get that the vectors in Equation 2.5 are linearly independent.

Corollary 2.1. *For $i = 1, \cdots, k$, the vector*

$$\begin{pmatrix} h_1\chi_1^i/d_i \\ . \\ . \\ . \\ h_k\chi_k^i/d_i \end{pmatrix}$$

is an eigenvector for each of the matrices M_r and the corresponding eigenvalue is $h_r\chi_r^i/d_i$.

Proof. Let v be the column vector as given in the above equation. From the definition of M_r, it is of the form

$$M_r = \begin{pmatrix} c_{r11} & .. & c_{r1k} \\ . & \cdots & . \\ . & \cdots & . \\ . & \cdots & . \\ c_{rk1} & .. & c_{rkk} \end{pmatrix}$$

So we have,

$$\begin{pmatrix} c_{r11} & .. & c_{r1k} \\ . & \cdots & . \\ . & \cdots & . \\ . & \cdots & . \\ c_{rk1} & .. & c_{rkk} \end{pmatrix} . \begin{pmatrix} h_1\chi_1^i/d_i \\ . \\ . \\ . \\ h_k\chi_k^i/d_i \end{pmatrix} = \begin{pmatrix} \sum_{t=1}^k c_{r1t}\frac{h_t\chi_t^i}{d_i} \\ . \\ . \\ . \\ \sum_{t=1}^k c_{rkt}\frac{h_t\chi_t^i}{d_i} \end{pmatrix}$$

Using lemma 2.2 we write,

$$\begin{pmatrix} c_{r11} & .. & c_{r1k} \\ . & \cdots & . \\ . & \cdots & . \\ . & \cdots & . \\ c_{rk1} & .. & c_{rkk} \end{pmatrix} . \begin{pmatrix} h_1\chi_1^i/d_i \\ . \\ . \\ . \\ h_k\chi_k^i/d_i \end{pmatrix} = \frac{h_r\chi_r^i}{d_i} \begin{pmatrix} h_1\chi_1^i/d_i \\ . \\ . \\ . \\ h_k\chi_k^i/d_i \end{pmatrix}.$$

This gives us that v is a right eigenvector of M_r having eigenvalue $\frac{h_r\chi_r^i}{d_i}$. □

Definition 2.4. *For each conjugacy class $\mathcal{C}_j$ of G, we define*

$$\mathcal{C}_{j'} = \{g^{-1} : \ g \in \mathcal{C}_j\}.$$

Clearly $\mathcal{C}_{j'}$ is a conjugacy class, as $x \in \mathcal{C}_{j'} \Rightarrow x^{-1} \in \mathcal{C}_j$. So $g^{-1}x^{-1}g \in \mathcal{C}_j$, $\forall g \in G$. Then, $g^{-1}xg = (g^{-1}x^{-1}g)^{-1} \in \mathcal{C}_{j'}$. From our knowledge of character theory, we have that $\chi_{j'} = \overline{\chi_j}$.

Therefore, we get

$$\begin{aligned}\sum_{j=1}^{k}\frac{h_j\chi_j^i\chi_{j'}^i}{d_i^2} &= \frac{1}{d_i^2}\sum_{j=1}^{k}h_j|\chi_j^i|^2\\ &= \frac{|G|}{d_i^2}\langle\chi^i,\chi^i\rangle\\ &= \frac{|G|}{d_i^2}.\end{aligned}$$

2.1 The Algorithm

Burnside's algorithm for the computation of the character table is a direct result of Lemma 2.2 and Corollary 2.1. The steps included in it are:

`Step 1.` Calculate the group elements of G and the conjugacy classes, $\mathcal{C}_1, \cdots, \mathcal{C}_k$.

`Step 2.` Calculate the class multiplication coefficients c_{rst} and the matrices M_r $(r = 1, \cdots, k)$.

`Step 3.` For the matrices $M_1, \cdots, M_k$ find the set of k linearly independent vectors $\mathbf{v_i} = (v_{i1}, \cdots, v_{ik})$ for $i = 1, \cdots, k$. Each of which is an eigenvector for the matrix M_r. We normalize these vectors i.e. $v_{i1} = 1$ for each i by setting $\mathcal{C}_1 = \{1\}$ as $h_1\chi_1^i/d_i = 1$.

`Step 4.` We are now in the position to compute the degrees of the k irreducible representations of G. Now

$$\sum_{j=1}^{k}\frac{v_{ij}v_{ij'}}{h_j} = \sum_{j=1}^{k}\frac{h_j\chi_j^i\chi_{j'}^i}{d_i^2}.$$

Using Equation 2.5 and Equation 2.4, we get the degrees d_i for $i = 1, \cdots, k$.

`Step 5.` Once we get the degrees d_i, the character values χ_j^i can be simply computed using

$$\chi_j^i = \frac{v_{ij}d_i}{h_j} \quad (i, j = 1, \cdots, k).$$

See Appendix A for the implementation of the above mentioned algorithm in GAP.

Chapter 3

Dixon's Modification of Burnside's algorithm

We have seen the Burnside's algorithm for the computation of the character table. In this chapter we will discuss about the modifications made to Burnside's algorithm by Dixon which enable us to compute the character table for groups of higher order without any round-off error.

3.1 Remarks about Burnside's algorithm

The main steps involved in Burnside's algorithm for the computation of character table are:

- Computation of the class multiplication constants c_{rst}.
- Calculating the eigenvalues and eigenvectors associated with the class matrix M_i.

If the whole group and its conjugacy classes are known then the first step is easy, but for a large group this involves a computation of lots of data. The second step is the main hindrance in computation, as the exact computation of eigenvectors for a large matrix is extremely difficult and often results in significant *round-off errors*. Also, it should be noted that for theoretical investigations, character values are required to be in their algebraic form instead of their numerical values.

3.1.1 Implications of Dixon's modification

If we transpose the problem of computation of group characters from the field of complex numbers into field of integers modulo p, for some suitable prime p, then we can not only avoid *round-off errors* but also have faster computation of the character values. This translates the problem from numerical computation to symbolic computation, which helps in the following ways,

- Exact calculation of eigenvalues and eigenvectors, as there are no round-off errors.
- There are only p possibilities $0, \cdots, p-1$ for the eigenvalues.

Using this, Dixon[Dix67] was able to achieve faster computation of character tables for groups of order up to 1000 or so.

3.2 Transposing the problem to $\mathbb{Z}_p$

Let e be the exponent of G. If $g \in G$ is of order m, then from Proposition 1.2, we have that each character of g is the sum of m-th roots of unity. In particular, each character value is a sum of e-th roots of unity $(e \geq m)$. If ζ is a primitive e-th root of unity, then all character values of G lie in $\mathbb{Z}[\zeta]$, the ring of polynomials in ζ with integer coefficients.
From *Dirichlet's* theorem [Vin54] on primes in an arithmetic progression we have that there is a prime p such that e divides $p-1$, and then we can find an integer z such that $z^e \equiv 1$ (mod p).
We define a ring homomorphism $\theta : \mathbb{Z}[\zeta] \to \mathbb{Z}_p$, defined by

$$f(\zeta) \mapsto f(z) \pmod{p}$$

The homomorphism θ allows us to transpose our problem from $\mathbb{C}$ into the finite field $\mathbb{Z}_p$.
We also have that $h_i, d_i \;\; (i = 1, 2, \cdots, k)$ divide $|G|$. Therefore none of them is divisible by p. Thus we get that θ maps the set of the k vectors $(h_1\chi_1^i/d_i, \cdots, h_k\chi_k^i/d_i) \;\; i = 1, \cdots, k$ into a set of k vectors linearly independent over $\mathbb{Z}_p$. Since θ is a homomorphism it sends the matrices $M_r \;\; (r = 1, \cdots, k)$ to $M_r^{\mathbb{Z}_p} \;\; (r = 1, \cdots, k)$ and also that image of the k linearly independent vectors under θ will be the common eigenvectors for the matrices $M_1^{\mathbb{Z}_p}, \cdots, M_k^{\mathbb{Z}_p}$. The i-th of these eigenvectors has the eigenvalue $\theta(h_r\chi_r^i/d_i)$ for the matrix $M_r^{\mathbb{Z}_p}$ $(r = 1, \cdots, k)$. Hence, we can conclude that the Step 3 of Burnside's algorithm can be carried out in $\mathbb{Z}_p$. Futher, Steps 4 and 5 are carried out in the finite field and final step of *Dixon's algorithm* is concerned with getting $\chi_j^i \;\; (i, j = 1, \cdots, k)$ from $\theta(\chi_j^i)$.

3.3 Details of Dixon's method

In Dixon's algorithm, the calculations involved in the computing the eigenvectors are carried out in $\mathbb{Z}_p$. Let $\mathcal{V}$ be the vector space of all column k-vectors in Z_p. Starting with a matrix, say $M_r^{\mathbb{Z}_p}$, we compute the null space of $M_r^{\mathbb{Z}_p} - \lambda I$ for $\lambda = 0, 1, \cdots, p-1$, and if the null space is nonzero, we calculate a basis for it. In general, at the j-th stage, we have already calculated subspaces $\mathcal{V}_1, \cdots, \mathcal{V}_s$ of $\mathcal{V}$ where each $\mathcal{V}_i$ is a set of common eigenvectors of the matrices $M_1^{\mathbb{Z}_p}, \cdots, M_{k-1}^{\mathbb{Z}_p}$, together with the zero vector. Moreover, $\mathcal{V}$ is the direct sum $\mathcal{V}_1 \oplus \cdots \oplus \mathcal{V}_s$. Then, for each $\mathcal{V}_i$ of dimension > 1 consider the action of $M_j^{\mathbb{Z}_p} - \lambda I$ on $\mathcal{V}_i$ for $\lambda = 0, 1, \cdots, p-1$, and hence reduce $\mathcal{V}_i$ to sum of eigenspaces of $M_j^{\mathbb{Z}_p}$. This process terminates at the r-th stage if each $\mathcal{V}_i$ has dimension 1, and this always happen for some $r \leq k$. When this stage is reached we define v_i as the basis element of the one-dimensional space $\mathcal{V}_i$ with v_i normalized so that the first component is 1.

In order to compute the degree $d_i^2 (\bmod\, p)$ of the character χ_i, it is required that $p > 2d_i \ \ (i = 1, \cdots, k)$, so as to uniquely determine d_i. This condition can be satisfied if we set

$$p > 2\sqrt{|G|}$$

as we know that $|G| = \sum_i d_i^2$.

3.3.1 Recovering the complex characters

Let ζ be a fixed primitive e-th root of unity, and suppose that ρ is an irreducible representation of G with character χ of degree d. Now, for each $g \in G$, $\chi(g)$ is the sum of the d eigenvalues of $\rho(g)$, which are all e-th roots of unity. So we get that,

$$\chi(g) \ = \ \zeta^{\alpha_1} + \cdots + \zeta^{\alpha_d}$$

and also

$$\chi(g^n) \ = \ \zeta^{n\alpha_1} + \cdots + \zeta^{n\alpha_d} \text{ for } n = 0, 1, \cdots .$$

Lemma 3.1. *If ζ is any fixed primitive e-th root of unity, then for $t = 0, 1, \cdots$, we have that*

$$\sum_{j=0}^{e-1} \zeta^{jt} = \begin{cases} e & \textit{if } e \textit{ divides } t \\ 0 & \textit{otherwise} \end{cases}$$

Proof. Writing t as, $t = ae + r$, for some non-negative integers a and r. Then, we have that

$$\zeta^t = \zeta^{ae}.\zeta r = \zeta^r \ \ (0 \leq r < e).$$

`Case I.` If $r = 0$ then $e|t$, and from the above relation we get that $\zeta^t = 1$. So we have

$$\sum_{j=0}^{e-1} \zeta^{jt} = \sum_{j=o}^{e-1} 1 = e.$$

`Case II.` If $r \neq 0$, then

$$\begin{aligned}\sum_{j=0}^{e-1} \zeta^{jt} &= 1 + \zeta^r + \zeta^{2r} + \cdots + \zeta^{(e-1)r} \\ &= \frac{\zeta^e - 1}{\zeta^r - 1} = 0\end{aligned}$$

□

Using lemma 3.1 we get that ζ^α is an eigenvalue with multiplicity $m(\alpha)$ in $\rho(g)$, with

$$m(\alpha) = (1/e) \sum_{n=0}^{e-1} \chi(g^n)\zeta^{-\alpha n}. \tag{3.1}$$

Therefore,

$$\chi(g) = \sum_{\alpha=0}^{e-1} m(\alpha)\zeta^\alpha$$

where $m(\alpha)$ is as defined above. Under the homomorphism θ, as defined in the previous section we get

$$m(\alpha) \equiv (1/e) \sum_{n=0}^{e-1} \theta(\chi(g^n))\varepsilon^{-\alpha n} \pmod p, \tag{3.2}$$

where ε is the e-th root of unity in $\mathbb{Z}_p$. As $p > 2\sqrt{|G|}$, we get that $m(\alpha)$ is uniquely defined by Equation 3.2 and the condition that $0 \leq m(\alpha) \leq d < p$. Thus, recovering the complex characters involves finding integers $m_{ij\alpha}$ such that $0 \leq m_{ij\alpha} \leq p$ and

$$m_{ij\alpha} \equiv \left(\frac{1}{e}\right) \sum_{n=0}^{e-1} \theta(\chi^i_{j(n)})\varepsilon^{-\alpha n} \pmod p$$

$(i, j = 1, 2, \cdots, k;\ s = 0, 1, \cdots, e-1)$ where $j(n)$ is defined by $g \in \mathcal{C}_j \Leftrightarrow g^n \in \mathcal{C}_{j(n)}$. Then

$$\chi^i_j = \sum_{\alpha=0}^{e-1} m_{ij\alpha}\zeta^\alpha \quad (i, j = 1, 2, \cdots, k). \tag{3.3}$$

3.4 The Burnside-Dixon algorithm

From the above discussion the Burnside-Dixon algorithm for the computation of character tables can be summed as:

`Step 1.` Calculate the group elements and the conjugacy classes of the group G and let $C_1 = 1$.

`Step 2.` Compute the integral constants c_{rst} and the class matrices $M_r (r = 1, \cdots, k)$.

`Step 3.` Find a prime p such that $p > 2\sqrt{|G|}$ and $e \equiv 1(\text{mod } p)$.

`Step 4.` Let M_r^F be the matrix M_r mod p, a $k \times k$ matrix in $\mathbb{F}_p$. Find the set of k linearly independent eigenvectors for each M_r^F

`Step 5.` Find the character degrees using the k eigenvectors computed in step 4.

`Step 6.` Get the character values in the finite field $\mathbb{F}_p$.

`Step 7.` Recover the complex values of the characters.

Refer to Appendix B for the implementation of the above described algorithm in GAP.

Part II

Group Ring and central idempotents

Chapter 4

Group Rings

In this chapter we shall introduce the notion of group rings and study some of its properties. Algebraically, group ring is a free module and a ring at the same time, which can be constructed from any given group any given ring.

Let G be a group and R a ring. We denote by RG the set of all formal linear combinations of the form

$$\alpha = \sum_{g \in G} a_g g$$

where $a_g \in R$ and $a_g = 0$ almost everywhere, that is, only a finite number of coefficients are different form 0 in each of these sums. The element α of RG, is also written as:

$$\alpha = \sum_{g \in G} a(g) g.$$

It should be noted that we have not taken G to be necessarily a finite group, but all the sums have been assumed to be finite.

Definition 4.1. *For an element $\alpha = \sum_{g \in G} a_g g$ we define the support of α to be the subset $supp\,(\alpha)$ of elements in G such that*

$$supp\,(\alpha) = \{g \in G : \ \ a_g \neq 0\}.$$

It can be observed that two elements $\alpha = \sum_{g \in G} a_g g$ and $\beta = \sum_{g \in G} b_g g$ of RG are equal if and only if $a_g = b_g, \ \forall g \in G$.

Let $\alpha = \sum_{g \in G} a_g g$ and $\beta = \sum_{g \in G} b_g g$ be two elements in RG, then their sum $\alpha + \beta$ in RG is defined component wise as:

$$\left(\sum_{g \in G} a_g g \right) + \left(\sum_{g \in G} b_g g \right) = \sum_{g \in G} (a_g + b_g) g.$$

Given two elements $\alpha = \sum_{g \in G} a_g g$ and $\beta = \sum_{h \in G} b_h h$ in RG, we define the product

$$\alpha\beta = \sum_{g,h \in G} a_g b_h gh = \sum_{u \in G} c_u u,$$

where

$$c_u = \sum_{gh=u} a_g b_h.$$

With the above defined operations, we get that RG is a ring with a unit, namely the element $1 = \sum_{g \in G} u_g g$ where the coefficient corresponding to the unit element of the group is 1 and $u_g = 0$ for every other element $g \in G$. We can also define the product of an elements in RG by elements $\lambda \in R$ as

$$\lambda \left(\sum_{g \in G} a_g g \right) = \sum_{g \in G} (\lambda a_g) g.$$

Thus we get that, RG is an R-module. Moreover, if R is commutative then RG is an algebra over R.

Definition 4.2. *The set RG, with the operations defined above, is called the group ring of G over R. If R is commutative, then RG is also called the group algebra of G over R.*

Consider the embedding $\imath : G \to RG$ which assigns to each element $x \in G$ the element $\imath(x) = \sum_{g \in G} a_g g$, where $a_x = 1$ and $a_g = 0$ if $g \neq x$. With the embedding $\imath$, G may be regarded as a subset of RG. Moreover, we can also say that, *G is a basis of RG over R*. Similary, the ring R can be regarded as subring of RG, by considering the mapping $\nu : R \to RG$ given by $\nu(r) = \sum_{g \in G} a_g g$, where $a_{1_G} = r$ and $a_g = 0$ if $g \neq 1_G$.

Definition 4.3. *The homomorphism $\varepsilon : RG \to R$ given by*

$$\varepsilon \left(\sum_{g \in G} a_g g \right) = \sum_{g \in G} a_g$$

is called the augmentation mapping of RG and its kernel, denoted by $\triangle(G)$, is called the augmentation ideal of RG.

An element $\alpha = \sum_{g\in G} a_g g$ of RG belongs to $\triangle(G)$, if

$$\varepsilon(\alpha) = \varepsilon\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g = 0.$$

Thus α can be written as:

$$\alpha = \sum_{g\in G} a_g g - \sum_{g\in G} a_g = \sum_{g\in G} a_g(g-1).$$

Clearly, all elements of the form $g-1, g \in G$ belong to $\triangle(G)$. Thus, we get that the set $\{g-1, g\in G, g\neq 1\}$ is a set of generators of $\triangle(G)$ over R. Since the elements in the set $\{g-1, g\in G, g\neq 1\}$ are linearly independent we get that:

Proposition 4.1. *The set $\{g-1, g\in G, g\neq 1\}$ is a basis of $\triangle(G)$ over R.*

Thus, we have that, $\triangle(G) = \{\sum_{g\in G} a_g(g-1) : g\in G, g\neq 1, a_g \in R\}$, where finitely many coefficients a_g are different from 0.

4.1 Augmentation Ideals

Let $\mathcal{I}(RG)$ be the set of all left ideal of the group ring RG.

Definition 4.4. *Let H be a subgroup of G, then we denote by $\triangle_R(G,H)$ the left ideal of RG generated by $\{h-1 : h\in H\}$.*

$$\triangle_R(G,H) = \left\{\sum_{h\in H} \alpha_h(h-1) : \quad \alpha_h \in RG\right\}.$$

In case, the ring R is fixed, then we omit R and denote $\triangle_R(G,H)$, simply as $\triangle(G,H)$. Observe that, $\triangle(G,G)$ is same as $\triangle(G)$.

Let H be a subgroup G, then a *transversal*(denoted by τ) of H in G is a set of representatives of the left cosets of H in G. If $\tau = \{q_i\}_{i\in I}$, then every element $g\in G$ can be written uniquely, as $g = q_i h_i,\ \ q_i \in \tau,\ h_i \in H$.

Proposition 4.2. *The set $B_H = \{q(h-1) \ : \ q\in\tau, h\in H, h\neq 1\}$ is a basis of $\triangle_R(G,H)$ over R.*

Proof. First we show that the set B_H is linearly independent over R. Consider the linear combination $\sum_{i,j} r_{ij} q_i(h_j - 1) = 0,\ r_{ij} \in R$. We write

$$\sum_{i,j} r_{ij} q_i h_j = \sum_i \left(\sum_j r_{ij} \right) q_i.$$

For all values of j, we have that $h_j \neq 1$, thus all the members in the above equation have disjoint support. As elements of G are linearly independent over R, therefore, all the coefficients must be 0, that is, $r_{ij} = 0$, for all i, j.
For $g \in G$, $g = q_i h_j$, for some $q_i \in \tau$ and some $h_j \in H$. Then

$$g(h-1) = q_i h_j (h-1) = q_i(h_j h - 1) - q_i(h_j - 1).$$

Thus we have established that every element of the form $g(h-1)$, with $g \in G, h \in H$ can be expressed as a linear combination of elements in B_H. □

For a normal subgroup H of G the canonical homomorphism $\omega : G \to G/H$, we can extended to $\omega^* : RG \to R(G/H)$ such that

$$\omega^* \left(\sum_{g \in G} a(g) g \right) = \sum_{g \in G} a(g) \omega(g).$$

Proposition 4.3. *With the above defined notations, Ker*$(\omega^*) = \triangle(G, H)$.

Proof. The inclusion $\triangle(G, H) \subset \operatorname{Ker}(\omega^*)$ holds trivially.
Now, consider the transversal τ of H in G. Then every element $\alpha \in RG$ can be written as $\alpha = \sum_{i,j} r_{ij} q_i h_j,\ r_{ij} \in R,\ q_i \in \tau,\ h_j \in H$. Let $\bar{q_i}$ be the image of q_i in G/H, then we have that

$$\omega^*(\alpha) = \sum_i \left(\sum_j r_{ij} \right) \bar{q_i}.$$

Now, $\alpha \in \operatorname{Ker}(\omega^*)$ if and only if $\sum_j r_{ij} = 0$ for each i. So for $\alpha \in \operatorname{Ker}(\omega^*)$, we have

$$\begin{aligned} \alpha &= \sum_{i,j} r_{ij} q_i h_j - \sum_i \left(\sum_j r_{i,j} \right) q_i \\ &= \sum_{i,j} r_{ij} q_i (h_j - 1) \in \triangle(G, H). \end{aligned}$$

Thus, $\operatorname{Ker}(\omega^*) \subset \triangle(G, H)$. □

Remark 4.1. *For a normal subgroup H of G, $\triangle(G,H)$ is a two sided ideal of RG and*

$$\frac{RG}{\triangle(G,H)} \cong R(G/H).$$

Now given a left ideal $I \in \mathcal{I}(RG)$, consider the set

$$\nabla(I) = \{g \in G : g-1 \in I\}.$$

Observe that $\nabla(I)$ is a subgroup of G. If $g, h \in \nabla(I)$ then we can write $gh-1$ as,

$$gh-1 = g(h-1) + g - 1 \in I,$$

thus, $gh \in \nabla(I)$. Also if $g \in \nabla(I)$ then

$$g^{-1} - 1 = -g^{-1}(g-1) \in I$$

therefore $g^{-1} \in \nabla(I)$.
Moreover, if I is a two sided ideal then $\nabla(I)$ is a normal subgroup of G.

We have established two mappings between the set of subgroups of G, $\mathcal{S}(G)$ and the set $\mathcal{I}(RG)$. One using $\triangle(G,H)$ and the other using $\nabla(I)$. The following gives the relationship between the two mappings.

Proposition 4.4. *If $H \in \mathcal{S}(G)$, then $\nabla(\triangle(G,H)) = H$.*

Proof. For $h \in H$, we have that $h-1$ belongs to $\triangle(G,H)$. So $h \in \nabla(\triangle(G,H))$, hence $H \subset \nabla(\triangle(G,H))$.
Set $1 \neq g \in \nabla(\triangle(G,H))$, then $g-1 \in \triangle(G,H)$ and thus can be written as,

$$g-1 = \sum_{i,j} r_{ij} q_i (h_j - 1).$$

As 1 appears in the left hand side of the inequality it must also appear in the right hand side of the above equation. Therefore, one of the q_i must be equal to 1, say $q_1 = 1$. From similar argument, we have that there is an element of the form $r_{1j}(h_j - 1)$ in the right hand side of the equality.
As all elements of G in the right hand side of the equation are pairwise different, we must have $g = h_j \in H$. Hence, $\nabla(\triangle(G,H)) \subset H$. □

It should be noted that with an ideal $I \in \mathcal{I}(RG)$, $\triangle(G, \nabla(I)) \subset I$. To verify that equality need not hold, set $I = RG$, then $\nabla(RG) = \{g \in G : g-1 \in RG\} = G$, hence $\triangle(G, \nabla(RG)) = \triangle(G) \neq RG$.

4.2 Semisimplicity of Group Rings

In this section we would discuss about the simplicity and semisimplicity of group rings. We will give the necessary and sufficient conditions on R and G for the group ring RG to be semisimple.

Definition 4.5. *Given a group ring and a subset H of the group G. Then we shall denote by $\widetilde{H}$ the following element of RG:*

$$\widetilde{H} = \sum_{h \in H} h.$$

If $|H|$ is invertible in R then we shall denote by $\widehat{H}$ the following element of RG:

$$\widehat{H} = \frac{\widetilde{H}}{|H|}.$$

Definition 4.6. *Let X be a subset of a group ring RG. The left annihilator of X is given by,*

$$Ann_l\,(X) = \{\alpha \in RG : \alpha x = 0,\, \forall x \in X\}.$$

The right annihilator of X is defined as

$$\mathrm{Ann}_r\,(X) = \{\alpha \in RG : x\alpha = 0,\, \forall x \in X\}.$$

Lemma 4.1. *Let H be a subgroup of G and let R be a ring. Then $Ann_r\,(\triangle(G,H)) \neq 0$ if and only if H is finite. In this case,*

$$Ann_r\,(\triangle(G,H)) = \widetilde{H}.RG$$

Furthermore, if $H \lhd G$ then the element $\widetilde{H}$ is central in RG and we have

$$Ann_r(\triangle(G,H)) = Ann_l\,(\triangle(G,H)) = RG.\widetilde{H}.$$

Proof. First assume that $\mathrm{Ann}_r\,(\triangle(G,H)) \neq 0$ and choose $\alpha = \sum_{g \in G} a_g g \neq 0$ in $\mathrm{Ann}_r\,(\triangle(G,H))$. For each $h \in H$, we have $(h-1)\alpha = 0$, which gives $h\alpha = \alpha$. Thus, we get

$$\alpha = \sum_{g \in G} a_g g = \sum_{g \in G} a_g hg.$$

Now, take $g_o \in supp(\alpha)$, then $a_{g_o} \neq 0$, so the above equation shows that $hg_o \in supp(\alpha)$ for all $h \in H$. Since $supp(\alpha)$ is finite, this clearly gives us that H must be finite. From the above argument, we get that, for $g_o \in supp(\alpha)$, then the coefficient of every element of the form hg_o is equal to the coefficient of g_o, hence α can be written as:

$$\alpha = a_{g_o}\widetilde{H}g_o + a_{g_1}\widetilde{H}g_1 + \cdots + a_{g_t}\widetilde{H}g_t = \widetilde{H}\beta, \ \ \beta \in RG.$$

Thus, if H is finite, then $\mathrm{Ann}_r\,(\triangle(G,H)) \subset \widetilde{H}.RG$.
The reverse inclusion follows trivially, since $h\widetilde{H} = \widetilde{H}$, thus, we have, $(h-1)\widetilde{H} = 0$, for all $h \in H$.
Now, if $H \lhd G$, then for any $g \in G$, we have that $g^{-1}Hg = H$, therefore, $g^{-1}\widetilde{H}g = \sum_{x\in H} g^{-1}xg = \sum_{x\in H} x = \widetilde{H}$. Thus $\widetilde{H}g = g\widetilde{H}$, for all $g \in G$. Hence $\widetilde{H}$ is central in RG. Consequently, $RG.\widetilde{H} = \widetilde{H}.RG$ and the result follows. □

Remark 4.2. *Putting $H = G$ in the above lemma, we get*

$$Ann_l\,(\triangle(G)) = Ann_r\,(\triangle(G)) = R.\widetilde{G}. \tag{4.1}$$

Lemma 4.2. *Let I be a two-sided ideal of a ring R. Suppose that there exists a left ideal J such that $R = I \oplus J$ (as left R-modules). Then $J \subset Ann_r\,(I)$.*

Proof. Take arbitrary elements $x \in J$, $y \in I$. Since J is a left ideal and I is two-sided, we have that $yx \in J \cap I = (0)$. Consequently, $yx = 0$ and thus $x \in \mathrm{Ann}_r\,(I)$. □

Lemma 4.3. *If the augmentation ideal $\triangle(G)$ is a direct summand of RG as an RG-module then G is finite and $|G|$ is invertible in R.*

Proof. Assume that $\triangle(G)$ is a direct summand of RG. The from the previous lemma, we get that $\mathrm{Ann}_r\,(\triangle(G)) \neq 0$, and so G is finite. Also $\mathrm{Ann}_r\,(\triangle(G))$ $=\mathrm{Ann}_l\,(\triangle(G)) = \widehat{G}.RG = \widehat{G}.R$. Writing RG as $RG = \triangle(G) \oplus J$ with $J \subset R\widetilde{G}$ and $1 = e_1 + e_2$, with $e_1 \in \triangle(G)$ and $e_2 \in J$. Now

$$1 = \varepsilon(1) = \varepsilon(e_1) + \varepsilon(e_2).$$

Since $\varepsilon(e_1) = 1$ as $e_1 \in \triangle(G) = \mathrm{Ker}\,\varepsilon$ and $e_2 = a\widehat{G}$, for $a \in R$ and $a\varepsilon(\widehat{G}) = 1$, therefore, $a|G| = 1$. This gives us that $|G|$ is invertible in R, with $a = |G|^{-1}$. □

We now state *Maschke's Theorem*, which gives the conditions for the group ring RG to be semisimple. The proof is similar to the one in Theorem 1.1, (for details see [SM02] Pg-141).

Theorem 4.1. ***Maschke's Theorem*** *Let G be a group. Then the group ring RG is semisimple if and only if the following conditions hold.*

1. *R is semisimple.*

2. *G is finite.*

3. $|G|$ *is invertible in* R*.*

If $R = K$, then we have that K is always semisimple and $|G|$ is invertible in K if and only if $|G| \neq 0$ in K, that is , if and only if $char(K) \nmid |G|$. Thus we have that:

Corollary 4.1. *Let* G *be a finite group and let* K *be a field. Then* KG*, is semisimple if and only if* $char(K) \nmid |G|$*.*

Chapter 5

Primitive central idempotents of rational group algebras

The primitive central idempotents of $\mathbb{C}G$ are given by $\frac{\chi(1)}{|G|}\sum_{g\in G}\chi(g^{-1})g$, where χ is an irreducible character of G and 1 is the identity of G. In this chapter we will discuss about finding the primitive central idempotents in the rational group algebra of nilpotent groups G, using the some series of subgroups of G, as given by Jespers [EJ03], without using the character table.

5.1 Idempotents of RG

Recall that, if e is a central idempotent in R, then R can be decomposed as a direct sum

$$R = Re \oplus R(1-e).$$

We now observe the construction of central idempotents in the group ring RG.

Lemma 5.1. *Let R be a ring with unity and let H be a subgroup of a group G. If $|H|$ is invertible in R, then $e_H = \frac{1}{|H|}\widetilde{H}$ is an idempotent of RG. Moreover, if $H \lhd G$ then e_H is central.*

Proof. In order, to show that e_H is an idempotent, consider the product

$$\begin{aligned} e_He_H &= \frac{1}{|H|^2}\widetilde{H}\widetilde{H} = \frac{1}{|H|^2}(\sum_{h\in H} h)\widetilde{H} = \frac{1}{|H|^2}\sum_{h\in H}(h\widetilde{H}) \\ &= \frac{1}{|H|^2}\sum_{h\in H}\widetilde{H} = \frac{1}{|H|^2}|H|\widetilde{H} = e_H. \end{aligned}$$

In lemma 4.1, we have already established that $e_H = \widehat{H}$ is central in RG if $H \lhd G$. □

In order to compute idempotent e_H in `GAP` we first construct the embedding of a group G into the group ring RG given by

```
o:=Embedding(G,RG);
```

Once we have the embedding then $e_H = \widehat{H}$ is defined as:

Function `Hat` to compute the idempotent $e_H = \widehat{H}$

```
Hat:=function(H,emb)
  local x;;
  return Sum(List(Elements(H), x-> x^emb))/Order(H);;
end;
```

We now give the decomposition of RG using one of the idempotent.

Proposition 5.1. *Let R be a ring and H be a normal subgroup of G. If $|H|$ is invertible in R, then we have*

$$RG = RGe_H \oplus RG(1 - e_H)$$

where

$$RGe_H = R(G/H) \text{ and } RG(1 - e_H) = \triangle(G, H).$$

Proof. From the above lemma, we have shown that e_H is central in RG, so it is clear that $RG = RGe_H \oplus RG(1 - e_H)$.

In order to see $RGe_H = R(G/H)$, we shall first show that $G/H \simeq Ge_H$. Consider the map $\phi : G \to Ge_H$ given by $g \mapsto ge_H$. Clearly, ϕ is a group homomorphism, with $\operatorname{Ker}(\phi) = H$, and therefore $Ge_H \simeq G/H$. As Ge_H is a basis of RGe_H over R, we have that $RGe_H \simeq R(G/H)$.

From Lemma 4.2, we get that $RG(1-e_H)$ is the annihilator of RGe_H and from Lemma 4.1, we get that $\operatorname{Ann}(RGe_H) = \triangle(G, H)$. □

Definition 5.1. *Let R be a ring and G be finite group, such that $|G|$ is invertible in R. The idempotent $e_G = \frac{1}{|G|}\sum_{g\in G} g = \frac{1}{|G|}\widetilde{G}$ is called the principal idempotent of RG.*

Using e_G in the previous proposition, we get that

$$RG = R \oplus \triangle(G). \tag{5.1}$$

Lemma 5.2. *Let R be a commutative ring and let I be an ideal of a group algebra RG. Then, the quotient ring RG/I is commutative if and only if $\triangle(G, G') \subset I$, where G' is the commutator subgroup of G.*

Proof. Let I be an ideal in RG such that RG/I is commutative. Then $\forall g, h \in G$ we have that $gh - hg \in I$, so $hg(g^{-1}h^{-1}gh - 1) \in I$. Since hg is invertible in RG, we get that $g^{-1}h^{-1}gh - 1 = (g, h) - 1 \in I$. Thus, we get that $\triangle(G, G') \subset I$.
Conversely, $gh - hg = hg((g, h) - 1) \in \triangle(G, G')$, if $\triangle(G, G') \subset I$, then we have that $gh = hg \pmod{I}$, for all $g, h \in G$ and hence RG/I is commutative. □

We use the above result to give the decomposition of the semisimple group algebra RG using the idempotent $e_{G'}$.

Proposition 5.2. *Let RG be a semisimple group algebra. Then we can write RG as a direct sum*

$$RG = RGe_{G'} \oplus \triangle(G, G'),$$

where $RGe_{G'}$ is the sum of all commutative simple components of RG and $\triangle(G, G')$ is the sum of all the others.

Proof. From Proposition 5.1, we already have that $RG = RGe_{G'} \oplus \triangle(G, G')$, and that $RGe_{G'} \simeq R(G/G')$. Clearly $RGe_{G'}$ is commutative, in order to complete the proof, it is enough to show that there is no commutative simple components in $\triangle(G, G')$.
We prove this by way of contradiction, suppose that we can decompose $\triangle(G, G')$ as, $\triangle(G, G') = A \oplus B$, where A is a commutative simple component and B is its complement. Then, $RG = RGe_{G'} \oplus A \oplus B$ so we have that $RG/B \simeq RGe_{G'} \oplus A$ is commutative. Now using Lemma 5.2, we get that $\triangle(G, G') \subset B$, which gives us a contradiction. □

5.2 Idempotents in the rational group algebra of finite nilpotent groups

If e is a primitive central idempotent of $\mathbb{Q}G$, then $G_e = \{g \in G : \ eg = e\}$. Observe that, G_e is a normal subgroup of G, as from the centrality of e we have that for any $h \in G$ and $g \in G_e$, we have

$$e.h^{-1}gh = h^{-1}(eg)h = h^{-1}eh = e.$$

Also,

$$e\widehat{G_e} = \frac{1}{|G_e|} \sum_{g \in G_e} eg = e,$$

therefore we get that e is a primitive central idempotent of $(\mathbb{Q}G)\widehat{G_e} \cong \mathbb{Q}(G/G_e)$.
If $G \neq \{1\}$, then we define

$$\varepsilon(G) = \prod_{M \in \mathcal{M}(G)} (1 - \widehat{M}),$$

where $\mathcal{M}(G)$ is the set of all minimal normal subgroups of G and set $\varepsilon(\{1\}) = 1$.
For a normal subgroup N of G, let M be subgroup of G containing N and $\overline{M}$ denote the factor group M/N. Now, if $N \neq G$, then we write

$$\varepsilon(G, N) = \prod_{\overline{M} \in \mathcal{M}(G/N)} (\widehat{N} - \widehat{M}) = \widehat{N} \prod_{\overline{M} \in \mathcal{M}(G/N)} (1 - \widehat{M}).$$

With the above notation, we agree that $\varepsilon(G, G) = \widehat{G}$. Thus we get,

$$\varepsilon(G, N) = \begin{cases} \widehat{G} & \text{if } N = G \\ \widehat{N} \prod_{\overline{M} \in \mathcal{M}(G/N)} (1 - \widehat{M}) & \text{if} N \neq G. \end{cases}$$

Remark 5.1. *Both $\varepsilon(G)$ and $\varepsilon(G, N)$ are central idempotents of $\mathbb{Q}G$.*

This can be implemented in GAP using the Hat function defined in section 5.1 by defining a function Epsilon having parameters: the group G, the normal subgroup N of G, the algebra $\mathbb{Q}G$ and the embedding of the group G into $\mathbb{Q}G$.

Function Epsilon to compute $\varepsilon(G, N)$

```
Epsilon:=function(G,N,emb,alg)
  local H, min,MinG, ele, M,phi,list;
  if N = G then
    return Hat(N,emb);;
  else
    H:=FactorGroup(G,N);;
    list:=[Hat(N,emb)];;
    min:=MinimalNormalSubgroups(H);;
    MinG:=MinimalNormalSubgroups(G);;
    phi:=NaturalHomomorphismByNormalSubgroup(G,N);;
    for M in MinG do
      if ImagesSet(phi,M) in min then
        Add(list,(One(alg) - Hat(M,emb)));;
      fi;;
    od;;
    return Product(list);;
  fi;;
end;
```

Using Proposition 5.1, we get $(\mathbb{Q}G)\widehat{N} \cong \mathbb{Q}(G/N)$, it is clear $\varepsilon(G, N)$ is the pre-image of $\varepsilon(G/N)$ in $\mathbb{Q}(G/N)$. Expressing a primitive central idempotent e of $\mathbb{Q}G$ as an orthogonal sum $e = e\widehat{N} + e(1 - \widehat{N})$, gives us, $e = e\widehat{N}$ or $e = e(1 - \widehat{N})$, because of the primitivity of e. Clearly, $e = e\widehat{N}$ if and only if $N \subseteq G_e$.

We now begin to construct primitive central idempotents of $\mathbb{Q}G$, using the method discussed in [EJ03].

Lemma 5.3. *Let e be a primitive central idempotent of $\mathbb{Q}G$, where G is a finite group. Then $G_e = \{1\}$ if and only if $\varepsilon(G)e = e$. Moreover, G has a faithful irreducible representation if and only if $\varepsilon(G) \neq 0$.*

Proof. Assume that $G_e = \{1\}$, then $\varepsilon(G)e \neq 0$ is a central idempotent of $\mathbb{Q}Ge$. Since e is a primitive central idempotent, it is the only central idempotent in $\mathbb{Q}G_e$, so $\varepsilon(G)e = e$.
Conversely, assume $\varepsilon(G)e = e$, then $\varepsilon(G) \neq 0$. Now, for all $M \in \mathcal{M}(G)$, $e\overline{M} \neq e$. Thus, for all $M \in \mathcal{M}(G)$, $M \nsubseteq G_e$. Since G_e is a normal subgroup of G and G is finite, G_e, has to be $\{1\}$, for otherwise G_e should be either minimal itself or either contain a minimal normal subgroup.

We now prove the second part of the lemma. Let $\{e_1, \cdots, e_n\}$ be the primitive central idempotents of $\mathbb{C}G$, with $\mathbb{C}Ge_i = L_{i1} \oplus \cdots \oplus L_{ir_i}$, direct sum of $\mathbb{C}G$-modules. The irreducible representation $\rho : G \to GL(L_{i1})$ given by $g \mapsto (\alpha e_i \mapsto \alpha e_i g)$ is faithful if and only if $G_{e_i} = \{1\}$. Also, $\varepsilon(G) \sum_{i=1}^{n} e_i = \varepsilon(G) \neq 0$ if and only if there exists a primitive central idempotent e_i of $\mathbb{C}G$ such that $\varepsilon(G)e_i \neq 0$. Since e_i is the only central idempotent of $\mathbb{C}Ge_i$, so the previous statement is true if and only if $\varepsilon(G)e_i = e_i$. This holds if and only if $G_{e_i} = \{1\}$, which is equivalent to ρ being faithful. □

Let $\mathcal{Z}(G)$ be the center of group G and $\mathcal{Z}_i(G)$ be the ith center of G. We now determine the condition when $\varepsilon(G) \neq 0$.

Proposition 5.3. *If G has a faithful representation, then $\mathcal{Z}(G)$ is cyclic.*

Proof. See Proposition 9.16 of [JL93] □

Lemma 5.4. *Let G be a finite group. If $\varepsilon(G) \neq 0$, then $\mathcal{Z}(G)$ is cyclic. The converse holds if G is a finite nilpotent group.*

Proof. If $\varepsilon(G) \neq 0$ then by Lemma 5.3, G has a faithful representation. Now Proposition 5.3 gives us that $\mathcal{Z}(G)$ is cyclic.

Conversely, assume that G is nilpotent and $\mathcal{Z}(G)$ is cyclic with size m. As $\varepsilon(1) = 1$, we may also assume that $G \neq \{1\}$. Let $A_1, \cdots, A_n$ be the minimal normal subgroups of G. Since for nilpotent groups, any non trivial normal subgroup intersects the center non trivially. Thus each A_i is also the minimal normal subgroup of $\mathcal{Z}(G)$. So each A_i has to be cyclic of prime order and central, so $A_i = \langle g^{o(g)/p_i} \rangle$, where p_i is a prime divisor of $o(g)$. Now $\varepsilon(G) = \prod_{i=1}^{n}(1 - \widehat{A_i}) \neq 0$. If $\varepsilon(G) = 0$, then

$$\varepsilon(G) = \prod_{p|m} \left(1 - \frac{1}{p} - \frac{g^{\frac{m}{p}}}{p} - \cdots - \frac{g^{\frac{m(p-1)}{p}}}{p} \right) = 0,$$

which gives us that the coefficient of identity in G must be 0. But

$$\prod_{p|m} \frac{p-1}{p} \neq 0$$

and

$$g^{\frac{k_1 m}{p_1}} \cdots g^{\frac{k_j m}{p_j}} = g^{\sum_{i=1}^{j} \frac{k_i m}{p_i}}$$

never equals the identity since m is not a divisor of $\sum_{i=1}^{j} \frac{k_i m}{p_i}$. □

We now give the description of the primitive central idempotents in the rational group algebra of a finite abelian group.

Corollary 5.1. *Let G be a finite abelian group. The primitive central idempotents of $\mathbb{Q}G$ are precisely all the elements of the form $\varepsilon(G, N)$, where N a subgroup of G such that G/N is cyclic. Further, if e is a primitive idempotent of $\mathbb{Q}G$, then Supp(e) is a subgroup of G, and e is a linear combination of idempotents of the form $\widehat{H}$, where H is a subgroup of G.*

Proof. First, we verify the result for finite cyclic groups. Let $A = \langle a \rangle$, be a finite cyclic group, then $\varepsilon(A)$ is a central idempotent of $\mathbb{Q}A$. Now, $\mathbb{Q}A\varepsilon(A) = \mathbb{Q}(a\varepsilon(A)) \simeq^{\phi} \mathbb{Q}(\xi_{|A|})$, where ϕ is given by $a\varepsilon(A) \mapsto \xi_{|A|}$, ($\xi_{|A|}$ is a $|A|^{th}$-primitive root of unity). Therefore, $\mathbb{Q}A\varepsilon(A)$ is a field and $\varepsilon(A)$ is primitive central idempotent of $\mathbb{Q}A$.

Now for a finite abelian group G, if N is a subgroup such that G/N is cyclic, then $\varepsilon(G, N)$ is a primitive central idempotent of $\mathbb{Q}(G/N) \simeq (\mathbb{Q}G)\widehat{N}$. Therefore, all elements of the form $\varepsilon(G, N)$ with N a subgroup of G such that G/N is cyclic are primitive central idempotents of $\mathbb{Q}G$.

If e is a primitive central idempotent of $\mathbb{Q}G$, then by Lemma 5.3 and 5.4, $\varepsilon(G/G_e)\overline{e} = \overline{e}$ and $\mathcal{Z}(G/G_e) = G/G_e$ is cyclic, where $\overline{e}$ is the image of the idempotent e in $\mathbb{Q}G\widehat{G_e} \cong \mathbb{Q}(G/G_e)$. Thus, we have that $\varepsilon(G/G_e)$ is a primitive central idempotent of $\mathbb{Q}(G/G_e)$, hence $\overline{e}$ is central idempotent in $\mathbb{Q}(G/G_e)\varepsilon(G/G_e)$. Thus, $\overline{e} = \varepsilon(G/G_e)$. Hence, it follows that $e = \varepsilon(G, G_e)$.

Now, let e be a primitive central idempotent of $\mathbb{Q}G$, then $e = \varepsilon(G, N)$, for some subgroup N of G such that G/N is cyclic. Thus, e is $\mathbb{Z}$-linear combination of elements of the form $\widehat{N}\widehat{M_1}\cdots\widehat{M_n}$, with $M_i/N \in \mathcal{M}(G/N)$, so $M_i \cap M_j = N$. Let $\mathcal{T}_i$ be the transversal for N in M_i. Since $\widehat{N}\widehat{N} = \widehat{N}$, it is easy to see that $\widehat{N}\widehat{M_1}\cdots\widehat{M_n} = \langle N, \widehat{\mathcal{T}_1, \cdots}, \mathcal{T}_n\rangle$, where $\langle N, \mathcal{T}_1, \cdots, \mathcal{T}_n\rangle$ is a subgroup of G.
We now consider *supp*(e). Suppose $\mathcal{M}(G/N) = \{M_1, \cdots, M_m\}$, we claim that *supp*$(e) = \langle N, \mathcal{T}_1, \cdots, \mathcal{T}_n\rangle$, a subgroup of G. It is clear that *supp*(e) is a subset of $\langle N, \mathcal{T}_1, \cdots, \mathcal{T}_n\rangle$. Since $\mathcal{T}_i$ are the transversals for N of groups which coincide only in N, so terms of the form $nt_1 \cdots t_m \in \langle N, \mathcal{T}_1, \cdots, \mathcal{T}_n\rangle$ cannot disappear in the summand of e. It can be shown that by induction on m that if, $nt_1 \cdots t_m = n't'_1 \cdots\ t'_m$, then necessarily $n = n', t_1 = t'_1, \cdots, t_m = t'_m$. □

Implementing the above corollary using `GAP`

Computing the primitive central idempotents of $\mathbb{Q}G$, G being a finite abelian group

```
GetPrimCenIdem:=function(G, list, emb, alg)
  local GModNCyclic, N, idem;;
  GModNCyclic:=[];;
  idem:=[];;
  for N in list do
    if IsCyclic(G/N) then
      Add(GModNCyclic,N);;
    fi;
  od;;
  for N in GModNCyclic do
    Add(idem,Epsilon(G,N, emb, alg));;
  od;
  return idem;
end;
```

Here we aim to show the generalization of the above corollary to all nilpotent groups. Let $\mathcal{C}_g$ be the conjugacy class of an element $g \in G$, it is known that the elements $\widehat{\mathcal{C}_g}$ $g \in G$ form the $\mathbb{Q}$-basis of the center of $\mathbb{Q}G$. Also let $(g, h) = g^{-1}h^{-1}gh$ be the commutator of g and h in G and $C_S(G)$ be the centralizer of a subset S of a group G.

Lemma 5.5. *Let G be a finite group 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 $\widehat{\mathcal{C}_g} = \widehat{\mathcal{C}_g}\widehat{\langle z\rangle}$.*

Proof. By assumption there exists $h \in G$ and $1 \neq z \in \mathcal{Z}(G)$ so that $h^{-1}gh = zg$. So, for any positive integer we have that $h^{-n}gh^n = z^n g$. It then follows that $\langle z\rangle\mathcal{C}_g \subseteq \mathcal{C}_g$.

Thus, $\langle z\rangle\mathcal{C}_g = \mathcal{C}_g$, therefore, $\widehat{\mathcal{C}_g} = \widehat{\mathcal{C}_g}\widehat{\langle z\rangle}$. Clearly, we may replace z with any power of z, if necessary, we may assume that z has prime order. □

Proposition 5.4. *Let G be a finite group and $e \in \mathbb{Q}G$. If e is a primitive central idempotent of $\mathbb{Q}G$ with G_e trivial then e is the sum of all G-conjugates of a primitive central idempotent e_1 in $\mathbb{Q}G_1$, where $G_1 = C_G(\mathcal{Z}_2(G))$, and $\cap_{g\in G}((G_1)_{e_1})^g = \{1\}$. The converse holds if G is nilpotent. In particular, for any primitive central idempotent e with G_e trivial, Supp$(e) \subseteq C_G(\mathcal{Z}_2(G))$.*

Proof. Suppose $e \in \mathbb{Q}G$ is a primitive central idempotent with $G_e = \{1\}$. Write $e = \sum_{g\in G}\alpha_g\widehat{\mathcal{C}_g}$, with each $\alpha_g \in \mathbb{Q}$. Using Lemma 5.5, we have that for any $g \in G$ with $g \notin C_G(\mathcal{Z}_2)$, there exists a non-trivial central element $w_g \in G$ of prime order such that $\widehat{\mathcal{C}_g} = \widehat{\mathcal{C}_g}\widehat{\langle w_g\rangle}$. As w_g is of prime order, we get that $\langle w_g\rangle$ is a minimal normal subgroup of G, so $\langle w_g\rangle \in \mathcal{M}(G)$. Then

$$\varepsilon(G)\widehat{\langle w_g\rangle} = \left(\prod_{M\in\mathcal{M}(G)}(1-\widehat{M})\right).\langle w_g\rangle = 0.$$

Thus e can be expressed as

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

Since $G_e = \{1\}$, Lemma 5.3 gives us that $e = e\varepsilon(G)$ and $\varepsilon(G)\widehat{\langle w_g\rangle} = 0$ we get that

$$e = e\varepsilon(G) = \sum_{g\in C_G(\mathcal{Z}_2)}\alpha_g\widehat{\mathcal{C}_g}\varepsilon(G).$$

We have thus established that

$$e = e\varepsilon(G) = \sum_{g\in C_G(\mathcal{Z}_2)}\alpha_g\widehat{\mathcal{C}_g}.\varepsilon(G).$$

So we have shown that *Supp*$(e) \subseteq G_1 = C_G(\mathcal{Z}_2(G))$. Note that e is not necessarily a primitive central idempotent of $\mathbb{Q}G_1$. We have that e is a central idempotent in $\mathbb{Q}G_1$. Therefore e can be expressed as a sum of primitive central idempotents of $\mathbb{Q}G_1$. Writing e as

$$e = e_1 + \cdots + e_k,$$

where e_i $(1 \le i \le k)$ is a primitive central idempotent in $\mathbb{Q}G_1$. Now from the standard argument we get that

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

the sum of all G-conjugates of a primitive central idempotent $e_1 \in \mathbb{Q}G_1$. Since e_1 is a primitive central idempotent of $\mathbb{Q}G_1$, for $h \in (G_1)_{e_1}$, we have $he_1 = e_1h$, therefore $g_i(he_1)g_i = g_i^{-1}e_1g_i = e_1^{g_i}$, which gives us $((G_1)_{e_1})^{g_i} = (G_1)_{e_1^{g_i}}$. Hence, it follows that $\cap_{i=1}^{n}((G_1)_{e_1})^{g_i} = G_e = \{1\}$, which proves the necessity of the conditions.
Conversely, assume that G is a finite nilpotent group and suppose e_1 is a primitive central idempotent of $\mathbb{Q}G_1$ with $G_1 = C_G(\mathcal{Z}_2(G))$ and assume $\cap_{g\in G}((G_1)_{e_1})^g = \{1\}$. Let $e = e_1^{g_1} + \cdots + e_1^{g_n}$ be the sum of all G-conjugates of e_1. It is clear that e is a central idempotent of $\mathbb{Q}G$ and $G_e = \{1\}$. We write $e = f_1 + \cdots + f_k$, a sum of primitive central idempotents of $\mathbb{Q}G$. Note that for any non-trivial central subgroup N of G, either $\widehat{N}e_1 = 0$ or $\widehat{N}e_1 = e_1$. However the latter is possible as it implies $N \subseteq (G_1)_{e_1}$ and thus

$$N \subseteq \cap_{g\in G}((G_1)_{e_1})^g = \{1\}.$$

So we get that $\widehat{N}e_1 = 0$ and thus $\varepsilon(G)e_1 = e_1$. Consequently, $\varepsilon(G)e = e$ and thus $\varepsilon(G)f_1 = f_1$. Therefore $G_{f_1} = \{1\}$ and thus by the first part of the proof, $f_1 \in \mathbb{Q}G_1$.
Hence $e = f_1$ is a primitive central idempotent of $\mathbb{Q}G$. □

We now move on to give the main result of [EJ03].

Theorem 5.1. *Let G be a finite nilpotent group. The primitive central idempotents of $\mathbb{Q}G$ are precisely all elements of the form*

$$\sum_g (\varepsilon(G_m, H_m))^g,$$

(the sum of all G-conjugates of $\varepsilon(G_m, H_m)$), where H_m and G_M are subgroups of G that satisfy all of the following properties:

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

Proof. We first aim to prove that the properties listed in the theorem are sufficient for $e = \sum_g(\varepsilon(G_m, H_m))^g$ to be a primitive central idempotent of $\mathbb{Q}G$. As a consequence of Corollary 5.1, properties (2) and (3) we get that $f_m = \varepsilon(G_m, H_m)$ is a primitive central idempotent of $\mathbb{Q}(G_m/H_m) \cong (\mathbb{Q}G_m)\widehat{H_m}$. Thus, f_m is a primitive central idempotent of $\mathbb{Q}G_m$. It should be noted that $H_m = (G_m)_{f_m}$, and by property (4), $G_m \lhd G_{m-1}$. Using the proof of Proposition 5.4 we get, $f_{m-1} = \sum_{g\in G_{m-1}} f_m^g$ (the sum of all distinct G_{m-1}-conjugates of f_m), is a central idempotent of $\mathbb{Q}G_{m-1}$. Property of (5) gives us that,

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

Proposition 5.4 and properties (2), (4) and (5) then imply that f_{m-1} is a primitive central idempotent of $\mathbb{Q}G_{m-1}(\widehat{H_{m-1}}) \cong \mathbb{Q}(G_{m-1}/H_{m-1})$. Therefore, a primitive central idempotent of $\mathbb{Q}G_{m-1}$. Repeating the above argument on $f_{m-2} = \sum_{g\in G_{m-2}} f_{m-1}^g$, the sum of all G_{m-2}-conjugates of f_{m-1} and that f_{m-2} is a primitive central idempotent of $\mathbb{Q}G_{m-2}$. By induction, we obtain that $f_0 = e$ is a primitive central idempotent of $\mathbb{Q}G$.
Conversely, let e be a primitive central idempotent of $\mathbb{Q}G$. Then $G_e\,(=\ H_0\,)$ is a normal subgroup of $G_0 = G$. Now, e is a primitive central idempotent of $\mathbb{Q}G\widehat{H_0} \cong \mathbb{Q}(G_0/H_0)$. Clearly $(G_0/H_0)_e = (G/G_e)_e = \{1\}$. If G_0/H_0 is abelian then from Corollary 5.1 we that G_0/H_0 is cyclic and $e = \varepsilon(G_0, H_0)$, as desired. Now suppose that G_0/H_0 is not abelian, then from Lemma 5.3 and 5.4 and Proposition 5.4, $\mathcal{Z}_2(G_0/H_0)$ is cyclic and e is the sum of all G_0/H_0-conjugates of a primitive central idempotent $e_1 \in \mathbb{Q}(G_1/H_0)$, where G_1 is a subgroup of G so that $G_1/H_0 = C_{G_0/H_0}(\mathcal{Z}_2(G_0/H_0)) \neq G_0/H_0$, and $\cap_{x\in G_0/H_0}(H_1/H_0)_{e_1}^x = \{1\}$, with H_1 the subgroup of G containing H_0 so that $H_1/H_0 = (G_1/H_0)_{e_1}$. So H_1 is a normal subgroup of G_1 and $\mathcal{Z}(G_1/H_1)$ is cyclic. It should be noted that the nilpotency class of G_1/H_0 is smaller than that of G. If G_1/H_0 is abelian then we know that $e_1 = \varepsilon(G_1, H_1)$ and thus the result follows.
But if G_1/H_0 is not abelian then the result follows by induction on the nilpotency class of G. □

Remark 5.2. *It follows from the proof that the distinct conjugates of $\varepsilon(G_m, H_m)$ are mutually orthogonal.*

We have used Theorem 5.1 to compute the primitive central idempotents of $\mathbb{Q}G$, when G is a finite nilpotent group. To see the implementation of Theorem 5.1 see Appendix C.

Part III

Appendix

Appendix A

GAP implementation of Burnside's algorithm

The following code demonstrates the implementation of Burnside's algorithm. The program computes the character table of symmetric group of order 4, S_4.

```
#Define group here.#
G:=SymmetricGroup(4);;

#Group Structure.#
time1:=Runtime();;
n:=Order(G);;
CC:=ConjugacyClasses(G);;
cc:=List(CC, Representative);;
k:=Length(CC);;

# Finding the size of the conjugacy classses.#
h:=[];;
for i in [1..k] do
   l:=Size(CC[i]);;
   Add(h,l);;
od;

# Function to find the class multiplication coefficients.#
cmc:=function(r,s,t, cc, CC)
   local z, CCl, els, g, gi, p,rlist, count;;
   z:=cc[t];;
```

```
    CCl:=CC[s];;
    els:=Elements(CCl);;
    rlist:=[];;
    for g in els do
      gi:=Inverse(g);;
      p:=z*gi;;
      Add(rlist,p);;
    od;
    count:=0;
    for g in CC[r] do
      if g in rlist then
        count:=count+1;;
      fi;
    od;
    return count;
  end;

# Function to find the inverse conjugacy class.#
  InverseClass:=function(x,G)
    local invcl, invx, cl, g,invg;
    cl:=ConjugacyClass(G,x);
    invcl:=[];
    for g in cl do
      invg:=Inverse(g);
      Add:=(invcl,invg);
    od;
    return invcl;
  end;

# Computation of the class matrices M_r.#
M:=[];;
  for r in [1..k] do
    m:=[];;
    i:=1;;
    while i<=k do
      j:=1;;
      l:=[];;
      while j<=k do
      Add(l, cmc(r,i,j,cc,CC));;
      j:=j+1;;
    od;
    Add(m,l);;
    i:=i+1;;
  od;
  Add(M,m);;
od;

# Computing the eigen vectors for the mtrices M[1],...,M[k].#
eigvec:=[];;
for i in [1..k] do
  e:=Eigenvectors(Rationals, TransposedMat(M[i]));
  Add(eigvec, e);;
od;

# Computing the character degrees.#
d:=[];;
# Now take the eigen vectors of the class matrix M[2].#
eig2:=eigvec[2];;
for i in [1..k] do
  sum:=0;;
  for j in [1..k] do
    sum:=sum+(eig2[i][j]*ComplexConjugate(eig2[i][j]))/h[j];;
  od;
  Add(d,Sqrt(n/sum));;
od;

# Computation of the character values.#
tbl:=[];;
for i in [1..k] do
  chi:=[];;
  for j in [1..k] do
    chiIJ:=(eig2[i][j]*d[i])/h[j];;
    Add(chi,chiIJ);
  od;
  Add(tbl, chi);
od;
```

```
# Displaying the character table.#
CharTbl:=function(tbl,CC,cc,h)
   Print("\n\n");
   Print(CC,"\n");;
   Print(h,"\n");;
   Display(tbl);;
end;
CharTbl(tbl,CC,cc,h);
time2:=Runtime();;
Print("\nEstimated␣runtime:", StringTime(time2-time1), "\n");
```

For S_4, the class matrices are :

```
         [ [  1,  0,  0,  0,  0 ],
           [  0,  1,  0,  0,  0 ],
  M[1] =   [  0,  0,  1,  0,  0 ],
           [  0,  0,  0,  1,  0 ],
           [  0,  0,  0,  0,  1 ] ]

         [ [  0,  1,  0,  0,  0 ],
           [  6,  0,  2,  3,  0 ],
  M[2] =   [  0,  1,  0,  0,  2 ],
           [  0,  4,  0,  0,  4 ],
           [  0,  0,  4,  3,  0 ] ]

         [ [  0,  0,  1,  0,  0 ],
           [  0,  1,  0,  0,  2 ],
  M[3] =   [  3,  0,  2,  0,  0 ],
           [  0,  0,  0,  3,  0 ],
           [  0,  2,  0,  0,  1 ] ]

         [ [  0,  0,  0,  1,  0 ],
           [  0,  4,  0,  0,  4 ],
  M[4] =   [  0,  0,  0,  3,  0 ],
           [  8,  0,  8,  4,  0 ],
           [  0,  4,  0,  0,  4 ] ]

         [ [  0,  0,  0,  0,  1 ],
           [  0,  0,  4,  3,  0 ],
M[5] = [  0,  2,  0,  0,  1 ],
       [  0,  4,  0,  0,  4 ],
       [  6,  0,  2,  3,  0 ] ]
```

The above mentioned code give the character table of S_4 in about 200 ms. The table is given by:

```
# Conjugacy classes of G. #
[ ConjugacyClass( SymmetricGroup( [ 1 .. 4 ] ), () ),
  ConjugacyClass( SymmetricGroup( [ 1 .. 4 ] ), (1,2) ),
  ConjugacyClass( SymmetricGroup( [ 1 .. 4 ] ), (1,2)(3,4) ),
  ConjugacyClass( SymmetricGroup( [ 1 .. 4 ] ), (1,2,3) ),
  ConjugacyClass( SymmetricGroup( [ 1 .. 4 ] ), (1,2,3,4) ) ]
# Size of classes. #
[ 1, 6, 3, 8, 6 ]
# The character table as a kxk matrix.#
[ [   1,   1,   1,   1,   1 ],
  [   3,   1,  -1,   0,  -1 ],
  [   2,   0,   2,  -1,   0 ],
  [   3,  -1,  -1,   0,   1 ],
  [   1,  -1,   1,   1,  -1 ] ]
```

Appendix B

GAP implementation of Burnside-Dixon algorithm

The following code demonstrates the implementation of Burnside-Dixon algorithm[LP10].

```
G:=AlternatingGroup(6);;

#Group Structure.#
time1:=Runtime();;
n:=Order(G);;
CC:=ConjugacyClasses(G);;
cc:=List(CC, Representative);;
k:=Length(CC);;
e:=Exponent(G);;

# Finding the size of the conjugacy classses.#
h:=[];;
for i in [1..k] do
   l:=Size(CC[i]);;
   Add(h,l);;
od;

# Function to find the class multiplication coefficients.#
cmc:=function(r,s,t, cc, CC)
   local z, CCl, els, g, gi, p,rlist, count;;
   z:=cc[t];;
   CCl:=CC[s];;
```

```
    els:=Elements(CCl);;
    rlist:=[];;
    for g in els do
      gi:=Inverse(g);;
      p:=z*gi;;
      Add(rlist,p);;
    od;
    count:=0;
    for g in CC[r] do
      if g in rlist then
        count:=count+1;;
      fi;
    od;
    return count;
  end;

#Computing the class matrix M2.#
M:=[];;
 for r in [1..k] do
   m:=[];;
   i:=1;;
   while i<=k do
     j:=1;;
     l:=[];;
     while j<=k do
       Add(l, cmc(r,i,j,cc,CC));;
       j:=j+1;;
     od;
     Add(m,l);;
     i:=i+1;;
   od;
   Add(M,m);;
 od;
M2:=M[2];;
 Display(M2);

#Finding the suitable prime.#
 limit:=2*RootInt(n,2);;
```

```
for pr in Primes do
  if pr > limit then
    if (pr mod e)=1 then p:=pr;; break; fi;
  fi;
od;

F:=GF(p);;
id:=Identity(F);;
ev:=Eigenvalues(F, M2*id);;
evecs:=List(Eigenspaces(F, M2*id), GeneratorsOfVectorSpace);;

#function to write elements of F as integers mod p>#
dom:=function(p,x)
return( Position(List([-(p-1)/2..(p-1)/2], i->i*id), x)-(p+1)/2);
end;

for sp in evecs do
  for c in ev do
    if sp[1]*M2*id = sp[1]*c then Print("\n", dom(p,c),":␣"); fi;
  od;
  for v in sp do
  Print(List(v, x->dom(p,x)), "␣,");
  od;
od;

#Function to calculate the inner product of two class functions.#
scp:=function(v,w)
return(Sum(List([1..Length(CC)], i-> Size(CC[i])*v[i]*w[i]))/Size(G));
end;
deg:=[];;
for v in Concatenation(evecs) do
  d:=Filtered( [1..(p-1)/2], x -> (x*id)^2 = scp(v,v)^-1);
  Print( [dom(p, scp(v,v)^-1), d], ",");
  Add(deg, d);;
od;

# Considering the 1. and 4. eigenspaces.#
for i in [1,4] do
```

```
    for a in [0..p-1] do
      for b in [a..p-1] do

  v:=evecs[i][1] + a*evecs[i][2];;
  w:=evecs[i][1] + b*evecs[i][2];;

  if IsSubset( List([1..(p-1)/2], x -> (x*id)^2,
    [scp(v,v), scp(w,w)]) then
    d1:=Filtered([1..(p-1)/2], x -> (x*id)^2 = scp(v,v)^-1)[1];;
    d2:=Filtered([1..(p-1)/2], x -> (x*id)^2 = scp(w,w)^-1)[1];;
    if IsInt(Size(G)/d1) and IsInt(Size(G)/d2) and
    scp(v,w)=0*Z(p) and
    d1^2 + d2^2 < Size(G) - 9^2 -10^2 then
      Print([a,b],",",List(d1*v,x-> dom(p,x)),",",
      List(d2*w, x-> dom(p,x)),"\n");
    fi;
  fi;
      od;
    od;
  od;

  epsq:= Z(p)^(p-1)/5;;
  phi:=[8,0,-1,-1,0,-17,18]*id;;
  for x in g{[6,7]} do
    m:=List([0..4], i->dom(p,(5*id)^-1*Sum(List([0..4],
        j->phi[Position(c1,ConjugacyClass(G,x^j))]*epsq^(-i*j))))));;
    Print("chi(g_",Position(g,x),")=",
    m*List([0..4], i->E(5)^i),"␣␣␣");
  od;
```

For A_6 the class matrix M_2 is given by:

```
[ [   0,   1,   0,   0,   0,   0,   0 ],
  [  45,   4,   9,   9,   4,   5,   5 ],
  [   0,   8,   9,   0,   4,   5,   5 ],
  [   0,   8,   0,   9,   4,   5,   5 ],
  [   0,   8,   9,   9,  17,  10,  10 ],
  [   0,   8,   9,   9,   8,  10,  10 ],
  [   0,   8,   9,   9,   8,  10,  10 ] ]
```

A_6 has 5 eigenspaces corresponding to the eigenvalues

$$\lambda = 0 * Z(61), Z(61)^{3}4, Z(61)^{4}2, Z(61)^{1}2, Z(61)^{2}2$$

which can also be expresses as:

```
eigval:=[];;
for e in ev do
  Add(eigval, dom(p,e));;
od;
eigval;
[ 0, −16, −9, 9, 5 ] #the eigenvalues of M2 in mod p(p=61).#
```

Finally we get the table of A_6 as:

```
1   1   1   1   1   1   1
5   1   2  −1  −1   0   0
5   1  −1   2  −1   0   0
8   0  −1  −1   0   A   B
8   0  −1  −1   0   B   A
9   1   0   0   1  −1  −1
10 −2   1   1   0   0   0

A = (1+Sqrt(5))/2
B = (1−Sqrt(5))/2
```

Appendix C

GAP implementation for finding the primitive central idempotents

The following code demonstrates the implementation of Theorem 5.1 in GAP. The program computes the primitive central idempotents of the rational group algebra, when G is a cyclic group of order 12. symmetric group of order 4, S_4.

```
#Program to find the primitive central idempotents
#of rational group algebra of a nilpotent group.

G:=CyclicGroup(12);;
Normal:=NormalSubgroups(G);;
Q:=Rationals;;
QG:=GroupRing(Q,G);;
Id:=Identity(QG);;
o:=Embedding(G,QG);;
LoadPackage("sonata");;
#list of all subgroups of G.
mlist:=Subgroups(G);;

#Defining Hat function
Hat:=function(H,emb)
   local x;;
   return Sum(List(Elements(H), x-> x^emb))/Order(H);;
end;

#Defining Epsilon(G,N).
```

```
Epsilon:=function(G,N,emb,alg)
  local H, min,MinG, ele, M,phi,list;
  if N = G then
    return Hat(N,emb);;
  else
    H:=FactorGroup(G,N);;
    list:=[Hat(N,emb)];;
    min:=MinimalNormalSubgroups(H);;
    MinG:=MinimalNormalSubgroups(G);;
    phi:=NaturalHomomorphismByNormalSubgroup(G,N);;
    for M in MinG do
      if ImagesSet(phi,M) in min then
        Add(list,(One(alg) - Hat(M,emb)));;
      fi;;
    od;;
    return Product(list);;
  fi;;
end;

#Primitive Central Idempotents of QG for
#a finite abelian group.
GetPrimCenIdem:=function(G, list, emb, alg)
  local GModNCyclic, N, idem;;
  GModNCyclic:=[];;
  idem:=[];;
  for N in list do
    if IsCyclic(G/N) then
      Add(GModNCyclic,N);;
    fi;
  od;;
  for N in GModNCyclic do
    Add(idem,Epsilon(G,N, emb, alg));;
  od;
  return idem;
end;

#constructing a directed tree of subgroups
Edge:=function(G,H,K)
```

```
  if IsSubgroup(G,H) and IsSubgroup(G,K) then
    if H=K then return 0;
    elif IsSubset(H,K) then return 1;
    else return 0;
    fi;
  else return 0;
  fi;
end;

#In order to get the depth first tree we
#need stacks ,which are defined as
Stack := function ()
  local stack;;
  stack := [];;
  return rec(
    push := function ( value )
      Add( stack , value );;
    end,
    pop := function ()
      local value;;
      value := stack[Length(stack)];;
      Unbind( stack[Length(stack)] );;
      return value;
    end,
    size:=function()
      return Length(stack);
    end,
    top:=function()
      return stack[Length(stack)];
    end
    );
end;;

DFS:=function(G,list ,node)
  local sta,tnode,visited ,i;;
  SortBy(list ,Order);;
  sta:=Stack();;
  sta.push(node);;
  visited:=[];;
  while sta.size() <> 0 do
    tnode:=sta.pop();;
    Add(visited, tnode);;
    #Print(tnode,"\n");
    for i in list do
      if Edge(G, i, tnode)=1 then
        #if i in visited then continue;
        Add(visited, i);;
        DFS(G,list,i);;
      else continue;
      fi;;
    od;
  od;;
  return visited;;
end;;


FindSublist:=function(G,l)
  local poss, i,j,k,d;;
  poss:=[];;
  for i in [1..(Length(l)-1)] do
    d:=[l[i]];;
    k:=i;;
    for j in [i+1..Length(l)] do
      if Edge(G,l[j],l[k]) = 1 then
        Add(d,l[j]);;
      fi;;
      k:=k+1;;
    od;;
  if d in poss then continue;;
  else Add(poss,d);;
  fi;;
  od;;
  return poss;;
end;;

FindAll:=function(G,list)
```

```
  local allposs, m, l, lposs, i, j;
  allposs:=[];;
  for j in [1..(Length(list)-1)] do
    l:=DFS(G, list, list[j]);;
    lposs:=FindSublist(G,l);;
    for i in lposs do
      if i in allposs then continue;
      else Add(allposs, i);;
      fi;;
    od;;
  od;;
  return allposs;;
end;;

Adjustedlists:=function(G,list)
  local poss, i;
  poss:=FindAll(G,list);;
  for i in poss do
    if Length(i) mod 2 <> 0 then
      if i[1] <> list[1] then
        Add(i, list[1]);;
        SortBy(i, Order);;
      fi;;
    fi;;
  od;;
  return poss;
end;;
adjposs:=Adjustedlists(G,mlist);;

GConjugate:=function(idem,G,alg)
  local g,sum,t,l,K;;
  l:=List(ConjugacyClasses(G), Representative);;
  K:=Length(l);;
  sum:=0*One(alg);;
  for g in l do
    t:=Inverse(g)*idem*g;;
    sum:=sum+t;;
  od;;
  sum:=sum/K;;
  return sum;
end;;

Checklist1:=function(G, list)
  if list[Length(list)]=G and Length(list) mod 2 =0 then
  return 1;;
  else return 0;;
  fi;
end;

Checklist2:=function(G, list)
  local i, count, k;;
  if Checklist1(G, list)=1 then
    k:=Length(list)/2;;
    count:=0;;
    for i in [1..k] do
      if IsNormal(list[Length(list)-i+1],list[i]) then
        if IsCyclic(Center(list[Length(list)-i+1]/list[i])) then
          count:=count+1;;
        fi;;
      fi;;
    od;;
    if count=k then return 1;
    else return 0;
    fi;
  else return 0;
  fi;
end;


Checklist3:=function(G, list)
  local i,k,count;;
  if Checklist2(G, list)=1 then
    count:=0;;
    k:=Length(list)/2;;
    if IsAbelian(list[k+1]/list[k]) then
      count:=count+1;;
    fi;;
    for i in [1..(k-1)] do
      if IsAbelian(list[Length(list) -i +1]/list[i]) then
        count:=count+1;;
      fi;
    od;;
    if count=1 then return 1;;
    else return 0;;
    fi;;
  else return 0;;
  fi;;
end;;


Checklist4:=function(G, list)
  local i,k,count,GiHi,UCS;;
  if Checklist3(G, list)=1 then
    count:=0;;
    k:=Length(list)/2;;
    for i in [1..k-1] do
      GiHi:=list[2*k-i+1]/list[i];;
      UCS:=UpperCentralSeries(GiHi);;
      if list[2*k -i]/list[i] = Centralizer(GiHi,UCS[2]) then
        count:=count+1;;
      fi;;
    od;;
    if count=k-1 then return 1;;
    else return 0;;
    fi;;
  else return 0;;
  fi;;
end;;

IsDesiredList:=function(G, list)
  local i,m,l,H,K,count,x,Comp;
 K:=[];;
  count:=0;;
  if Checklist4(G, list)=1 then
```

```
      m:=Length(list)/2;;
      for i in [1..(m-1)] do
        H:=FactorGroup(list[Length(list)-i+1],list[i]);;
         for x in H do
           Add(K,ConjugateSubgroup(list[i+1], x));;
         od;;
      Comp:=Intersection(K);;
      if Comp = list[i] then count:=count+1;; fi;;
      od;;
      if count = (m-1) then return 1;;
      else return 0;;
      fi;;
   else return 0;;
   fi;;
end;;
PrimitiveCentralIdempotentsUsingJLP:=function(G,poss, emb, alg)
   local lposs, l,m, i, idem, pci;;
   pci:=[];;
   lposs:=Filtered(poss, l-> IsDesiredList(G,l) = 1);;
   for l in lposs do
      m:=Length(l)/2;;
      idem:=Epsilon(l[m+1],l[m], emb, alg);;
      Add(pci, GConjugate(idem,G,alg));;
      od;;
   return pci;;
end;;

PritiveCentralIdempotentUsingJLP(G,adjposs,o,QG);
```

Appendix D

Graphs and Trees

For finding the list

$$H_0 \subseteq H_1 \subseteq \cdots \subseteq H_m \subseteq G_m \subseteq \cdots \subseteq G_1 \subset G_0 = G,$$

we first make a list of all the subgroups of G.

The `Subgroups` function in the *Sonata* package of `GAP` gives us a list of all subgroups sorted in an ascending order of their *order*. Once we have the list of all subgroups we make a a graph with a subgroups as its vertices. For subgroups H and K, there is an edge between the two nodes if and only if $H \subset K$. It is clear that the above mentioned graph is a directed graph, as $H \subset K$ is not equivalent to $K \subset H$.Let V be the collection all vertices and e be the set of all the edges, then $\mathcal{G} = (V, E)$ is the graph of the sugroups of G.

D.1 Representing Graphs

There are two basic ways to represent graphs: by an *adjacency matrix* and by an *adjacency list* representation. We have used here the adjacency matrix representation. Let $\mathcal{G} = (V, E)$ be a graph with number of nodes, $|V| = n$ and $m = |E|$, number of edges. Let $V = \{1, \cdots, n\}$ be the vertices of $\mathcal{G}$, and take a $n \times n$ matrix A, where $A[u, v]$ is equal to 1 if the graph contains an edge (u, v) and 0 otherwise. It should be noted that we set $A[u, u] = 0$. Since we are dealing with a directed graph, therefore the matrix we get is not symmetric.

We now make the a graph for a given group G in `GAP`.

```
#function to check if there is an edge from H to K.
Edge:=function(G,H,K)
  if IsSubgroup(G,H) and IsSubgroup(G,K) then
```

```
    if H=K then return 0;
    elif IsSubset(H,K) then return 1;#check for IsSubgroup
    else return 0;
    fi;
  else return 0;
  fi;
end;
#----------------------------------------------------------
N:=Length(mlist);;
M:=[];;
for i in [1..N] do
  tlist:=[];;
  for j in [1..N] do
    Add(tlist, Edge(G,mlist[j],mlist[i]));;
  od;
  Add(M, tlist);;
od;
#The Matrix M is the adjacency matrix representation of the graph.
Display(M);
```

D.2 Graph Transversal- Depth First Search

There are two algorithms for solving the problem of graph transversal, the *breadth first search*(BFS) and the *depth first search*(DFS). We are mainly concerned with DFS for transversal of our graph of subgroups of G. In DFS we start at a node s and try the first edge leading out of it, to a node, say v. We then follow the first edge leading out of v and continue in this fashion until we hit a "dead end". We then backtrack until we get to node with an unexplored neighbor, and resume from there on.

DFS is implemented using stacks, which is data structure from which we can select an element in *last-in, first-out* (LIFO) order. The following code demonstrated the generation of stacks in GAP.

```
Stack := function ()
  local stack;;
  stack := [];;
  return rec(
    push := function ( value )
```

```
      Add( stack, value );;
    end,
    pop := function ()
      local value;;
      value := stack[Length(stack)];;
      Unbind( stack[Length(stack)] );;
      return value;
    end,
    size:=function()
      return Length(stack);
    end,
    top:=function()
      return stack[Length(stack)];
    end
    );
end;;
```

Implementing DFS in GAP using stacks.

```
DFS:=function(G,list,node)
  local sta,tnode,visited,i;;
  SortBy(list,Order);;
  sta:=Stack();;
  sta.push(node);;
  visited:=[];;
  while sta.size() <> 0 do
    tnode:=sta.pop();;
    Add(visited, tnode);;
    #Print(tnode,"\n");
    for i in list do
      if Edge(G, i, tnode)=1 then
        #if i in visited then continue;
        Add(visited, i);;
        DFS(G,list,i);;
      else continue;
      fi;;
    od;
  od;;
  return visited;;
end;;
```

Bibliography

[Bur04] W. Burnside, *Theory of Groups of Finite Order*, 2 ed., Dover Pheonix, 2004.

[CR62] C.W. Curtis and I. Reiner, *Representation theory of finite groups and associated algebras*, Wiley, New York, 1962.

[Dix67] John D. Dixon, *High Speed Computation of Group Characters*, Numerische Mathematik **10** (1967), 446–450.

[EJ03] Antonio Paques Eric Jespers, Guilherme Leal, *Central Idempotents in the Rational Group Algbra of a Finite Nilpotent Group*, Journal of Algebra and Its Applications **2** (2003), 57–62.

[Inn10] Inneke Van Gelder, *Idempotents in Group Rings*, Ph.D. thesis, Vrije Universiteit Brussels, 2010.

[JL93] Gordon James and Martin Liebeck, *Representations and Characters of Groups*, Addison-Wesley, 1993.

[KET06] Jon Kleinberg and Éva Tardos, *Algorithm design*, Pearson Education, 2006.

[LP10] Klaus Lux and Herbert Pahlings, *Representations of groups - a computational approach*, Cambridge University Press, New York, 2010.

[SM02] S.K. Sehgal and C. Polcino Milies, *An introduction to group rings*, Kluwer, Dordrecht, 2002.

[The90] The GAP Group, *GAP- Reference Manual.*

[Vin54] I.M. Vinogradov, *Elements of Number Theory*, 5 ed., Dover New York, 1954.

[Wei03] Steven H. Weintraub, *Representation Theory of Finite Groups: Algebras and Arithmetic*, Graduate Studies in Mathematics. V:59, 2003.

Index

FG-module, 6
irreducible, 6
submodule, 6
GAP functions
Epsilon, 38
GetPrimCenIdem, 41
Hat, 36

Burnside's algorithm, 17
Burnside-Dixon algorithm, 22

Character, 8
degree, 8
inner product, 8
irreducible, 9
Character table, 10
orthogonality relations, 10
Class multiplication coefficients, 14
Class multiplication matrix, 15
Class sums, 14

Graph, 67
adjacency matrix representation, 67
Group rings, 27
algebras, 28
augmentation ideal, 28, 29
augmentation mapping, 28
semisimplicity, 31

Idempotents in group rings, 35
$\widehat{H}$, 32, 35
decomposition of group ring, 36
principal idempotent, 36

Maschke's Theorem, 6, 33

Representation, 5
faithful, 5

Schur's Lemma, 7