KWAME NKRUMAH UNIVERSITY OF SCIENCE AND TECHNOLOGY,KUMASI

Separating Sets for the Unitary Group $U_2(\mathbb{F}_{q^2})$

By

Yao Elikem Ayekple B.Sc, M.Sc

A THESIS SUBMITTED TO THE DEPARTMENT OF MATHEMATICS,
KWAME NKRUMAH UNIVERSITY OF SCIENCE AND TECHNOLOGY IN
PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE DEGREE
OF DOCTOR OF PHILOSOPHY MATHEMATICS

October, 2015

Declaration

I, Yao Elikem Ayekple, declare that this submission is my own work towards the award of the PhD degree and that, to the best of my knowledge, it contains no material previously published by another person or material which has been accepted for the award of any other degree of the university except where due acknowledgement has been made to the text.

KNUST

Yao Elikem Ayekple ....

Student Signature Date

Certified by:

Dr. F. T Oduro ....

Supervisor Signature Date

Certified by:

Dr. K. Baah ....

Supervisor Signature Date

YANSAPƆ WƆSANE NO BADWENM

Certified by:

Prof. S. K Amponsah ....

Head of Department Signature Date

Dedication

To my late parents: Sydney Kofi Ayekple and Fidelia Mansa Ayekple.

KNUST

NYANSAPƆ WƆSANE NO BADWENMA

Abstract

A separating set for a group G with respect to the group CG is a set of simultaneously diagonalisable linear operators $\{T_1,...,T_r\}$ of C that distinguish the invariant subspaces of CG with their eigenspaces. In this thesis, we study the character table of the irreducible representation of the unitary group G and construct the modified character table which consists of the eigenvalues that the class sum of each conjugacy class of G assigns to an irreducible representation of G. The separating set for G is then obtained by extracting the class sums which is associated to each irreducible character distinct pair of eigenvalues.

KNUST
NYANSAPƆ WƆSANE NO BADWENMA

Acknowledgment

To God Almighty, creator of everything; to the Lord whose name is JAH, who ever liveth with his mercies and grace, who has been my source of inspiration and brought me to its logical conclusion.Thank you Almighty one.

My gratitude goes to my supervisors: Dr F.T. Oduro and Dr.K.Baah-Gyamfi of Department of Mathematics, KNUST, Kumasi for their guidance and directions and Prosper Akrobotu for his unparalleled contribution.

I also thank all members of the Mathematics department. God bless you.

I am very grateful to my wife for her unflinching support throughout my work. Last, but not least, my appreciation also goes to my family for their marvellous support and encouragement all this while.

KNUST
NYANSAPƆ WƆSANE NO BADWENMA

Contents

KNUST

KNUST

List of Tables

KNUST

NYANSAPƆ WƆSANE NO BADWENMA

Chapter 1

Introduction

1.1 Overview

A separating set for a group G with respect to the group algebra CG is a set of simultaneously diagonalisable linear operators $\{T_i\}_1^s$ of $\mathbb{C}G$ that distinguish the invariant subspaces of CG with their eigenspaces. This chapter takes us to the background of the thesis, and we state the problem with its justification. The objectives are stated implicitly. Limitations of the study ends the chapter.

1.2 Background of study

In [**?**], Steinberg establishes that naturally, groups arise as sets of symmetries (of an object), which are closed under composition and under taking inverses.The collection of unitary groups $U(n)$ is a set of distance – preserving transformations, which include the translations.The action of a group is the first step to take to find a representation of a group. The action takes us to a vector space V over some ground field for which the vector space structure is preserved. The complex field is the basic field to take a representation. A group homomorphism from G to $GL(V$) “is the same as” a representation of G on V . Classifying, all representations of an infinite arbitrary group up to an isomorphism is an enormous task, so in this thesis, we concentrate on finite groups, where very good general theorems exist. In the $x - y$ plane, if we take a reflection across any of the axes in the plane, it is the same as the reflection in the other axis, geometrically. That is, any two reflections in the x–y plane have the same *type* of effect on the plane. Similarly, except for the choice of the pairs getting moved, two permutations of a set that are so identical that the transposition(fixing everything else whiles swapping two elements) look the same.

Therefore, all transpositions have the same *type* of effect on elements of the set. The same except for the point of view' concept is what is known as conjugacy.

KNUST

For a group G, two elements h and g are called conjugate when

$$g = xhx^{-1}$$

for some $x \in G$.

It is a symmetric relationship, since $h = ygy^{-1}$ where $y = x^{-1}$. For

$$xgx^{-1} = h$$

In a group G, if $g \in G$, its conjugacy class is the set of elements conjugate to it:

$$Cg = \{xgx^{-1}, x \in G\}$$

And if G is abelian, each element is its own conjugacy class.

Given two square matrices A and B, then to determine if A and B represent the same linear transformation requires probing into some invariant properties of these matrices. The obvious thing to consider is the size. Suppose without loss of generality that A and B are of the same size, then we know that A and B will be a representation of the same linear transformation if they are similar matrices, i.e. there exists an invertible matrix P such that $B = PAP^{-1}$. In terms of group actions, this will mean A and B are conjugates and hence are in the same orbit.

The group in question will be the general linear group $GL_n(\mathbb{C})$. This action is said to be linear if we consider $GL_n(\mathbb{C})$ as a vector space of dimension n^2

. Using the invariant, characteristic polynomial (or eigenvalues), we observe that the matrices $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ possess identical characteristic polynomial but represent different linear transformations and hence this invariant alone will not be sufficient in arriving at a solution. However, considering both the eigenvalues and and geometric multiplicities of the eigenvalues, a solution can be obtained and hence these two invariants give a separating set.

Let G be a group and V be the group algebra $\mathbb{C}G$. Let $\{T_i\}_{i=1}^n$ be a collection af simultaneously diagonalizable linear transformations of V whose eigenspaces are direct sums of the $G-$invariant subspaces of V. For each $G-$invariant subspace V_i, let $m_i = (\lambda_{i1},...,\lambda_{in})$ be the $n-$ tuple of eigenvalues where $1 \leq j \leq n$, and λ_{ij} is the eigenvalue of T_j associated to V_i. If m_i =6 m_k whenever V_i 6= V_k, then the set $\{T_i\}_{i=1}^n$ is said to be a *separating set* for V.

Given a representation V of a finite group G, it is shown in [**?**] that the separating sets for G reduce the complexity of computing the isotypic projections.

The representation of the unitary groups are in matrix form. Its eigenvalues are then determined using the characteristic polynomial to put them in classes.

The representation of a group is by its characters. Essential information of a group is carried by its characters which is a function from the group to a field of complex numbers, i.e. $\chi : G \to C. \to \otimes$. In performing calculations, characters in representations are the fundamental tools employed. The subgroup of unitary matrices are hardly known.

In this thesis, the concentration would be on irreducible representation, which contains no proper invariant subspaces. As we already know, every complex representation of a finite abelian group is completely reducible, and every irreducible representation is 1 – dimensional. An analogous proposition for every finite group is that a representation is completely reducible if it decomposes as direct sum of irreducible sub – representations. The characters of the representations are used to determine its reducibility.

The cardinality of a set is the number of elements in the set with the set of natural numbers starting from 1 as its domain. The cardinality of a set is denoted as $|A|$.The number of elements in the conjugacy class of unitary group is determined by the cardinality of the class.

There have been several studies such as Derksen and Kemper[**?**], Dixon[**?**] and Dufresne[**?**] on separating sets over the past years with researches employing different approaches. In this thesis, representation theory is employed to examine the separating set of the unitary group $U_2(\mathrm{F}q^2)$. The eigenvalues that a class sum associates to the irreducible characters are used to obtain the separating set based on the class sums which can actually distinguish each of the irreducible characters.

The group $U_2(\mathbb{F}_q^2)$ is sometimes stated as G in the work. The character values of the conjugacy classes with similar forms are the same. Finally, we see the methods used in separating the class representatives by using the modified character table.

1.3 Problem Statement

Given a representation V of a finite group G, one would like to compute the isotypic projection i.e. projections of $h \in V$ onto the G-invariant subspaces of V. Direct computations require large amount of time depending on the size of the group and with the help of separating sets the complexity is reduced.

1.4 Justification of The Research

The computational complexity of computing the isotypic projections is reduced when using separating sets. It is therefore more efficient to use minimal separating

sets.

1.5 Objectives

The goal is to research methods for finding minimal separating sets for the unitary group $U_2(\mathrm{F}_{q^2})$ This research examines the unitary group $U_2(\mathrm{F}_{q^2})$ with the following specific objectives:

1. To determine the cardinality of each conjugacy class.
2. To construct the character table of $U_2(\mathrm{F}_{q^2})$.
3. To find the minimal separating sets for $U_2(\mathrm{F}_{q^2})$.

1.6 Limitation of The Research

The direct sum and direct product were conducted in one-dimensional space. The more than one dimensional space calculations have not been tried yet. One of the chief difficulties in this task is the determination of the conjugacy classes, as in the unitary group we cannot exploit the Jordan form or rational canonical form of a matrix.

1.7 Organisation of The Study

The study comprises five chapters. Chapter one introduces the thesis. It consists of the background to the study, Problem statement, Objective of the study, Justification of the study, Limitation of the study and Organisation of the study.

Chapter two reviews the related literature.Chapter three consists of the definition and theorems that are related to irreducible and character of groups. Chapter four takes us to the replenish include representations and character table that calculates the minimal separating sets. Chapter five is the conclusion and recommendation of the study.

KNUST
NYANSAPƆ WƆSANE NO BADWENMA

Chapter 2

Literature Review

In this study, we seek to employ representation theory to examine the separating sets of the unitary groups. An efficient way to approach this study is by first probing the irreducible representations of the unitary group as they serve as the building block of the representations of the group.

In 1963, Moshinsky [?] established the bases of all irreducible representations of the unitary group U_{2j+1} to be the set of polynomials in the components of $(2j+1)$- dimensional vectors and the solution of certain invariant partial differential equations. Moshinsky [?] observed that these polynomials, for the unitary group U_{2j+1} and the solid spherical harmonic (polynomials in the components of 3-dimensional vectors), for the rotation group R_3 have the same role. Moshinsky [?] employed these polynomials in defining and determining the reduced Wigner coefficients for the unitary groups. Moshinsky [?] then applied a factorization method to the results and obtained the Wigner coefficients of the Unitary group U_{2j+1}. He also, showed in his paper [?] how to eliminate the ambiguity in the explicit expression for the Wigner coefficients by using operators that characterize completely the rows of representations of unitary groups for a particular chain of subgroups.

Itzykson et al [?] in their 1966 paper, *Unitary Groups: Representations and Decompositions*, reviewed basic definitions and the constructions of irreducible representations using the tensor method and pointed out the link to the infinitesimal approach. In their paper, Itzykson and Nauenberg focused on the detailed procedure employed to obtain Clebsch-Gordan series and on the problem of finding the (SU_m, SU_n) content of an irreducible representation of SU_{mn} or SU_{m+n}.

Later in 1970, Dixon [?] presented some efficient ways of computing irreducible representation and the characters of finite groups. In his paper [?], Dixon [?] described an efficient way of decomposing a reducible unitary representation into irreducible components. However, given a single faithful unitary representation of a group, one can efficiently construct a complete set of irreducible unitary representations of the group and also, efficient method for computing the precise values of a character from approximated values.

KNUST

In the reduction of a unitary representation, the theory on which his method was based is stated as if G is a finite subgroup of order g in $U(d)$, then G is irreducible unless for at least one element of E_{rs} of the standard basis for $M(d)$ the matrix

$$E = \frac{1}{g} \sum_{X \in G} X^* E_{rs} X$$

is not scalar. where $U(d)$ denotes the group of all d ×
d matrices.
Where $E(X) = XE$ for all $X \in G$ and when E is not scalar the eigenspaces of E reduce G. E may be computed by an iteration process using only a set of generators for G.

Theorem 2.0.1. *Let S be a finite set consisting of h elements of $U(d)$ and suppose that the unit matrix $I \in S$. We define a linear mapping $\sigma : M(d) \rightarrow M(d)$ by*

$$\sigma(B) = \frac{}{h} \sum_{U \in S} U^* B U$$

Then for each $A_0 \in M(d)$ we can define a sequence A_n in $M(d)$ by putting

$A_n = \sigma^n = \sigma^n(A_0)$ for $n = 1,2,...$ Then $A(n)$ is always convergent in $M(d)$ and its limit, say A, has the property $AU = UA$ for all $U \in S$.

Proof

The norm $||.||$ on $M(d)$ defined by $||B||^2$= trace B^*B.

$$||\sigma(B)|| = ||B|| \text{ implies that } UB = BU \text{ for all } U \in S. \tag{2.1}$$

The properties of the norm show that for any $B \in M(d)$,

$$||\sigma(B)|| = \left|\left|h^{-1}\sum_{U\in S} U^*BU\right|\right| \leq h^{-1}\sum_{U\in S}||U * BU|| \tag{2.2}$$

$$= h^{-1}\sum_{U\in S}||B|| = ||B|| \tag{2.3}$$

U are unitary. The equality sign in equation 2.2 holds when all the matrices U^*BU (for $U \in S$) lie on the same ray through 0 in $M(d)$.

Now, $I \in S$.

So, $||\sigma(B)|| = ||b||$

$\Rightarrow \exists\lambda_U \geq 0$ such that

$$U * BU = \lambda_U B \ \forall \ U \in S$$

$$\{\lambda_u : \lambda_u \in \mathrm{R}\} \ B =$$

$||U * BU||$, So,

$$||B|| = ||\lambda_U B|| = \lambda_U||B||$$

Hence, either $B = 0$

Or else $\lambda_U = 1 \ \forall U \in S.$

$\Rightarrow UB = BU \ \forall U \in S$ hence equation 2.1 is proved.

Let $B_n = A_n - A$ for $n = 0,1,2,....$

$\sigma(A) = A \Rightarrow (||B_n||)$ is monotonically decreasing.
By the definition of A, $lim||B_{nk}|| = 0$ so the sequence (A_n) converges to A.

Definition 2.0.2. Let E_{rs}(r,s=1,...,d) be the standard basis for $M(d)$; that is,E_{rs} is the matrix whose r,sth entry is 1 and whose other entries are all 0.

Let $H_{rs}(r,s = 1,...,d)$ for $M(d)$ by

$$\begin{aligned} H_{rs} &= E_{rr} \text{ if } r = s, \\ &= E_{rs} + E_{sr}\; r > s, \\ &= i(E_{rs} - E_{sr})\; r < s \end{aligned}$$

Theorem 2.0.3. *Suppose S is a reducible set of matrices (S generates a reducible subgroup of* $U(d)$*).*

Then for at least one H_{rs} *the limit* $lim\sigma^n(H_{rs}) = H$*, say, is not scalar and we can reduce S into a number of not necessarily irreducible components as follows. Since H is hermittian, there exists an orthonormal basis* $v_1,...,v_d$ *of the underlying* $d-$ *dimensional unitary space such that this basis is made up of listing successively orthonormal bases for eigenspaces for H for the different eigenvalues. Then, if C is the unitary matrix whose columns are* $v_1,...,v_d$*,*

$$C * UC = \begin{pmatrix} U_1 & & & \\ & U_2 & & \\ & & . & \\ & & & . \\ & & & & . \end{pmatrix} \textit{for all } U \in S$$

KNUST
NYANSAPO WO SANE NO BADWENMA

U_k

The (r,s)*th entry of the matrix on the right-hand side is* $v_r^* U v_s$ *and this is 0 when* v_r *and* v_s *are eigenvectors for different eigenvalues of H.*

Proof

S is completely reducible because $S \subset U(d)$.

$\Longrightarrow \exists$ a non-scalar $B \in M(d)$ such that $UB = BU\ \forall\ U \in S$.
So $\delta(B)$ =

B.

H_{rs} forms a basis for $M(d)$

$\exists\ B_{rs} \in$ **e** such that $B = {}^{\mathrm{P}}\beta_{rs}, H_{r,s}$,

$\Longrightarrow B = \lim \sigma^n(B) = {}^{\mathrm{P}}\beta_{rs} \lim\sigma^n(H_{rs})$ because σ is linear.
Since B is not scalar, at least one $\lim\sigma^n(H_{rs})$ is not scalar.

Suppose $H = \lim\sigma^n(H_{rs})$ is not scalar.

$HU = UH\forall\ U \in S$ by theorem 2.0.1

$\Longrightarrow$ for any eigenvalue α_i of H the corresponding eigenspace is mapped into itself by multiplication by any $U \in S$.

If $Hv = \alpha_i v$,

Then,

$H(Uv) = U(Hv) = \alpha_i(Uv)$.

$\Longrightarrow\quad v_r^* U v_s = 0$ whenever v_r and v_s are eigenvectors for H for different eigenvalues.

In 1991, Katriel [**?**], established a theorem regarding the explicit form of the eigenvalues of the class sums of the symmetric group S_n. Katriel [**?**] then employed the theorem to show that the center of CS_n is generated by polynomials in the set of elements consisting of the generators of the center of the CS_{n-k} augmented by single-cycle class sums $((2))_n,((3))_n,...,((k+1))_n$. He also used the theorem in establishing that the irreducible representations of S_n with up to k rows are fully given by the class sums $((2))_n$,$((3))_n$,...,$((k))_n$. Further investigations by Katriel [?] showed that the k class sums $((2))_n$,$((3))_n$,...,$((k+1))_n$ is sufficient for specifying the irreducible representations of S_n for all $n > k$. Katriel in his work was able to show that the class sum of transpositions sufficiently yields separating sets for S_n for $n < 5$ and in addition showed that the first four class sums are enough as long as $n < 41$.

The role of Gelfrand-Graev characters and their degenerate counterparts in the representation theory of finite Lie groups enabled Thiem and Vinroot [?], to restate the character theory of the finite unitary groups in the language of symmetric functions via a characteristic map. This transformation motivated a combinatorial approach to the study of degenerate Gelfand-Graev characters of the finite unitary group. In their paper, Theim and Vinroot, were able to derive the formula for the character values of the Gelfand-Graev character of $U_n(\mathbb{F}_{q^2})$ by using a remarkable formula for the character values of the Gelfand-Graev character of $GL_n(\mathbb{F}_{q^2})$.

In 2003, Derksen et al [?] documented interesting results on separating sets using invariant theory in their book *Computational Invariant Theory*[?]. Dersken and Kemper were able to show that the existence of finite separating sets; invariants of degree at most the order of the group G form a separating set.

In 2004, Melissa Banister [?] also approached the study of separating sets by means of representation theory. Melissa [?] probed into the representation theory of alternating and dihedral groups and by employing class sums, she carefully examined how the irreducible representations of such groups can be distinguished.

Emilie Dufresne [?] later approached the study of separating sets geometrically. In 2009, Dufresne in her paper [?], showed that the only groups capable of having polynomial separating algebras are those generated by reflections. Dufresne also showed that a group may have complete intersection separating algebras only if the group is generated by bireflections.

KNUST

These are definitions, propositions and theorems with their corollaries stated without proof.

Theorem 2.0.4. *Let G be a finite group. If there exists a geometric separating algebra which is a polynomial ring, then the action of G on V is venerated by reflections.*

Corollary 2.0.5. *Let G be a finite group. If the characteristic of K does not divide the order of G, then there exists a geometric separating algebra which is a polynomial ring if and only if the action of G on V is generated by reflections.*

Theorem 2.0.6. *Let G be a finite group. If there exists a graded geometry separating algebra which is a complete intersection, then the action of G on V is generated by bireflections.*

Definition 2.0.7. *A subset E of $K[V]^G$, is a geometric separating set if, for all u and v in $\overline{V}$, the two following equivalent statements hold:*

- *if there exists f in $K[V]^G$ such that $f(u)$ 6= $f(v)$, then there exists h in E such that $h(u)$ 6= $h(v)$;*
- *$f(u) = f(v)$, for all f in $K[V]^G$ if and only if $h(u) = h(v)$ for all h in E.*

NYANSAPO WO SANE NO BADWENMA

KNUST

Definition 2.0.8. *The separating scheme* S_G *is the unique reduced scheme having the same underlying topological space as the product* $V \times_{V//G} V$*, that is,* $\mathrm{S}_G := (V \times_{V//G} V)_{red}$.

Theorem 2.0.9. *Let* $A \subset \mathrm{K}[V]^G$ *be a subalgebra, then the following statements are equivalent:*

1. *A is a geometric separating algebra;*
2. *if* $W = Spec(A)$*, then the natural morphism* $\mathrm{S}_G \rightarrow (V \times_W V)_{red}$ *is an isomorphism;*
3. *if* δ *denotes the map* $\delta : \mathrm{K}[V] \longrightarrow \mathrm{K}[V] \otimes_{\mathrm{K}} \mathrm{K}V$ *sending an element of f of* $\mathrm{K}[V]$ *to* $f \otimes 1 - 1 \otimes f$*, then, the ideals* $(\delta(A))$ *and* $(\delta(\mathrm{K}[V]^G))$ *have the same radical in the ring* $\mathrm{K}[V] \otimes_{\mathrm{K}} \mathrm{K}[V]$*,i.e,*

$$\mathrm{p}\delta(A) = \mathrm{p}\overline{\delta(\mathrm{K}[V]_G)};$$

Theorem 2.0.10. *If G is reductive, then a subalgebra* $A \subset \mathrm{K}[V]^G$ *is a geometric algebra if and only if the morphism of schemes* $\theta : V//G \longrightarrow = W = Spec(A)$ *corresponding to the inclusion* $A \subset \mathrm{K}[V]^G)$ *is a radical morphism.*

Proposition 2.0.11. *If G is a finite group, then the separating scheme is a union of* $|G|$ *linear subspaces, each of dimension n. There is a natural correspondence between these linear spaces and the elements of G. Moreover, if* H_σ *and* H_τ *denote the subspaces corresponding to the elements* σ *and* τ *of G respectively, then the dimension of the intersection* $H_\sigma \cap H_\tau$ *is equal to the dimension of the subspace fixed by* τ^{-1} *in V.*

Proposition 2.0.12. *Let* $A \subset \mathrm{K}[V]^G$ *be a graded subalgebra. If the map of schemes* $\theta : V//G \longrightarrow W = Spec(A)$ *is injective, then the extension* $A \subset \mathrm{K}[V]^G$

is integral.

Corollary 2.0.13. *If the action of G on V is reductive, and if $A \subset \mathbb{K}[V]^G$ is a graded geometric separating algebra, then the extension $A \subset \mathbb{K}[V]^G$ is integral.*

In 2013, Emilie [?] in her paper [?] examined Nagata's famous counterexample to Hilbert's fourteenth problem which shows that the ring of invariants of an algebraic group action on an affine algebraic variety is not always finitely generated. Emilie [?] agreed to the assertion that invariant rings are always quasi-affine and that finite separating sets always exist. In her paper, [?], Emilie [?] established new techniques for obtaining a quasi-affine variety on which the ring of regular functions is equal to a given invariant ring. She also gave a new basis for identifying separating algebras. This new technique and basis were applied to some known examples and in a new construction.

Although rings of invariants are not always finitely generated, there always exists a finite separating set.

Theorem 2.0.14. *Let $\mathbb{G}_a$ act on V as above. The following 6 homogeneous polynomials are invariants and form a separating set E in $\mathbb{K}[V]^{\mathbb{G}_A}$:*

$$f_1 = x, f_2 = 2x^3t - s^2, f_3 = 3x^6u - 3x^3ts + s^3, f_4 = xv -$$
$$s, f_5 = s^2v + 2x^3tv - 3x^5u, f_6 = -18x^3tsu + 9x^6u^2 +$$
$$8x^3t^3 + 6s^3u - 3t^2s^2.$$

Lemma 2.0.15. $\mathbb{K}[V]^{\mathbb{G}_a} \subset \mathbb{K}[f_1, f_2, f_3, f_4, \frac{1}{x}]$.

Proposition 2.0.16. *We have $\mathbb{K}[V]^{\mathbb{G}_a} \subset \mathbb{K} \oplus (x,s)\mathbb{K}[V]$.*

Lemma 2.0.17. *Define a $\mathbb{K}-$algebra map*

KNUST
NYANSAPO W SANE NO BADWENMA

$\varphi : \mathsf{K}[x,s,t,u,v] \longrightarrow \mathsf{K}[x,v,t,u]$, $f(x,s,t,u,v)$ 7→

$\varphi(f)(x,v,t,u) := f(x,xv,t,u,v)$,

and a derivation Δ^0 *on* $\mathsf{K}[x,v,t,u]$:

$$\delta' = x^2\frac{\partial}{\partial u} + xv\frac{\partial}{\partial t} + t\frac{\delta}{\partial u}.$$

It follows that

(a) $\delta^0 \circ \varphi = \varphi \circ D$*, in particular,* φ *maps ker D to ker* Δ^0;

(b) ker $\delta^0 = \mathsf{K}[h_1,h_2,h_3,h_4]$*, where*

$h_1 = x$, $h_2 = 2xt - v^2$, $h_3 = 3x^3u - 3xvt + v^3$, $h_4 =$

$8xt^3 + 9x^4u^2 - 18x^2tuv - 3t^2v^2 + 6xuv^3 = (h_{32} +$

$h_{23})/x_2$.

Proof. (a) For $f = f(x,s,t,u,v) \in \mathsf{K}[x,s,t,u,v]$, we have

$$\begin{aligned}(\Delta' \circ \phi)(f) &= (x^2\frac{\partial}{\partial v} + xv\frac{\partial}{\partial t} + t\frac{\partial}{\partial u})f(x,xv,t,u,v)\\ &= x^3\phi(\frac{\partial f}{\partial s}) + x^2\phi(\frac{\partial f}{\partial v}) + xv\theta\phi(\frac{\partial f}{\partial t}) + t\phi(\frac{\partial f}{\partial u})\\ &= \phi\Big(x^3\frac{\partial f}{\partial s} + x^2\frac{\partial f}{\partial s} + s\frac{\partial f}{\partial t} + t\frac{\partial f}{\partial u}\Big) = (\phi \circ D)(f)\end{aligned}$$

.

(b) Since Δ is a triangular monomial derivation of a four dimensional polynomial ring, its kernel is generated by at most four elements. Alternatively, one can use van den Essen's algorithm. The derivation Δ^0 can be extended to $\mathsf{K}[x,v,t,u]_x$ and as $\Delta'(\frac{v}{x^2}) = 1$,. The Slice theorem yields

$$(ker\Delta')_x = \mu - \frac{v}{x^2}(\mathbb{K}[x,v,t,u,\frac{1}{x}]) = \mathbb{K}[h_1,h_2,h_3,\frac{1}{x}]m \qquad (2.4)$$

Consider the additional invariant $h_4 := h_2^3 + h_3^2/x^2 \in \mathbb{K}[x,v,t,u]_x$. We claim $ker\Delta^0 = \mathsf{K}[h_1,h_2,h_3,h_4] = R$. Equation 2.4 implies $R \subseteq \Delta^0 \subseteq R_x$.

KNUST

Next we look at the ideal of relations modulo x between the generators of R,

$$I := \{P \in \mathrm{K}[X_1,X_2,X_3,X_4] | P(h_1,h_2,h_3,h_4) \in (x)\mathrm{K}[x,v,t,u]\}$$

$$= \{P \in \mathrm{K}[X_1,X_2,X_3,X_4] | P(0,-v^2,v^3,-3t^2v^2) = 0\} = (X_1,X_{32} + X_{23})\mathrm{K}[X_1,X_2,X_3,X_4].$$

KNUST

□

Campbell [?] in his masters thesis "*Irreducible characters of* 2 × 2 *unitary matrix groups over finite fields*", constructed the character table for the irreducible representations for the group of unitary 2 × 2 matrices over finite field. He also, showed the similarities existing between this table and the method for constructing the character table for the general linear group.

Chapter 3

Methodology

3.1 Introduction

In this chapter, we establish the setting, basic terminologies as well as the tools and machineries necessary for thorough understanding of the main text.

3.2 Basic Definitions and Theorems

Definition 3.2.1. *A nonempty set G, with binary operation * is a group P if the following conditions are satisfied*

I. $a * b \in G$ for $a,b \in G$(Closure)

II.$(a * b) * c = a * (b * c)$ for $a,b,c \in G$(Associativity) III. $(a * e) = a$

for $a,e \in G$,where e is the identity element in G

IV. $(a * a^{-1}) = e$ for $a,a^{-1} \in G$ where a^{-1} is the inverse element of G.

Definition 3.2.2. *Let* $(G,*)$ *and* $(H,\circ)$ *be groups. A homomorphism is a map*

$$\varphi : G \longrightarrow H$$

such that $\varphi(x * y) = \varphi(x) \circ \varphi(y)$ *for all* $x, y \in G$.

In other words, a homomorphism is a map which preserves the algebraic structure between two groups. This map conveys information about one of the group from known structural properties of the other group.

Definition 3.2.3. *The homomorphism* φ *is said to be an isomorphism if* φ *is bijective. In this case, G is said to be isomorphic to H which is written as* $G \,\tilde{}= H$. *If* φ *is an isomorphism such that* $H = G$ *then we say that* φ *is an automorphism.*

Quaternion group

Proposition 3.2.4. *Let G be any group. Define, for any* $g \in G$, *the maps*

$\phi : G \longrightarrow G$ *defined by* $\phi(h) =$

ghg^{-1},

is an automorphism.

Proof. Consider the map

$$\psi : G \longrightarrow G \text{defined by,} \psi(k) = g^{-1}kg.$$

Then,

$$(\phi \circ \psi)(k) = \phi(\psi(k)) = \phi(g^{-1}kg)$$

$$= g(g^{-1}kg)g^{-1},$$

$$= gg^{-1}kgg^{-1}, =$$

$$k.$$

This implies that $\phi \circ \psi = id$ and hence $\phi^{-1} = \psi$.

Similarly, $\psi \circ \phi = id$.

Thus, ϕ is bijective. Also,

$$\phi(hk) = ghkg^{-1} = ghg^{-1}gkg^{-1},$$

$$= \phi(h)\phi(k).$$

This implies ϕ is a homomorphism. Hence ϕ is an isomorphism from G to G.

Therefore, ϕ is an automorphism. □

Definition 3.2.5. *Let* $G = \mathbb{F}^*_{q^2}$ *be the group of units of the quadratic field extension* $\mathbb{F}_{q^2}$ *of the finite field* $\mathbb{F}_q$*. The map*

$$N : \mathbb{F}^*_{q^2} \longrightarrow \mathbb{F}^*_{q^2}, \text{ defined by}$$

$$N(x) = x\overline{x},$$

is a hormomorphism

Proof.

$$\text{Indeed,} N(xy) = xy\overline{xy},$$
$$= xy\overline{x}\overline{y} = x\overline{x}y\overline{y},$$

$$= N(x)N(y).$$

Thus, the map N is a group homomorphism(the homomorphism N is called the **norm map**). □

Proposition 3.2.6. *Using the subgroup* $\mathcal{L} = \{x \in \mathbb{F}^*_{q^2} | x\overline{x} = 1\}$ *of the multiplicative group* $\mathbb{F}^*_{q^2}$*. The map*

$Q : \mathbb{F}^*_{q^2} \longrightarrow \mathcal{L}$*, defined by*

KNUST

$$Q(x) = \frac{x}{\overline{x}},$$

is a homomorphism

Proof. For any $x, y \in \mathbb{F}^*_{q^2}$ we have,

$$Q(xy) = \frac{xy}{\overline{xy}} = \frac{x}{\overline{x}}\frac{y}{\overline{y}} = Q(x)Q(y).$$

Hence, the map Q is a homomorphism. □

Definition 3.2.7. *Let* φ *be the homomorphism defined in Definition 3.2.2. The kernel of* φ *denoted* $\ker(\varphi)$ *is a subgroup of the group* $(G,*)$ *such that* $\ker(\varphi) = \{x \in G|\varphi(x) = e \in H$ *where* e *is the identity element*$\}$.

Proposition 3.2.8. *1. The kernel of the norm map in Proposition 3.2.5 is given by the subgroup* $\mathcal{L} = \{x \in \mathbb{F}^*_{q^2} | xx = 1\}$_ *, where,* L=[∞]*. The group* $\mathbb{F}^*_{q^2}$ *is a cyclic group of order* $q^2 - 1$*. Suppose* η *is the generator of* $\mathbb{F}^*_{q^2}$ *then* $\eta^{q2-1} = \eta^{(q-1)(q+1)} = 1$*. This implies* η^{q-1} *is a generator of* $\ker(N)$ *as* $xx = 1$ — ⇔ $x^{q+1} = 1$*. This shows that the order of* $\ker(N)$, $|\mathrm{L}| = q + 1$*.*

2. The kernel of the map Q *in Proposition 3.2.6 is given by* $\ker(Q) = \{x \in \mathbb{F}^*_{q^2} | \frac{x}{\overline{x}} = 1\} = \mathbb{F}^*_q$*. Since the multiplicative group* $\mathbb{F}^*_q$ *is of order* $q - 1$*, we have,* $|\ker(Q)| = q - 1$*.*

Definition 3.2.9. *Let* V *be a finite dimensional vector space. The general linear group* $GL(V)$ *is the group of all invertible linear maps from* V *to* V*.*

Remark 3.2.10. *Let $n > 0$ be an integer and suppose V is of dimension n. Then for a given basis of V, the general linear group $GL(V)$ is isomorphic to the group of all invertible $n \times n$ matrices $GL_n(\mathbb{C})$, that is, $GL(V) \tilde{=} GL_n(\mathbb{C})$.*

Definition 3.2.11. *' Let X be a set and G be a group. The group G is said to act on X if there exists a mapping*

$$\rho : G \times X \longrightarrow X$$

called an action defined by

$$\rho(g,x) = gx \; \forall g \in G \; \forall x \in X$$

such that

1. $1x = x \forall x \in X$,
2. $(gh)x = g(hx)$ *for* $g,h \in G$ *and* $\forall x \in X$.

X is referred to as a G-set.

Proposition 3.2.12. *1. Let G be a group and X be a nonempty set. The map defined by $gx = x \forall g \in G$ and $\forall x \in X$ is an action of G on X known as the trivial action.*

2. *Let G be a multiplicative group. The multiplication in G defines an action*

$$l : G \times G \longrightarrow G$$
$$(g,h) \mapsto gh.$$

By the associative property and identity element of the group G, this map clearly defines an action of G on itself.

3. *Let G be a group. The map*

$$G \times G \longrightarrow G$$

$$(g,h)\ 7\!\to ghg^{-1}$$

is an action of G on itself known as conjugation.

Theorem 3.2.13 (Cayley's theorem). *Every finite group G is isomorphic to a subgroup of the symmetric group S_G.*

Definition 3.2.14. *Let G be a group which acts on the set X and let $x \in X$.*

The subset

$$Gx = \{gx : g \in G\} \subseteq X$$

of X is said to be the orbit of $x \in X$.

The subgroup

$$G_x = \{g \in G : gx = x\} \subseteq G$$

of G is known as the stabilizer of x.

The stabilizer subgroup of x is also known as the isotropy subgroup of x.

Remark 3.2.15. 1. The orbits for a group action are equivalent classes for the relation $x \sim y$ if $y = gx$ for some $g \in G$.

2. The orbits partition the G-set X, i.e. $S = \mathrm{S}_{x\in X}\,\mathrm{O}(x)$ is a union of disjoint orbits.

3. The orbits of an element x and of gx are equal.

4. If X consists of just one orbit, we say that G acts transitively on X. That is, every element of X is carried to every other element by some element of the group G.

KNUST

Theorem 3.2.16 (The orbit-stabilizer theorem)**.** *Let X be a G-set, $x \in X$. Let G_x be the stabilizer of x and Gx be the orbit of x. Then the map*

$$\psi : G/G_x \longrightarrow Gx \quad \text{defined by}$$

$$\psi(gG_x) = gx,$$

is an isomorphism of G- sets. In particular, $|G| = |G_x||Gx|$.

(By a homomorphism of G-sets X,Y we mean a map

$\psi : X \longrightarrow Y$ such that, $\psi(gx) = g\psi(x)\ \forall g \in G$and $x \in X$.)

Proof. 1. ψ is well defined.

For all $g,h \in G$,

$$gG_x = hG_x \Rightarrow h^{-1}g \in G_x \Rightarrow h^{-1}gx = x \Rightarrow gx = hx.$$

2. ψ is a homomorphism of G-sets.

   For all $g,h \in G$,

$$\psi(g(hG_x)) = \psi(ghG_x) = ghx = g(hx) = g\psi(hG_x).$$

3. ψ is surjective.

$$\forall y = gx \in Gx, y = gx = \psi(gG_x).$$

4. ψ is injective.

   For all $g,h \in G$,

KNUST

$$\psi(gG_x) = \psi(hG_x) \Rightarrow gG_x = hG_x.$$

Since ψ is homormorphic and on G–sets and also bijective, ψ is isomorphic. □

Proposition 3.2.17. *Let M be a G-set. For each $x \in G$, define $M^x = \{m \in M | xm = m\}$. Then*

$$\frac{1}{|G|}\sum_{x\in G}|M^x| = \text{number of orbits in } M.$$

Proof. M^x considers the set of all points m in M that are stable under the action of $x \in G$. Hence, if we are looking at the number of all x's that fixes the points m in M then we are looking at the sum

$$\sum_{x\in G}|M^x|$$

but this, in terms of the stabilizer subgroup is

$$\sum_{m\in M}|G_m|.$$

Hence,

$$\sum_{x\in G}|M^x| = \sum_{m\in M}|G_m|.$$

Suppose $m,n \in M$ are in the same orbit. Then by the orbit-stabilizer theorem, we have

$$|G_m| = \frac{|G|}{|Gm|} = \frac{|G|}{|Gn|} = |G_n|$$

KNUST
NYANSAPO WO SANE NO BADWENMA

Thus,

$$\sum_{n\in Gm} |G_n| = |Gm||G_m|.$$

But by the orbit-stabilizer theorem $|Gm||G_m|$ is equal to $|G|$ and hence

$$\sum_{n\in Gm} |G_n| = |G|.$$

Suppose there are k distinct orbits that partition the set M then the sum $\sum_{m\in M} |G_m|$ is

$$\sum_{m\in M} |G_m| = \sum_{i=1}^{k}\sum_{n\in Gm} |G_n| = \sum_{i=1}^{k} |G| = k|G|.$$

Substituting we have,

$$\frac{1}{|G|}\sum_{x\in G}|M^x| = \frac{k|G|}{|G|} = k.$$

Therefore $\frac{1}{|G|}\sum_{x\in G}|M^x|$ is the number of orbits in *M.* □

Definition 3.2.18. *Let a group G act on itself by conjugation. If x ∈ G then the set*

$$O(x) = \{y \in G \mid y = gxg^{-1} \textit{ for some } g \in G\}$$

is called the conjugacy class of x and the set

$$C_G(x) = \{g \in G | gxg^{-1} = x\}$$

is said to be the centralizer of x in G. The centralizer $C_G(x)$ of x in G is also stabilizer G_x of x.

Proposition 3.2.19. *The quaternion group Q has 5 conjucacy classes.*

Proof. $Q = \{\pm 1, \pm I, \pm J, \pm K\}$ together with the operation, multiplication determined by

$$I^2 = J^2 = K^2 = -1,\ IJ = K,$$

$$JK = I,\ KI = J.$$

KNUST

Thus, $JI = KI^2 = -K = -IJ$.

Similarly, $KJ = -JK$, $IK = -KI$. 1 is the unit element and $-I$, $-J$, $-K$ are the inverses of I, J, K respectively.

Let $X \in Q$ be any arbitrary element. Then,

$$X1 = 1X \text{ and},$$

$$X(-1) = (-1)X$$

This implies that $C_1 = \{1\}$ and $C_2 = \{-1\}$ are conjugacy classes of Q.

Also,

$$JI(-J) = -JIJ = IJJ = -I,\ KJ(-K) = -KJK = JKK$$

$$= -J.$$

Similarly,

$$IJ(-I) = -IJI = JII = -J,$$

$$KJ(-K) = -KJK = JKK = -J,$$

$$IK(-I) = -K,\ JK(-J) = -K.$$

Thus, the other conjugacy classes of Q are

$$C_3 = \{I, -I\},$$

$$C_4 = \{J,-J\},\ C_5 = \{K,-K\}.$$

Therefore, there are 5 conjugacy classes of Q. □

Proposition 3.2.20. *Let $G \subset S_4$ be the set of all permutations with sign* $+1$*. Then G is a subgroup of S_4 with 4 conjugacy classes.*

Proof.

$$C_1 = \{(1)\},$$

$$C_2 = \{(12),(13),(14),(23),(24),(34)\},$$

$$C_3 = \{(123),(124),(132),(142),(234),(243),(134),(143)\},$$

$$C_4 = \{(12)(34),(13)(24),(14)(23)\},\ C_5 = \{(1234),(1243),(1324),(1423),(1342),(1432)\}.$$

The sign of a permutation is $+1$ if the permutation can be written as a product of even transpositions and -1 if it can be written as a product of odd transpositions.

From this definition, we observe that all elements in C_2 have the sign -1 and those in C_4 have the sign $+1$. The identity element (1) is of sign $+1$. Let us now obtain the sign for elements in the class C_3,C_5.

Let (abc) be an arbitrary element in C_3. We have,

$$(abc) = (ac)(ab),$$

which implies every 3- cycle can be written as a product of 2 transpositions. Since the number 2 is even the sign of all 3 -cycles is $+1$.

Take an arbitrary element $(abcd) \in C_5$, we have,

$$(abcd) = (ad)(ac)(ab),$$

which implies that every 4-cycle can be written as a product of 3 transpositions.

Since the number 3 is odd the sign of all 4 - cycles is -1.

Now we can clearly list the elements in G.

$G = \{(1),(123),(124),(132),(142),(234),(243),(134),(143),(12)(34),(13)(24),(14)(23)\}$. Thus $|G| = 12$.

Let $f,g \in S_4$. If $sgn(f) = sgn(g) = 1$, then $sgn(fg) = sgn(f)sgn(g) = 1$.

Also, $sgn(e) = 1$. Hence G is a subgroup of S_4.

As $|G| = 12$ and there are 4 ways to express 12 as a sum of squares

$$12 = 12 \cdot 1^2,$$

$$12 = 8 \cdot 1 + 2^2,$$

$$12 = 4 \cdot 1^2 + 2 \cdot 2^2,\ 12$$

$$= 3 \cdot 1^2 + 3^2.$$

The first case is ruled out as G is not abelian. So the number k of conjugacy classes is an element of $\{4,8,9\}$.

In S_4 all elements of a given cycle structure are conjugate. It suffices to only determine how the class $C_3, C_4 \subset S_4$ of $(12)(34)$ and (123) decompose into conjugacy classes C_3^i, C_4^j of G.

By direct computations we observe that,

$$(123) \circ (12)(34) \circ (132) =$$

$$(14)(23),\ (124) \circ (12)(34) \circ$$

$$(142) = (13)(24).$$

This shows that C_4 does not decompose in G.

Also,

$$(124) \circ (123) \circ (142) = (243), (142) \circ (123) \circ (124) = (134)$$

KNUST

So the conjugacy class of (123) in G contains at least 3 elements. However, allC_3^j must contain the same number of elements as there is an element of S_4 conjugation by which maps one to any other (this uses the fact that conjugating elements in G by elements in S_4 produces another element in G). Thus they have cardinality 4 or 8, but k is at least 4 and hence it must be 4. Therefore, $k = 4$. □

Definition 3.2.21. *Let G be a group. The center of G is the subgroup*

$$Z(G) = \{x \in G | x = gxg^{-1} \forall g \in G\}$$

consisting of all elements commuting with every element of G.

Definition 3.2.22. *Let G be a finite group and let n be the number of conjugacy classes of order greater than 1. The class equation of G is*

$$|G| = Z(G) + \sum_{i=1}^{n}[G : C_G(x_i)] ,$$

where x_i is a class representative of each conjugacy class of order greater than 1.

3.3 Cardinality

Let A and B be sets.

Definition 3.3.1. *If there is a bijection $f : A \to B$ between A and B, then*

$|A| = |B|$. *Example*

If $A = \{x,y,z\}, B = \{\alpha,\beta,\gamma\}$, then $|A| = |Y|$ because $\{(x,\alpha),(y,\beta),(c,\gamma)\}$ is a bijection between the sets A and B. The cardinality of each of A and B is 3.

Definition 3.3.2. *The product rule*

If the $P_1,P_2,...,P_n$ are sets, then, $|P_1 \times P_2 \times . \quad ... \times P_n| = |P_1|.|P_2|...|P_n|$

Definition 3.3.3. *The sum rule*

If $A_1,A_2,A_3,...A_n$ are disjoint sets, then:

$$|A_1 \cup A_2 \cup ... \cup A_n| = |A_1| + |A_2| + ... + |A_n|$$

3.4 Lie group

Definition 3.4.1. *A lie group is a nonempty subset G which satisfies the following conditions:*

a. G is a group.

b. G is a smooth manifold. This means that G is a differentiable manifold.

c. In particular, the group operation of multiplication,

$$\mu : (gh) \longrightarrow gh \text{ and the inverse map}$$

$$i : G \longrightarrow G$$

$$i : g \longrightarrow g^{-1}\text{are differentible maps(smooth)}$$

Definition 3.4.2. *A Lie Algebra over a field* k = R *or* C *is a vector space* g *together with a bilinear map*

$$\mathrm{g} \times \mathrm{g} \longrightarrow \mathrm{g},$$

$$(X,Y)\ 7\rightarrow [X,Y],$$

KNUST
NYANSAPƆ WↃ SANE NO BADWENMA

known as the Lie bracket such that

1. *$[X,Y] = -[Y,X]$ (anti-commutativity),*
2. *$[[X,Y],Z] + [[Y,Z],X] + [[Z,X],Y] = 0$ (Jacobi identity).*

Definition 3.4.3. *A Compact Lie group is a Lie group which is compact topological manifold. A Lie group which is connected as a topological manifold is said to be a connected Lie group.*

Remark 3.4.4. *A unitary group $G = U(n)$ is a compact, connected Lie group.*

Chapter 4

Review of Separating Sets

4.1 Representation of finite groups

4.1.1 Introduction

In Mathematics, the word "representation" basically means "structure-preserving function". Thus in group theory and ring theory, one would at least say a representation is a homomorphism. Roughly speaking, a representation of a group G is simply a representation of G by matrices or linear transformations. Let V be a finite-dimensional complex vector space.

Definition 4.1.2. *A representation of a group G in a vector space V is a homomorphism*

$$\phi : G \longrightarrow GL(V),$$

or

$$\phi : G \longrightarrow GL_n(\mathbb{C}).$$

Definition 4.1.3. *The degree or dimension of a representation is the dimension of the vector space V.*

Definition 4.1.4. *Let G be a finite group. The homomorphism*

$$\phi : G \longrightarrow GL(V),$$

KNUST

defined by

$$\phi(g) = 1 \forall g \in G,$$

is said to be a trivial representation.

Definition 4.1.5. *Let $G = S_n$ and $GL(V) = \mathbb{C}$. Let*

$$sgn : G \longrightarrow \mathbb{C} \text{ defined by,}$$

$$sgn(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even} \\ -1 & \text{if} \sigma \text{ is odd} \end{cases},$$

be the sign of a cycle in S_n. The homomorphism

$$\phi : G \longrightarrow \mathbb{C},$$

$$\sigma \mapsto sgn(\sigma),$$

is a representation of S_n of degree 1. This representation ϕ is referred to as the sign representation.

Proposition 4.1.6. *Let $V = \mathbb{R}^2$ be a vector space over $\mathbb{R}$ and $G = \langle g \rangle$ be the cyclic group generated by g and of order r. The homomorphism*

$$\phi : G \longrightarrow GL(V) \quad \text{defined by}$$

$$\phi(g^r) = \begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix},$$

is a representation of the cyclic group G.

Let $G = S_n$ and V be a finite dimensional complex vector space. Define a homomorphism

$\phi : G \longrightarrow GL(V)$ on the standard basis elements by

$\phi_\sigma(e_i) = e_{\sigma(i)}$ where $\sigma \in G$ and $e_i \in V$.

Permuting the rows of the identity matrix with respect to σ we obtain a matrix representation for $\phi_\sigma \forall \sigma \in S_n$.

In particular, for $n = 3$ we have

$$\phi_{(1)} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \phi_{(12)} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \phi_{(123)} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

$$\phi_{(23)} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad \phi_{(13)} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad \phi_{(132)} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Definition 4.1.7. *Let G be a finite group. Let V be a vector space with basis of V_G. Left multiplication by $g \in G$ permutes the basis and extends to an invertible linear transformation of V . This gives a representation known as the regular representation of G and is of degree $|G|$.*

Definition 4.1.8. *A permutation matrix is a matrix for which every row or column has exactly one non-zero entry 1.*

A permutation representation is a representation for which every element of a group acts by a permutation matrix.

An example of a permutation representation is the regular representation.

KNUST

Definition 4.1.9. *Let*

$$\phi : G \longrightarrow GL(V)$$

be a representation. A subspace W of a vector space V is said to be stable under G or G-invariant if $\forall g \in G$ and $w \in W$ there exists a homomorphism

$$\phi|_W : G \longrightarrow GL(W) \text{ defined by } \phi|_W$$

$$(g)(w) = \phi_g(w)$$

such that $\phi_g(w) \in W$.

The homomorphism $\phi|_W$ is said to be a subrepresentation of G.

Definition 4.1.10. *Two representations*

$$\phi : G \longrightarrow GL(V) \qquad \text{and } \psi : G \longrightarrow GL(W),$$

are said to be equivalent if there exist an invertible linear transformation

$$T : V \longrightarrow W \text{ such that } T\phi_g T^{-1}$$

$$= \psi_g \, \forall g \in G.$$

This is denoted by $\phi \sim \psi$.

Definition 4.1.11 (Irreducible)**.** *Let*

$$\phi : G \longrightarrow GL(V)$$

be a representation. ϕ is said to be an irreducible representation if the only G-invariant subspaces of V are 0 *and V .*

Every degree one representation of a group is irreducible since there are no proper non-zero subspaces. The converse however is not always true. That is, not every irreducible representation has degree one. For example when a matrix is not diagonalizable, the corresponding representation is a direct sum of irreducible representations, not all of which are of degree 1.

Definition 4.1.12. *Let G be a group. A vector space V is said to be completely reducible if it is a direct sum of G-invariant subspaces of V . That is* $V = \oplus_{i=1}^{n} V_i$ *where V_i is a non-zero G-invariant subspace of V for each i. A representation*

$$\phi : G \longrightarrow GL(V)$$

is completely reducible if V is completely reducible and the restriction $\phi|_{V_i}$ is irreducible.

Definition 4.1.13. *Let V be an inner product space. A representation*

$$\rho : G \longrightarrow GL(V)$$

is said to be a unitary representation, if $\forall g \in G$, v,w,$\in V$

h$\rho(g)(v)$,$\rho(g)(w)$i = hv,wi.

Definition 4.1.14. *Given an inner product space V and a subspace W of V , there exists a direct sum decomposition $V = W \oplus W^{\perp}$.* **Definition 4.1.15.** *Let V be a complex vector space. The map,*

$$\langle\bullet,\bullet\rangle : V \times V \longrightarrow \mathbb{C},$$

such that

1. $\langle v,w\rangle = \overline{\langle w,v\rangle}.$

2. $\langle \lambda u + v,w\rangle = \lambda\langle u,w\rangle + \langle v,w\rangle$ *for* $\lambda \in \mathbb{C}$, $u,v,w \in V.$

3. $\langle v,v\rangle \geq 0.$

4. $\langle v,v\rangle = 0 \leftrightarrow v = 0.$

is said to be a Hermitian inner product on V. **Definition 4.1.16.**

Let

$$\rho : G \longrightarrow GL(V)$$

be a representation of G. The map,

$$(\bullet,\bullet) : V \times V \longrightarrow \mathbb{C} \text{ defined by}$$

$$(v,w) = \sum_{g\in G} \langle \rho(g)(v),\rho(g)(w)\rangle$$

is a Hermitian inner product and $\forall g \in G$, $v,w \in G$ *we have*

$$(\rho(g)(v),\rho(g)(w)) = (v,w)$$

that is $\rho(g)$ *is unitary with respect to* $(\bullet,\bullet)$.

Lemma 4.1.17. *A G-invariant subspace* $W \subset V$ *has an G-invariant complement* $U \subset V$.

Proof. Let U be the orthogonal complement of W,

KNUST
NYANSAPƆ WƆSANE NO BADWENMA

$$U = W^{\perp} = \{u \in V \,|\mathrm{h}u,w\mathrm{i} = 0 \forall w \in W\}.$$

This is a subspace since for $\lambda \in$ C, $u,v \in U$ and $w \in W$ we have,

$$\mathrm{h}\lambda u + v,w\mathrm{i} = \lambda \mathrm{h}u,w\mathrm{i} + \mathrm{h}v,w\mathrm{i} = 0,$$

if $v \in U \cap W \Rightarrow \mathrm{h}v,v\mathrm{i} = 0 \Rightarrow v = 0$.

Using the property: $x^{\perp\perp} = x$, we obtain

$$(U + W)^{\perp} = U^{\perp} \cap W^{\perp} = W^{\perp\perp} \cap W^{\perp} = W \cap W^{\perp} = \{0\} \Rightarrow U + W = V.$$

Finally, if $g \in G$, $u \in U$, $w \in W$ and ρ is a unitary representation of G then,

$$\mathrm{h}\rho(g)(u),w\mathrm{i} = \mathrm{h}\rho(g^{-1})\rho(g)(u),\rho(g^{-1})(w)\mathrm{i} \text{ since } \rho \text{ is unitary } \Rightarrow$$

$$\mathrm{h}\rho(g)(u),w\mathrm{i} = 0 \text{ since } \rho(g^{-1})(w) \in W.$$

Therefore U is invariant. □

Let us now show that every complex representation can be decomposed into a direct sum of irreducible subrepresentation.

Theorem 4.1.18 (Masche)**.** *Let V be a representation of a finite group G. Suppose W is a G-invariant subspace of V . Then there exists a G-invariant subspace U of V such that V = W ⊕ U.*

Proof. Let $W^{\perp}$ be a complement of W in V such that $V = W \oplus W^{\perp}$. Let $\alpha : V \longrightarrow W$ be the projection of V onto W along $W^{\perp}$ be defined such that if $v = w + w^{\perp}$ then $\alpha(v) = w$.

Let $\overline{\alpha}$, the average of α over G be defined as

$$\overline{\alpha}(v) = \frac{1}{G}\sum_{g \in G} \varphi(g)\alpha(\varphi(g^{-1})(v)) \;\; \forall v \in V$$

and ϕa representation of *G.*

For simplicity, we set $\phi(g)\alpha(\phi(g^{-1})(v))$ to $g\alpha(g^{-1}v)$. To complete the proof, we prove that $\overline{\alpha}$ is a linear transformation and to do so, we prove the following claim.

Claim 4.1.19. *1.* $\overline{\alpha} : V \longrightarrow W$*.*

2. $\overline{\alpha}(w) = w \; \forall w \in W$*.*

3. If $h \in G$ *then* $h\alpha(\overline{v}) = \alpha(h\overline{v}) \forall v \in V$

Proof of Claim4.1.19. 1. $\forall v \in V$ we have, $\alpha(g^{-1}v) \in W$ and hence $g\alpha(g^{-1}v) \in gW \subset W \; \forall v$ since W is G-invariant.

2.

$$\begin{aligned}
\overline{\alpha}(w) &= \frac{1}{|G|}\sum_{g \in G} g\alpha(g^{-1}w) \\
&= \frac{1}{|G|}\sum_{g \in G} g(g^{-1}w), \\
&= \frac{1}{|G|}\sum_{g \in G} w \\
&= \frac{1}{|G|}|G|w, \\
&= w.
\end{aligned}$$

,

Thus, 1, and 2 implies $\overline{\alpha}$ projects V onto W.

3.

$$
\begin{aligned}
h\overline{\alpha}(v) &= h\frac{1}{|G|}\sum_{g\in G} g\alpha(g^{-1}v),\\
&= \frac{1}{|G|}\sum_{g\in G} hg\alpha(g^{-1}v),\\
&= \frac{1}{|G|}\sum_{g\in G} hg\alpha(g^{-1}h^{-1}hv)\\
&= \frac{1}{|G|}\sum_{g\in G} hg\alpha((hg)^{-1}hv), \quad ,\\
&= \frac{1}{|G|}\sum_{g\in G} k\alpha(k^{-1}hv\\
&= \frac{1}{|G|}\sum_{g\in G} kk^{-1}hv,\\
&= \frac{1}{|G|}\sum_{g\in G} hv,\\
&= hv, \qquad\qquad) \text{ where } k = hg,
\end{aligned}
$$

$= \overline{hv}$ by 2.

Thus, $\overline{\alpha}$ is a linear transformation. □

Finally, we prove the claim

Claim 4.1.20. kerα $\overline{is}$ *G- invariant.*

Proof of Claim 4.1.20. Let $v \in$ kerα, then $\alpha(\overline{hv}) = h\alpha(v) = \overline{0}$ and hence $hv \in$ ker$\overline{\alpha}$. □

Now, $V = \overline{Im}(\alpha) \oplus \ker\alpha$. But $\overline{Im}(\alpha) = W$ and set $\overline{\ker}\alpha = U$. Therefore, $V = W \oplus U$ is a G-subspace decomposition. □

Let $Hom_G(V,W)$ denote the set of all homomorphisms from V to W

Lemma 4.1.21 (Schur)**.** *Let ϕ and ψ be irreducible representations of G and $T \in Hom_G(V,W)$. Then T is either invertible or $T = 0$, consequently,*

1. *if $\phi \sim \psi$, then $Hom_G(\phi,\psi) = 0$*
2. *If $\phi = \psi$, then $T = \lambda I$ with $\lambda \in$ C.*

Proof. See [?] □

4.2 Character Theory

In this section, we review an important tool in the study of representation theory, the "character" of a representation. Informally, the character of a group is a function of the group which associates to each element, the trace of the corresponding matrix representation. In general, the character of a group encodes salient information about the representation in a more condensed form, but is a more specific case, the characters of irreducible representations tend to convey much salient informations and properties of a group and we can therefore use it to study the group's structure. According to Ayekple [?],When it comes to the classification of finite simple groups, character theory plays a major role.

Definition 4.2.1. *Let V be a finite-dimensional vector space over a field say* $K = C$ *and let*

$$\phi : G \longrightarrow GL(V),$$

be a representation of a group G on V. The character of ϕ is the function

$$\chi_\phi : G \longrightarrow C \text{ defined by}$$

$$\chi_\phi(g) = Tr(\phi(g)),$$

where Tr is the trace of a linear map.

Definition 4.2.2. *Let $\phi : G \longrightarrow GL(V)$ be a representation.*

1. *The character χ_ϕ is said to be irreducible if ϕ is irreducible.*

2. *The character χ_ϕ is linear if the dimension of ϕ is one.*

Remark 4.2.3. 1. If $\phi : G \longrightarrow GL_n(\mathrm{C})$ is a representation defined by $\phi_g = (\phi_{ij}(g))$ then

$$\chi_\varphi(g) = \sum_{i=1}^{n} \varphi_{ii}(g).$$

2. If G is finite and k is of characteristic 0 then the kernel of the character χ_ϕ is the normal subgroup,

$$\ker\chi_\phi = \{g \in G|\chi_\phi(g) = \chi_\phi(1)\},$$

which is simply, the kernel of the representation ϕ.

Proposition 4.2.4. *Let*

$$\phi : G \longrightarrow GL(V),$$

be a representation. Then

$$\chi_\phi(1) = \deg\phi.$$

Proof. By definition, $\chi_\phi(g) = Tr(\phi(g))$ and hence for $g = 1$ we have,

$$\chi_\phi(1) = Tr(\phi(1)) = Tr(I) = \dim V = \deg\phi.$$

□

Lets us now examine one of the properties of a character of a representation. One of the main properties is that the character depends on the equivalent classes of the representation.

Proposition 4.2.5. *If ϕ and τ are equivalent representations, then*

$$\chi_\phi = \chi_\tau.$$

Proof. Suppose $\phi,\tau : G \longrightarrow GL_n(\mathbb{C})$ are equivalent representations. Then there exist an invertible matrix $T \in GL_n(\mathbb{C})$ such that

$$\phi_g = T\tau_g T^{-1} \forall g \in G,$$

$$\Rightarrow \chi_\phi(g) = Tr(T\tau_g T^{-1}),$$

$$= Tr(T^{-1}T\tau_g), \text{ by the properties of a trace } =$$

$$Tr(\tau_g) = \chi_\tau(g).$$

□

The next property shows that the character is invariant on conjugacy classes.

Proposition 4.2.6. *Let ϕ be a representation of a group G. Then $\forall g, h \in G$*

$$\chi_\phi(g) = \chi_\phi(hgh^{-1}).$$

Proof.

$$\chi_\phi(hgh^{-1}) = Tr(\phi(hgh^{-1})),$$

$$= Tr(\phi(h)\phi(g)\phi(h^{-1})),$$

$$= Tr(\phi(h^{-1})\phi(h)\phi(g)), \quad \text{by the properties of a trace}$$

$$= Tr(\phi(g)), =$$

$$\chi_\phi(g).$$

□

Proposition 4.2.7. *Let $\phi : G \longrightarrow GL(V)$ be a representation of the finite group G. Then*

$$\chi_{\phi}(g^{-1}) = \chi_{\phi}(g)\ \forall g \in G.$$

Proof. For any $g, \in, G$, the order of g is finite and hence its representation has a finite number of eigenvalues.

Suppose ϕ is an n-dimensional representation of the finite group G. Let $\lambda_1,...,\lambda_n \in$ C, $|\lambda_i| = 1 \forall i$ be the eigenvalues of the matrix associated to $\phi(g)$. Suppose,

$$\phi(g) = \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & \vdots \\ \vdots & \cdots & \cdots & 0 \\ 0 & \cdots & 0 & \lambda_n \end{pmatrix}.$$

Then

$$\chi_{\varphi}(g) = \sum_{i=1}^{n} \lambda_i \ .$$

Now, the eigenvalues of the matrix associated to $\phi(g^{-1})$ are $\lambda_1^{-1}, \lambda_2^{-1}, \ldots, \lambda_n^{-1}$ and hence,

$$\phi(g^{-1}) = \begin{pmatrix} \lambda_1^{-1} & 0 & \cdots & 0 \\ 0 & \lambda_2^{-1} & \cdots & \vdots \\ \vdots & \cdots & \cdots & 0 \\ 0 & \cdots & 0 & \lambda_n^{-1} \end{pmatrix}.$$

Thus,

KNUST
NYANSAPO WO SANE NO BADWENMA

$$\chi_\varphi(g^{-1}) = \sum_{i=1}^{n} \lambda_i^{-1} = \sum_{i=1}^{n} \overline{\lambda_i}$$

$$= \overline{\sum_{i=1}^{n} \lambda_i},$$

,

$$= \overline{\chi_\phi(g)}.$$

□

KNUST

Definition 4.2.8 (Group algebra)**.** *Let G be a group. Define* C*G* = {*f*|*f* : *G* −→ C}*. Then* C*G is an inner product space with* + *and* × *given by*

$$(f_1 + f_2)(g) = f_1(g) + f_2(g),\ (cf)(g) =$$

$$cf(g),$$

and with inner product defined by

$$\langle f_1, f_2\rangle = \frac{1}{|G|}\sum_{g\in G} \overline{f_1(g)} f_2(g)$$

.

C*G is called the group algebra of G.*

Theorem 4.2.9 (Schur orthogonality relations)**.** *Let* $\phi : G \longrightarrow U_n(\mathbb{C})$ *and* $\rho :$

$G \longrightarrow U_m(\mathbb{C})$ *be inequivalent irreducible unitary representations. Then*

$\langle \rho_{kl}, \varphi_{ij}\rangle = 0.$

$$\langle \varphi_{kl}, \varphi_{ij}\rangle = \begin{cases} \frac{1}{n} & if\ i = k \text{ and } j = l, \\ 0 & otherwise \end{cases}$$

1.

2..

Proof. See [**?**]. □

Definition 4.2.10 (Class function)**.** *A class function is a function f* : *G* −→ C *for which*

f is constant on conjugacy classes of G or equivalently, $f(g) = f(hgh^{-1})\forall g, h \in G$*.*

W J SANE NO BADWENMA

From Proposition 4.2.6, one can clearly deduce that a character of a representation is a class function. The space of class functions is the center of the group algebra $\mathbb{C}G$ and is denoted by $Z(\mathbb{C}G)$.

Proposition 4.2.11. *Let M be a G-set. Let $M^x = \{m \in M | x \triangleright m = m\}$ for each $x \in G$. Then the character π of the permutation representation on $\mathbb{C}M$ is given by $\pi(x) = |M^x|$.*

Proof. We start by defining a vector space for the permutation representation, followed by a linear map and a basis for the vector space.

Let $V = \mathbb{C}M$ be a vector space and let the linear map

$$\rho(x) : V \longrightarrow V,$$

be a permutation representation on V.

Let

$$\delta_m : M \longrightarrow \mathbb{C} \quad \text{defined by}$$

$$\delta_m(n) = \begin{cases} 1 & \text{if } m = n \\ 0 & otherwise \end{cases}.$$

We claim that the set $\{\delta_m\}_{m \in M}$ is the basis for V.

Given $f \in V$ is $f = \sum_{m \in M} \lambda_m \delta_m$ for some $\lambda_m \in \mathbb{C}$ we have for every $n \in M$,

$$f(n) = \sum_{m \in M} \lambda_m \delta_m(n) = \lambda_n.$$

This implies that for every $f \in V$ we can write,

$$f = \sum f(m)\delta_m,$$

KNUST

$m\in M$

which is a linear combination of the δ_m and thus $\{\delta_m\}$ spans V.

Next, we show that the set $\{\delta_m\}$ is linearly independent.

Suppose that

$$\sum_{m\in M}\lambda_m\delta_m = 0,$$

is the zero function, then acting it on n gives,

$$\sum_{m\in M}\lambda_m\delta_m(n) = 0,$$

$$\Longrightarrow \lambda_n = 0.$$

This shows that the $\{\delta_m\}$ is a linearly independent set.

Therefore $\{\delta_m\}$ is a basis for V.

Now, we act the permutation representation $\rho(x)$ on the basis vectors, since acting a linear map on the basis vectors gives the entries a_{nm} of its matrix representation.

$$\rho(x)(\delta_m) = \sum_{n\in M} a_{nm}\delta_n \qquad \text{where} \quad a_{nm}\in \mathbb{C}.$$

Let $\rho(x)(\delta_m) = \delta_m(x^{-1}\ )$ which is a function in V and since every function in V can be written as a linear combination of the basis we have,

$$\delta_m(x^{-1}\ ) = \sum_{n\in M}\delta_m(x^{-1}\triangleright n)\delta_n .$$

By comparison we have,

$$a_{nm} = \delta_m(x^{-1}\triangleright n).$$

KNUST

The character π is defined by

$$\pi(x) = tr(\rho(x)) = \sum_{m \in M} \delta_m(x^{-1} \rhd m) \quad ,$$

but

$$\delta_m(x^{-1} \rhd m) = \begin{cases} 1 & \text{if } x^{-1} \rhd m = m \Rightarrow m = x \rhd m \\ 0 & otherwise \end{cases} \quad .$$

We can restrict M to M^x since $\forall m \notin M^x,\ \delta_m(x^{-1} \rhd m) = 0$.

Therefore

$$\pi(x) = \sum_{m \in M^x} \delta_m(x^{-1} \rhd m) = \sum_{m \in M^x} 1 = |M^x| \quad .$$

□

Theorem 4.2.12 (First orthogonality relation)**.** *Let ϕ and ψ be irreducible representations of G. Then*

$$\langle \chi_\varphi, \chi_\psi \rangle = \begin{cases} 1 & \varphi \sim \psi \\ 0 & \varphi \nsim \psi \end{cases} .$$

Thus, the irreducible characters of a group G form an orthonormal set of class functions.

Proof. Suppose ϕ and ψ are unitary representations.

$$\begin{aligned} \langle \chi_\varphi, \chi_\psi \rangle &= \frac{1}{|G|} \sum_{g \in G} \overline{\chi_\varphi(g)} \chi_\psi(g), \\ &= \frac{1}{|G|} \sum_{g \in G} \sum_{i=1}^{n} \overline{\varphi_{ii}(g)} \sum_{j=1}^{m} \psi_{jj}(g) \\ &= \sum_{i=1}^{n} \sum_{j=1}^{m} \frac{1}{|G|} \sum_{g \in G} \overline{\varphi_{ii}(g)} \psi_{jj}(g), \\ &= \sum_{i=1}^{n} \sum_{j=1}^{m} \langle \varphi_{ii}(g), \psi_{jj}(g) \rangle. \end{aligned} \quad ,$$

By the Schur's orthogonality theorem $\langle \varphi_{ii}(g), \psi_{jj}(g) \rangle = 0$ if $\varphi \nsim \psi$ and hence $\langle \chi_\varphi, \chi_\psi \rangle = 0$ if $\varphi \nsim \psi$.

If $\phi \sim \psi$, then we may assume $\phi = \psi$. Under such circumstances, the Schur's orthogonality relation tell us

$$\langle \varphi_{ii}(g), \psi_{jj}(g) \rangle = \begin{cases} \frac{1}{n} & i = j \\ 0 & i \neq j \end{cases}$$

This implies that

$$\langle \chi_\varphi, \chi_\psi \rangle = \sum_{i=1}^{n} \langle \varphi_{ii}(g), \psi_{jj}(g) \rangle = \sum_{i=1}^{n} \frac{1}{n} = 1 .$$

□

Theorem 4.2.13 (Second orthogonality relation)**.** *Let C, C^0 be conjugacy classes of G. Let g ∈ C and h ∈ C$_0$ and s be the number of inequivalent representations of G. Then*

$$\sum_{i=1}^{s} \overline{\chi_i(g)} \chi_i(h) = \begin{cases} \frac{|G|}{|C|} & C = C' \\ 0 & C \neq C' \end{cases} .$$

Proof. Let *C* be a conjugacy class of *G*. Define the function

$\delta_C : G \longrightarrow \mathbb{C}$ by,

$$\delta_C = \begin{cases} 1 & g \in C, \\ 0 & \text{otherwise} \end{cases} .$$

Let

$$\delta_C = \sum_{i=1}^{s} \langle \chi_i, \delta_C \rangle \chi_i .$$

Then

KNUST
NYANSAPO
W J SANE NO BADWENMA

$$\begin{aligned}
\delta_C(h) &= \sum_{i=1}^{s}\langle\chi_i,\delta_C\rangle\chi_i(h),\\
&= \sum_{i=1}^{s}\frac{1}{|G|}\sum_{x\in G}\overline{\chi_i(x)}\delta_C(x)\chi_i(h)\\
&= \frac{1}{|G|}\sum_{i=1}^{s}\left(\sum_{x\in C}\overline{\chi_i(x)}\right)\chi_i(h),\\
&= \frac{1}{|G|}\sum_{i=1}^{s}\left(|C|\overline{\chi_i(g)}\right)\chi_i(h),\\
&= \frac{|C|}{|G|}\sum_{i=1}^{s}\overline{\chi_i(g)}\chi_i(h).
\end{aligned}$$

,

By definition of δ_C, we have that $\delta_C(h) = 1$ whenever $h \in G$ and in this case we must have,

$$\sum_{i=1}^{s}\overline{\chi_i(g)}\chi_i(h) = \frac{|G|}{|C|},$$

and $\delta_C(h) = 0$ whenever h 6∈ C and this implies

$$\sum_{i=1}^{s}\overline{\chi_i(g)}\chi_i(h) = 0 .$$

Therefore

$$\sum_{i=1}^{s}\overline{\chi_i(g)}\chi_i(h) = \begin{cases}\frac{|G|}{|C|} & C = C'\\ 0 & C \neq C'\end{cases} .$$

□

Corollary 4.2.14. *The number of inequivalent irreducible representations of a finite group G is equal to the number of conjugacy classes of G.*

For a proof to the corollary, kindly refer to [**?**].

Let us now build some notations which are salient for the understanding of the remaining theorems and proofs.

If V is a vector space and ϕ is a representation of a finite group G. Then for $m \in \mathbb{Z}$ with $m > 0$, we set

$$mV = \bigoplus_{i=1}^{m} V,$$
$$m\varphi = \bigoplus_{i=1}^{m} \varphi.$$

KNUST

Let $\{\phi^i,\ldots,\phi^s\}$ be a complete set of irreducible unitary representation of G. Set, up to equivalence, $d_i = \deg\phi^i$.

Definition 4.2.15. *Let $\phi : G \longrightarrow GL(V)$ be a representation of a group G. If $\varphi \sim \bigoplus_{i=1}^{s} m_i\varphi^i$ then the integer, m_i is said to be the multiplicity of ϕ^i in ϕ. If $m_i > 0$ then ϕ^i is said to be an irreducible constituent of ϕ.*

Remark 4.2.16. If $\varphi \sim \bigoplus_{i=1}^{s} m_i\varphi^i$ then

$$\deg \varphi = \sum_{i=1}^{s} m_i d_i .$$

Lemma 4.2.17. *Let ϕ,φ and τ be representation of a group G. Then $\chi_\phi = \chi_\varphi + \chi_\tau$.*

Proof. Suppose that $\varphi : G \longrightarrow GL_n(\mathbb{C})$ and $\tau : G \longrightarrow GL_n(\mathbb{C})$ are irreducible representations of G. Then $\phi : G \longrightarrow GL_{m+n}(\mathbb{C})$ is of the form

$$\phi(g) = \begin{pmatrix} \varphi_g & 0 \\ 0 & \tau_g \end{pmatrix} \chi_\phi(g) = Tr(\phi(g)) = Tr(\varphi(g)) + Tr(\tau(g)),$$
$$= \chi_\varphi(g) + \chi_\tau(g),$$

Thus,$\chi_\phi = \chi_\varphi + \chi_\tau$ □

The above lemma implies that every character is an integral linear combination of irreducible characters.

Theorem 4.2.18. *Let $\phi^1,...,\phi^s$ be a complete set of representations of the equivalence classes of irreducible representations of G and let* $\varphi \sim \bigoplus_{i=1}^{s} m_i\varphi^i$ *then* m_i = hχ_{ϕ_i},χ_φi*. Therefore there exists a unique decomposition of ϕ into irreducible constituents and ϕ is determined up to equivalence by its character.*

Proof. By Lemma 4.2.17,

$$\chi_\varphi = \sum_{i=1}^{s} m_i \chi_{\varphi^i}$$

Thus,

$$\langle \chi_{\varphi^i}, \chi_\varphi \rangle = \sum_{k=1}^{s} m_i \langle \chi_{\varphi^i}, \chi_{\varphi^k} \rangle$$

$$= m_i \text{ for } i = 1,2,...,s$$

by the orthogonality relation. The other statements are generated from Proposition 4.2.5. □

Corollary 4.2.19. *A representation τ is irreducible if and only if* hχ_τ,χ_τi = 1*.*

Proof. Suppose $\tau \sim \bigoplus_{i=1}^{s} m_i\varphi^i$. Then

$$h\chi_{\tau},\chi_{\tau}i = \overset{s}{\underset{i=1}{X}} m_{2i},$$

by the orthonormality of the irreducible characters. Since $m_i \geq 0$ is a positive integer, hχ_τ,χ_τi = 1 if and only if there exist a j such that $m_j = 1$ and $m_i = 0$ for i 6= j. This is only possible if τ is irreducible.□

Let $G = S_3$ act on the set $X = 1,2,3$. Let $\sigma,\alpha \in S_3$ such that

$\sigma(1) = 2$, $\sigma(2) = 1$, and $\sigma(3) = 3$, $\alpha(1) =$
1, $\alpha(2) = 3$, and $\alpha(3) = 2$.

Let $\phi : S_3 \longrightarrow GL(V)$ be a 2-dimensional representation of S_3 is given by

$$\varphi(\sigma) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \ \varphi(\alpha) = \frac{1}{2}\begin{pmatrix} 1 & -\sqrt{3} \\ \sqrt{3} & -1 \end{pmatrix}.$$

$$\varphi(\sigma \circ \alpha) = \frac{1}{2}\begin{pmatrix} -1 & -\sqrt{3} \\ -\sqrt{3} & -1 \end{pmatrix}, \ \varphi(\alpha \circ \sigma) = \frac{1}{2}\begin{pmatrix} -1 & \sqrt{3} \\ -\sqrt{3} & -1 \end{pmatrix}$$

$$\varphi(\sigma \circ \alpha \circ \sigma) = \frac{1}{2}\begin{pmatrix} 1 & -\sqrt{3} \\ -\sqrt{3} & -1 \end{pmatrix}, \ \varphi(e) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

,

KNUST

Theorem 4.2.20. *The 2-dimensional representation φ of S_3 is irreducible.*

Proof. The character of this representation is given by,

$$\chi_\phi(e) = 2, \chi_\phi(\sigma) = \chi_\phi(\alpha) = \chi_\phi(\sigma \circ \alpha \circ \sigma) = 0, \chi_\phi(\sigma \circ \alpha) = \chi_\phi(\alpha \circ \sigma),$$

Thus, computing the inner product gives

$$\begin{aligned} \langle \chi_\varphi, \chi_\varphi \rangle &= \frac{1}{|S_3|}\sum_{g \in S_3} |\chi_\varphi|, \\ &= \frac{1}{6}((-1)^2 + (-1)^2 + (2^2)) \\ &= 1. \end{aligned}$$

,

Thus, ϕ is an irreducible representation. □

Let $f : \mathbb{C}^2 \longrightarrow \mathbb{C}^2$ be given by multiplication by the matrix

$$a = \frac{1}{2}\begin{pmatrix} -1 & -\sqrt{3} \\ \sqrt{3} & -1 \end{pmatrix}.$$

Then,

$$\begin{aligned} a^2 &= \frac{1}{2}\begin{pmatrix} -1 & -\sqrt{3} \\ \sqrt{3} & -1 \end{pmatrix} \frac{1}{2}\begin{pmatrix} -1 & -\sqrt{3} \\ \sqrt{3} & -1 \end{pmatrix} \\ &= \frac{1}{4}\begin{pmatrix} -2 & -2\sqrt{3} \\ -2\sqrt{3} & -2 \end{pmatrix}, \\ &= \frac{1}{2}\begin{pmatrix} -1 & \sqrt{3} \\ -\sqrt{3} & -1 \end{pmatrix}. \end{aligned}$$

,

and

$$\begin{aligned} a^3 &= \frac{1}{2}\begin{pmatrix} -1 & -\sqrt{3} \\ \sqrt{3} & -1 \end{pmatrix} \frac{1}{2}\begin{pmatrix} -1 & \sqrt{3} \\ -\sqrt{3} & -1 \end{pmatrix} \\ &= \frac{1}{4}\begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}, \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

,

Define the map

$$\phi : \mathbb{Z}_3 \longrightarrow GL_2(\mathbb{C}) \text{ by, } \phi(n) = a^n.$$

For all $x,y \in \mathbb{Z}_3$ we have,

$$\begin{aligned} \phi(x+y) &= a^{x+y}, \\ &= a^x a^y, \\ &= \phi(x)\phi(y). \end{aligned}$$

Therefore ϕ is a representation.

Computing the characters yields,

$$\chi_\varphi(0) = Tr\left(\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\right) = 2$$

$$\chi_\varphi(1) = Tr(a) = \frac{1}{2}(-2) = -1,$$

$$\chi_\varphi(2) = Tr\left(a^2\right) = -1,$$

Next, we compute the inner product.

$$\begin{aligned}\langle \chi_\varphi, \chi_\varphi \rangle &= \frac{1}{3}\sum_{x\in\mathbb{Z}_3} \overline{\chi_\varphi(x)}\chi_\varphi(x),\\ &= \frac{1}{3}(2^2 + (-1)^2 + (-1)^2)\\ &= \frac{1}{3}(4+1+1) = 2.\end{aligned}$$

,

Since hχ_ϕ,χ_ϕi 6= 1, we conclude that ϕ is not irreducible.

Theorem 4.2.21. *Recall the quaternion group is the set Q = {±1,±I,±J,±K} together with the operation, multiplication determined by*

$$I^2 = J^2 = K^2 = -1,\ IJ = K,$$

$$JK = I,\ KI = J.$$

Thus, $JI = KI^2 = -K = -IJ$.

Similarly, $KJ = -JK$, $IK = -KI$. 1 is the unit element and $-I$, $-J$, $-K$ are the inverses of I, J, K respectively.

Consider the Pauli matrices:

KNUST
W J SANE NO BADWENMA

$$\hat{I} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \hat{J} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \hat{K} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

The map

$$\phi : Q \longrightarrow GL_2(\mathbb{C}) \text{ defined by,}$$
$$\pm 1 \mapsto \pm id,$$
$$\pm X \mapsto \pm \hat{X} \text{ where } X = I, J, K$$

is an irreducible representation of Q.

Proof. To show that ϕ is a representation, we show that it is a homomorphism.

$$\phi(IJ) = \phi(K) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

$$\phi(I)\phi(J) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},$$

$$= \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} = \phi(IJ),$$

$$\phi(-IJ) = \phi(-K) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

$$\phi(-I)\phi(J) = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},$$

$$\begin{pmatrix}0 & i\\ i & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix} = \begin{pmatrix}-i & 0\\ 0 & i\end{pmatrix} = \phi(-IJ),$$

$$\phi(JK) = \phi(I)\begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix},$$

$$\phi(J)\phi(K) = \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}\begin{pmatrix}0 & i\\ i & 0\end{pmatrix} = \begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix} = \phi(JK),$$

$$\phi(KI) = \phi(J)\begin{pmatrix}0 & i\\ i & 0\end{pmatrix},$$

$$\phi(K)\phi(I) = \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix} = \begin{pmatrix}0 & i\\ i & 0\end{pmatrix} = \phi(KI).$$

Continuing for the other elements, we observe that ϕ is a homomorphism.

Therefore ϕ is a representation.

Computing the character χ_ϕ of the Pauli representation of Q gives

$$\chi_\phi(\pm 1) = \pm 2, \text{ and } \chi_\phi(\pm X) = 0, \text{ where } X = I,J,K.$$

Next, we compute the inner product

$$\langle \chi_\varphi, \chi_\varphi \rangle = \frac{1}{8}((-2)^2 + (2)^2) = 1$$

Thus, ϕ is an irreducible representation. □

Character Table

A character table, roughly, is a two dimensional table whose rows correspond to irreducible representations and whose columns corresponds to the classes of group elements.

Definition 4.2.22. *Let G be a finite group with s conjugacy classes and s irreducible characters. The character table of G is an array with s rows labeled by the s inequivalent irreducible characters of G and s columns labeled by the s conjugacy classes of G. The entries in a row are values of the character on the representatives of the respective conjugacy classes of G.*

Remark 4.2.23. It is customary to label the first row by the trivial character and the first column by the conjugacy classes of the identity. The entries in the first column encode informations about the degree of the irreducible characters. Each conjugacy class, say the jth conjugacy class C_j, is indicated by a representative $c_j \in C_j$ and hence each (i,j)th entry has values $\chi_i(c_j)$.

Theorem 4.2.24. *Given a finite group G with conjugacy classes $C_1, C_2, ... C_d$ and irreducible characters $\chi_1, \chi_2, ..., \chi_d$. If $\Gamma \in M_d(\mathbb{C})$ is the character table,* Table 4.1: The character table.

	c_1	c_2	...	c_s
χ_1	$\chi_1(c_1)$	$\chi_1(c_2)$	...	$\chi_1(c_s)$
χ_2	$\chi_2(c_1)$	$\chi_2(c_2)$	...	$\chi_2(c_s)$
...	...	...	...	...
χ_s	$\chi_s(c_1)$	$\chi_s(c_2)$	...	$\chi_s(c_s)$

$\Gamma_{ij} = \chi_i(x_j), x_j \in C_j$, *then*

$$|det(\Gamma)| = \sqrt{\frac{|G|^d}{|C_1|...|C_d|}}.$$

Proof. We have that $\Gamma = [\Gamma_{ij}]$ where $\Gamma_{ij} = \chi_i(x_j), x_j \in C_j$.

Let Γ^0 be a matrix defined by

KNUST

$$\Gamma^0 = [|C_i|\overline{\Gamma_{ji}}],$$

where $\overline{\Gamma_{ij}}$ are the elements of the conjugate transpose $\Gamma^\dagger$ of Γ.

Post multiply Γ by Γ^0

$$\Gamma\Gamma' = [\Gamma_{ij}] \left[|C_i|\overline{\Gamma_{ji}}\right],$$

The entries of this matrix looks like:

$$\begin{aligned}
(\Gamma\Gamma')_{ij} &= \sum_{k=1}^{d} \Gamma_{ik}\overline{\Gamma_{jk}}|C_k|, \\
&= \sum_{k=1}^{d} \chi_i(x_k)\overline{\chi_j(x_k)}|C_k| \\
&= \sum_{g\in G} \chi_i(g)\overline{\chi_j(g)}, \\
&= |G|\langle\chi_i, \chi_j\rangle, \quad ,
\end{aligned}$$

but by the orthonormality of irreducible characters we have

$$\langle\chi_i, \chi_j\rangle = \begin{cases} 1 & \text{ifif } i = j \\ 0 & \text{if } i \; 6= j \end{cases}.$$

This implies that $h\chi_i,\chi_j i = \delta_{ij}$ and hence

$$(\Gamma\Gamma^0)_{ij} = |G|\delta_{ij}.$$

NYANSA PO WOSANE NO BADWENMA

The product $(\Gamma\Gamma^0)_{ij}$ can be written as

$$\begin{aligned}(\Gamma\Gamma')_{ij} &= |C_i|\Gamma_{ij}\overline{\Gamma_{ji}},\\ &= |C_i|\left(\Gamma\Gamma^{\dagger}\right)_{ij},\end{aligned}$$

dividing through by $|C_i|$ we have,

$$\frac{1}{|C_i|}(\Gamma\Gamma')_{ij} = \left(\Gamma\Gamma^{\dagger}\right)_{ij}.$$

Substituting the expression for $(\Gamma\Gamma^0)_{ij}$ into the above equation we have,

$$\Gamma\Gamma^{\dagger}\right)_{ij} = \frac{1}{|C_i|}|G|\delta_{ij}.$$

This shows that the product $\Gamma\Gamma^{\dagger})$ is a diagonal $d \times d$ matrix and hence the determinant will be the product of its main diagonal entries i.e.

$$det\left(\Gamma\Gamma^{\dagger}\right) = \prod_{i=1}^{d}\frac{|G|}{|C_i|}.$$

From the properties of determinant of matrices we have,

$$det\left(\Gamma\Gamma^{\dagger}\right) = det\left(\Gamma\right)det(\Gamma^{\dagger}) ,$$

$= det\left(\Gamma\right)\overline{det}$ (Γ) by properties of conjugate transpose,

$= |det(\Gamma)|^2.$

Therefore,

$$\begin{aligned}|det\left(\Gamma\right)|^2 &= \prod_{i=1}^{d}\frac{|G|}{|C_i|},\\ &= \frac{|G|^d}{\prod_{i=1}^{d}|C_i|}.\end{aligned}$$

KNUST
W J SANE NO BADWENM

Taking the square root of both sides gives;

$$|det\left(\Gamma\right)| = \sqrt{\frac{|G|^d}{\prod_{i=1}^{d}|C_i|}}.$$

□

Let $G = \{f \in S_4 | sgn(g) = +1\}$. From Proposition 3.2.20, we know that there are 4 conjugacy classes of G and thus, by Corollary 4.2.14, there are 4 irreducible characters of G.

The conjugacy classes of G are;

$C_1 = \{(1)\}$,

$C_2 = \{(12)(34),(13)(24),(14)(23)\}$,

$C_3 = \{(123),(134),(142),(243)\}$, $C_4 =$

$\{(132),(143),(124),(234)\}$.

Theorem 4.2.25. *Let $\chi_1,\chi_2,\chi_3,\chi_4$ be the characters of the irreducible representations of G where χ_1 is the character of the 1-dimensional trivial representation which takes every element of the group and assigns a 1.*

Table 4.2: Character Table of G

•	C_1	C_2	C_3	C_4
χ_1	1	1	1	1
χ_2	1	1	$e^{\frac{2\pi}{3}i}$	$e^{\frac{4\pi}{3}i}$
χ_3	1	1	$e^{\frac{-2\pi}{3}i}$	$e^{\frac{-4\pi}{3}i}$
χ_4	3	-1	0	0

Proof. The entries in the first row are just the character of the 1-dimensional trivial irreducible representation of *G.* All entries are 1 because the trace of 1 is 1.

Now, suppose the degree of the remaining irreducible representations are d_2,d_3,d_4 then

$$1^2 + d_2^2 + d_3^2 + d_4^2 = |G| = 12,$$
$$d_2^2 + d_3^2 + d_4^2 = 11.$$

Therefore, we seek non-negative integer values of d_2,d_3,d_4 such that the above equation is satisfied. We observe that the only non-negative integer values that satisfy the above equation are

$$d_2 = 1, d_3 = 1, \text{ and } d_4 = 3.$$

Since the character of the identity always gives the degree of the irreducible representations, we have the proof for the entries in the first column.

For the 1-dimensional irreducible representations, we have a simple way of computing their character without actually knowing the representation itself. This can be done be examining the properties the elements in the conjugacy classes

carry.

Consider the conjugacy class C_2, we have that $\forall f \in C_2\, f \circ f = e = (1)$.
Taking the character χ of both sides we have

$$\chi(f \circ f) = \chi(e),$$
$$\Longrightarrow \chi(f)\chi(f) = \chi(e),$$
$$\Longrightarrow \chi^2(f) = 1,$$

Next, suppose that $f,g,h \in C_2$ are distinct elements. Then $f \circ g = h$ and hence

$$\chi(f \circ g) = \chi(h), \Longrightarrow$$
$$\chi(f)\chi(g) = \chi(h),$$

But all elements in the same conjugacy class have the same character and hence $\chi(f) = \chi(g) = \chi(h)$. Thus

$$\chi(f)\chi(f) = \chi(f), \Longrightarrow$$

$$\chi^2(f) = \chi(f),$$

but we already have $\chi^2(f) = 1$, hence by substitution, we have $\chi(f) = 1\ f \in C_2$. Thus the other 1-dimensional characters of the elements in the conjugacy class C_2 are given as

$$\chi_1(C_2) = \chi_2(C_2) = \chi_3(C_2) = 1.$$

Now, let us consider the conjugacy classes C_3 and C_4. These two classes share some properties: $\forall f \in C_3$ and $\forall g \in C_4$ we have $f \circ f = g$.

This implies that

$$\chi^2(f) = \chi(g).$$

Let the character $\chi(f) = \chi_2(C_2) = a$ and $\chi_2(C_3) = \chi(g) = b$. Then we have that $a^2 = b$.

To obtain the values of a and b we use the orthogonality of irreducible characters. As at this stage the only character that has a complete row is the trivial character χ_1 thus we have,

$$\langle \chi, \chi_1 \rangle = \frac{1}{|G|} \sum_{f \in G} \chi(f)\overline{\chi_1(f)} = 0$$

$$\Longrightarrow \frac{1}{12}(1 + 3 + 4a + 4b) = 0$$

$$\Longrightarrow a + b = -1.$$

Substituting $a^2 = b$ into the above equation we obtain a quadratic equation

$$a^2 + a + 1 = 0 \tag{4.1}$$

Applying the quadratic formula to Equation (4.1) we arrive at

$$a = \frac{-1 \pm i\sqrt{3}}{2}.$$

We see that a is a complex number and its conjugate. We then convert a to the polar form $re^{i\varphi}$ of complex numbers to obtain

$$\phi = \pm\frac{2\pi}{3},\ r = 1$$
$$a = e^{\pm\frac{2\pi}{3}i}.$$

Thus we have,$b = a^2 = e^{\pm\frac{4\pi}{3}i}$.

This shows that there are two possibilities for the 1-dimensional irreducible character $\chi(C_3)$ and $\chi(C_4)$.

$$a = e^{\frac{2\pi}{3}i}, \quad b = e^{\frac{4\pi}{3}i},$$

or

$$a = e^{-\frac{2\pi}{3}i}, \quad b = e^{-\frac{4\pi}{3}i}$$

Thus these are the two 1-dimensional characters of the conjugacy classes C_3 and C_4.

$$\chi_2(C_3) = e^{\frac{2\pi}{3}i},\ \chi_2(C_4) = e^{\frac{4\pi}{3}i}$$
$$\chi_3(C_3) = e^{-\frac{2\pi}{3}i},\ \chi_3(C_4) = e^{-\frac{4\pi}{3}i}$$

Finally, for the last row we use the orthonormality conditions.

Suppose $\chi_4(C_2) = a, \chi_4(C_3) = b, \chi_4(C_4) = c$.

Then

$$\langle \chi_4, \chi_1 \rangle = \frac{1}{|G|}\sum_{g\in G} \chi_4(g)\overline{\chi_1(g)} = 0$$
$$\implies \frac{1}{12}(3 + 3a + 4b + 4c) = 0,$$

Simplifying gives

$$3 + 3a + 4b + 4c = 0. \tag{4.2}$$

We also have,

$$\langle \chi_4, \chi_2 \rangle = \frac{1}{|G|}\sum_{g\in G} \chi_4(g)\overline{\chi_2(g)} = 0$$

$$\implies \frac{1}{12}(3 + 3a + 4be^{-\frac{2\pi}{3}i} + 4ce^{-\frac{4\pi}{3}i}) = 0.,$$

Simplifying yields

$$3 + 3a + 4be^{-\frac{2\pi}{3}i} + 4ce^{-\frac{4\pi}{3}i} = 0. \tag{4.3}$$

$$\langle \chi_4, \chi_3 \rangle = \frac{1}{|G|}\sum_{g\in G} \chi_4(g)\overline{\chi_3(g)} = 0$$

$$\implies \frac{1}{12}(3 + 3a + 4be^{\frac{2\pi}{3}i} + 4ce^{\frac{4\pi}{3}i}) = 0,,$$

which yields

$$3 + 3a + 4be^{\frac{2\pi}{3}i} + 4ce^{\frac{4\pi}{3}i} = 0. \tag{4.4}$$

Orthonormality gives,

$$\langle \chi_4, \chi_4 \rangle = \frac{1}{|G|}\sum_{g\in G} |\chi_4(g)|^2 = 1,$$

$$\implies \frac{1}{12}(9 + 3a^2 + 4b^2 + 4c^2) = 1 .$$

Simplifying gives us

$$3a^2 + 4b^2 + 4c^2 = 3. \tag{4.5}$$

Equating Equation (4.3) and Equation (4.4) we have,

$$3 + 3a + 4be^{-\frac{2\pi}{3}i} + 4ce^{-\frac{4\pi}{3}i} = 3 + 3a + 4be^{\frac{2\pi}{3}i} + 4ce^{\frac{4\pi}{3}i},$$

simplifying we have,

$$be^{-\frac{2\pi}{3}i} + ce^{-\frac{4\pi}{3}i} = be^{\frac{2\pi}{3}i} + ce^{\frac{4\pi}{3}i},$$

grouping like terms yields,

KNUST

$$b(e^{-\frac{2\pi}{3}i} - e^{\frac{2\pi}{3}i}) = c(e^{\frac{4\pi}{3}i} - e^{-\frac{4\pi}{3}i}).$$

Using one of the properties of complex numbers that is a complex number minus its complex conjugate is 2 times the imaginary part of the complex number we obtain

$$b\left(2i\sin\left(\frac{2\pi}{3}\right)\right) = c\left(2i\sin\left(\frac{4\pi}{3}\right)\right)$$

$$\Longrightarrow bi\sqrt{3} = -ci\sqrt{3}, \quad ,$$

$$\Longrightarrow b = -c \quad \text{by cancellation.}$$

Next, we substitute $b = -c$ into Equation (4.2)

$$3 + 3a - 4c + 4c = 0,\ 3$$

$$+\ 3a = 0, \Longleftrightarrow a = -1.$$

Finally, we substitute $a = -1$ and $b = -c$ into Equation (4.5)

$$3 + 4c^2 + 4c^2 = 3,$$

$$\Longrightarrow 8c^2 = 0,\ c$$

$$= 0.$$

Thus $b = c = 0$ and $a = -1$ and hence the proof of the result of the last row. □

NYANSAPO WO SANE NO BADWENMA

Recall, the quaternion group Q is a group of order $|Q| = 8$. From Proposition 3.2.19, we know that there are 5 conjugacy classes of Q and thus, by Corollary 4.2.14, there are 5 irreducible characters of Q.

Proposition 4.2.26. *Let $\chi_1,\chi_2,\chi_3,\chi_4,\chi_5$ be the characters of the irreducible representations of G where χ_1 is the character of the 1-dimensional trivial representation.*

Then the character table of G is shown below:

Table 4.3: The character table of the quaternion group Q.

	1	-1	I	J	K
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	1	1	-1	1	-1
χ_4	1	1	-1	-1	1
χ_5	2	-2	0	0	0

Proof. The first row is verified by the definition of the character of the trivial representation.

Let d_i for $i = 1,2,3,4,5$ be the degree of the 5 irreducible representations of Q.

Then $|Q| = 8 = \mathrm{P}_{5\,i=1}\, d_{2\,i}$

For the trivial representation, $d_1 = 1$ thus

$$8 = 1 + \mathrm{X}_{i=2} d^{2}_{i},$$

$$\Longrightarrow 7 = \mathrm{X}_{i=2} d^{2}_{i}.$$

This implies, $d_2 = 1$, $d_3 = 1$, $d_4 = 1$ and $d_5 = 2$.

All the d^0s take 1 except the last d that takes the remaining number, and for this

KNUST

, 2 us remaining so $d_5 = 2$.

This verifies the entries in the first column.

The entries in the last row are obtained from the characters of the 2-dimensional irreducible representation in Proposition 4.2.21. Suppose ϕ is a 1-dimensional representation, then $\phi(I) = \phi(-I)$. If χ is any of the irreducible characters of Q besides the irreducible character, then since χ is a class function,$\chi(I) = \chi(-I)$.

By the properties of elements in Q and of representations of a group, we have,

$$\phi(I) = \phi(-I),$$

$$= \phi(-1)\phi(I), \Leftrightarrow$$

$$\phi(-1) = 1,$$

and

$$\phi(I^2) = \phi(-1) = 1, \Rightarrow$$

$$\phi(I)\phi(I) = 1,$$

Thus $\phi(I) \in \{-1,1\}$. Similarly, for J and K we have, $\phi(J),\phi(K) \in \{-1,1\}$. Since the only complete row at this stage is the row corresponding to χ_1, we can apply the orthogonality relation.

Let $a = \chi(I)$, $b = \chi(J) = b$ and $\chi(K)$. Then

$$\begin{aligned}\langle \chi, \chi_1 \rangle &= \frac{1}{|G|}\sum_{x\in Q}\overline{\chi(x)}\chi_1(x) = 0,\\ &= \frac{1}{|G|}\sum_{x\in Q}\chi(x) = \frac{1}{8}(2+2a+2b+2c) = 0\end{aligned}$$

,

$$\Rightarrow a + b + c = -1.$$

Thus, from the fact that $\phi(I^2) = 1$, we have, $a,b,c \in \{-1,1\}$.

For the rows to be independent, we permute the possible values of *a*,*b* and *c* as follows:

$a = 1, \quad b = -1\ c = -1, a =$

$-1\ b = 1\ c = -1, a = -1\ b$

$= -1\ c = 1.$

These account for the remaining entries in the table. □

4.3 Young Tableaux

The convenient way of determining the dimensionalities of higher dimensional irreducible representations of unitary groups and their basis functions is the use of Young tableau.

A "box" is used as a basic unit of Young tableau as shown below that denotes a basis state:

□

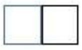
The box represents any state, if an entry is voided.

A designated box by a number denotes one of the basis states in some reference order. Illustratively, for $U(2)$, we have

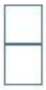
$$U_1 = \boxed{1 \qquad\qquad} U_2 = \boxed{2}$$

Direct product construction is the utility of Young tableaux. There are two types of states, for the two-fold direct products of $U(2)$, that is symmetric and antisymmetric.

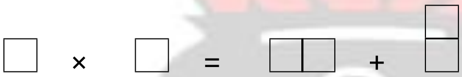
The Young tableau for a generic two-particle symmetric state is:



and the two-particle antisymmetric state is:

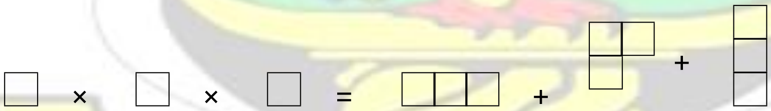


In the framework of Young tableaux, the two-fold direct product is written as :



The three-fold direct product illustrates the conventions used in the construction of Young tableaux and their labelling [**?**].

The generic tableaux are:



We say that the tableau is a tableau on the diagram λ, or that λ is the shape of the tableau. A standard tableau is a tableau in which the entries are the numbers 1 to n each occurring once.

Rules to construct irreducible representations of the group $N \times N$

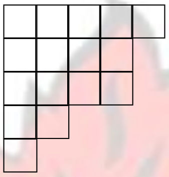
The group $SU(N)$ is the group of $N \times N$ complex unitary matrices ($UU^{\dagger} = 1$) with unit determinant ($det(U) = 1$).

KNUST

- The complex multiplet $\psi_i(i = 1,...,N)$ which belong to the fundamental representation of $SU(N)$ (ie the lower dimension non trivial representation,) $\psi_i \dashrightarrow U_{ij}\psi_j$ is represented by a box:

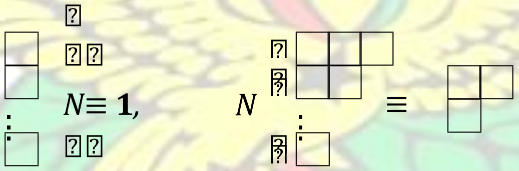
$$\psi_1 \equiv \square \equiv N$$

- A Young tableau is a diagram of *left-justified* rows of boxes where any row is *not longer* than the row on top of it, e.g.

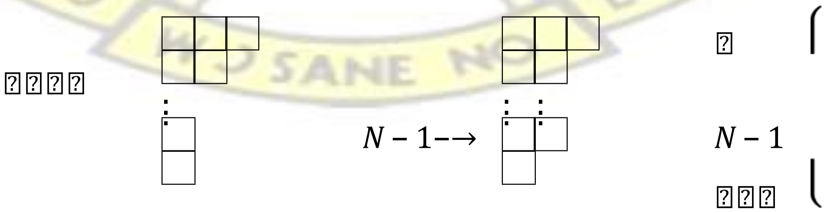


- Any column cannot contain more than N boxes.

- Any column with exactly N boxes can be crossed out since it correspond to the trivial representation (the singlet),



- The complex conjugate of a given irreducible representation is represented by a tableaux obtained by switching any column of k boxes with a column of ($N - k$) boxes, e.g.



- From the previous rule: the complex conjugate multiplet $\bar{\psi}_i (i = 1,...,N)$ $(\psi_i \longrightarrow \bar{\psi}_j U_{ji}^{\dagger} = U_{ij}^{*} \bar{\psi}_j)$ is represented by a column of $N - 1$ boxes:

$$\bar{\psi}_i \equiv \left.\begin{array}{c}\square\\ \square\\ \vdots\\ \square\end{array}\right\} N-1 \equiv \bar{\mathbf{N}}.$$

KNUST

- Any irreducible representation of $SU(N)$ can be constructed starting from the fundamental irreducible representation. The *direct product* of irreducible representations with the following rules:

  - Write the two tableaux which correspond to the direct product of irreducible representations and label successive rows of the second tableau with indices *a,b,c,...,*

  - Attach the boxes from the second to the first tableau, one at a time following the order *a,b,c,...,* in all the possible ways. The resulting diagrams should be valid Young tableaux i.e., with no two or more *a* in the same column (neither *b* or *c* or ...).

  - Two generated tableaux with the same shape but labels *distributed differently* have to be kept. If two tableaux are *identical* only one has to be kept.

  - Counting the labels from the first row from *right* to *left*, then the second row (from right to left) and so on, at any given box position there should be no more *b* than *a*, more *c* than *b* and so on.

- The adjoint representations is the irreducible representations with dimension equal to the dimension of the group (i.e. N^2-1) and can be

constructed by a direct product of the fundamental representation and its complex con-
jugate:

$$\overline{N} \otimes N \equiv N - \left.\begin{array}{c}\square\\ \square\\ \vdots\\ \square\end{array}\right\} 1 \otimes \square = N - \left.\begin{array}{l}\square\square\\ \square\\ \vdots\\ \square\end{array}\right\} 1 \oplus \left.\begin{array}{c}\square\\ \square\\ \vdots\\ \square\end{array}\right\} N = (N^2 - 1) \oplus 1$$

From the conjugation rule above it is clear that the adjoint representation is self conjugate $\overline{N^2 - 1} = N^2 - 1$

Chapter 5

Main Results: Separating sets for the unitary group $U_2(\mathrm{F}_{q^2})$

5.1 Introduction

Let F_{q^2} be a quadratic field extension of the finite field F_q. Let $G = \{U \in GL_2(\mathrm{F}_{q^2}) | U^T U = I\}$ be the group of unitary 2× 2 matrices over the field F_{q^2}. In this Chapter, we probe into the character table of the unitary group $U_2(\mathrm{F}_{q^2}) = G$ defined over the finite field F_{q^2} by first examining the conjugacy classes and the irreducible representations of G, the character table is then constructed for the separation.

5.2 Hermitian form

Given a field K, we can obtain a quadratic extension field (a field extension of degree 2) by constructing the quotient field $K[x]/\mathrm{h}f(x)\mathrm{i}$ where $\mathrm{h}f(x)\mathrm{i}$ is the ideal generated by the irreducible polynomial of degree 2. A typical example of such field extensions is the field of complex numbers C over R which is normally seen as C $\tilde{}$= R/hx^2 + 1i. One can also think of C as the adjoining of R by the square root of -1, i and this is usually written as R(i) = {a + bi|a,b ∈ R}.

When we talk of an automorphism α on the extension field L over K, written as L/K, we are simply referring to an isomorphism α from L to L which fixes K. We also note that there are only two distinct automorphisms on any quadratic extension field:

- the trivial automorphism - an automorphism which fixes every element of the quadratic extension field,
- the order 2 automorphism - an automorphism α such that $\alpha^2 = 1$ where 1 represent the identity map.

For the quadratic extension C we have, besides the trivial automorphism fixing all of C, an order 2 automorphism

$$\alpha : C \longrightarrow C, \text{ defined by}$$

$$a + bi \; 7{\rightarrow} \; a - bi = \overline{a + bi}.$$

The complex conjugation.

Thus in a more general setting, we denote this order 2 automorphism by $\alpha(a) = a \forall a \in K$.

The field F_{q^2} is a quadratic field extension of F_q where $q = p^k$ for p a prime and k a positive integer which is obtained by adjoining to F_q a square root of any generator of $\mathbb{F}_q^*$.

The non-trivial order 2 automorphism on F_{q^2} is given by

KNUST

$$\alpha : \mathrm{F}_{q2} -\!\!\to \mathrm{F}_{q2}\, x$$

$$7\!\to x^{q}.$$

Definition 5.2.1. *Let V be an n-dimensional vector space defined over the quadratic field extension L . Then the map* $\mathrm{H} : V \times V -\!\!\to L$ *is said to be a Hermitian form if for all u,v,w ∈ V and a ∈ L 1.* $\mathrm{H}(u+v,w) = \mathrm{H}(u,w) + \mathrm{H}(v,w)$.

2. $\mathrm{H}(u,v+w) = \mathrm{H}(u,v) + \mathrm{H}(u,w)$.

3. $\mathrm{H}(au,v) = a\mathrm{H}(u,v) = \mathrm{H}(u,av).$ ¯

4. $\mathrm{H}(u,v) = \overline{\mathrm{H}(v,u)}.$

Remark 5.2.2. We say that a Hermitian form H is non-degenerate if $\forall v \in V$ $\exists w \in V$ such that $\mathrm{H}(v,w)$ 6= 0.
A vector space V over L/K endowed with a non-degenerate Hermitian form H is said to be a **unitary space** over L/K.

Definition 5.2.3. *Given a unitary vector space V and an invertible linear transformation τ. If τ is an isometry of the Hermitian form* H *such that*

$$\mathrm{H}(\tau u,\tau v) = \mathrm{H}(u,v) \forall u,v \in V,$$

then τ is said to be a unitary transformation.

The group $U(V) = \{\tau \in GL(V) | \mathrm{H}(\tau u,\tau v) = \mathrm{H}(u,v) \forall u,v \in V\}$ *of unitary transformations is a unitary group.*

Remark 5.2.4. 1. Given a basis for the unitary vector space V, the group $U_n(L) = \{U \in GL_n(L) | U = (\overline{U^T})^{-1}\}$ of $n{\times}n$ unitary matrices is isomorphic to $U(V)$.

KNUST

2. Given a basis in V, a matrix representation M of a linear transformation $\tau \in GL(V)$, and the matrix representation H of the Hermitian form H

then $\tau \in U(V)$ if and only if $M^T HM = \overline{H}$.

□ □
1 0
We shall restrict our focus to two Hermitian forms given by I = □ □
□ □
0 1

□ □
0 1 and
J = □ □.
□ □ 1
0

□ □ a

b
We note that for any A = □ □ ∈ $U_2(L)$, we have
□ □ c

d

$$A^T J\overline{A} = J,$$

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\begin{pmatrix} c & a \\ d & b \end{pmatrix}\begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

$$\begin{pmatrix} \overline{a}c + a\overline{c} & \overline{b}c + a\overline{d} \\ \overline{a}d + b\overline{c} & \overline{b}d + b\overline{d} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$
,

This shows that using the form J, A is unitary if and only if

$ad + bc = \overline{1}, \overline{ac} + ac =$

_ _ $\overline{b}d + \overline{b}d = 0.$

Similarly for the form I, A is unitary if and only if

$$a\bar{a} + b\bar{b} = 1 = c\bar{c} + d\bar{d},\ a\bar{b} + c\bar{d} = 0.$$

5.3 Conjugacy classes of G

The conjugacy classes of any group partition the group and hence we begin this section with a brief analysis of the order of the group G.

Proposition 5.3.1. *Let $G = \{U \in GL_2(\mathbb{F}_{q^2}) | U^T U = I\}$ be the group of unitary 2×2 matrices over the field $\mathbb{F}_{q^2}$ using the Hermitian form I. Then $|G| = (q-1)q(q+1)^2$.*

Proof. To prove this proposition, we first prove the claim

Claim 5.3.2. *Let $U \in GL_2(\mathbb{F}_{q^2})$. Then $U \in G$ if and only if U is of the form*

$$U = \begin{pmatrix} a & b \\ -\bar{b}D & \bar{a}D \end{pmatrix}$$ *where $|D| = D\bar{D} = 1$ and $a\bar{a} + b\bar{b} = 1$, for $a, b \in \mathbb{F}_{q^2}$*

proof of claim 5.3.2. ”⇐”

By definition of G we show that $U\,U^{T} = I$ where I is the identity matrix of $GL_2(\mathbb{F}_{q^2})$.

KNUST
NYANSAPO WO SANE NO BADWENMA

$$
\begin{aligned}
\overline{U}^T U &= \begin{pmatrix} \bar{a} & \bar{b} \\ -b\overline{D} & a\overline{D} \end{pmatrix}^T \begin{pmatrix} a & b \\ -\bar{b}D & \bar{a}D \end{pmatrix} \\
&= \begin{pmatrix} \bar{a} & -b\overline{D} \\ \bar{b} & a\overline{D} \end{pmatrix} \begin{pmatrix} a & b \\ -\bar{b}D & \bar{a}D \end{pmatrix}, \\
&= \begin{pmatrix} a\bar{a} + b\bar{b}|D| & \bar{a}b - \bar{a}b|D| \\ a\bar{b} - a\bar{b}|D| & b\bar{b} + a\bar{a}D \end{pmatrix}, \\
&= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.
\end{aligned}
$$

,

$\Rightarrow U^T U = I$ and hence $U \in G$.

“⇐”

Suppose

$$U = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(F^2{}_q).$$

Let $D = det(U) = ad - bc$. $U \in G$ implies that

$$\overline{U}^T U = I,$$

$$\Rightarrow \overline{U}^T = U^{-1}.$$

Thus,

$$\begin{pmatrix} \bar{a} & \bar{c} \\ \bar{b} & \bar{d} \end{pmatrix} = \frac{1}{D} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

By equality of matrices and simplification we have that $d = a\overline{D}$, $c = -\bar{b}D$.

Substituting into the expression for D above we have,

$$D = \bar{a}aD + b\bar{b}D \Longrightarrow a\bar{a} + b\bar{b} = 1.$$

Also,

$$\det(\overline{U}^T U) = \det(I)$$

$$\det(\overline{U}^T)\det(U) = 1, \qquad ,$$

$$\Rightarrow D\overline{D} = 1.$$

Thus,

$$U = \begin{pmatrix} a & b \\ -\bar{b}D & \bar{a}D \end{pmatrix}$$ where $|D| = 1$ and $a\bar{a} + b\bar{b} = 1$.

□

KNUST

To complete the proof of proposition 5.3.1, we consider different cases for which $a\bar{a} + b\bar{b} = 1$ holds.

Case 1 : $a = 0$**.**

$a\bar{a} + b\bar{b} = 1 \Longrightarrow |b| = 1$ and hence $b \in \mathcal{L} = \{x \in \mathbb{F}^*_{q^2} | x\bar{x} = 1\}$, the kernel of the norm map. Since $|L| = q + 1$ we have, $(q + 1)$ choices for b. Also, $|D| = 1 \Longrightarrow D \in L$ and hence there are $(q + 1)$ choices for D. Since $a = 0$ implies the matrix only depends on b and D and thus there are a total of $(q+1)^2$ possibilities for U.

Case 2 : $b = 0$**.**

By a similar argument as in case 1, we obtain $(q + 1)$ possibilities for U.

Case 3: *a* 6= 0 **and** *b* 6= 0**.** *b* 6= 0 and $a\bar{a} + b\bar{b} = 1$ implies $a\bar{a}$ = 1.6 *a* 6= 0 implies $a\bar{a} \in \mathbb{F}_q \backslash \{0,1\}$ and thus there are only $q - 2$ possibilities for $a\bar{a}$ and this also determines $b\bar{b}$. This gives $(q + 1)$ choices for a and also for b. In this case, the matrix U depends on the three variables a,b and D. Since D has $(q + 1)$ possibilities we have that there are $(q - 2)(q + 1)^3$ for the matrix U.

Thus, putting all the 3 cases together we have

$$|G| = (q+1) + (q+1) + (q-2)(q+1)^3 = (q-1)q(q+1)^2.$$

□

Now we analyze the conjugacy class representatives of the unitary group $G = U_2(\mathbb{F}_{q^2})$ using the Hermitian form J and show the total number of elements in each conjugacy class.

Let

$$a_x = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix},\ b_{x,y} = \begin{pmatrix} x & y \\ 0 & x \end{pmatrix} : y \neq 0,\ c_{x,y} = \begin{pmatrix} x & 0 \\ o & y \end{pmatrix} : y \neq x,\ d_{x,y} = \begin{pmatrix} x & y \\ y & x \end{pmatrix} : y \neq 0,$$

be elements of the unitary group G. The elements a_x,$b_{x,y}$,$c_{x,y}$ and $d_{x,y}$ are representatives of the conjugacy classes of the unitary group G.

Proposition 5.3.3. *The conjugacy class corresponding to a_x has $q+1$ class representatives.*

Proof. $a_x = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} \in G$ and by definition, we have $x\bar{x} = 1$ which implies $x \in$ L, the kernel of the norm map in Proposition 3.2.8. As the order of L is $q+1$, we have that there are $q+1$ possible choices for x and hence for a_x.

Computing the center of a_x, we observe that for any

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

in G, if we set $D = ad - bc$, we have

$$
\begin{aligned}
Aa_xA^{-1} &= \frac{1}{D}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \\
&= \frac{1}{D}\begin{pmatrix} ax & bx \\ cx & dx \end{pmatrix}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}, \\
&= \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}.
\end{aligned}
$$

,

KNUST

This shows that a_x commutes with every other element in G and hence it is in the center $Z(G)$ of G. However, the center $Z(G)$ consist of all elements in G whose conjugacy class has exactly one element and thus, we have a total of $1(q + 1) = q + 1$ class representatives. □

Proposition 5.3.4. *The conjugacy class corresponding to $b_{x,y}$,y 6= 0 has* $(q - 1)(q + 1)^2$ *elements.*

Proof. $b_{x,y} \in G$ is unitary if and only if $\overline{b^T_{x,y}}Jb_{x,y} = J$. This implies that

$$x\bar{x} = 1 \;\Rightarrow\; x \in G,$$

$$\bar{x}y + x\bar{y} = 0.$$

The last equality implies $\frac{y}{\bar{y}} = -\frac{x}{\bar{x}}$ and this shows that the homomorphism Q defined in Proposition 3.2.6 maps y to $-\frac{x}{\bar{x}}$ where $x \in$ L. Proposition 3.2.8 shows that there are precisely $q - 1$ of such $y \in \mathbb{F}^*_{q^2}$ for which this holds. There are $q + 1$ choices for $x \in$ L and thus, there are $(q - 1)(q + 1)$ possible

choices for $b_{x,y}$.

Computing the centralizer of $b_{x,y}$, we have for any arbitrary

□ □ a

b

□ □ ∈ G where $D = ad - bc$ 6= 0,

  c

d

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x & y \\ 0 & x \end{pmatrix} \left(\frac{1}{D} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \right) = \begin{pmatrix} x & y \\ 0 & x \end{pmatrix}$$

$$\frac{1}{D} \begin{pmatrix} Dx - acy & a^2y \\ -c^2y & acy + Dx \end{pmatrix} = \begin{pmatrix} x & y \\ 0 & x \end{pmatrix}.$$

,

By equality of matrices we have,

$Dx - acy = Dx, \Rightarrow acy = 0.$

$-c^2y = 0,\ y$ 6= $0 \Rightarrow c = 0,$

$a^2y = Dy, \Rightarrow D = a^2, Dx$

$= x, \Rightarrow D = 1.$

Now, $D = a^2$ implies that $ad - bc = a^2$ and hence $d = a$ as $c = 0$.

$$C_G(b_{x,y}) = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in G | a, b \in \mathbb{F}_{q^2} \right\}$$

  Thereforeis the centralizer of $b_{x,y}$,y 6= 0.

The order of this subgroup is dependent on the number of choices available for both a and b.

The element b has q choices as b can take the value 0 whiles a is such that $\bar{a}a = 1$ shows that $a \in$ L and hence it has $q + 1$ choices.

Thus $|C_G(b_{x,y})| = q(q + 1)$. The size of the conjugacy class of each $b_{x,y}$ is the index of $C_G(b_{x,y})$ in G, that is

$$[G : C_G(b_{x,y})] = \frac{|G|}{|C_G(b_{x,y})|} = \frac{(q-1)q(q+1)^2}{q(q+1)} = (q-1)(q+1)$$

.

    x y x z

Further computations show that   ∼   if and only if the image of

    0 x 0 x

y and z coincide in L under the map Q, in other words y and z lie in the same coset$\mathbb{F}_q^* = \ker(Q)$.

The cardinality of this set being $q - 1$, shows there are $q - 1$ repetitions in the counting of the number of choices of $b_{x,y}$. Thus the number reduces to $q + 1$. Therefore, there are a total of $(q + 1) \cdot (q - 1)(q + 1) = (q - 1)(q + 1)^2$ elements in this class. □

KNUST

Proposition 5.3.5. *The conjugacy class corresponding to $c_{x,y}$,y 6= x is of order* $\frac{(q-2)q(q+1)^2}{2}$.

Proof. $c_{x,y} \in G$ is unitary implies$c_{x,y}^T J\overline{c_{x,y}} = J \Rightarrow x\overline{y} = 1.$

Since y 6= x and $x\overline{y}$ = 1, we have, xx 6= $\overline{1}$ and also x 6= 0. Thus counting the number of choices for x gives $(q - 2)(q + 1)$ and that of y is obtained from x by using $x\overline{y} = 1$.

0 1

For P =   we observe that

1 0

0 1 x 0 0 1 y 0

$Pc_{x,y}P^{-1}$ =   = $\,$.

         1 0 0 y 1 0 0 x

    x 0 y 0

This implies that   ∼   and hence there arechoices for $\frac{(q-2)(q+1)}{2}$

0 y 0 x

$c_{x,y}$.

  a b

Let g =   ∈ G, and $D = ad - bc$ then $gc_{x,y}g^{-1} = c_{x,y}$ implies

� � *c d*

$$,\ \frac{1}{D}\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}x & 0\\ 0 & y\end{pmatrix}\begin{pmatrix}d & -b\\ -c & a\end{pmatrix}=\begin{pmatrix}x & 0\\ 0 & y\end{pmatrix}$$

Hence

$$\frac{1}{D}\begin{pmatrix}adx-cby & -abx+aby\\ cdx-cdy & -cbx+ady\end{pmatrix}=\begin{pmatrix}x & 0\\ 0 & y\end{pmatrix}.$$

$adx - cby = Dx$

$-cbx + ady = Dy$

$-adx + aby = 0$ $cdx -$

$cdy = 0$

This implies that $ad = D$ 6= 0 and hence a 6= 0 6= d, also $cd = 0$, $ab = 0$ and $cb = 0$ ⇒ $c = 0$, $b = 0$. This computations show that the centralizer of $c_{x,y}$ is given by

$$C_G(c_{x,y}) = \left\{\begin{pmatrix}a & 0\\ 0 & d\end{pmatrix} \in G \mid a, d \in \mathbb{F}_{q^2}\right\}$$

and is of order $(q-1)(q+1)$ since there are q^2-1 for a and d is determined from $ad = D$. Thus,

$$[G : C_G(c_{x,y})] = \frac{|G|}{|C_G(c_{x,y})|} = \frac{(q-1)q(q+1)^2}{(q-1)(q+1)} = q(q+1)$$

.

Hence there are $\frac{(q-2)(q+1)}{2}\cdot q(q+1) = \frac{(q-2)q(q+1)^2}{2}$ elements in this class. □

Proposition 5.3.6. *The conjugacy class corresponding to $d_{x,y},y$ 6= 0 is of order* $\frac{(q-1)q^2(q+1)^2}{2}$.

Proof. $d_{x,y} \in G$ is unitary if and only if $d^T_{x,y}J\overline{d_{x,y}} = J$ which implies

$\overline{x}x + y\overline{y} = 1,$ (5.1) $xy + yx = 0.$ (5.2)

– –

Equation 5.1 + Equation 5.2 ⇒ $(x + y)\overline{(x + y)} = 1 \Rightarrow x + y \in$ L and Equation 5.1 - Equation 5.2 ⇒ $(x - y)\overline{(x - y)} = 1 \Rightarrow x - y \in$ L. To count x

and y we consider two cases:
case 1 : $x = 0$.

If $x = 0$ then $y\bar{y} = 1 \Rightarrow y \in$ L and hence there are $q + 1$ choices for y. **case 2**

: x 6= 0 6= y.

Let $u,v \in$ L and set $x = \frac{u+v}{2}$ and $y = \frac{u-v}{2}$ such that $x \pm y \in$ L.

If x 6= 0 and y 6= 0 then we have u 6= ±v and hence there are $q + 1$ choices for v and $q + 1 - 2 = q - 1$ choices for u. Thus, there are $(q - 1)(q + 1)$ choices in this case.

Therefore putting all the two cases together gives $(q+1)+(q-1)(q+1) = q(q+1)$ choices for $d_{x,y}$.

To avoid double counting, we divide by 2 as computing

$$-\frac{1}{a^2}\begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix}\begin{pmatrix} x & y \\ y & x \end{pmatrix}\begin{pmatrix} -a & 0 \\ 0 & a \end{pmatrix},$$

shows that

$$\begin{pmatrix} x & y \\ y & x \end{pmatrix} \sim \begin{pmatrix} x & -y \\ -y & x \end{pmatrix}.$$

Thus, there are $\frac{q(q+1)}{2}$ choices for $d_{x,y}$.

� � a

b

Suppose that g = � � ∈ G then solving $gd_{x,y}g^{-1} = d_{x,y}$ for a,b,c and d

� � c

d

yields $a = d$ and $b = c$.

This shows that the centralizer of $d_{x,y}$ is given by

KNUST
NYANSAPO WO SANE NO BADWENMA

$$C_G(d_{x,y}) = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \in G | a, b \in \mathbb{F}_{q^2} \right\}.$$

We have that $a\bar{a} + b\bar{b} = 1$ and $a\bar{b} + a\bar{b} = 0$.

To compute the order of $C_G(d_{x,y})$, we consider 3 cases for counting a and b.

case 1 : $a = 0$.

If $a = 0$ we have $b\bar{b} = 1 \Rightarrow b \in G$ and hence there are $q + 1$ choices for b. **case 2 :** $b = 0$.

With a similar argument as in case 1 we obtain $q + 1$ choices for a.

case 3 : a 6= 0 6= b.

If a 6= 0 and b 6= 0 then $a \pm b \in$ L and by a previous argument we have $(q-1)(q+1)$ choices.

Thus, there are $2(q + 1) + (q - 1)(q + 1) = (q + 1)^2$ choices in all.

$$[G : C_G(d_{x,y})] = \frac{(q-1)q(q+1)^2}{(q+1)^2} = (q-1)q.$$

Therefore, there are ($(q-1)q \cdot \frac{q(q+1)^2}{2} = \frac{(q-1)q^2(q+1)^2}{2}$ elements in the conjugacy class corresponding to $d_{x,y}$. □

The table below shows the number of elements in each conjugacy class.

Table 5.1: Conjugacy Class Representative of G.

Representatives	No. elements	No. classes	Total elements
a_x	1	$q + 1$	$q + 1$
$b_{x,y}$	$(q - 1)(q + 1)$	$(q + 1)$	$(q - 1)(q + 1)^2$
$c_{x,y}$	$q(q + 1)$	$\frac{(q-2)(q+1)}{2}$	$\frac{(q-2)q(q+1)^2}{2}$
$d_{x,y}$	$(q - 1)q$	$\frac{q(q+1)}{2}$	$\frac{(q-1)q^2(q+1)}{2}$

We observe from Table 5.1 that the total number of conjugacy classes is $(q + 1)^2$. This implies there are $(q + 1)^2$ irreducible representations of the group G.

KNUST

5.4 Irreducible characters of $U_2(\mathsf{F}_{q^2})$

In this section we give a brief account of the irreducible characters of the group $G = U_2(\mathsf{F}_{q2})$ and to do so we will need some of the major subgroups of G. We start with the Borel subgroup B of G which is defined as

$$B = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in G | a, b, d \in \mathbb{F}_{q^2} \right\}.$$

Counting the number of elements in B requires counting the choices available for the elements a,b,d of F_{q2}. Using the properties of the unitary group G established in the previous section and with a careful examination we observe that $|B| = (q - 1)q(q + 1)$.

Now, we consider the permutation representation of G which has dimension q+1. This representation contains the trivial representation.

Let V be the q-dimensional representation obtained from the permutation representation of G. The character χ_V of V is such that

$$\chi_V(a_x) = q, \chi_V(b_{x,y}) = 0, \chi_V(c_{x,y}) = 1, \chi_V(d_{x,y}) = -1.$$

Computing the inner product

$$\langle \chi_V, \chi_V \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_V(g) \overline{\chi_V(g)},$$

we have hχ_V,χ_Vi = 1 which implies that V is an irreducible representation.

Let $\eta : \mathbb{F}_{q^2}^* \longrightarrow \mathbb{C}^*$ be a 1-dimensional character on $\mathbb{F}_{q^2}^*$.

We can define a 1-dimensional representation of G as

$$U_\eta(A) = \eta(\det(A)).$$

For any $A \in G$, $det(A) = 1$ and hence giving rise to $q + 1$ forms of such 1-dimensional representation, U_η.

The values of the characters on the representative of the conjugacy classes listed above are given as

$\chi_{U_\eta}(a_x) = \eta(x)^2, \chi_{U_\eta}(b_{x,y}) = \eta(x)^2, \chi_{U_\eta}(c_{x,y}) = \eta(x)\eta(y), \chi_{U_\eta}(d_{x,y}) = \eta(x^2 - y^2).$

Also, we have a q-dimensional representation V_η of G given by the tensor product of V and U_η

$$V_\eta = V \otimes U_\eta.$$

The character χ_{V_η} of V_η takes the following values on the conjugacy classes

	a_x	$b_{x,y}$	$c_{x,y}$	$d_{x,y}$
χ_{V_η}	$q\eta(x)^2$	0	$\eta(x)\eta(y)$	$-\eta(x^2 - y^2)$

Counting the number of irreducible characters there are of this type, we observe that there are $q + 1$ as χ_{U_η} has a total of $q + 1$ candidates.

To obtain the other irreducible characters we consider other representations that can be obtained from inducing from larger subgroups of G.

Thus we define our next subgroup of G as

$$D = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} |a, b, d \in \mathbb{F}_{q^2} \right\}$$

Let η and β be two 1-dimensional characters on $\mathbb{F}^*_{q^2}$. Let $\varphi : D \longrightarrow \mathbb{C}^*$ defined by

$$\varphi \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \eta(a)\beta(d)$$

be a 1-dimensional representation on D. By lifting this representation to B, we are able to then construct a $(q + 1)$-dimensional representation $W_{\eta,\zeta}$ which is induced from B to G. This induced representation $W_{\eta,\beta}$ has the character $\chi_{W_{\eta,\beta}}$ which takes the following values on the conjugacy classes.

	$a_{x,y}$	$b_{x,y}$	$c_{x,y}$	$d_{x,y}$
$\chi_{W_{\eta,\zeta}}$	$(q+1)\eta(x)\zeta(x)$	$\eta(x)\zeta(x)$	$\eta(x)\zeta(y) + \eta(y)\zeta(x)$	0

Suppose α is the generator of $\mathbb{F}^*_q$ and ζ be a $(q+1)$th root of unity. Then careful examination shows that $W_{\eta,\zeta}$ is irreducible if and only if $\zeta(\alpha)$ 6= $\eta\alpha(\eta)$. Counting the number of irreducible characters of this type shows that there are $\frac{(q-2)(q+1)}{2}$ irreducible characters. Thus, we have obtained

$$2(q+1) + \frac{(q-2)(q+1)}{2} = \frac{(q+1)(q+2)}{2}$$

irreducible characters and hence there are still ($(q+1)^2 - \frac{(q+1)(q+2)}{2} = \frac{q(q+1)}{2}$ irreducible characters to be found.

Let $H = \left\{ \begin{pmatrix} x & y \\ y & x \end{pmatrix} \in G \right\}$ be a subgroup of G. The order of this group is $(q+1)^2$ and hence $[G:H] = (q-1)q$

Another way to obtain a new character is by considering the induced representation from the subgroup H to G.

Given two distinct 1-dimensional characters η,ζ on the subgroup L, we obtain a 1-dimensional representation $\varphi : H \longrightarrow \mathbb{C}^*$ defined by

$$\varphi\begin{pmatrix} x & y \\ y & x \end{pmatrix} = \eta(x+y)\zeta(x-y)$$

If we induce the 1-dimensional representation φ to G we obtain a $q(q-1)$dimensional representation $Ind\varphi$ whose character takes the following values on the conjugacy classes of G:

•	a_x	$b_{x,y}$	$c_{x,y}$	$d_{x,y}$
$\chi_{Ind\varphi}$	$(q-1)q\eta(x)\zeta(x)$	0	0	$\eta(x+y)\zeta(x-y) + \eta(x-y)\zeta(x+y)$

Computing the inner product we obtain h$\chi_{Ind\varphi},\chi_{Ind\varphi}$i $= q-1$. This implies that $Ind\varphi$ is not irreducible.

KNUST
NYANSAPO WOSANE NO BADWENMA

To obtain an irreducible representation we first compute the tensor product of V and $W_{\eta,\zeta}$. The character of this representation $V \otimes W_{\eta,\zeta}$ take the following values on the conjugacy classes:

	a_x	$b_{x,y}$	$c_{x,y}$	$d_{x,y}$
$\chi_{V\otimes W_{\eta,\zeta}}$	$q(q+1)\eta(x)\zeta(x)$	0	$\eta(x)\beta(y) + \eta(y)\zeta(x)$	0

Now, let us consider the character $X_{\eta,\zeta}$ given by

KNUST

$$X_{\eta,\zeta} = \chi_{V\otimes W_{\eta,\zeta}} - \chi_{W_{\eta,\zeta}} - \chi_{Ind\varphi}.$$

This character is of dimension $q - 1$ and take the following values on each of the conjugacy classes :

	a_x	$b_{x,y}$	$c_{x,y}$	$d_{x,y}$
$X_{\eta,\zeta}$	$(q-1)\eta(x)\zeta(x)$	$-\eta(x)\zeta(x)$	0	$\eta(x+y)\zeta(x-y) + \eta(x-y)\zeta(x+y)$

We observe that $X_{\eta,\zeta}$ is irreducible as $hX_{\eta,\zeta},X_{\eta,\zeta}i = 1$.

Counting the number of such characters gives $\frac{q(q+1)}{2}$. Summing all the number of irreducible characters we get

$$2(q+1) + \frac{(q-2)(q+1)}{2} + \frac{q(q+1)}{2} = (q+1)^2$$

which is the same as the number of conjugacy classes.

5.5 Separating sets

Proposition 5.5.1. *Let W be an isotypic subspace of the vector space V , and let χ be the character of the irreducible subspace corresponding to W. Define*

$$y_0 = \frac{\chi(1)}{|G|}\sum_{g\in G}\chi(g^{-1})g.$$

Then the isotypic projection of $h \in V$ onto W is given by y_0h.

Remark 5.5.2. The computational complexity of these projections can be reduced if we consider a separating set for the group G with respect to the vector space V.

Definition 5.5.3. *Let G be a group and V be the group algebra* C*G. Let* $\{T_i\}_{i=1}^n$*be a collection of simultaneously diagonalizable linear transformations of V whose eigenspaces are direct sums of the G-invariant subspaces of V. For each Ginvariant subspace V_i, let m_i = (λ_{i1},...,λ_{in}) be the n-tuple of eigenvalues where*

1 ≤ j ≤ n, and λ_{ij} is the eigenvalue of T_j associated to V_i. If m_i =6 m_k whenever V_i 6= V_k, then the set$\{T_i\}_{i=1}^n$ *is said to be a separating set for V.*

Given a separating set $\{T_i\}_{i=1}^n$ for a vector space V, the computation of the isotypic projections of each $h \in G$ can be obtained as follows :

1. project h onto the eigenspaces of T_1.

2. project the result from 1 onto each of the eigenspaces of T_2.

3. project the result from 2 onto each of the eigenspaces of T_3.

4. continue the projection in this manner till the eigenspaces of T_n.

After projecting onto the eigenspaces of T_n, each eigenspace projection becomes a different isotypic projection of h[**?**].

5.6 Modified character table

In this section, we examine one of the ways of constructing a separating set of a finite group G. This method, the class sum method, uses eigenvalues that a class sum associates to the irreducible characters to obtain the separating set based on the class sums which can actually distinguish each of the irreducible characters.

Definition 5.6.1. *Let G be a finite group with a conjugacy class C. The class sum $\overline{C}$ of C is the sum of all elements of the conjugacy class C. That is,*

$$\overline{C} = \sum_{g \in C} g$$

Remark 5.6.2. The class sum $\overline{C}$ is an element of the center $Z(\mathbb{C}G)$ of the group algebra $\mathbb{C}G$.

Since, the separating sets are obtained by examining the eigenvalues a class sum assigns to the irreducible characters, let us probe into how this eigenvalues are obtained.

Suppose W is a n-dimensional irreducible representation and let $\lambda_W(\overline{C})$ be the eigenvalue $\overline{C}$ assigns to W. Knowing that the trace of a linear transformation is the sum of its eigenvalues, we have

$$Tr(\overline{C}) = n\lambda_W(\overline{C}).$$

Also,

$$Tr(\overline{C}) = \sum_{g \in C} Tr(g) = |C|\chi_W(g)$$

) for any $g \in C$.

By comparing the two expressions for $Tr(\overline{C})$ we obtain a formula for computing the eigenvalue $\lambda_W(C)$.

Proposition 5.6.3. *Let W be an irreducible representation of G with corresponding character χ. Then the class sum of the conjugacy class C will assign the eigenvalue*

$$\lambda_W(C) = |C|\frac{\chi(g)}{\dim(W)}$$

for any $g \in C$,

to W.

Definition 5.6.4. *Given a character table of a group G with s conjugacy classes $C_1,...,C_s$, the modified character table of G is an array whose (i,j)th entries are obtained by scaling the (i,j)th entry of the character table of* G by $\frac{|C_j|}{\chi_i(1)}$ *where i,j ∈ {1,2,...,s}. This table encodes informations about the eigenvalues that each class sum assigns to each irreducible representation.*

Definition 5.6.5. *The semi-modified character table of a group G is an array whose elements are obtained by dividing the ith row of the character table of G by χ_i for* 1 *≤ i ≤ s.*

Recall from Theorem 4.2.25, the character table of the subgroup G of S_4.

	(1)	(12)(34)	(123)	(132)
χ_1	1	1	1	1
χ_2	1	1	$e^{\frac{2\pi}{3}i}$	$e^{\frac{4\pi}{3}i}$
χ_3	1	1	$e^{\frac{-2\pi}{3}i}$	$e^{\frac{-4\pi}{3}i}$
χ_4	3	-1	0	0

Recall that the conjugacy classes C_1, C_2, C_3 and C_4 are of sizes, 1,3,4,and 4 respectively and the degrees of the 4 irreducible representations are 1,1,1, and 3.

Thus, to obtain the modified character table of G we scale each (i,j)th entry by $\frac{|C_j|}{\chi_i((1))}$ with i,j ∈ {1,2,3,4}.

Direct computations yields: The class sum corresponding to the conjugacy classes

	(1)	(12)(34)	(123)	(132)
χ_1	1	3	4	4
χ_2	1	3	$4e^{\frac{2\pi i}{3}}$	$4e^{\frac{4\pi i}{3}}$
χ_3	1	3	$4e^{-\frac{2\pi i}{3}}$	$4e^{-\frac{4\pi i}{3}}$
χ_4	1	-1	0	0

Table 5.2: Modified character table of $G \subset S_4$.

C_1, C_2, C_3 and C_4 is given by

$$C_1 = (1),$$

KNUST
NYANSAPO WOSANE NO BADWENMA

$\overline{C_2} = (12)(34) + (13)(24) + (14)(23)$, $\overline{C_3} = (123) + (134) + (243)$,

$$\overline{C_4} = (132) + (143) + (124) + (234).$$

From Table 5.2 we observe that, the set of all class sums $\{C_1, C_2, C_3, C_4\}$ form a separating set of size 4 as it assigns distinct 4-tuple of eigenvalues to each of the irreducible representations of G.

However to reduce the computations required for the eigenspace projection, it is more efficient to consider separating sets of minimal sizes.

Upon examining the 3 non-trivial class sums $\overline{C_2}, \overline{C_3}, \overline{C_4}$, we note that the class sum $\overline{C_3}$ or $\overline{C_4}$ assign distinct eigenvalues to all 4 irreducible representations and hence $\{\overline{C_3}\}$ or $\{\overline{C_4}\}$ form a separating set of size 1.

Also,

$$\{\overline{C_2}, \overline{C_3}, \overline{C_4}\}, \{\overline{C_2}, \overline{C_3}\}, \{\overline{C_3}, \overline{C_4}\}, \{\overline{C_2}, \overline{C_4}\}$$

are separating sets of sizes 3,2,2 and 2 respectively.

Proposition 5.6.6. Recall the character table of the quaternion group Q from Proposition 4.2.26 Using Definition 5.6.4, we construct the modified character table below:

	1	−1	I	J	K
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	1	1	-1	1	-1
χ_4	1	1	-1	-1	1
χ_5	2	-2	0	0	0

	1	−1	I	J	K
χ_1	1	1	2	2	2
χ_2	1	1	2	-2	-2

χ_3	1	1	-2	2	-2
χ_4	1	1	-2	-2	2
χ_5	1	-1	0	0	0

Table 5.3: The modified character table of the quaternion group Q.

A meticulous examination of Table 5.3, shows that pairwise combinations of the class sums, $-I+I$,$-J+J$ and $-K+K$ assign distinct pairs of eigenvalues to each irreducible representations of Q.

In particular, the set $\{-J+J,-K+K\}$ assigns to χ_1 the pair $\{2,2\}$; to χ_2 the pair $\{-2,-2\}$; to χ_3 the pair $\{2,-2\}$; to χ_4 the pair $\{-2,2\}$ and to χ_5 the pair $\{0,0\}$.

Therefore, the set $\{-J+J,-K+K\}$,$\{-I+I,-J+J\}$ and $\{-I+I,-K+K\}$ are separating sets of size 2.

These give the minimal separating sets as there are no separating sets of size 1. This is because, none of the individual class sums independently distinguish all the 4 irreducible representations with it's eigenvalues.

Nevertheless, there are separating sets of sizes 3,4 and 5.

Proposition 5.6.7. *Let W be an isotypic subspace of* C*G, and let χ be the character of the irreducible submodule corresponding to W. Define*

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

The isotypic projection of f onto W is then given by zf.

Definition 5.6.8. *A separating set G with respect to V is a set of simultaneously diagonalizable linear operators $\{T_1,...T_s\}$ of* C*G that distinguish the isotypic subspaces of V with their eigenspaces. Each isotypic subspace will equal exactly one intersection of eigenspaces $E_1 \cap ... \cap E_s$, where E_i is an eigenspace of T_i. This means* *that if W_i and W_j are distinct isotypic subspaces of V then some T_k assigns a different eigenvalue to each of them.*

Proposition 5.6.9. *Let W be irreducible module of G with corresponding character χ. Then the class sum of K will assign the eigenvalue*

$$\lambda_W(C^K) = |K|\frac{\chi(g}{dim(W)}$$

to W where g is any element of K.

KNUST

5.6.10 Separating Sets for Direct Products of Groups

Let *G* and *H* be two finite groups and let $\{\chi_1,...,\chi_s\}$ and $\psi,...,\psi_t$ be the complete set of irreducible characters of *G* and *H*, respectively. Then a complete set of irreducible characters of *G* × *H* is given by

$$\{\chi_i\psi_j\}_{1\leq i\leq s,,1\leq j\leq t}$$

and if $g \in G$ and $h \in H$ we have $\chi_i\psi_j(g,h) = \chi_i(g)\psi_i(h)$.

5.6.11 Separating Sets for the Dihedral Group

Theorem 5.6.12. $\{C^r\}$ *form a separating set of minimal size for the dihedral group* D_{2n}*.*

Proof. Case 1:*n* is odd. Then the character table of D_{2n} is as follows:

	1	$r^a(1 \leq a \leq \frac{n-1}{2})$	s
χ_1	1	1	1
χ_2	1	1	-1
ψ_j	2	$2.cos(\frac{2\pi}{n}ja)$	0
$(1 \leq j \leq \frac{n-1}{2})$			

We can construct the semi-modified character table easily:

	1	$r^a(1 \leq a \leq \frac{n-1}{2})$	s
χ_1	1	1	1
χ_2	1	1	-1
ψ_j	2	$cos(\frac{2\pi}{n}ja)$	0
$(1 \leq j \leq \frac{n-1}{2})$			

Now we can see that class sum corresponding to s serves to distinguish χ_1 and χ_2 from each other and from all the ψ_j. Now we show that the class sum corresponding to r will distinguish all of the ψ_j from one another. Suppose C^r assigns the same eigenvalue to ψ_x and ψ_y. Then this implies that

$$cos\left(\frac{2\pi x}{n}\right) = cos\left(\frac{2\pi y}{n}\right).$$

□

Theorem 5.6.13. *For any number q relatively prime to n,{C^{rq},C^s} will form a separating set for the dihedral group D_{2n}.*

Proof. First we will show that all the ψ_j are distinguished from one another by these class sums. From the proof of theorem 5.6.12, we know that it suffices to show that if 1 $\leq \{j, k\} \leq \frac{n-1}{2}$, then $cos\left(\frac{2\pi jq}{n}\right) = cos\left(\frac{2\pi kq}{n}\right)$ implies $j = k$. If the former is true, then there are two cases to consider.

Case 1: $\left(\frac{2\pi jq}{n}\right) + \left(\frac{2\pi kq}{n}\right) + 2\pi m$ for some $m \in \mathbb{Z}$. Then $(j - k)q = mn$ and since n and q are relatively prime we have that $n|(j - k)$. However, since n and q are relatively prime we have that $n|(j-k)$. However, $j, k \in \{1, ..., \frac{n-1}{2}\}$ and thus their difference is bounded above by $\frac{n-1}{2}$.

Case 2: $\left(\frac{2\pi jq}{n}\right) = -\left(\frac{2\pi kq}{n}\right) + 2\pi m.$ Then we have that $(j + k)m = mn$ and thus, since $gcd(n,q) = 1$,$n|(j + k)$. But $j + k \leq \frac{n-1}{2} + \frac{n-1}{2} = n -$1 so this is impossible.

Thus C^{r_q} assigns a different eigenvalue to each irrep ψ_j, regardless of whether n is even or odd. In the case where n is odd, we still have χ_1 and χ_2 distinguished from each other and from all the ψ_j as before, so the parity of q is irrelevant. In the case where n is even, it can be seen from the table that we must have q odd; otherwise, we will not distinguish χ_1 from χ_3 or χ_2 from χ_4 with the two class sums. This is already known to be true because n is even and $\gcd(q,n) = 1$. Thus $\{C^{r_q},C^s\}$ suffices as a separating set for the dihedral group when $\gcd(n,q) = 1$. □

5.7 Separating sets of the unitary group $U_2(\mathsf{F}_{q^2})$

In this section,we construct the character table of $U_2(\mathsf{F}_{q^2})$ from the irreducible characters which we briefly discussed in section 5.4 but carefully derived in [**?**], and later construct the modified character table in order to obtain the separating sets of the unitary group $U_2(\mathsf{F}_{q^2})$.

Let $C^{a_x}, C^{b_{x,y}}, C^{c_{x,y}}, C^{d_{x,y}}$ be the class sum corresponding to the conjugacy classes of $a_x, b_{x,y}, c_{x,y}$ and $d_{x,y}$ respectively. The character table of $U_2(\mathsf{F}_{q^2})$ is given as

	a_x	$b_{x,y}$	$c_{x,y}$	$d_{x,y}$
χ_{U_η}	$\eta(x)^2$	$\eta(x)^2$	$\eta(x)\eta(y)$	$\eta(x^2-y^2)$
χ_{V_η}	$q\eta(x)^2$	0	$\eta(x)\eta(y)$	$-\eta(x^2-y^2)$
$\chi_{W_{\eta,\zeta}}$	$(q+1)\eta(x)\zeta(x)$	$\eta(x)\zeta(x)$	$\eta(x)\zeta(y)+\eta(y)\zeta(x)$	0
$X_{\eta,\zeta}$	$(q-1)\eta(x)\zeta(x)$	$-\eta(x)\zeta(x)$	0	$-[\eta(m)\zeta(n)+\eta(n)\zeta(m)]$

Table 5.4: Character table of G

The dimension of each of the irreducible representations of G are $1,q,q+1,q-1$ and $m = x+y$ and $n = x-y$. Using this dimensions and the character table, Table 5.4 we construct the semi-modified character table for G:

	a_x	$b_{x,y}$	$c_{x,y}$	$d_{x,y}$
$\chi_{U_{\eta^*}}$	$\eta(x)^2$	$\eta(x)^2$	$\eta(x)\eta(y)$	$\eta(x^2-y^2)$
$\chi_{V_{\eta^*}}$	$\eta(x)^2$	0	$\frac{\eta(x)\eta(y)}{q}$	$-\frac{\eta(x^2-y^2)}{q}$

$\chi W^*_{\eta,\zeta}$	$\eta(x)\zeta(x)$	$\frac{\eta(x)\zeta(x)}{q+1}$	$\frac{\eta(x)\zeta(y)+\eta(y)\zeta(x)}{q+1}$	0
$X^*_{\eta,\zeta}$	$\eta(x)\zeta(x)$	$-\frac{\eta(x)\zeta(x)}{q-1}$	0	$-\frac{[\eta(m)\zeta(n)+\eta(n)\zeta(m)]}{q-1}$

Table 5.5: Semi-modified character table of G.

	$b_{x,y}$	$c_{x,y}$	$d_{x,y}$
$\chi_{U_{\eta^*}}$	$\eta(x)^2$	$\eta(x)\eta(y)$	$\eta(x^2-y^2)$
$\chi_{V_{\eta^*}}$	0	$\frac{\eta(x)\eta(y)}{q}$	$-\frac{\eta(x^2-y^2)}{q}$
$\chi_{W_{\eta,\zeta^*}}$	$\frac{\eta(x)\zeta(x)}{q+1}$	$\frac{\eta(x)\zeta(y)+\eta(y)\zeta(x)}{q+1}$	0
X_{η,ζ^*}	$-\frac{\eta(x)\zeta(x)}{q-1}$	0	$-\frac{[\eta(m)\zeta(n)+\eta(n)\zeta(m)]}{q-1}$

Table 5.6: Separating Set Table

From Table 5.5, we observe that the class sum corresponding to $b_{x,y}$,$c_{x,y}$ or $d_{x,y}$ assigns distinct eigenvalues to all four irreducible representations and hence distinguishes each of the irreducible characters. This, by definition of a separating set serves as a separating set of size 1. Further investigation, shows that the class sums $C^{b_{x,y}}$,$C^{c_{x,y}}$, and $C^{d_{x,y}}$, altogether and in a pairwise combination, assign distinct list of eigenvalues to each irreducible character of G. Thus, the sets $\{C_{b_{x,y}},C_{c_{x,y}}\}$, $\{C_{c_{x,y}},C_{d_{x,y}}\}$, $\{C_{b_{x,y}},C_{d_{x,y}}\}$ and $\{C_{b_{x,y}},C_{c_{x,y}},C_{d_{x,y}}\}$ are separating sets of size 2,2,2 and 3 respectively.

Proposition 5.7.1. *The sets $\{C^{b_{x,y}}\}$, $\{C^{c_{x,y}}\}$ and $\{C^{d_{x,y}}\}$ are minimal separating sets for the unitary group $U_2(\mathrm{F}_{q^2})$.*

KNUST
NYANSAPO WO SANE NO BADWENMA

Chapter 6

Conclusion

6.1 Introduction

KNUST

In this, we conclude on the overview of [?] and the objectives of the thesis.

6.2 Review

In the review work of [?] of separating sets in chapter 4, separating sets of several different groups, including products, the dihedral group and the alternating group were examined.

In the aforementioned chapter, separating sets of minimal size for the dihedral group that correspond to minimal sets of generators for the group was see. It was also shown that the structure of CA_n is closely connected to that of CS_n and various methods for achieving a decomposition with the use of separating sets were examined.

In [?], conjecture 5.1 seems likely to hold for all *n*, but remains a challenge to verify. The separating set given by the aforementioned conjecture is suspected to be of minimal size.

6.3 Summary

The cardinality of the group $U_2(\mathrm{F}_{q^2})$ was determined as $(q-1)q(q+1)2$ in [?] .

For each conjugate class their cardinality is given as $\bar{A}(q+1)$,b_{xy} have element $\bar{A}(q-1)(q+1)^2$,elements c_{xy} is of order $\frac{(q-2)q(q+1)}{2}$ and that d_{xy} has an order of $\frac{(q-1)q^2(q+1)}{2}$.

The character table was constructed with each conjugacy class.

Our build up to character theory in chapter 3 enabled us to efficiently examine the separating sets of the quaternion group Q and the subgroup $G \subset S_4$ in chapter 4. The knowledge gathered was employed in probing into the irreducible characters presented in [**?**] and thus by constructing the semi-modified character table we were able to extract the separating sets for the unitary group $U_2(\mathrm{F}_{q^2})$. Our investigations lead to the conclusion that, the minimal separating sets of the group $U_2(\mathrm{F}_{q^2})$ are the individual class sums corresponding to the conjugacy classes of the representatives $b_{x,y}$,$c_{x,y}$ and $d_{x,y}$.

6.4 Furtherwork

In attempt to prove the aforementioned conjecture would intriguing and challenging future direction of research [**?**]

It would be interesting to look at other groups which have a minimal set of generators which have a minimal set of generators for which the corresponding class shows form separation sets. Further studies can be conducted into irreducible characters in 2-dimensional and the separation of U_2 groups. The young tableaux of the representation can be looked at.

REFERENCES

[1] Ayekple Elikem Yao (2006). Representation theory of finite groups. Unpublished Master’s thesis,Department of Mathematics, Kwame Nkrumah university of Science and Technology,Kumasi,Ghana.

[2] Banister Melissa (2004). Separating Sets for the alternating and Dihedral Groups.PhD thesis.

[3] Campbell John J. (2014). The irreducible characters of 2 × 2 unitary matrix groups over finite fields. Master’s thesis, University of Alberta.

[4] Derksen Harmand and Kemper Gregor (2002) . Computational invariant the-

ory.

[5] John D Dixon(1970). Computing irreducible representations of groups. Mathematics of Computation, 24(111):707–712.

[6] Dufresne Emilie(2009) . Separating invariants and finite reflection groups. *Advances in Mathematics*, 221(6):1979–1989.

[7] Dufresne Emilie(2013) . Finite separating sets and quasi – affine quotients. *Journal of Pure and Applied Algebra*, 2(217):247–253.

[8] Faraut Jacques (2008). Analysis on Lie groups: *an introduction*, volume 110. Cambridge University Press.

[9] Fulton William and Harris Joe (1991) . Representation theory. a first course. *Graduate Texts in Mathematics*, 129.

[10] Itzykson Claude and Nauenberg Michael (1966). Unitary groups: Representations and decompositions. *Reviews of Modern Physics*, 38(1):95

[11] Katriel J (1991). Some useful results concerning the representation theory of the symmetric group. *Journal of Physics A: Mathematical and General* 24(22):5227.

[12] Moshinsky Marcos (1963). Bases for the irreducible representations of the unitary groups and some applications. *Journal of Mathematical Physics*, 4(9):1128 –1139.

[13] Rotman Joseph J (2006). A first course in abstract algebra with applications. *AMC*,10:12.

[14] Steinberg Benjamin (2009). Representation theory of finite groups.

[15] Thiem Nathaniel and Vinroot C Ryan (2009). Gelfand − graev characters of the finite unitary groups. *the electronic journal of combinatorics*, 16(1):R146.

[16] Webb Peter (2007). Finite group representations for the pure mathematician. *The manuscript of the book is available on the author web page http://www. math.umn. edu/∼ webb/RepBook/index. html*, 74:76.

[17] Wikipedia (2015). Compact group − wikipedia, the free encyclopedia. [On − line; accessed 15 − September − 2015]

[18] Wikipedia (2015). Lie algebra − wikipedia, the free encyclopedia.On − line; accessed 15 − September − 2015]

[19] *www.cmth.ph.ic.uk/people/d.vvdensky/groups/chapter 9.pdf*.[18 − September − 2015]

KNUST

NYANSAPƆ WƆSANE NO BADWENMA