The Irreducible Representations of D2n

Melissa Soto

Follow this and additional works at: https://scholarworks.lib.csusb.edu/etd

Part of the Algebra Commons

Recommended Citation
https://scholarworks.lib.csusb.edu/etd/12

This Thesis is brought to you for free and open access by the Office of Graduate Studies at CSUSB ScholarWorks. It has been accepted for inclusion in Electronic Theses, Projects, and Dissertations by an authorized administrator of CSUSB ScholarWorks. For more information, please contact scholarworks@csusb.edu.
THE IRREDUCIBLE REPRESENTATIONS OF $D_{2n}$

A Thesis

Presented to the

Faculty of

California State University,

San Bernardino

In Partial Fulfillment

of the Requirements for the Degree

Master of Arts

in

Mathematics

by

Melissa Marie Soto

March 2014
The Irreducible Representations of $D_{2n}$

A Thesis

Presented to the

Faculty of

California State University,

San Bernardino

by

Melissa Marie Soto

March 2014

Approved by:

Giovanna Llosent, Committee Chair  
Laura Wallace, Committee Member  
James Paul Vicknair, Committee Member  
Peter Williams, Chair,  
Department of Mathematics

Date

Charles Stanton  
Graduate Coordinator,  
Department of Mathematics
Irreducible representations of a finite group over a field are important because all representations of a group are direct sums of irreducible representations. Maschke tells us that if $\phi$ is a representation of the finite group $G$ of order $n$ on the $m$-dimensional space $V$ over the field $K$ of complex numbers and if $U$ is an invariant subspace of $\phi$, then $U$ has a complementary reducing subspace $W$.

The objective of this thesis is to find all irreducible representations of the dihedral group $D_{2n}$. The reason we will work with the dihedral group is because it is one of the first and most intuitive non-abelian group we encounter in abstract algebra. I will compute the representations and characters of $D_{2n}$ and my thesis will be an explanation of these computations. When $n = 2k + 1$ we will show that there are $k + 2$ irreducible representations of $D_{2n}$, but when $n = 2k$ we will see that $D_{2n}$ has $k + 3$ irreducible representations. To achieve this we will first give some background in group, ring, module, and vector space theory that is used in representation theory. We will then explain what general representation theory is. Finally we will show how we arrived at our conclusion.
I wish to thank Dr. Giovanna Llosent for her help in organizing and developing this paper. Moreover, I would like to thank Dr. Laura Wallace and Dr. James Paul Vicknair for their invaluable comments. Furthermore, I would like to thank the faculty and staff in the Mathematics Department for their guidance and support. The Math department has been extremely supportive as I finished the last part of my Masters Degree from CSUSB while living in Iowa. Finally, I would like to thank my family for all their love and patience while I studied mathematics, especially my husband Robert, to whom I dedicate this thesis.
Table of Contents

Abstract iii

Acknowledgements iv

1 Background 1
   1.1 Group Theory . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 1
   1.2 Ring Theory . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4
   1.3 Module Theory . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 8
   1.4 Vector Space Theory . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 12

2 General Representation Theory 15
   2.1 Linear Representations and KG-modules . . . . . . . . . . . . . . . . . . 15
   2.2 Examples of KG-modules . . . . . . . . . . . . . . . . . . . . . . . . . . . 19
   2.3 Irreducible Representations of $D_8$ . . . . . . . . . . . . . . . . . . . . . 24
   2.4 Character Theory . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 33

3 The Representation Theory of $D_{2n}$ 40
   3.1 Introduction . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 40
   3.2 Conjugacy Classes of $D_{2n}$ . . . . . . . . . . . . . . . . . . . . . . . . . . 44
   3.3 Commutator Subgroup of $D_{2n}$ . . . . . . . . . . . . . . . . . . . . . . . . 48
   3.4 Irreducible Representations of $D_{2n}$ . . . . . . . . . . . . . . . . . . . . . 52

4 Conclusion 57

Bibliography 58
Chapter 1

Background

In order to understand group representation theory, or linear representation theory, it is important to be well versed in many areas of abstract algebra: group theory, ring theory, module theory, and vector space theory. In this chapter we will highlight many of the results that are needed to understand group representation theory. We begin by looking at group theory.

1.1 Group Theory

We start this section by defining a group.

Definition 1.1.1. A group is an ordered pair \((G, \cdot)\), where \(G\) is a set and \(\cdot\) is a binary operation on \(G\) satisfying the following axioms:

(i) \(\forall a, b \in G \text{ we have that } a \cdot b \in G\),

(ii) \(\cdot\) is associative,

(iii) \(\exists e \in G, \text{ called an identity in } G \text{ such that } \forall a \in G \text{ we have } a \cdot e = e \cdot a = a\),

(iv) \(\forall a \in G \text{ there exists an element } a^{-1} \text{ of } G, \text{ called an inverse of } a, \text{ such that } a \cdot a^{-1} = a^{-1} \cdot a = e\).

Note that we usually write \(ab\) instead of \(a \cdot b\) when dealing with multiplicative groups. A group \(G\) is called abelian if \(ab = ba \forall a, b \in G\). We also say that a group \(G\) is finite if \(G\) is a finite set. If \(H \subseteq G\) then we say \(H\) is a subgroup of \(G\), denoted by
Proposition 1.1.1 (One Step Subgroup Test). A nonempty subset \( H \) of the group \( G \) is a subgroup of \( G \) iff \( xy^{-1} \in H \) \( \forall x, y \in H \).

Given a group \( G \) and an element \( g \in G \) we define the cyclic group generated by \( g \) as follows: \( \langle g \rangle = \{ g^k : k \in \mathbb{Z} \} \). Note the following fact:

Proposition 1.1.2. A cyclic group is abelian.

It will be important for us to determine when two groups “look the same” and we will say that two groups that “look the same” are isomorphic. Let us define this more precisely by first defining the notion of a homomorphism:

Definition 1.1.2 (Group Homomorphism). Let \((G, \cdot)\) and \((H, \ast)\) be groups. Then a map \( \phi : G \to H \) is called a group homomorphism iff \( \phi(x \cdot y) = \phi(x) \ast \phi(y) \) \( \forall x, y \in G \).

The kernel of a group homomorphism \( \phi : G \to H \) is the set \( \ker \phi = \{ g \in G : \phi(g) = e_H \} \). The image of a group homomorphism \( \phi \) is given by the set \( \text{im} \phi = \{ \phi(g) : g \in G \} \). We say that a group homomorphism \( \phi \) is a group isomorphism if \( \phi \) is a group homomorphism that is also bijective. We note the following useful result.

Proposition 1.1.3. Let \( \phi : G \to H \) be a group homomorphism. Then \( \ker \phi \leq G \) and \( \text{im} \phi \leq H \).

A group has special subgroups called normal subgroups that allow us to create quotient groups. Before we define this notion let us define what a coset is. Then we will define the order of a group and give an important result called Lagrange’s Theorem which relates the order of a group with the order of its subgroups.

Definition 1.1.3. Let \( H \leq G \). For any \( a \in G \) define \( aH = \{ ah : h \in H \} \). The set \( aH \) is called the left coset of \( H \) in \( G \) containing \( a \).

Definition 1.1.4. The order of a group \( G \) is the cardinality of the group \( G \) and is denoted by \(|G|\).

Theorem 1.1.1 (Lagrange’s Theorem). If \( G \) is a finite group and \( H \leq G \), then \(|H| \) divides \(|G|\).
Now let \( N \leq G \). We say that \( N \) is normal in \( G \) if \( \forall x \in N \) and \( \forall g \in G \) we have that \( gxg^{-1} \in N \) and we denote this by writing \( N \triangleleft G \). The following is a major result that highlights the importance of normal subgroups.

**Theorem 1.1.2** (Quotient Groups). Let \( G \) be a group and let \( N \triangleleft G \). Then the set \( G/N = \{gN : g \in G\} \) is a group under the operation \((aN)(bN) = abN \forall a, b \in G\). We call \( G/N \) a quotient group of \( G \).

The following is an important result that gives the connection between group homomorphisms and quotient groups.

**Theorem 1.1.3** (First Isomorphism Theorem). Let \( \phi : G \to H \) be a group homomorphism. Then \( \ker\phi \triangleleft G \) and \( G/\ker\phi \cong \text{im}\phi \).

Note then that if the kernel of \( \phi \) is trivial then \( \phi \) is one-to-one, or injective. Also if \( \text{im}\phi = H \) and \( \ker\phi = 1_G \) then \( \phi \) is a group isomorphism. Also note that if \( N \triangleleft G \), then the map \( G \to G/N \) defined by \( g \mapsto gN \) is a surjective group homomorphism with kernel \( N \). This map is called the natural projection of \( G \) onto \( G/N \). Also note that the left cosets of \( H \) in \( G \) for any subgroup \( H \) of \( G \) partition \( G \), i.e., we can write \( G \) as a disjoint union of its left cosets. Another way to partition \( G \) is through its conjugacy classes, which we define next.

**Definition 1.1.5.** The conjugacy class of \( g \in G \) is the set \([g] = \{xgx^{-1} | x \in G\}\).

We also note that if \( G \) is abelian, then for any \( x \in G \) we have that \([x] = \{x\}\) since if \( y \) is conjugate to \( x \) in \( G \), then \( y = gxg^{-1} \) for some \( g \in G \). But \( G \) is abelian so \( gxg^{-1} = gg^{-1}x = x \), i.e. \( y = x \). We finish by discussing group actions and a special action that plays a role in linear representation theory.

**Definition 1.1.6** (Group Action). A group action of a group \( G \) on a set \( A \) is a map from \( G \times A \to A \), written as \( g \cdot a \), for all \( g \in G \) and \( a \in A \) satisfying the following properties:

(i) \( g_1 \cdot (g_2 \cdot a) = (g_1 \cdot g_2) \cdot a, \forall g_1, g_2 \in G, \forall a \in A \), and

(ii) \( 1_G \cdot a = a \forall a \in A \).

**Definition 1.1.7** (Permutation Representation). Let \( G \) be a group acting on a nonempty set \( A \). For each \( g \in G \) the map \( \sigma_g : A \to A \) defined by \( \sigma_g : a \mapsto g \cdot a \) is a permutation.
of $A$. (This $g \cdot a$ is the map from $G \times A$ to $A$ in the group action def above) There is a homomorphism associated to an action of $G$ on $A$: $\phi: G \to S_A$ defined by $\phi(g) = \sigma_g$, called the permutation representation.

In particular we note that $G$ can act on itself by left multiplication. This will help us define a linear representation of $G$ called the regular representation of $G$ in Chapter 2.

1.2 Ring Theory

In Chapter 2 we use the notion of a group ring which we define in this section. Hence it is important to have some basic definitions from ring theory such as subrings, ideals, and ring homomorphisms. Moreover, the basic homomorphisms theorems of the theory of groups can be extended to the theory of rings and we list those here. Furthermore, special concepts such as integral domain, division ring, and fields are an important part of linear representation theory and thus reviewed here.

**Definition 1.2.1.** A ring $R$ is a set together with two binary operations $+$ and $\cdot$ (called addition and multiplication) satisfying the following axioms:

(i) $(R,+)$ is an abelian group,

(ii) $\cdot$ is associative: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, and

(iii) the distributive laws hold in $R$: for all $a,b,c \in R$ $(a + b) \cdot c = a \cdot c + b \cdot c$ and $a \cdot (b + c) = a \cdot b + a \cdot c$.

We say that a ring $R$ is commutative if multiplication is commutative, i.e. $ab = ba \ \forall a,b \in R$. A ring $R$ is said to have an identity (or contain a 1) if there is an element $1 \in R$ with $1 \cdot a = a \cdot 1 = a$ for all $a \in R$. A subset $S$ of $R$ is called a subring of $R$ if $S$ is a ring under the same two operations of the ring $R$. We obtain a result similar to the One Step Subgroup Test.

**Proposition 1.2.1** (Subring Test). A nonempty subset $S$ of the ring $R$ is a subring of $R$ iff $\forall a,b \in S$ we have that $a - b \in S$ and $ab \in S$.

Example of rings include the set of integers, $\mathbb{Z}$, the set of rationals $\mathbb{Q}$, the set of reals, $\mathbb{R}$, and the set of complex numbers, $\mathbb{C}$, all under ordinary addition and
multiplication. The set of $n \times n$ matrices with entries in a ring $R$, denoted by $M_n(R)$, is a ring under matrix multiplication and matrix addition. As in group theory we have a notion of ring homomorphisms.

**Definition 1.2.2** (Ring Homomorphism). Let $R$ and $S$ be rings. A ring homomorphism is a map $\phi : R \to S$ satisfying the following:

(i) $\phi(a + b) = \phi(a) + \phi(b)$ $\forall a, b \in R$, i.e. $\phi$ is a group homomorphism on the additive group $(R, +)$, and

(ii) $\phi(ab) = \phi(a)\phi(b)$ $\forall a, b \in R$

The kernel of a ring homomorphism $\phi : R \to S$ is the set of elements in $R$ that map to 0 in $S$, denoted by $\ker \phi = \{a \in R : \phi(a) = 0_S\}$. The image of $\phi$, denoted by $\text{im} \phi$ or $\phi(R)$ is the set $\{\phi(r) : r \in R\}$ A ring isomorphism is a bijective ring homomorphism.

We note the following important result:

**Proposition 1.2.2.** Let $R$ and $S$ be rings and let $\phi : R \to S$ be a ring homomorphism.

(i) The kernel of $\phi$ is a subring of $R$.

(ii) The image of $\phi$ is a subring of $S$.

We have a notion similar to normal subgroups which we define next.

**Definition 1.2.3.** Let $R$ be a ring, let $I$ be a subset of $R$, and let $r \in R$.

1. $rI = \{ra | a \in I\}$ and $Ir = \{ar | a \in I\}$

2. A subset $I$ of $R$ is a left ideal of $R$ if

   (i) $I$ is a subring of $R$, and

   (ii) $I$ is closed under left multiplication by elements of $R$, i.e., $rI \subseteq I$ for all $r \in R$.

Similarly $I$ is a right ideal if (i) holds and in place of (ii) we have the following:

(ii)' $I$ is closed under right multiplication by elements of $R$, i.e., $Ir \subseteq I$ for all $r \in R$.

3. A subset $I$ that is both a left and right ideal is called an ideal, (or a two-sided ideal) of $R$. 
Note for commutative rings the notion of left, right, two-sided ideal coincide. Moreover we say an ideal \( I \) of \( R \) is a proper ideal if and only if \( I \) does not coincide with \( R \), i.e., \( I \nsubseteq R \). Now define the set \( R/I = \{r + I : r \in R\} \). Since \( R \) is an abelian group under addition then \( R/I \) is a group under addition. It can be shown that the following two operations are well defined for all \( r, s \in R \):

(a) \((r + I) + (s + I) = (r + s) + I\), and

(b) \((r + I)(s + I) = (rs) + I\).

It can also be shown that set \( R/I \) under the above operations satisfies the ring axioms, thus \( R/I \) is a ring, called the quotient ring of \( R \) by \( I \). We also get a result that is analogous to the First Isomorphism Theorem for Groups.

**Theorem 1.2.1.** (The First Isomorphism Theorem for Rings)

1. If \( \phi : R \to S \) is a homomorphism of rings, then the kernel of \( \phi \) is an ideal of \( R \), the image of \( \phi \) is subring of \( S \) and \( R/\ker \phi \) is isomorphic as a ring to \( \phi(R) \).

2. If \( I \) is any ideal of \( R \), then the map \( R \to R/I \) defined by \( r \mapsto r + I \) is a surjective ring homomorphism with kernel \( I \) (this homomorphism is called the natural projection of \( R \) onto \( R/I \)). Thus every ideal is the kernel of a ring homomorphism and vice versa.

We define a few special rings and then go over rings that play a special role in linear representation theory. First we start by defining zero divisors.

**Definition 1.2.4.** Let \( R \) be a ring.

1. A nonzero element \( a \) of \( R \) is called a zero divisor if there is a nonzero element \( b \in R \) such that either \( ab = 0 \) or \( ba = 0 \).

2. Assume \( R \) has an identity \( 1 \neq 0 \). An element \( u \) of \( R \) is called a unit in \( R \) if there is some \( v \) in \( R \) such that \( uv = vu = 1 \). The set of units in \( R \) is denoted \( R^\times \).

**Definition 1.2.5.** A commutative ring with identity \( 1 \neq 0 \) is called an integral domain if it has no zero divisors.

Another special ring is the following:
Definition 1.2.6 (Division Ring). A ring $R$ with identity $1$, where $1 \neq 0$, is called a division ring, if every nonzero element $a \in R$ has a multiplicative inverse, i.e., there exists $b \in R$ such that $ab = ba = 1$. A commutative division ring is called a field.

The following ring plays an important part in representation theory.

Definition 1.2.7 (Group Ring). Let $R$ be an arbitrary ring with identity $1 \neq 0$ and let $G = \{g_1, g_2, \ldots, g_n\}$ be any finite group with group operation written multiplicatively. The group ring of $G$ over $R$ is the set of all formal sums $\sum_{i=1}^{n} \alpha_i g_i$ where $\alpha \in R$ with component wise addition and multiplication $(\alpha g_i)(\beta h_i) = (\alpha \beta)(g_i h_i)$ (where $\alpha$ and $\beta$ are multiplied in $R$ and $g_i h_i$ is the product in $G$) extended to sums via the distributive law.

Note that for a finite group $G$ and a ring $R$, the group ring $RG$ is not an integral domain since for any $g \in G$ such that $g \neq 1$ we have that $g^n - 1 = (g-1)(g^{n-1} + \cdots + 1) = 0$ in $RG$. We finish this section with a few last definitions.

Definition 1.2.8 (Characteristic of a ring). The characteristic of a ring $R$ is the smallest positive integer $n$ such that $1 + 1 + \cdots + 1 = 0$ ($n$ times) in $R$; if no such integer exists the characteristic of $R$ is $0$. The characteristic of $R$ is denoted by $\text{char}(R)$.

Definition 1.2.9 (Center of a Ring). Let $R$ be a ring. Let the center of a ring be denoted by $Z(R) = \{a \in R : ax = xa, \forall x \in R\}$

Definition 1.2.10. Let $A$ be a subset of $R$.

1. Let $(A)$ denote the smallest ideal of $R$ containing $A$, called the ideal generated by $A$. It can be shown that $(A)$ is the intersection of all ideals of $R$ that contain $A$.

2. Let $RA$ denote the set of all finite sums of elements of the form $ra$ with $r \in R$ and $a \in A$ i.e., $RA = \{\sum_{i=1}^{n} r_i a_i : r_i \in R, a_i \in A, n \in \mathbb{Z}^+\}$ (where the convention is $RA = 0$ if $A = \emptyset$). We can similarly define $AR$ and $RAR$. Note that we can show that $RA$ is the left ideal generated by $A$, $AR$ is the right ideal generated by $A$, and $RAR = (A)$. In particular if $R$ is commutative then $RA = AR = (A)$.

3. An ideal generated by a single element $a \in R$ is called a principal ideal and is denoted by $(a)$.

4. An ideal generated by a finite set, say $\{a_1, a_2, \ldots, a_m\}$ is called a finitely generated ideal and is denoted by $(a_1, a_2, \ldots, a_m)$.
Definition 1.2.11. Let $R$ be a nonzero ring.

1. A nonzero element $e$ in a ring $R$ is called idempotent if $e^2 = e$.

2. Idempotents $e_1$ and $e_2$ are said to be orthogonal if $e_1e_2 = e_2e_1 = 0$.

3. An idempotent $e$ is said to be primitive if it cannot be written as a sum of two (commuting) orthogonal idempotents.

4. The idempotent $e$ is called a primitive central idempotent if $e \in Z(R)$ and $e$ cannot be written as a sum of two orthogonal idempotents in the ring $Z(R)$.

1.3 Module Theory

In Chapter 2 we will see that every representation of a group $G$ over a field $K$ is in one-to-one correspondence with a left module over the group ring $KG$. Thus in this section we will highlight the elementary aspects of the theory of modules.

Definition 1.3.1. Let $R$ be a ring (not necessarily commutative nor with a 1). A left $R$-module or a left module over $R$ is a set $M$ together with

1. a binary operation $+$ on $M$ under which $M$ is an abelian group, and

2. an action of $R$ on $M$ (that is, a map $R \times M \to M$) denoted by $r.m$, for all $r \in R$ and for all $m \in M$ that satisfies

   (a) $(r+s).m = r.m + s.m$, for all $r, s \in R, m \in M$

   (b) $(rs)m = r(sm)$, $r, s \in R, m \in M$

   (c) $r.(m+n) = r.m + r.n$, $r \in R, m, n \in M$

   If the ring has a 1 we impose the additional axiom:

   (d) $1.m = m$, for all $m \in M$

The descriptor “left” in the above definition indicates that the ring elements appear on the left. “Right” $R$-modules can be defined analogously. If the ring $R$ is commutative and $M$ is a left $R$-module then we can make $M$ into a right $R$-module by defining $m.r = r.m$ for $m \in M, r \in R$. If $R$ is not commutative, axiom 2(b) in general will not hold with this definition, thus not every left $R$-module is a right $R$-module. The
term “module” in this thesis will always mean “left module”. Modules satisfying 2(d) are called unital modules. Analogously to group and ring theory we have a notion of submodules and a test for submodules.

**Definition 1.3.2 (R-submodule).** Let $R$ be a ring and let $M$ be an $R$-module. An $R$-submodule of $M$ is a subgroup $N$ of $M$ which is closed under the action of ring elements, i.e., $r.n \in N$, for all $r \in R, n \in N$.

**Proposition 1.3.1 (Submodule Criterion).** Let $R$ be a ring and let $M$ be an $R$-module. A subset $N$ of $M$ is a submodule of $M$ if

1. $N \neq 0$, and
2. $x + ry \in N$ for all $r \in R$ and for all $x, y \in N$.

We say that an $R$-module $M$ is irreducible or simple if $M \neq 0$ and if 0 and $M$ are the only submodules of $M$.

**Definition 1.3.3.** Let $R$ be a ring and let $M$ and $N$ be $R$-modules.

1. A map $\phi : M \to N$ is an $R$-module homomorphism if it respects the $R$-module structures of $M$ and $N$, i.e.,
   
   (a) $\phi(x + y) = \phi(x) + \phi(y)$, for all $x, y \in M$ and 
   (b) $\phi(rx) = r\phi(x)$, for all $r \in R, x \in M$

2. An $R$-module homomorphism is an isomorphism (of $R$-modules) if it is both injective and surjective. The modules $M$ and $N$ are said to be isomorphic, denoted $M \cong N$, if there is some module isomorphism $\phi : M \to N$.

3. If $\phi : M \to N$ is an $R$-module homomorphism, then denote the kernel of $\phi$ by $\ker \phi = \{ m \in M : \phi(m) = 0 \}$. Denote the image of $\phi$ by $\phi(M) = \{ \phi(m) : m \in M \}$. It can be shown that $\ker \phi$ is a submodule of $M$ and that $\phi(M)$ is a submodule of $N$.

4. Let $M$ and $N$ be $R$-modules and define $\text{Hom}_R(M, N)$ to be the set of all $R$-module homomorphisms from $M$ into $N$.
A couple of notes. First of all, if $R$ is a field, $R$-module homomorphisms are called linear transformations. We will formally define these in the next section. Secondly, when $R$ is commutative then $\text{Hom}_R(M,M)$ is an $R$-algebra. We will also see in Chapter 2 that the group ring $KG$ is $K$-algebra, thus we define in general what an $R$-algebra is and $R$-algebra homomorphism.

**Definition 1.3.4** ($R$-algebra). Let $R$ be a commutative ring with identity. An $R$-algebra is a ring $A$ with identity together with a ring homomorphism $f : R \to A$ mapping $1_R \mapsto 1_A$ such that the subring $f(R)$ of $A$ is contained in the center of $A$.

**Definition 1.3.5** ($R$-algebra Homomorphism). If $A$ and $B$ are two $R$-algebras, an $R$-algebra homomorphism (or isomorphism) is a ring homomorphism (isomorphism, respectively) $\phi : A \to B$ mapping $1_A$ to $1_B$ such that $\phi(r.a) = r.\phi(a)$ $\forall r \in R$ and $\forall a \in A$.

**Definition 1.3.6.** The ring $\text{Hom}_R(M,M)$ is called the endomorphism ring of $M$ and will be denoted by $\text{End}_R(M)$. Elements of $\text{End}_R(M)$ are called endomorphisms.

When $R$ is commutative there is a natural map(projection) from $R$ to $\text{End}_R(M)$ given by $r \mapsto rId_M$ where the latter endomorphism is just multiplication by $r$ on $M$. The image of $R$ is contained in the center of $\text{End}_R(M)$ so if $R$ has an identity, $\text{End}_R(M)$ is an $R$-algebra.

**Proposition 1.3.2.** Let $R$ be a ring, let $M$ be an $R$-module and let $N$ be a submodule of $M$. The (additive,abelian) quotient group $M/N$ can be made into an $R$-module by defining an action of elements of $R$ by $r.(x + N) = (r.x) + N$ for all $r \in R, x + N \in M/N$. The natural projection map $\pi : M \to M/N$ defined by $\pi(x) = x + N$ is an $R$-module homomorphism with kernel $N$.

As in group and ring theory we have a First Isomorphism theorem for Modules.

**Theorem 1.3.1** (First Isomorphism theorem for Modules). Let $M, N$ be $R$-modules and let $\phi : M \to N$ be an $R$-module homomorphism. Then $\ker\phi$ is a submodule of $M$ and $M/\ker\phi \cong \phi(M)$.

We now describe the generation of modules and the direct sum of modules.

**Definition 1.3.7.** Let $M$ be an $R$-module and let $N_1, N_2, \ldots, N_n$ be submodules of $M$. 

1. The sum of $N_1, N_2, \ldots, N_n$ is the set of all finite sums of elements from the sets $N_i$: $\{ \sum_{i=1}^{m} a_i : a_i \in N_i \forall 1 \leq i \leq m \}$. We denote this sum by $N_1 + N_2 + \cdots + N_n$.

2. For any subset $A$ of $M$ let $RA = \{ \sum_{i=1}^{m} r_i a_i : r_i \in R, a_i \in A, m \in \mathbb{Z}^+ \}$ (where the convention is $RA = 0$ if $A = \emptyset$). We call $RA$ the submodule of $M$ generated by $A$. If $N$ is a submodule of $M$ (possibly $N = M$) and $N = RA$, for some subset $A$ of $M$, then we call $A$ the set of generators or generating set for $N$, and we say that $N$ is generated by $A$.

3. A submodule $N$ of $M$ (possibly $N = M$) is finitely generated if there is some finite subset $A$ of $M$ such that $N = RA$.

**Definition 1.3.8.** Let $M_1, M_2, \ldots, M_n$ be a collection of $R$-modules. The collection of $n$-tuples $(m_1, m_2, \ldots, m_n)$ where $m_i \in M_i \forall 1 \leq i \leq n$ with addition and action of $R$ defined componentwise is called the direct product of $M_1, M_2, \ldots, M_n$ and is denoted by $M_1 \oplus M_2 \oplus \cdots \oplus M_n$.

The next proposition allows us to find out when a sum of submodules of $M$ is isomorphic to a direct product of these submodules.

**Proposition 1.3.3.** Let $N_1, N_2, \ldots, N_k$ be submodules of the $R$-module $M$. Then the following are equivalent:

1. The map $\pi : N_1 \oplus N_2 \oplus \cdots \oplus N_k \rightarrow N_1 + N_2 + \cdots + N_k$ defined by $\pi(a_1, a_2, \ldots, a_k) = a_1 + a_2 + \cdots + a_k$ is an isomorphism (of $R$-modules): $N_1 + N_2 + \cdots + N_k \cong N_1 \oplus N_2 \oplus \cdots \oplus N_k$.

2. $N_j \cap (N_1 + N_2 + \cdots + N_{j-1} + N_j + \cdots + N_k) = 0$ for all $j \in \{1, 2, \ldots, k\}$.

3. Every $x \in N_1 + N_2 + \cdots + N_k$ can be written uniquely in the form $a_1 + a_2 + \cdots + a_k$ with $a_i \in N_i \forall 1 \leq i \leq k$.

Finally we will see that the group rings that we work with will satisfy something called the *descending chain condition*.

**Definition 1.3.9.** An $R$-module $M$ is said to satisfy the descending chain condition (D.C.C.) on $R$-submodules iff every properly descending chain of submodules of $M$, $N_1 \supset N_2 \supset \cdots \supset N_k \supset \cdots$, contains only a finite number of elements.
1.4 Vector Space Theory

We can now use the language of module theory to define a vector space $V$ over a field $K$. We say that a set $V$ is a vector space over the field $F$ if it is an $F$-module. Since a field is commutative we know that left modules and right modules coincide so it is not necessary to distinguish between the two, although by convention our scalars are written on the left. In this section then we highlight some definitions and theorems that are quite useful when looking at vector spaces.

Let $K$ be a field and let $V$ be a vector space over $K$. We call a map $f : V \to V$ a linear transformation if $f$ is an $F$-module homomorphism. We denote by $GL(V)$ the set of all bijective linear transformations from $V$ to $V$. We have that $GL(V)$ is a group under composition, called the general linear group.

A subset $S$ of $V$ is called a set of linearly independent vectors if the equation $a_1 v_1 + a_2 v_2 + \cdots + a_k v_k = 0$ where $a_i \in K$ and $v_i \in V \forall 1 \leq i \leq k$ implies that $a_1 = a_2 = \cdots = a_k = 0$. We say that a set $B$ of vectors in $V$ span $V$ if every vector in $V$ can be written as a $K$-linear combination of a finite number of vectors in $B$. A $K$-basis for a vector space $V$ is an ordered set of linearly independent vectors that span $V$. If $V$ has a finite $K$-basis $B$ then the cardinality of $B$ is called the dimension of $V$ over $K$ and is denoted as $\dim_K V$. The dimension of $V$ is finite if the basis $B$ is finite, otherwise we say that the $V$ is infinite dimensional.

We note that if $\dim_K V = n < \infty$ then $V \cong K^n$ and in particular any two finite dimensional vector spaces are isomorphic if they have the same dimension over $K$. A subset $W$ of $V$ is called a subspace of $V$ if it is a $K$-vector space. We also note the following result:

**Proposition 1.4.1.** Let $V$ be a vector space over $K$ and let $W$ be a subspace over $V$. Then $V/W$ is a $K$-vector space and

$$\dim_K V = \dim_K W + \dim_K V/W.$$  

An important area of study in vector space theory is the study of the different “invariants” of a linear transformation, including its eigenvectors, eigenspaces, and invariant subspaces. These are concepts that are definitely used in the study of linear representation. So we will define those here.
Let $K$ be a field, $V$ be a $K$-vector space and $\phi \in \text{Hom}_K(V,V)$. Then a nonzero element $v \in V$ is called an eigenvector of $\phi$ corresponding to the eigenvalue $\lambda$ if and only if $\phi(v) = \lambda v$. We say that a nontrivial subspace $U$ of $V$ is an eigenspace of $\phi$ corresponding to $\lambda$ if $\phi(u) = \lambda u \ \forall u \in U$. Finally we say that a subspace $U$ of $V$ is invariant under $\phi$ if $\phi(u) \in U \ \forall u \in U$. Note that an eigenspace of $\phi$ is invariant under $\phi$.

Now let $K$ be a field, $V, W$ be finite dimensional $K$-vector spaces, $B = \{b_1, \ldots, b_m\}$ be a basis for $V$, $E = \{e_1, \ldots, e_n\}$ be a basis for $W$, and $\phi \in \text{Hom}_K(V,W)$. Then we can define a matrix associated to $\phi$ with respect to $B$ and $E$, denoted by $M^E_B[\phi]$ as follows.

Let $M^E_B[\phi] = (a_{ij})$ where $\phi(b_j) = \sum_{i=1}^{n} a_{ij} e_i \ \forall 1 \leq j \leq m$.

Thus to find the eigenvalues of a linear transformation $\phi \in \text{Hom}_K(V,V)$ we proceed by solving the equation $\det(A - \lambda I) = 0$, where $A$ is the associated matrix of $\phi$ with respect to some basis $B$ of $V$. We can then proceed to find the eigenspace of $\phi$ associated to an eigenvalue $\lambda$ by solving the equation $(A - \lambda I)v = 0$.

We say that two $n \times n$ matrices $A$ and $B$ are similar if there is an invertible $n \times n$ matrix $P$ such that $P^{-1}AP = B$. Two linear transformations $\phi, \psi : V \to V$ are called similar if there exists an invertible linear transformation $\rho : V \to V$ such that $\rho^{-1}\phi \rho = \psi$. We say a matrix $A$ is diagonalizable if it is similar to a diagonal matrix.

An $n \times n$ matrix with $\lambda$ along the diagonal and 1 along the first superdiagonal is called the Jordan block of size $k$ with eigenvalue $\lambda$ and is depicted below:

$$
\begin{pmatrix}
\lambda & 1 \\
\lambda & \ddots \\
\ddots & \ddots & 1 \\
\lambda & 1 & \\
\lambda & & & \\
\end{pmatrix},
$$

where the blank entries are all zero. We say that a matrix is in Jordan canonical form if it is a block diagonal matrix with Jordan blocks along the diagonal, i.e., it is of the following form:

$$
\begin{pmatrix}
J_1 \\
J_2 \\
\ddots \\
J_t
\end{pmatrix}.
An important result in vector space theory states that every $n \times n$ matrix is similar to a matrix in Jordan canonical form.

Finally we define a positive definite, hermitian symmetric form, orthogonal and orthonormal vectors, and inner products.

**Definition 1.4.1.** Let $V$ be a $\mathbb{C}$-vector space. A map $f : V \times V \rightarrow \mathbb{C}$ is said to be a positive definite, hermitian symmetric form on $V$ iff the following conditions hold for all $u, v, w \in V$ and for all $\alpha \in \mathbb{C}$.

1. $f(u, v) \geq 0$ and $f(u, u) = 0$ iff $u = 0$,
2. $f(u, v) = f(v, u)$,
3. $f(\alpha u, v) = \alpha f(u, v)$, and
4. $f(u, v + w) = f(u, v) + f(u, w)$.

A mapping $f$ that satisfies the properties above is also called an inner product on $V$ and we usually denote $f(u, v)$ by just $(u, v)$. A $\mathbb{C}$-vector space $V$ that has an inner product is called an inner product space.

**Definition 1.4.2.** A subset $\{v_1, \ldots, v_k\}$ of the $n$-dimensional inner product space $V$ is called orthogonal iff $(v_i, v_j) = 0$ whenever $i \neq j$. It is called normal iff $(v_i, v_i) = 1$ for all $1 \leq i \leq k$. The set is called orthonormal iff $(v_i, v_j) = \delta_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$ for all $1 \leq i, j \leq k$. 
Chapter 2

General Representation Theory

This chapter is an introduction to the representation theory of finite groups, which is a branch of mathematics that studies algebraic structures by “representing” their elements as linear transformations of vector spaces and modules over these algebraic structures. In this project the structure will be the dihedral group and I will be representing its elements as linear transformations of vector spaces, but working with the invertible matrices will be much easier. These linear transformations will provide information about the groups themselves. Finally, we note that modules are the “representation objects” for rings in the sense that the axioms for an $R$-module specify a “ring action” of $R$ on some abelian group $M$ which preserves the abelian group structure of $M$. So in order to discuss the representations of a group we need some terminology. Hence the definitions and theorems below.

2.1 Linear Representations and KG-modules

In this section we would like to establish an important connection between linear representations of a group $G$ and $KG$-modules, thus we start with the following definitions.

Definition 2.1.1. Let $G$ be a finite group, let $K$ be a field, and let $V$ be a $K$-vector space.

1. A linear representation of $G$ is any group homomorphism from $G$ into $GL(V)$. The degree of the representation is the dimension of $V$. 
2. Let \( n \in \mathbb{Z}^+ \). A matrix representation of \( G \) is any homomorphism from \( G \) into \( GL_n(K) \), where \( GL_n(K) \) denotes the group of invertible matrices.

3. A linear or matrix representation is faithful if it is injective.

Recall that from vector space theory we know that if \( V \) is a finite dimensional vector space of dimension \( n \), then by fixing a basis of \( V \) we can obtain a matrix representation of any linear transformation from \( V \) to \( V \). We actually obtain an isomorphism from \( GL(V) \) to \( GL_n(K) \). Therefore any representation of \( G \) on a finite dimensional vector space gives us a matrix representation and vice versa.

As we stated in Section 1.2, the group ring of \( G \) over \( K \) is the set of all formal sums of the form \( \sum_{g \in G} \alpha_g g \) where \( \alpha_g \in K \) with componentwise addition and multiplication \( (\alpha_g)(\beta h) = (\alpha \beta)(gh) \) (where \( \alpha \) and \( \beta \) are multiplied in \( K \) and \( gh \) is the product in \( G \)) extended to sums via the distributive law.

Example 2.1.1. Let \( G = \langle g \rangle \) be the cyclic group of order \( n \in \mathbb{Z}^+ \) and let \( K \) be a field. Then we obtain the group ring \( K\langle g \rangle = \{ \sum_{i=0}^{n-1} \alpha_i g^i | \alpha_i \in K \} \). If we let \( \psi : K[x] \to K\langle g \rangle \) be the map where \( x^k \mapsto g^k \) where \( k \geq 0 \) and extend \( \psi \) \( K \)-linearly, then \( \psi \) is a ring homomorphism, \( \psi \) is surjective, and \( \ker \psi = \langle x^n - 1 \rangle \). Therefore, by the first Isomorphism theorem for rings we have a special relationship between the group ring \( K\langle g \rangle \) and the infinite dimensional polynomial ring \( K[x] \) which states that \( K\langle g \rangle \cong K[x]/\langle x^n - 1 \rangle \).

Example 2.1.2. Let \( G = D_8 \) and \( K = \mathbb{R} \). An example of addition and multiplication in \( \mathbb{R}D_8 \) where \( \alpha, \beta \in \mathbb{R}D_8, \alpha = r + r^2 - 2s, \) and \( \beta = -3r^2 + rs \) is the following:

\[
\alpha + \beta = (r + r^2 - 2s) + (-3r^2 + rs)
\]

\[
= r + r^2 - 2s - 3r^2 + rs
\]

\[
= r - 2r^2 - 2s + rs,
\]

and

\[
\alpha \beta = (r + r^2 - 2s)(-3r^2 + rs)
\]

\[
= -3r^3 + r^2 s + 3 - r^3 s + 6r^2 s - 2r^3
\]

\[
= -3 - 5r^3 + 7r^2 s + r^3 s,
\]
Moreover, \( \mathbb{R} \) is in the center of \( \mathbb{R}D_8 \), i.e., \( \mathbb{R} \subseteq Z(\mathbb{R}D_8) \) and since \( 1 < |D_8| < \infty \) then \( \mathbb{R}D_8 \) is not an integral domain by our discussion in Section 1.2 (see discussion after Definition 1.2.7).

We note the following results concerning group rings.

**Proposition 2.1.1.** \( KG \) is a commutative ring if and only if \( G \) is abelian.

**Proposition 2.1.2.** \( KG \) is a vector space over \( K \) with the elements of \( G \) as a basis.

**Proposition 2.1.3.** Since \( K \) is in the center of \( KG \) then \( KG \) is a \( K \)-algebra.

The most important result that allows us view representations of a group \( G \) over a field \( K \) as a \( KG \)-modules is the following. We let \((V, \phi)\) denote the representation \( \phi : G \to GL(V) \).

**Theorem 2.1.1.** There is a bijection between \( KG \)-modules and pairs \((V,\phi)\):

\[
\begin{array}{c}
\{ V \text{ is a } KG\text{-module} \} \leftrightarrow \{ V \text{ is a } K\text{-vector space} \text{ and} \\
\phi : G \to GL(V) \}
\end{array}
\]

**Proof.** Assume that \( \phi : G \to GL(V) \) is a representation of \( V \) over \( K \). Let \( G = \{g_1, g_2, \ldots, g_n\} \). We make \( V \) into a \( KG \)-module by defining the following action of \( G \) on \( V \) and extending linearly: \( g.v = \phi(g)(v) \forall g \in G \). Thus the action of an element in \( KG \) on \( V \) is given by

\[
(\sum_{i=1}^{n} a_i g_i).v = \sum_{i=1}^{n} a_i \phi(g_i)(v) \quad \forall \sum_{i=1}^{n} a_i g_i \in KG, v \in V.
\]

Checking that the \( V \) is a \( KG \)-module requires some work but we will check a special case of 2(b) given in the axioms of modules in Section 1.2. Let \( g_i, g_j \in G \). Then note that

\[
(g_i g_j).v = \phi(g_i g_j)(v) \quad \text{by definition of the action}
\]

\[
= (\phi(g_i) \circ \phi(g_j))(v) \quad \text{since } \phi \text{ is a group homomorphism}
\]

\[
= \phi(g_i)(\phi(g_j)(v))
\]

\[
= g_i.(g_j.v) \quad \text{by definition of the action}.
\]

We can extend this argument by linearity and show that any element of \( KG \) satisfies axiom 2(b). Similarly we can show that the other axioms hold.
Conversely, suppose now that we have a $KG$-module $V$. Since $K$ is a subring of $KG$ we can restrict the action of $KG$ to $K$ and see that we get that $V$ is a $K$-module, i.e. a $K$-vector space. We define the following map $\phi : G \to GL(V)$ sending $g \mapsto \phi_g$ where we define $\phi_g : V \to V$ as follows: for all $v \in V$, let $\phi_g(v) = g.v$. We claim that $\phi_g$ is an invertible linear transformation and the $\phi$ is a group homomorphism.

Let $\alpha \in K$ and let $u,v \in V$. Then $\phi_g(\alpha u + v) = g.(\alpha u + v) = \alpha g.u + g.v = \alpha \phi_g(u) + \phi(v)$. We also see that $(\phi_{g^{-1}} \circ \phi_g)(v) = \phi_{g^{-1}}(\phi_g(v)) = \phi_{g^{-1}}(g.v) = g^{-1}.(g.v) = (g^{-1}g).v = v$ for all $v \in V$. Thus $\phi_{g^{-1}} \circ \phi_g$ is the identity transformation. Similarly $\phi_g \circ \phi_{g^{-1}}$ is also the identity transformation. Finally we show that $\phi$ is a group homomorphism. Note that for any $v \in V$ and that for any $g,h \in G$ we get that $(\phi_g \circ \phi_h)(v) = g.(h.v) = (gh).v = \phi_{gh}(v)$. Thus we see that $\phi(g) \circ \phi(h) = \phi(gh)$. \hfill $\Box$

Thus, giving a representation $\phi : G \to GL(V)$ on a vector space $V$ over $K$ is equivalent to giving a $KG$-module. Under this correspondence we shall say that the $KG$-module $V$ affords the representation $\phi$ of $G$.

We now extend the notion of invariant spaces of a transformation.

**Definition 2.1.2 (G-Stable).** If $V$ is a $KG$-module affording a representation $\phi$, then the subspace $U$ of $V$ is called $G$-invariant or $G$-stable if $\phi_g(u) \in U$ for all $g \in G$, for all $u \in U$ (i.e., $g \cdot u \in U$ for all $g \in G$, for all $u \in U$). In fact the $KG$-submodules of $V$ are precisely the $G$-stable subspaces of $V$.

The following result is used often in our project.

**Proposition 2.1.4.** If $h : G \to H$ is any group homomorphism and $\phi : H \to GL(V)$ is a representation of $H$ with representation space $V$, then the composition $\phi \circ h : G \to GL(V)$ is a representation of $G$.

**Proof.** First of all since $h$ and $\phi$ are both group homomorphisms then their composition is also a group homomorphism. Thus by definition $\phi \circ h$ is a linear representation of $G$. \hfill $\Box$

We end this section by recalling a definition from Section 1.3 and giving other relevant definitions and a proposition that we will find useful.

**Definition 2.1.3.** Let $R$ be a ring and let $M$ be a nonzero $R$-module.
1. The module $M$ is said to be irreducible (or simple) if its only submodules are 0 and $M$; otherwise $M$ is called reducible.

2. The module $M$ is said to be indecomposable if $M$ cannot be written as $M_1 \oplus M_2$ where $M_1$ and $M_2$ are modules (or submodules of $M$).

3. The module $M$ is said to be completely reducible if its direct sum of irreducible submodules.

4. A representation is called irreducible, reducible, indecomposable, decomposable or completely reducible according to whether the KG-module affording it has the corresponding property.

5. If $M$ is a completely reducible $R$-module, any direct summand of $M$ is called a constituent of $M$ (i.e., $N$ is a constituent of $M$ if there is a submodule $N'$ of $M$ such that $M = N \oplus N'$.

**Proposition 2.1.5.**

All degree one representations are irreducible (or simple), indecomposable, and completely reducible.

### 2.2 Examples of KG-modules

Since there is a one-to-one correspondence between $KG$-modules and linear representations of $G$, in this section we give examples of $KG$-modules and the representation that is afforded by each of them.

**Example 2.2.1 (Trivial Module).** Let $V$ be a one-dimensional $K$-vector space (i.e. $V$ is a $K$-module). We make $V$ into a $KG$-module by defining the following the ring action: $g \cdot v = gv = v \forall v \in V$. So this module affords a linear representation $T: G \rightarrow GL(V)$ where $g \mapsto T(g) = T_g = I_V \forall g \in G$. The corresponding matrix representation of $G$ is the following $T: G \rightarrow GL_1(K) = K^X = K \setminus \{0\} = \{a|a \in K\}$, the multiplicative group where $\dim_K V = \deg T = 1$. $T$ is not faithful since the $\ker T = G$. Furthermore, since the trivial representation is 1-dimensional then it is irreducible (or simple), indecomposable, and completely reducible.
Example 2.2.2. Let $V$ be any $n$-dimensional $K$-vector space for $n \in \mathbb{Z}^+$ with basis \{e_1, \cdots, e_n\}. Again $V$ is $K$-module but we can make $V$ into a $KS_n$-module by defining a ring action $\sigma_i \cdot e_j = e_{\sigma_i(j)} \forall \sigma_i \in S_n$ and $\forall i, j \in \{1, \cdots, n\}$ and extending linearly. Thus, $V$ affords a linear representation $\psi : S_n \rightarrow GL(V)$ where $\sigma_i \mapsto \psi_\sigma_i$ and $\psi_\sigma_i : V \rightarrow V$ which is defined as $\psi_\sigma_i(e_j) = e_{\sigma_i(j)} \forall \sigma_i \in S_n$ and $\forall i, j \in \{1, \cdots, n\}$. Finally since $\ker \psi = 1_{S_n}$ then $\psi$ is faithful.

Note that $V$ is reducible since it contains the following two proper, nonzero submodules:

\[
N = \{\alpha_1 e_1 + \cdots + \alpha_n e_n | \alpha_1 = \cdots = \alpha_n \} = \{\alpha_1(e_1 + \cdots + e_n)\} = \text{span}_K\{(e_1 + \cdots + e_n)\},
\]

and

\[
I = \{\alpha_1 e_1 + \cdots + \alpha_n e_n | \alpha_1 + \cdots + \alpha_n = 0 \}.
\]

Moreover since $N$ is 1-dimensional, then it is irreducible, indecomposable, and completely reducible. However, if the characteristic of the field $K$ does not divide $n$, then $I$ is also irreducible. Since $N$ and $I$ are $KS_n$ submodules of $V$ then they are $S_n$ - stable.

Example 2.2.3 (Regular Representation). Let $G$ be a group of order $|G| = n$ and let $V$ be the vector space $KG = \text{span}_K\{g_1 \cdots g_n\}$. Note $V$ is a $KG$-module by defining the following ring action and extending $K$-linearly: $g \cdot g_i = gg_i \forall g, g_i \in G$. Thus $V$ affords a representation of $G$ given by $\mathcal{R} : G \rightarrow GL(KG)$ where $g \mapsto \mathcal{R}_g$ and $\mathcal{R}_g(g_i) = g \cdot g_i = gg_i \forall g, g_i \in G$. Note that $\dim_K(KG) = |G|$ and $\mathcal{R}$ is faithful since $\ker \mathcal{R} = 1_G$. If we define

\[
N = \{\alpha_1 g_1 + \cdots + \alpha_n g_n | \alpha_1 = \cdots = \alpha_n \} = \{\alpha_1(g_1 + \cdots + g_n)\} = \text{span}_K\{(g_1 + \cdots + g_n)\},
\]

and

\[
I = \{\alpha_1 g_1 + \cdots + \alpha_n g_n | \alpha_1 + \cdots + \alpha_n = 0 \}
\]
then $N$ is 1-dimensional which implies $N$ is irreducible, indecomposable, and completely reducible. Note: If we define the linear functional $\phi_i : V \rightarrow K$ by $\sum_{i=1}^n a_i g_i \mapsto \sum_{i=1}^n a_i$, $a_i \in K$ then $\ker \phi_i = I$. From linear algebra we know $V = \ker \phi_i \oplus \ker \phi_i$. Since the $\dim(\ker \phi) = 1$ and $\dim(KG) = |G|$ we see that $\dim (\ker \phi_i)$ is forced to be $n - 1$. Since $N$ and $I$ are $KG$ submodules of $KG$ then they are $G-stable$. In fact $N$ and $I$ happen to be 2-sided ideals of $KG$. Finally, the regular representation is reducible when $|G| > 1$. However later we will determine the conditions under which the regular representation is completely reducible and how we can decompose it into a direct sum of submodules, i.e. $KG = U_1 \oplus \cdots U_n$ where $U_1 \oplus \cdots U_n$ where $U_i$, $1 \leq i \leq n$ are irreducible.

In many situations we will see that it is easier to specify an explicit "matrix representation" of a group $G$ rather than to exhibit a $KG$-module. Therefore below are examples of matrix representations of a group $G$.

**Example 2.2.4.** Let $G = \langle g \rangle \cong \mathbb{Z}_n$, where $|G| = n$ and let $\zeta = e^{\frac{2\pi k}{n}} = \cos \left(\frac{2\pi k}{n}\right) + sin \left(\frac{2\pi k}{n}\right)$. Then $h : G \rightarrow K^x = GL_1(K)$ where $g^i \mapsto \zeta^i$ is a matrix representation of degree 1. Here $h$ is faithful $\iff \zeta$ is a primitive $n$th root of 1. Moreover, since $\deg(h)=1$ then it is irreducible(or simple), indecomposable, and completely reducible. In fact any homomorphism of $G$ into the multiplicative group $K^x$ is irreducible(or simple), indecomposable, and completely reducible.

**Example 2.2.5.** A matrix representation of the dihedral group with presentation $D_{2n} = \langle r, s | r^n = s^2 = 1, rs = sr^{-1} \rangle$ is given by $\phi : D_{2n} \rightarrow GL_2(\mathbb{R})$ where $r \mapsto R = \begin{pmatrix} \cos \frac{2\pi}{n} & -\sin \frac{2\pi}{n} \\ \sin \frac{2\pi}{n} & \cos \frac{2\pi}{n} \end{pmatrix}$ and $s \mapsto S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. More specifically, $R$ is the matrix of linear transformations which rotates the $xy$-plane about the origin in counter clockwise by $\frac{2\pi}{n}$ radians and $S$ reflects the plane about the $y = x$. These matrices act as symmetries of an $n$-gon and satisfy the relations of $D_{2n}$. Thus this representation is faithful. This representation is irreducible for $n \geq 3$ because there are no $D_{2n}$-stable 1-dimensional subspaces since a rotation by $2\pi/n$ sends no line in $\mathbb{R}^2$ to itself. In other words, we cannot find a subspace $U$ of $\mathbb{R}^2$ such that $\phi_r(u) \in U$ and $\phi_s(u) \in U$ for all $u \in U$.

Note: A linear representation would be $\phi : D_{2n} \rightarrow GL(\mathbb{R}^2)$ where $r \mapsto \phi_r$ and $s \mapsto \phi_s$, where $\phi_r : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ by $\phi_r(x, y) = \left(x \cos \frac{2\pi}{n} - y \sin \frac{2\pi}{n}, x \sin \frac{2\pi}{n} + y \cos \frac{2\pi}{n}\right)$ and $\phi_s : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ by $\phi_s(x, y) = (-y, x)$.
Example 2.2.6. The matrix representation of the Quaternion group with presentation $Q_8 = \langle i, j | i^4 = j^4 = 1, i^2 = j^2, i^{-1}ji = j^{-1} \rangle$ is given by $\phi : Q_8 \to GL_2(\mathbb{C})$ where $i \mapsto I = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}$ and $j \mapsto J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

This representation is faithful since $I$ and $J$ satisfy the same relations of $Q_8$. Hence, $Q_8 \cong \langle I, J \rangle \leq GL_2(\mathbb{C})$.

We know that $\phi$ is irreducible if and only if the only $Q_8$-stable subspaces of $V = \mathbb{C}^2$ are 0 and $\mathbb{C}^2$. Moreover, we know the invariant subspaces of $V$ under $\phi_i$ are the eigenspaces $\epsilon_{\sqrt{-1}} = \text{span}_\mathbb{C} \{ \begin{pmatrix} 1 \\ 0 \end{pmatrix} \}$ and $\epsilon_{-\sqrt{-1}} = \text{span}_\mathbb{C} \{ \begin{pmatrix} 0 \\ 1 \end{pmatrix} \}$, with corresponding eigenvalues $\sqrt{-1}$ and $-\sqrt{-1}$, respectively. But, neither of these spaces are invariant under $\phi_j$. Therefore, $\phi$ is irreducible.

Example 2.2.7. Let $\mathbb{H}$ be the real Hamilton quaternions ring, i.e. $\mathbb{H} = \text{span}_\mathbb{R} \{1, i, j, k\}$. We know that $\mathbb{H}$ is an $\mathbb{R}$-vector which implies $\mathbb{H}$ is an $\mathbb{R}$-module. But we want to make $\mathbb{H}$ into a $\mathbb{R}Q_8$-module. So we define the ring action by left multiplication $i \cdot x = ix$ and $j \cdot x = jx \ \forall x \in \mathbb{H}$. Thus, this module affords a linear representation $\mathcal{R} : Q_8 \to GL(\mathbb{H})$ by $i \mapsto \mathcal{R}_i$ and $j \mapsto \mathcal{R}_j$ where $\mathcal{R}_i : \mathbb{H} \to \mathbb{H}$ where $x \mapsto i \cdot x$ and $\mathcal{R}_j : \mathbb{H} \to \mathbb{H}, x \mapsto j \cdot x$ $\forall x \in \mathbb{H}$.

Note that we have the left regular representation of $Q_8$, i.e, $\mathcal{R} : Q_8 \to GL(\mathbb{R}Q_8) = GL(\mathbb{H})$. Now we can easily write out the explicit matrices of each of the elements of $Q_8$ with respect to the basis $\{1, i, j, k\}$.

$\mathcal{R}_i(1) = i \cdot 1 = i = 0 \cdot 1 + 1 \cdot i + 0 \cdot j + 0 \cdot k = i$

$\mathcal{R}_i(i) = i \cdot i = i^2 = -1 = -1 \cdot 1 + 0 \cdot i + 0 \cdot j + 0 \cdot k = k$

$\mathcal{R}_i(j) = i \cdot j = ij = k = 0 \cdot 1 + 0 \cdot i + 0 \cdot j + 1 \cdot k = i$

$\mathcal{R}_i(k) = i \cdot k = ik = -j = 0 \cdot 1 + 0 \cdot i - 1 \cdot j + 0 \cdot k = -j$

For each linear transformation there is an associated matrix representation, $\mathcal{M}_i$ given by $\mathcal{M}_i = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$. Similarly we can obtain $\mathcal{M}_j = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & -1 \\ 0 & -1 & 1 & 0 \end{pmatrix}$. 


This linear action gives a homomorphism of $Q_8$ into $GL_4(\mathbb{R})$. Therefore, the matrix representation of the Quaternion group is

$$R : Q_8 \to GL_4(\mathbb{R})$$

where

$$i \mapsto \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & -1 & 0 & 0 \end{pmatrix} \quad \text{and} \quad j \mapsto \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & -1 \\ 0 & -1 & 1 & 0 \end{pmatrix}.$$

This representation is irreducible, however, if we extend the field to the complex numbers then it becomes reducible since there exists a complex matrix $P$ such that $P^{-1}\phi(g)P$ is a direct sum of $2\times2$ block matrices for all $g \in Q_8$. Therefore an irreducible representation over a field $K$ may become reducible when the field is extended. In fact "reducible" representations are those with a corresponding matrix representation whose matrices are in block triangular form, whereas decomposable representations are in block diagonal form.

**Definition 2.2.1** (Equivalent Linear Representations). Two representations of $G$ are equivalent (or similar) if the KG-modules affording them are isomorphic modules. Representations which are not equivalent are called inequivalent.

**Definition 2.2.2** (Equivalent Matrix Representations). Two representations $\phi$ and $\psi$ are equivalent if there is a fixed invertible matrix $P$ such that $P\phi(g)P^{-1} = \psi(g)$ for all $g \in G$.

Finally we present a result that will have important consequences, as we will see in the next section.

**Theorem 2.2.1** (Maschke). Let $G$ be a finite group and let $K$ be a field whose characteristic does not divide $|G|$. If $V$ is any KG-module and $U$ is any submodule of $V$, then $V$ has a submodule $W$ such that $V = U \oplus W$ (i.e., every submodule is a direct summand.)

**Corollary 2.2.2.** If $G$ is a finite group and $K$ is a field whose characteristic does not divide $|G|$, then every finite generated KG-module is completely reducible(equivalently, every K-representation of $G$ of finite degree is completely reducible)

**Corollary 2.2.3.** Let $G$ be a finite group, let $K$ be a field whose characteristic does not divide $|G|$ and let $\phi : G \to GL(V)$ be a representation of $G$ of finite degree. Then there
is a basis of $V$ such that for each $g \in G$ the matrix $\phi(g)$ with respect to this basis is block diagonal:

$$
\begin{pmatrix}
\phi_1(g) \\
\phi_2(g) \\
\vdots \\
\phi_m(g)
\end{pmatrix}
$$

where $\phi_i$ is an irreducible matrix representation of $G$, $1 \leq i \leq m$.

### 2.3 Irreducible Representations of $D_8$

In the last section we discussed a very important correspondence between $KG$-modules and pairs $(V, \phi)$, where $V$ is a vector space over $K$ and $\phi$ is a representation of $G$. That is, there is a bijection between $KG$-modules and representations of $G$ or we say a $KG$ module affords a representation. In this section we will let $K = \mathbb{C}$, unless otherwise stated, and we will compute the irreducible representations of $D_8$. Along the way we will discuss characters of a representation and note that a representation of $G$ affords a character. We will then see that there is a correspondence between these characters and equivalence classes of complex representations. We learn that the complex representations of finite groups (specifically $D_8$) are characterized by their characters. Finally, we discuss other useful properties of characters.

One of the most important theorems in section that I will use in my project will be the following:

**Theorem 2.3.1.** Let $G$ be a finite group. Then:

1. $\mathbb{C}G \cong M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_r}(\mathbb{C})$ as $\mathbb{C}$-modules.

2. $\mathbb{C}G$ has exactly $r$ distinct isomorphism types of irreducible modules and these have complex dimensions $n_1, n_2, \ldots, n_r$ (and so $G$ has exactly $r$ inequivalent irreducible complex representation of the corresponding degrees).

3. $\sum_{i=1}^{r} n_i^2 = |G|

4. $r$ equals the number of conjugacy classes in $G$.

We will use this theorem now to find the complex irreducible representations of $D_8$. Recall a presentation of $D_8$ is $\langle r, s | r^4 = s^2 = 1, rs = sr^{-1} \rangle$, i.e. $D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$,
and a matrix representation of $D_8$ is given by $\phi : D_8 \to GL_2(\mathbb{R})$ where

\[
r \mapsto R = \begin{pmatrix}
\cos(\pi/2) & -\sin(\pi/2) \\
\sin(\pi/2) & \cos(\pi/2)
\end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}
\quad \text{and} \quad
s \mapsto S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.
\]

More specifically, $R$ is the matrix of a linear transformation which rotates the $xy$-plane about the origin in a counter-clockwise direction by $\pi/2$ radians and $S$ is the matrix of a linear transformation that reflects the plane about the line $y = x$. These matrices act as symmetries of a square and satisfy the relations of $D_8$. We can also consider $D_8$ as the group of permutations of a regular 4-gon or even just of its 4 vertices since the dihedral group is a subgroup of the symmetric group. This representation is faithful. Furthermore, this representation is irreducible because there are no $D_8$-stable 1-dimensional subspaces since a rotation by $\pi/2$ sends no line in $\mathbb{R}^2$ to itself. In other words, $\not\exists U \subset \mathbb{R}^2$ such that $\phi_r(u) \in U$ and $\phi_s(u) \in U$ for all $u \in U$. Later we will also show that this representation is irreducible by looking at its character.

Now using the fact that $\phi$ is a homomorphism, the matrices $\phi(g)$ for all $g \in D_8$ are the following:

- $\phi(r) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ is given above.

- $\phi(r^2) = \phi(r)\phi(r) = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$

- $\phi(r^3) = \phi(r^2)\phi(r) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

- $\phi(1) = \phi(r^4) = \phi(r^2)\phi(r^2) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

- $\phi(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is also given above.

- $\phi(sr) = \phi(s)\phi(r) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

- $\phi(sr^2) = \phi(s)\phi(r^2) = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$
\[ \phi(sr^3) = \phi(s)\phi(r^3) = \phi(s)\phi(r^2)\phi(r) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \]

Note that \( D_8 \cong \langle R, S \rangle \leq GL_2(\mathbb{R}) \) and that \( \phi \) is a degree 2 representation of \( D_8 \). But \( D_8 \) has five conjugacy classes so by Theorem 1 there should be four more representations we can find. Specifically we want to find the "irreducible complex" representations of \( D_8 \). To help us find them we define some new terminology and recall a proposition from Section 2.1.

**Definition 2.3.1.** Let \( G \) be a group and let \( x, y \in G \). Then

1. \([x, y] = x^{-1}y^{-1}xy\) is the called the **commutator** of \( x \) and \( y \).

2. \( G' = \langle [x, y] | x, y \in G \rangle \) is the **subgroup of \( G \)** generated by commutators of elements of \( G \). That is, the **commutator subgroup** of \( G \).

Recall Proposition 2.1.4, if \( \rho : G \to H \) is any group homomorphism and \( \phi \) is a representation of \( H \) then the composition \( \rho \circ \phi : G \to GL(V) \) is a representation of \( G \). This result in addition to the following corollaries of Theorem 2.3.1 will help us find all the degree 1 representations of \( D_8 \).

**Corollary 2.3.2.** Let \( A \) be a finite abelian group. Every irreducible complex representation of \( A \) is 1-dimensional (i.e. is a homomorphism from \( A \to \mathbb{C}^X \)) and \( A \) has \( |A| \) inequivalent irreducible complex representations. Furthermore, every finite dimensional complex matrix representation of \( A \) is equivalent to a representation into a group of diagonal matrices.

**Corollary 2.3.3.**

The number of inequivalent (irreducible) degree 1 complex representations of any finite group \( G \) equals \( |G/G'| \) where \( G' \) is the commutator.

**Proposition 2.3.1.** Let \( G \) be a group, \( x, y \in G \), let \( H \trianglelefteq G \). Then \( G/G' \) is the largest abelian quotient of \( G \) in the sense that if \( H \triangleleft G \) and \( G/H \) is abelian, then \( G' \trianglelefteq H \).

Hence these results give us the following plan of attack. We will find the commutator subgroup \( H \) of \( D_8 \). Then we will find the degree one representations \( \phi : D_8/H \to \)
\(GL(\mathbb{C})\) guaranteed by the proposition and corollary above. Then since we have the natural homomorphism denoted by

\[
\pi : D_8 \rightarrow D_8/H
\]

we can compose \(\phi\) with \(\pi\) to obtain the representation \(\phi \circ \pi : D_8 \rightarrow GL(\mathbb{C})\).

We claim that \(H = \{1,r^2\}\) is the commutator subgroup of \(D_8\). We know that \(H\) is a normal subgroup of \(D_8\) so we can construct the quotient group \(D_8/H = \{H,rH,sH, srH\}\). We note that \(Z(D_8/H) = D_8/H\). Therefore \(D_8/H\) is abelian and has order 4. Note that the only quotient group of \(D_8\) that has larger order is \(D_8/\{0\} \cong D_8\) which is not abelian. Thus by Proposition 2.3.1, \(H\) must be the commutator of \(D_8\). Since \(D_8/H\) is a finite abelian group then by Corollary 2.3.2 every irreducible complex representation of \(D_8/H\) is 1-dimensional, i.e, \(\phi : D_8/H \rightarrow GL(\mathbb{C})\). Moreover \(D_8/H\) has \(|D_8/H| = 4\) inequivalent irreducible complex representations. These are the following, where we only define the representations on the generators of \(D_8\):

\[
\overline{\phi}_1 : D_8/H \rightarrow GL_1(\mathbb{C}), \text{ where } rH \mapsto 1 \text{ and } sH \mapsto 1
\]

\[
\overline{\phi}_2 : D_8/H \rightarrow GL_1(\mathbb{C}), \text{ where } rH \mapsto 1 \text{ and } sH \mapsto -1
\]

\[
\overline{\phi}_3 : D_8/H \rightarrow GL_1(\mathbb{C}), \text{ where } rH \mapsto -1 \text{ and } sH \mapsto 1
\]

\[
\overline{\phi}_4 : D_8/H \rightarrow GL_1(\mathbb{C}), \text{ where } rH \mapsto -1 \text{ and } sH \mapsto -1
\]

It can be shown that these mappings are group homomorphisms that are not faithful. But we want representations of \(D_8\), not \(D_8/H\). So we will use Proposition 2.1.4 to find the representations of \(D_8\). Let us denote \(\overline{\phi}_i = \phi_i \circ \pi\) where \(1 \leq i \leq 4\) and we have

- \(\phi_1 = \phi_1 \circ \pi : D_8 \rightarrow GL_1(\mathbb{C})\) and \(\overline{\phi}_1(r) = (\phi_1 \circ \pi)(r) = \phi_1(\pi(r)) = \phi_1(rH_1) = 1\) and \(\overline{\phi}_1(s) = (\phi_1 \circ \pi)(s) = \phi_1(\pi(s)) = \phi_1(sH_1) = 1\). Therefore the representation is \(\overline{\phi}_1 : D_8 \rightarrow GL_1(\mathbb{C})\) where \(r \mapsto 1\) and \(s \mapsto 1\)

- \(\phi_2 = \phi_2 \circ \pi : D_8 \rightarrow GL_1(\mathbb{C})\) and \(\overline{\phi}_2(r) = (\phi_2 \circ \pi)(r) = \phi_2(\pi(r)) = \phi_2(rH_1) = 1\) and \(\overline{\phi}_2(s) = (\phi_2 \circ \pi)(s) = \phi_2(\pi(s)) = \phi_2(sH_1) = -1\). Therefore the representation is \(\overline{\phi}_2 : D_8 \rightarrow GL_1(\mathbb{C})\) where \(r \mapsto 1\) and \(s \mapsto -1\)

- \(\phi_3 = \phi_3 \circ \pi : D_8 \rightarrow GL_1(\mathbb{C})\) and \(\overline{\phi}_3(r) = (\phi_3 \circ \pi)(r) = \phi_3(\pi(r)) = \phi_3(rH_1) = -1\) and \(\overline{\phi}_3(s) = (\phi_3 \circ \pi)(s) = \phi_3(\pi(s)) = \phi_3(sH_1) = 1\). Therefore the representation is \(\overline{\phi}_3 : D_8 \rightarrow GL_1(\mathbb{C})\) where \(r \mapsto -1\) and \(s \mapsto 1\)
• $\phi_4 = \phi_4 \circ \pi : D_8 \to GL_1(\mathbb{C})$ and $\tilde{\phi}_4(r) = (\phi_4 \circ \pi)(r) = \phi_4(\pi(r)) = \phi_4(rH_1) = -1$

and $\tilde{\phi}_4(s) = (\phi_4 \circ \pi)(s) = \phi_4(\pi(s)) = \phi_4(sH_1) = -1$. Therefore the representation is $\tilde{\phi}_4 : D_8 \to GL_1(\mathbb{C})$ where $r \mapsto -1$ and $s \mapsto -1$.

From the problem above which we described before, we already know the fifth representation of $D_8$ which is $\phi_5 : D_8 \to GL_2(\mathbb{C})$, where $r \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $s \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

Again, since $D_8$ has five conjugacy classes, then by Theorem 2.3.1 we know $\mathbb{C}D_8$ has exactly five distinct isomorphism types of irreducible modules which have complex dimensions 1, 1, 1, 1, and 2. Equivalently we can say $D_8$ has exactly five inequivalent irreducible complex representations of the corresponding degrees. But most importantly each representation afforded by the $\mathbb{C}D_8$-module affords a character, which we will define now.

**Definition 2.3.2 (Character of a Representation).** If $\phi$ is a representation of $G$ afforded by the KG-module $V$, the character of $\phi$ is the function $\chi : G \to K$ defined by $\chi(g) = \text{tr}(\phi(g))$, where the $\text{tr}(\phi(g))$ is the trace of the matrix $\phi(g)$ with respect to some basis of $V$ (i.e., the sum of the diagonal entries of that matrix). The character is called irreducible or reducible according to whether the representation is irreducible or reducible, respectively. The degree of a character is the degree of the representation affording it.

**Definition 2.3.3 (Principal Character).** The character of the trivial representation is the function $\chi(g) = 1$ for all $g \in G$.

Recall the conjugacy class of of $g \in G$ is $[g] = \{xgx^{-1} | x \in G\}$. We know that $D_8$ has the following five conjugacy classes: $[1]$, $[r]$, $[s]$, $[r^2]$, and $[sr]$. We show below that the character of a representation of $G$ is a class function, i.e., a function from $G$ into $K$ which is constant on the conjugacy classes of $G$.

**Lemma 2.3.1.** Let $\phi$ be a representation of $G$ of degree $n$ with character $\chi$. Then $\chi$ is a class function.

**Proof.** Since $\phi(g^{-1}xg) = (\phi(g))^{-1}\phi(x)\phi(g)$ for all $g, x \in G$, we see that by taking the trace
of both sides we get the following:

\[
\begin{align*}
tr[\phi(g^{-1}xg)] &= tr[\phi(g^{-1})\phi(x)\phi(g)] \\
&= tr(\phi(x)) \\
\Rightarrow \chi(g^{-1}xg) &= \chi(g)
\end{align*}
\]

The character table of \(D_8\) is the \(5 \times 5\) table of character values where the conjugacy classes, \(1, s, r, r^2, sr\) are located along the top row and the list of irreducible characters down the first column. The entry in the table in row \(\chi_i\) and column \(g_j\) is \(\chi_i(g_j)\). Moreover, by convention we make the principal character the first row, the identity the first column, and we list the characters in increasing order by degrees. Finally, the character table of a finite group is unique up to a permutation of its rows and columns. Note that we have already found where each \(\phi_i, (i = 1...5)\) sends the generators \(r\) and \(s\), thus it is easy to compute \(\chi_i(r)\) and \(\chi_i(s)\) for all \(1 \leq i \leq 5\). Thus we can place each of these values in columns three and four of the character table, but we still need to fill in the entries for columns one, two, and five. Thus, we need to find the value of the characters \(\chi_i\) for all \(1 \leq i \leq 5\) evaluated at \(1, r^2,\) and \(sr\). So we use the fact that \(\phi_i(g)\) is a group homomorphism to help us fill in the last 15 entries.

To fill column one, we compute the following:

\[
\begin{align*}
\chi_1(1) &= tr(\phi_1(1)) = 1 \\
\chi_2(1) &= tr(\phi_2(1)) = 1 \\
\chi_3(1) &= tr(\phi_3(1)) = 1 \\
\chi_4(1) &= tr(\phi_4(1)) = 1 \\
\chi_5(1) &= tr(\phi_5(1)) = 2.
\end{align*}
\]

We call this first column the identity column. Since the first four representations are of degree 1 then by definition they are irreducible representations (or simple modules).
To fill in the second column, we compute the following:

\[
\chi_1(r^2) = tr(\phi_1(r^2)) = tr[\phi_1(r)\phi_1(r)] = tr[1 \cdot 1] = tr[1] = 1
\]

\[
\chi_2(r^2) = tr(\phi_2(r^2)) = tr[\phi_2(r)\phi_2(r)] = tr[1 \cdot 1] = tr[1] = 1
\]

\[
\chi_3(r^2) = tr(\phi_3(r^2)) = tr[\phi_3(r)\phi_3(r)] = tr[-1 \cdot -1] = tr[1] = 1
\]

\[
\chi_4(r^2) = tr(\phi_4(r^2)) = tr[\phi_4(r)\phi_4(r)] = tr[-1 \cdot -1] = tr[1] = 1
\]

\[
\chi_5(r^2) = tr[\phi_5(r^2)] = tr\left[\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\right] = tr\left[\begin{pmatrix} -1 & -0 \\ 0 & -1 \end{pmatrix}\right] = -2
\]

Finally we use the following computations to fill in the fifth column and our work from before to fill in the columns for conjugacy classes \([r]\) and \([s]\).

\[
\chi_1(sr) = tr(\phi_1(sr)) = tr[\phi_1(s)\phi_1(r)] = tr[1 \cdot 1] = tr[1] = 1
\]

\[
\chi_2(sr) = tr(\phi_2(sr)) = tr[\phi_2(s)\phi_2(r)] = tr[-1 \cdot 1] = tr[-1] = -1
\]

\[
\chi_3(sr) = tr(\phi_3(sr)) = tr[\phi_3(s)\phi_3(r)] = tr[1 \cdot -1] = tr[-1] = -1
\]

\[
\chi_4(sr) = tr(\phi_4(sr)) = tr[\phi_4(s)\phi_4(r)] = tr[-1 \cdot -1] = tr[1] = 1
\]

\[
\chi_5(sr) = tr(\phi_5(sr)) = tr\left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\right] = tr\left[\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\right] = 0
Let us keep exploring the structure of the $\mathbb{C}D_8$ group ring ($\mathbb{C}—$algebra). We recall the following definition from Section 1.2 and we state Wedderburn’s theorem, another result that has far reaching consequences for our group ring.

**Definition 2.3.4.** Let $R$ be a nonzero ring.

1. A nonzero element $e$ in a ring $R$ is called idempotent if $e^2 = e$.

2. Idempotents $e_1$ and $e_2$ are said to be orthogonal if $e_1 e_2 = e_2 e_1 = 0$.

3. An idempotent element $e$ is said to be primitive if it cannot be written as a sum of two (commuting) orthogonal idempotents.

4. The idempotent $e$ is called a primitive central idempotent if $e \in Z(R)$ and $e$ cannot be written as a sum of two orthogonal idempotents in the ring $Z(R)$.

**Theorem 2.3.4** (Wedderburn’s). Let $R$ be a nonzero ring with 1 (not necessarily commutative). Then the following are equivalent:

1. every $R$-module is projective

2. every $R$-module is injective

3. every $R$-module is completely reducible

4. the ring $R$ considered as a left $R$-module is a direct sum: $R \cong L_1 \oplus L_2 \oplus \cdots L_n$, where each $L_i$ is a simple module (i.e., a simple left ideal) with $L_i = Re_i$, for some $e_i \in R$ with

   (i) $e_i e_j = 0$ if $i \neq j$

   (ii) $e_i^2 = e_i$ for all $i$

   (iii) $\sum_{i=1}^{n} e_i = 1$
5. as rings, $R$ is isomorphic to a direct product of matrix rings over division rings, 
i.e., $R \cong R_1 \times R_2 \times \cdots \times R_r$ where $R_j$ is a two-sided ideal of $R$ and $R_j$ is isomorphic
to the ring of all $n_j \times n_j$ matrices with entries in a division ring $\Delta_j$, $j = 1, 2, \cdots, r$.
The integer $r$, the integers $n_j$, and the division ring $\Delta_j$ (up to isomorphism) are
uniquely determined by $R$.

Now since we are working over the field $\mathbb{C}$, which is an algebraically closed field,
it turns out that each of the division rings in Wedderburn’s theorem is actually isomorphic
to $\mathbb{C}$. Thus in part (5) of Wedderburn’s theorem we get that

$$R \cong M_{n_1}(\mathbb{C}) \times M_{n_2}(\mathbb{C}) \times \cdots \times M_{n_r}(\mathbb{C}).$$

Hence another useful way of thinking of the elements of $R$ is as $n \times n$ (block diagonal)
matrices of the form

$$
\begin{pmatrix}
A_1 \\
A_2 \\
\vdots \\
A_r
\end{pmatrix}
$$

where $A_i \in M_{n_i}(\mathbb{C})$ for $i = 1, 2, \ldots, r$ and $n = \sum_{i=1}^r n_i$.

We say that a ring $R$ satisfying any of the (equivalent) properties in Wedderburn’s Theorem is semisimple with minimum condition (D.C.C). Note that an $R$-module $Q$ is injective if and only if whenever $Q$ is a submodule of any $R$-module $M$, then $M$ has a submodule $N$ such that $M = Q \oplus N$. Now let’s recall Maschke’s Theorem:

**Theorem 2.3.5** (Maschke). Let $G$ be a finite group and let $K$ be a field whose characteristic does not divide $|G|$. If $V$ is any $KG$-module and $U$ is any submodule of $V$, then $V$ has a submodule $W$ such that $V = U \oplus W$ (i.e., every submodule is a direct summand.)

Thus we see that group ring $KG$ where $|G|$ does not divide the characteristic of $K$ is injective and thus obtain the following corollary to Wedderburn’s Theorem:

**Corollary 2.3.6.** If $G$ is a finite group and $K$ is a field whose characteristic does not divide $|G|$, then the group algebra $KG$ is a semisimple ring.

So as a ring we see that $\mathbb{C}D_8 \cong M_1(\mathbb{C}) \times M_1(\mathbb{C}) \times M_1(\mathbb{C}) \times M_1(\mathbb{C}) \times M_2(\mathbb{C})$ and
as a vector space over \( \mathbb{C} \)

\[
\mathbb{C}D_8 \cong \text{span}_{\mathbb{C}} \left\{ \begin{pmatrix}
\phi_1(g) & 0 & 0 & 0 & 0 \\
0 & \phi_2(g) & 0 & 0 & 0 \\
0 & 0 & \phi_3(g) & 0 & 0 \\
0 & 0 & 0 & \phi_4(g) & 0 \\
0 & 0 & 0 & 0 & \phi_5(g)
\end{pmatrix} : g \in D_8 \right\}.
\]

(2.1)

Thus we identify the identity in \( \mathbb{C}D_8 \) with the \( 6 \times 6 \) identity matrix contained on the right hand side of (2.1). Thus we can see that \( \mathbb{C}D_8 \) has five primitive orthogonal idempotents. These are given by

\[
z_1 = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0
\end{pmatrix},
\]

\[
z_2 = \begin{pmatrix}
0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0
\end{pmatrix},
\]

\[
z_3 = \begin{pmatrix}
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0
\end{pmatrix},
\]

\[
z_4 = \begin{pmatrix}
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0
\end{pmatrix},
\]

\[
z_5 = \begin{pmatrix}
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1
\end{pmatrix}.
\]

Hence we can identify the left ideals of \( \mathbb{C}D_8 \) with \( L_i = \mathbb{C}D_8 z_i \) for all \( 1 \leq i \leq 5 \) which gives us the irreducible representations of \( \mathbb{C}D_8 \). Note then, that these left ideals give a complete set of isomorphism classes of irreducible \( \mathbb{C}D_8 \)-modules. So as a left module over itself we see that \( \mathbb{C}D_8 \cong L_1 \oplus L_2 \oplus L_3 \oplus L_4 \oplus L_5 \oplus L_5 \). We also know that any left \( \mathbb{C}D_8 \)-module can be written as a direct sum of irreducible \( \mathbb{C}D_8 \)-modules isomorphic to these five. Hence we have described the structure of \( \mathbb{C}D_8 \) as a group ring and the structure of all left \( \mathbb{C}D_8 \)-modules.

### 2.4 Character Theory

Now many times it is difficult to compute or even write down the representations for large groups. Yet we are able to calculate numerical invariants that allow us to
characterize the similarity classes of representations of our groups. We have already introduced these numerical invariants of linear representations, called characters, and now we explore some of their properties.

When calculating the irreducible representations of $\mathbb{C}D_8$ we did not need to use the properties of characters, but sometimes it is easier to calculate the characters of irreducible representations of a group by exploiting some nice properties of characters. We have already seen that characters are class functions. We now note another one: since the trace of any $n \times n$ identity matrix is $n$ we see that for any character $\chi : G \to K$, $\chi(e_g)$ is equal to the degree of the representation $\phi$ associated with $\chi$, where $e_g$ is the identity element in $G$. Also note that since $tr(AB) = tr(BA)$ for any matrices, then whenever $A$ is invertible we get that $tr(A^{-1}BA) = tr(B)$. Hence, we obtain the following theorem.

**Theorem 2.4.1.** Equivalent representations have the same character.

**Proof.** Let $\phi_1$ and $\phi_2$ be equivalent linear representations of the finite group $G$ with representation spaces $V_1$ and $V_2$ respectively. Let us show that $\phi_1$ and $\phi_2$ have the same character. By assumption, there exists a isomorphism $h \in Hom_K(V_1,V_2)$ such that

$$h\phi_1(g)h^{-1} = \phi_2(g), g \in G.$$ 

Now let $\chi_1(g)$ be the character of $\phi_1$. Thus

$$\chi_1(g) = tr[\phi_1(g)] = tr[h^{-1}\phi_2(g)h] = tr[\phi_2(g)hh^{-1}] = tr[\phi_2(g)] = \chi_2(g).$$

Therefore, $\chi_1(g) = \chi_2(g)$.

Now suppose $CG = M_{n_1}(\mathbb{C}) \times M_{n_2}(\mathbb{C}) \times \cdots \times M_{n_r}(\mathbb{C})$, where $r$ denotes the number of conjugacy classes of $G$. Let $L_1, L_2, \ldots, L_r$ denote the non-isomorphic irreducible representations of $G$ and let $\chi_i$ be the corresponding character, called the irreducible character, for all $1 \leq i \leq r$. Since any left $CG$-module is isomorphic to a direct sum of irreducible left $CG$-modules we see that its associated character is a sum of the characters associated to the irreducible representations. In fact, it can be shown that $\chi_1, \chi_2, \ldots, \chi_r$ are a basis for the space of all complex class functions.

Now to establish other useful properties of characters we will define the following product, which turns out to be a Hermitian inner product on the space of class functions:

$$(\theta, \psi) = \frac{1}{|G|} \sum_{g \in G} \theta(g)\overline{\psi(g)}.$$
Here the bar denotes complex conjugation. It can be shown that the product \((-,-)\) is Hermitian, that is for all \(\alpha, \beta \in \mathbb{C}\) the following properties are satisfied:

(a) \((\alpha \theta_1 + \beta \theta_2, \psi) = \alpha(\theta_1, \psi) + \beta(\theta_2, \psi)\),

(b) \((\theta, \alpha \psi_1 + \beta \psi_2) = \alpha(\theta, \psi_1) + \beta(\theta, \psi_2)\), and

(c) \((\theta, \psi) = (\psi, \overline{\theta})\).

With respect to this product it can be shown that the irreducible characters of \(G\) form an orthonormal basis on the space of class functions, i.e. not only do the characters form a basis, but also \((\chi_i, \chi_j) = \delta_{ij}\). The following propositions and theorems allow us to prove this fact but in addition provide a useful orthogonality relation on the irreducible characters.

**Proposition 2.4.1.** Let \(z_1, \ldots, z_r\), be the orthogonal primitive central idempotents in \(\mathbb{C}G\) labelled in such a way that \(z_i\) acts as the identity on the irreducible \(\mathbb{C}G\)-module \(M_i\), and let \(\chi_i\) be the character afforded by \(M_i\). Then

\[
z_i = \frac{\chi_i(1)}{|G|} \sum_{g \in G} \chi_i(g^{-1})g.
\]

**Proof.** Let \(z = z_i \in \mathbb{C}G\). Then \(z = \sum_{g \in G} \alpha_g g\). Let \(\phi\) be the regular representation of \(G\) whose character is \(\rho\),

\[
\rho : G \to \mathbb{C} \rho(g) = tr(\phi(g))
\]

where \(tr(\phi(g)) = 0\) if \(g \neq 1\) or \(tr(\phi(g)) = |G|\) if \(g = 1\).

Recall

\[
\mathbb{C}G \cong M_{n_1}(\mathbb{C}) \times M_{n_2}(\mathbb{C}) \times M_{n_r}(\mathbb{C})
\]

\[
\cong n_1M_1 \oplus n_2M_2 \oplus \cdots \oplus n_rM_r
\]

where \(M_i\) are left \(\mathbb{C}G\)-modules (simple ideals), \(1 \leq i \leq r\). But we know that every \(M_i\) affords a \(\chi_i\). Therefore,

\[
\rho = n_1\chi_1 + n_2\chi_2 + \cdots + n_r\chi_r
\]
And since \( n_i = tr(1) = \chi_i(1) \) we have

\[
\rho = \chi_1(1)\chi_1 + \chi_2(1)\chi_2 + \cdots + \chi_r(1)\chi_r
\]

\[
= \sum_{j=1}^{r} \chi_j(1)\chi_j
\]

So our goal is to show that the coefficient \( \alpha_g = \frac{\chi_j(1)}{|G|} \chi_j(g^{-1}) \) and we have

\[
\rho(zg^{-1}) = \sum_{j=1}^{r} \chi_j(1)\chi_j(zg^{-1})
\]

So let \( z = \sum_{h \in G} \alpha_h h \). Then

\[
\Rightarrow \quad zg^{-1} = \sum_{h \in G} \alpha_h h(g^{-1})
\]

\[
\Rightarrow \quad \rho(zg^{-1}) = \rho(\sum_{h \in G} \alpha_h h(g^{-1}))
\]

\[
= \sum_{h \in G} \alpha_h \rho(hg^{-1})
\]

\[
= \alpha_g \rho(1)
\]

\[
= \alpha_g |G|.
\]

Also note that \( \rho(zg^{-1}) = \sum_{j=1}^{r} \chi_j(1)\chi_j(zg^{-1}) \Rightarrow \alpha_g |G| = \sum_{j=1}^{r} \chi_j(1)\chi_j(zg^{-1}) \).

Let \( \phi_j \) be an irreducible representation afforded by \( M_j \) where \( 1 \leq j \leq r \). We know that representation problems are simplified by noting that every linear representation of \( G \) (a group homomorphism) defines a corresponding representation of the the group algebra \( \mathbb{C}G \) (a linear transformation). With that said we have

\[
\phi^* : \mathbb{C}G \rightarrow End(M_j) \Rightarrow \phi_j(zg^{-1}) = \phi_j(z) \cdot \phi_j(g^{-1}).
\]

where \( \phi^* \) is a linear transformation. Thus,

\[
\phi^* : \mathbb{C}G \rightarrow End(M_j) \Rightarrow \phi_j(zg^{-1}) = \phi_j(z) \cdot \phi_j(g^{-1}).
\]
where $\phi^*$ is a linear transformation. Thus,

$$
\chi_j(zg^{-1}) = \text{tr}(\phi_j(zg^{-1}))
$$

$$
= \begin{cases} 
\text{tr}(0) & \text{if } j \neq i \\
\text{tr}(\phi_i(g^{-1})) & \text{if } j = i 
\end{cases}
$$

$$
= \begin{cases} 
0 & \text{if } j \neq i \\
\chi_i(g^{-1}) & \text{if } j = i 
\end{cases}
$$

$$
= \delta_{ij}\chi_i(g^{-1})
$$

So we can see that $\chi_j(zg^{-1}) = \delta_{ij}\chi_i(g^{-1})$. Finally, we have that

$$
\sum_{j=1}^{r} \chi_j(1)\chi_j(zg^{-1}) = \alpha_g|G|
$$

$$
\Rightarrow \sum_{j=1}^{r} \chi_j(1)\delta_{ij}\chi(g^{-1}) = \alpha_g|G|
$$

$$
\Rightarrow \alpha_g = \frac{1}{|G|}\chi_i(1)\chi_i(g^{-1}).
$$

- \textbf{Proposition 2.4.2.} If $\chi$ is any character of $G$ then $\chi(g)$ is the sum of roots of 1 in $\mathbb{C}$ and $\chi(g^{-1}) = \overline{\chi(g)}$ for all $g \in G$.

\textbf{Proof.} Let $\phi$ be a representation of $G$ whose character is $\chi$. That is,

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

$$
g \mapsto \phi(g)
$$

and

$$
\chi : G \rightarrow K,
$$

$$
\chi(g) = \text{tr}(\phi(g))
$$

Let $g \in G$ be a fixed element where $|g| = n$ and let $m(x)$ denote the minimal polynomial of $g$ acting on $V$. Since $m(x)|x^n - 1$ (where $x^n - 1$ is the cyclotomic polynomial in $\mathbb{C}$), then $m(x)$ has distinct roots $\Rightarrow \phi(g)$ is diagonalizable with $n^{th}$ roots of 1 on the
diagonal which implies that there exist some square matrix $A$ such that

$$
\phi(g) = A^{-1} \begin{pmatrix}
\zeta_1 \\
\zeta_2 \\
\vdots \\
\zeta_r
\end{pmatrix} A
$$

$$
\Rightarrow \text{tr}(\phi(g)) = \text{tr}
\begin{pmatrix}
\zeta_1 \\
\zeta_2 \\
\vdots \\
\zeta_r
\end{pmatrix}
$$

$$
\Rightarrow \text{tr}(\phi(g)) = \zeta_1 + \cdots + \zeta_r.
$$

Therefore $\phi(g)$ is the sum of roots of 1 in $\mathbb{C}$. Furthermore, if $\zeta$ is a root of 1 in $\mathbb{C}$, then $\zeta^{-1} = \bar{\zeta}$. Therefore, the inverse of a diagonal matrix with roots of 1 on the diagonal is the diagonal matrix with the complex conjugates of those roots of 1 on the diagonal. That is,

$$
\begin{pmatrix}
\zeta_1 \\
\zeta_2 \\
\vdots \\
\zeta_r
\end{pmatrix}^{-1}
$$

where $i = 1, 2, \ldots, r$.

Finally since the complex conjugates of a sum is the sum of the complex conjugates, i.e., $\bar{A} + \bar{B} = \bar{A + B}$, then

$$
\chi(g^{-1}) = \text{tr}[\phi(g^{-1})] = \overline{\text{tr}[\phi(g^{-1})]} = \overline{\chi(g)}.
$$

\[\square\]

**Theorem 2.4.2.** Let $G$ be a finite group and $\chi_1, \cdots, \chi_r$ be the irreducible characters of $G$ over $\mathbb{C}$. Then with respect to the inner product $(\cdot, \cdot)$ defined above we have

$$
(\chi_i, \chi_j) = \delta_{ij}
$$
and the irreducible characters are an orthonormal basis for the space of class functions. In particular, if \( \theta \) is any class function then

\[
\theta = \sum_{i=1}^{r} (\theta, \chi_i) \chi_i.
\]

This is usually called the First Orthogonality Relation for Group Characters.

We finish this chapter by stating one more definition and two results that will aid greatly in computing the irreducible representations of \( D_{2n} \).

**Definition 2.4.1** (Norm of a Class function). For \( \theta \) any class function on \( G \) the norm of \( \theta \) is \( (\theta, \theta)^{1/2} \) and will be denoted by \( ||\theta|| \)

**Proposition 2.4.3** (Irreducibility criterion). If \( \phi \) is a complex representation of \( G \) affording \( \chi \) then \( \phi \) is irreducible if and only if the norm is 1.

Finally if \( \theta \) and \( \psi \) are any two characters of representations of \( G \) we can simplify the computations of \( (\theta, \psi) \) as follows: If \( \kappa_1, \ldots, \kappa_r \) are the conjugacy classes of \( G \) with sizes \( d_1, \ldots, d_r \) and representatives \( g_1, \ldots g_r \) respectively, then the value \( \theta(g_i)\overline{\psi(g_i)} \) appears \( d_i \) times in the sum for \( (\theta, \psi) \), once for each element of \( \kappa_i \). Collecting these terms gives us the following:

\[
(\theta, \psi) = \frac{1}{|G|} \sum_{i=1}^{r} d_i \theta(g_i)\overline{\psi(g_i)},
\]

a sum only over the conjugacy classes of \( G \). In particular we obtain the following:

\[
||\theta||^2 = (\theta, \theta) = \frac{1}{|G|} \sum_{i=1}^{r} d_i |\theta(g_i)|^2.
\]
Chapter 3

The Representation Theory of $D_{2n}$

3.1 Introduction

Before we prove the main result of this section let us explore a bit. In section 2.3 we saw that the linear representations of $\rho : D_8 \rightarrow GL_2(\mathbb{C})$ given by $r \mapsto R = \begin{pmatrix} \cos(\pi/2) & -\sin(\pi/2) \\ \sin(\pi/2) & \cos(\pi/2) \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $s \mapsto S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is of degree 2 and irreducible. Now let $\theta = \frac{2\pi}{n}$ and observe the following.

Lemma 3.1.1. There exists a matrix $A \in GL_2(\mathbb{C})$ such that $R = A \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix} A^{-1}$.

Proof. By solving the characteristic equation $det(R - \lambda I) = 0$, we can see that

\[
\begin{vmatrix} \cos \theta - \lambda & -\sin \theta \\ \sin \theta & \cos \theta - \lambda \end{vmatrix} = 0
\]

\[
\Rightarrow \cos^2 \theta - 2\lambda \cos \theta + \lambda^2 = 0
\]

\[
\Rightarrow \lambda^2 \theta - 2\lambda \cos \theta + 1 = 0
\]

\[
\Rightarrow \lambda = \frac{2 \cos \theta \pm \sqrt{4 \cos^2 \theta - 4}}{2}
\]

\[
= \frac{2 \cos \theta \pm \sqrt{\cos^2 \theta - 1}}{2}
\]

\[
= \cos \theta \pm \sqrt{-\sin^2 \theta}
\]
Since for $n \geq 3$ we have that $0 \leq \theta \leq \pi \Rightarrow \sin \theta > 0$. Hence $\lambda = \cos \theta \pm i \sin \theta \Rightarrow \lambda = e^{\pm \theta}$. Computing the eigenspace associated with $\lambda_1 = e^{i \theta}$ we see that
\[
\begin{bmatrix}
\cos \theta - \lambda_1 & -\sin \theta & 0 \\
\sin \theta & \cos \theta - \lambda_1 & 0 \\
0 & 0 & 0
\end{bmatrix}
\rightarrow
\begin{bmatrix}
-i \sin \theta & -\sin \theta & 0 \\
\sin \theta & i \sin \theta & 0 \\
0 & 0 & 0
\end{bmatrix}
\rightarrow
\begin{bmatrix}
-i \sin \theta & -\sin \theta & 0 \\
0 & 0 & 0
\end{bmatrix}.
\]
This implies then that $-ix \sin \theta - y \sin \theta = 0 \Rightarrow \sin \theta(ix + y) = 0 \Rightarrow y = -ix$. Thus we see that $E_{\lambda_1} = \text{span} \left\{ \begin{pmatrix} 1 \\ -i \end{pmatrix} \right\}$. Similarly we obtain that $E_{\lambda_2} = \text{span} \left\{ \begin{pmatrix} 1 \\ i \end{pmatrix} \right\}$. Direct computation show that
\[
\begin{bmatrix}
1 & 1 \\
-i & i
\end{bmatrix}
\begin{bmatrix}
e^{i \theta} & 0 \\
0 & e^{-i \theta}
\end{bmatrix}
\begin{bmatrix}
1 & 1 \\
-i & i
\end{bmatrix}^{-1}
= R.
\]
Thus, $A = \begin{pmatrix} 1 & 1 \\ -i & i \end{pmatrix}$.

**Corollary 3.1.1.** Let $\rho_\theta : D_{2n} \to GL_2(\mathbb{C})$ be given by $r \mapsto R = \begin{pmatrix} e^{i \theta} & 0 \\ 0 & e^{-i \theta} \end{pmatrix}$, $s \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Then $\rho_\theta$ and $\rho$ are equivalent representations of $D_{2n}$.

**Proof.** By Theorem 2.4.1 it is sufficient to show that the characters on the generators is the same. Clearly the trace of $S$ for both representations is the same and since $R$ is similar to $\begin{pmatrix} e^{i \theta} & 0 \\ 0 & e^{-i \theta} \end{pmatrix}$ then by our lemma their traces are the same.

In Section 2.3 we explored $D_8$ (n=4). Now let us explore $D_{10}$ (n=5) so that we can motivate how we found the representations of $D_{2n}$ in general. By the results in section 3.2 later in this chapter we know that $D_{10}$ has four conjugacy classes. We list the classes here:

\[
\begin{align*}
[1] &= \{1\}, \\
[r] &= \{r, r^{-1}\} = \{r, r^4\}, \\
[r^2] &= \{r^2, r^{-2}\} = \{r^2, r^3\}, \\
[s] &= \{s, sr, sr^2, sr^3, sr^4\},
\end{align*}
\]
From the results in section 3.3 later in this chapter we know the commutator subgroup of \( D_{10} \) is \( D'_{10} = \{1, r, r^2, r^3, r^4\} \) which gives us 2 degree 1 representations

\[
\phi_1: D_{10} \rightarrow \mathbb{C} \\
r \mapsto 1 \\
s \mapsto 1
\]

and

\[
\phi_2: D_{10} \rightarrow \mathbb{C} \\
r \mapsto 1 \\
s \mapsto -1
\]

in a process similar to how we analyzed \( D_8 \) in section 2.3. We know from example 2.2.5 and from the corollary above (3.3.1) that one degree two irreducible representations of \( D_{10} \) is given by

\[
\rho_1: D_{10} \rightarrow GL_2(\mathbb{C})
\]

where

\[
r \mapsto R' = \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix}, s \mapsto S, \theta = \frac{2\pi}{5}.
\]

Hence we have 3 irreducible representations of \( D_{10} \); we just need one more. We note that \( R' \) is a rotation of the \( xy \)-plane by \( 2\pi/5 \) radians. Could it be possible that if we rotate the pane by \( 4\pi/5 \) radians that we get another irreducible representation of \( D_{2n} \), i.e.,

\[
\rho_2: D_{10} \rightarrow GL_2(\mathbb{C}),
\]

\[
r \mapsto R' = \begin{pmatrix} e^{2i\theta} & 0 \\ 0 & e^{-2i\theta} \end{pmatrix}, s \mapsto S
\]

another degree two representation. First note that \( r^5 = 1 \) and

\[
\begin{pmatrix} e^{2i\theta} & 0 \\ 0 & e^{-2i\theta} \end{pmatrix}^5 = \begin{pmatrix} (e^{2i\theta})^5 & 0 \\ 0 & (e^{-2i\theta})^5 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}
\]
since $e^{2i\theta}$ and $e^{-2i\theta}$ are fifth roots of unity. Hence if we send
\[
sm \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} e^{2i\theta} & 0 \\ 0 & e^{-2i\theta} \end{pmatrix}^m
\]
we see that $\rho_2$ is an injective homomorphism, i.e., a faithful representation of $D_{10}$. But is it irreducible? From the last result in Section 2.4, Proposition 2.4.3, we just need to show that the norm of the character afforded by $\rho_2$ is equal to 1. We use the following table to organize our computations.

<table>
<thead>
<tr>
<th>Conjugacy Class</th>
<th>Size of Conj.</th>
<th>$\chi_2(a)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$[a]$</td>
<td>Class</td>
<td></td>
</tr>
<tr>
<td>$[1]$</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>$[r]$</td>
<td>2</td>
<td>$2\cos\left(\frac{4\pi}{5}\right)$</td>
</tr>
<tr>
<td>$[r^2]$</td>
<td>2</td>
<td>$2\cos\left(\frac{8\pi}{5}\right)$</td>
</tr>
<tr>
<td>$[s]$</td>
<td>5</td>
<td>0</td>
</tr>
</tbody>
</table>

A quick calculation shows that

\[
(\chi_2, \chi_2) = \frac{1}{10} \left[1 \cdot \chi_2(1)^2 + 2 \cdot \chi_2(r)^2 + 2\chi_2(r^2)^2 + 5\chi_2(s)^2\right]
= \frac{1}{10} \left[4 + 2 \cdot 4\cos^2\left(\frac{4\pi}{5}\right) + 2 \cdot 4\cos^2\left(\frac{8\pi}{5}\right) + 0\right]
= \frac{4}{10} \left[1 + 2\cos^2\left(\frac{4\pi}{5}\right) + 2\cos^2\left(\frac{8\pi}{5}\right)\right]
= \frac{2}{5} (2.5)
= 1
\]

Thus $\rho_2$ is irreducible. But now the question becomes, is the representation equivalent to either $\theta_1, \theta_2$, or $\rho_1$. By dimension of the representation space we know that $\rho_2$ cannot be equivalent to $\theta_1$, or $\theta_2$. But what about $\rho_1$? By theorem 2.4.1 we see that they would be equivalent if they had the same character, but

\[
\chi_1(r) = 2\cos\left(\frac{2\pi}{5}\right) \neq 2\cos\left(\frac{4\pi}{5}\right) = \chi_2(r)
\]
So $\rho_1$ and $\rho_2$ cannot be equivalent. Thus we have found all four irreducible representations of $D_{10}$. To find the representations of $D_{2n}$ in general we explored $D_{2n}$ for certain values of $n$; $n = 4, 6, 8$ to get an idea on how to attack the representations when $n$ is even and $n = 3, 5, 7$ to understand better the case of when $n$ is odd. My results are summarized in the next three sections.

3.2 Conjugacy Classes of $D_{2n}$

The main result of section 3.2 is the following:

**Theorem 3.2.1.** Let $D_{2n} = \langle r, s | r^n = s^2 = 1, rs = sr^{-1} \rangle = \{1, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1} \}$, where $n \in \mathbb{Z}^+, n \geq 3$.

1. If $n$ is even, i.e., $n = 2k$ for $k \geq 2$, then $D_{2n}$ has $k + 3$ conjugacy classes.

2. If $n$ is odd, i.e., $n = 2k + 1$ for $k \geq 1$, then $D_{2n}$ has $k + 2$ conjugacy classes.

To prove this, we first need to prove the following lemmas

**Lemma 3.2.1.** Let $D_{2n} = \langle r, s | r^n = s^2 = 1, rs = sr^{-1} \rangle$ such that $n \in \mathbb{Z}^+, n \geq 3$. Then $r^m s = sr^{-m}$ for all $m$ in $\mathbb{Z}$.

**Proof.** By induction on $m$. If $m = 1$ then $rs = sr^{-1}$ by our presentation. Let $m > 1$ and suppose $r^m s = sr^{-m}$. We need to show $r^{m+1} s = sr^{-(m+1)}$. We start with the left hand side and use our assumptions to get the right hand side.

$$
\begin{align*}
    r^{m+1} s &= r^m \cdot r \cdot s \\
    &= r^m (r \cdot s) \\
    &= r^m (sr^{-1}) \\
    &= (r^m s) r^{-1} \\
    &= (sr^{-m}) r^{-1} \\
    &= sr^{-m-1} \\
    &= sr^{-(m+1)}
\end{align*}
$$
Lemma 3.2.2. If $x \in D_{2n}$ such that $x \neq r^m$ for any $0 \leq m \leq n$, then $rx = xr^{-1}$.

Proof. If $x \in D_{2n}$ such that $x \neq r^m$ for any $0 \leq m \leq n$, then $x = sr^m$ for some $0 \leq m \leq n$. Thus,

$$rx = r(sr^m) = (rs)r^m = (sr^{-1})r^m = s(r^{-1}r^m) = s(r^m)^{-1} = (sr^m)^{-1} = xr^{-1}$$

Lemma 3.2.3. Let $n = 2k, k \in \mathbb{Z}^+, k \geq 2$, then the conjugacy classes of $D_{2n}$ are

$$[1] = \{1\},$$
$$[r] = \{r, r^{-1}\},$$
$$[r^2] = \{r^2, r^{-2}\},$$
$$\vdots$$
$$[r^{k-1}] = \{r^{k-1}, r^{-(k+1)}\},$$
$$[r^k] = \{r^k\}$$
$$[sr] = \{sr^{2b-1} : b = 1, \ldots, k\},$$
$$[sr^2] = \{sr^{2b} : b = 1, \ldots, k\}.$$

Proof. We know that if $x \in Z(D_{2n})$, then $[x] = \{x\}$. Thus since $Z(D_{2n}) = \{1, r^k\}$ we see that $[1] = \{1\}$ and $[r^k] = \{r^k\}$.

Claim 1: $[r^m] = \{r^m, r^{-m}\}$ for all $1 \leq m \leq k - 1$.

" $\supseteq$ " We know $r^m \in [r^m]$ by definition. So all that is left to show is that $r^{-m} \in [r^m]$,
i.e., $r^{-m} = y^{-1}r^my$ for some $y \in D_{2n}$. By the previous lemma

$$rx = xr^{-1}$$
$$\Rightarrow r^{-1} = x^{-1}rx$$
$$\Rightarrow r^{-m} = (x^{-1}rx)^m$$
$$= (x^{-1}rx)(x^{-1}rx)\cdots(x^{-1}rx)$$
$$= x^{-1}r^mx$$
$$\Rightarrow r^{-m} \in [r^m].$$

“$\subseteq$” Let $g \in [r^m] \Rightarrow g = x^{-1}r^mx$ for some $x \in D_{2n}$. We need to show that $g \in \{r^m, r^{-m}\}$.

**Case 1** Suppose $x = r^t$ for some $0 \leq m \leq n - 1$. Then

$$g = (r^t)^{-1}r^mr^t$$
$$= r^{-t}r^mr^t$$
$$= r^m \in \{r^m, r^{-m}\}$$

**Case 2** Suppose $x \neq r^t$ for all $0 \leq t \leq n$. Then $x = sr^t$ for some $0 \leq t \leq n-1$.

Thus,

$$g = (sr^t)^{-1}r^m(sr^t)$$
$$= r^{-t}sr^m sr^t$$
$$= r^{-t}ssr^{-m}r^t$$
$$= r^{-t}r^{-m}r^t$$
$$= r^{-m} \in \{r^m, r^{-m}\}$$

**Claim 2:** $[sr] = \{sr^{2b-1} : b = 1, \cdots k\}$.

“$\supseteq$” By induction on $b$. Let $b = 1$. Then $sr^{2(1)-1} = sr^1 = sr \in [sr]$ by definition. Let $1 < b < k$ and suppose $sr^{2b-1} \in [sr]$. This means $sr^{2b-1} = x^{-1}sr x$ for some $x \in D_{2n}$. We will show that $sr^{2(b+1)-1} = sr^{2b+1} \in [sr]$. Again by lemma
3.2.2 we have
\[ r(sr^{2b+1}) = (sr^{2b+1})^r - 1 \]
\[ \Rightarrow sr^{2(b+1)} = r^{-1}sr^{2b+1}r^{-1} \]
\[ = r^{-1}sr^{2b} \]
\[ = r^{-1}(sr^{2b-1}+1) \]
\[ = r^{-1}(sr^{2b-1}r) \]
\[ = r^{-1}(x^{-1}sr^{-1})r \]
\[ = (xr)^{-1}(sr)(xr) \in [sr] \]

"⊆" Let \( x \in [sr] \Rightarrow x = y^{-1}(sr)y \) for some \( y \in D_{2n} \).

**Case 1** Let \( y = r^m, 0 \leq m \leq n - 1 \). Then
\[ x = r^{-m}(sr)^m \]
\[ = (r^{-m}s)^{m+1} \]
\[ = sr^{m+1}r^{m+1} \]
\[ = sr^{2m+1} \]

Now \( 2m + 1 \) is odd \( \Rightarrow 2m + 1 (mod2k) = 2b - 1 \) for some \( 1 \leq b \leq k \). Thus
\( x \in \{sr^{2b-1}|b = 1, \ldots, k\} \).

**Case 2** Let \( y = sr^m, 0 \leq m \leq n - 1 \). Then
\[ x = (sr^m)^{-1}sr^{sr^m} \]
\[ = r^{-m}s^{-1}sr^{sr^m} \]
\[ = r^{-m}s^{-1}s^{-1}r^{m} \]
\[ = sr^{m+1}r^{m-1} \]
\[ = sr^{2m-1} \]

Again \( 2m - 1 \) is odd \( \Rightarrow (2m - 1)mod(2k) = 2b - 1 \) for some \( 1 \leq b \leq k \). Thus
\( x \in \{sr^{2b-1}|b = 1, \ldots, k\} \).

**Claim 3:** \([sr^2] = \{sr^{2b} : b = 1, \ldots, k\}\)

"⊇" By induction on \( b \). Let \( b = 1 \). Then \( sr^2 \in [sr^2] \) by definition. Let \( 1 \leq b \leq k \) and suppose \( sr^{2b} \in [sr] \). This means \( sr^{2b} = x^{-1}(sr)x \) for some \( x \in D_{2n} \). We will show that \( sr^{2(b+1)} = sr^{2b+2} \). Once again by the previous lemma we...
have that
\[ r(st^{2b+2}) = (st^{2b+2})r^{-1} \]
\[ \Rightarrow st^{2b+2} = r^{-1}st^{2b}r^{-1} \]
\[ = r^{-1}(x^{-1}stx)r \]
\[ = (xr)^{-1}(sr)(xr) \in [sr] \]

“⊆” Let \( x \in [sr^2] \Rightarrow x = y^{-1}(sr^2)y \) for some \( y \in D_{2n} \).

**Case 1** Let \( y = r^m, 0 \leq m \leq n - 1 \). Then
\[ x = r^{-m}(sr^2)r^m \]
\[ = st^m r^{m+2} \]
\[ = st^{2m+2} \]

Since \( 2m + 2 \mod (2k) \) is even \( \Rightarrow x = sr^{2b} \) for some \( 1 \leq b \leq k \) \( \Rightarrow x \in \{sr^{2b} | b = 1, \cdots, k \} \Rightarrow x \in \{sr^{2b} : b = 1, \cdots k \} \)

**Case 2** Let \( y = sr^m, 0 \leq m \leq n - 1 \). Then
\[ x = (sr^m)^{-1}(sr^r)(sr^m) \]
\[ = r^{-m}s^{-1}st^{2}sr^m \]
\[ = r^{-m}sr^{-2}r^m \]
\[ = st^m r^{m-2} \]
\[ = st^{2m+2} \]

Again since \( 2m - 2 \mod (2k) \) is even \( \Rightarrow x = sr^{2b} \) for some \( 1 \leq b \leq k \).

By counting the conjugacy classes listed in this lemma, we see that part (a) of Theorem 1 is proved. Part (b) is proved similarly by proving the following lemma:

**Lemma 3.2.4.** If \( n = 2k + 1, n \in \mathbb{Z}^+, k \geq 1 \), then the conjugacy classes of \( D_{2n} \) are
\[ [1] = \{1\}, [r] = \{r, r^{-1}\}, [r^2] = \{r^2, r^{-2}\}, \cdots, [r^{k-1}] = \{r^{k-1}, r^{-(k+1)}\}, [r^k] = \{r^k, r^{-k}\}, [s] = \{sr^b | b = 1, \cdots n\} \].

### 3.3 Commutator Subgroup of \( D_{2n} \)

From our discussions in Section 2.3, we know that if we can find the commutator subgroup of \( D_{2n}, D_{2n}' \), then this will help us in finding \( |D_{2n}/D_{2n}'| \) degree 1 irreducible representations of \( D_{2n} \). Thus the goal of this section is to prove the following theorem:
Theorem 3.3.1. Let $D_{2n} = \langle r, s | r^n = s^2 = 1, rs = sr^{-1} \rangle$. Then $D'_{2n} = \langle r^2 \rangle$.

First we prove the following lemmas

Lemma 3.3.1. $\langle r^2 \rangle \triangleleft D_{2n}$.

Proof. Let $x \in D_{2n}, y \in \langle r^2 \rangle$. We need to show $xyx^{-1} \in \langle r^2 \rangle$. Since $y \in \langle r^2 \rangle$, then $y = (r^2)^b = r^{2b}$ for some $b \in \mathbb{Z}$.

Case 1 Suppose $x = r^m, 0 \leq m \leq n - 1$. Then $xyx^{-1} = r^m r^{2b} r^{-m} = r^{2b} \in \langle r^2 \rangle$.

Case 2 Suppose $x = sr^m, 0 \leq m \leq n - 1$. Then

$$xyx^{-1} = sr^{m} r^{2b} (sr^{m})^{-1} = sr^{m} r^{2b} r^{-m} s = sr^{2b}s = ssr^{-2b} = r^{-2b} = (r^2)^{-b} \in \langle r^2 \rangle$$

Thus $\langle r^2 \rangle \triangleleft D_{2n}$.

Lemma 3.3.2. $D_{2n}/\langle r^2 \rangle$ is abelian.

Proof. We prove this using two cases, when $n$ is odd and when $n$ is even.

Case 1 Suppose $n$ is odd. If $n$ is odd, then since 2 is relatively prime to $n$ we see that

$$\langle r^2 \rangle = \{1, r, r^2, \ldots, r^{n-1}\}$$

$$\Rightarrow |\langle r^2 \rangle| = n$$

$$\Rightarrow [D_{2n} : \langle r^2 \rangle] = \frac{|D_{2n}|}{|\langle r^2 \rangle|} = \frac{2n}{n} = 2$$

$$\Rightarrow D_{2n}/\langle r^2 \rangle \cong \mathbb{Z}/2\mathbb{Z}$$

$$\Rightarrow D_{2n}/\langle r^2 \rangle$$ is abelian.
Case 2 Suppose $n$ is even. Then \( \langle r^2 \rangle = \{1, r, r^2, \ldots, r^{n/2}\} \Rightarrow |\langle r^2 \rangle| = n/2 \). Thus, 
\[
[D_{2n} : \langle r^2 \rangle] = \frac{|D_{2n}|}{|\langle r^2 \rangle|} = 2n/(n/2) = 4.
\]
Since all groups of order 4 are abelian then 
\( D_{2n}/\langle r^2 \rangle \) is abelian.

We now prove Theorem 3.3.1 above:

**Proof.** We proceed by set inclusion.

\( \supseteq \) We know \( D'_{2n} = \{[x, y] | x, y \in D_{2n}\} \). Since \( r, s \in D_{2n} \) then \( [s, r] \in D'_{2n} \). Note that
\[
[s, r] = s^{-1}r^{-1}sr = s^{-1}srr = r^2
\]
Hence \( r^2 \in D_{2n}' \Rightarrow \langle r^2 \rangle \leq D_{2n}' \)

\( \subseteq \) By lemma 3.3.1 we know that \( \langle r^2 \rangle \triangleleft D_{2n} \), thus we can construct the quotient group 
\( D_{2n}/\langle r^2 \rangle \). By lemma 3.3.2 we know that \( D_{2n}/\langle r^2 \rangle \) is abelian. Since the commutator 
\( D'_{2n} \) is the smallest subgroup of \( D_{2n} \) such that \( D_{2n}/D'_{2n} \) is abelian this means that 
\( D'_{2n} \leq \langle r^2 \rangle \).

Therefore, \( D'_{2n} = \langle r^2 \rangle \).

**Corollary 3.3.2.** If $n$ is odd, then \( D_{2n} \) has two degree 1 (irreducible) representations.

**Proof.** Let \( H = D'_{2n} = \langle r^2 \rangle \). By lemma 2 we know that \( D_{2n}/H \cong \mathbb{Z}/2\mathbb{Z} \). Note also that 
\( rH = H \) since \( r \in H \). Thus \( D_{2n}/H = \{H, sH\} \). So two representations of \( D_{2n}/H \) are given by the following:

\[
\begin{align*}
\bar{\phi}_1 & : D_{2n}/H \to \mathbb{C} \\
& \quad rH \mapsto 1 \\
& \quad sH \mapsto 1
\end{align*}
\]

\[
\begin{align*}
\bar{\phi}_2 & : D_{2n}/H \to \mathbb{C} \\
& \quad rH \mapsto 1 \\
& \quad sH \mapsto -1
\end{align*}
\]
Since \( \pi : D_{2n} \to D_{2n}/H, x \mapsto xH \) is a group homomorphism, then \( \phi_1 = \overline{\phi}_1 \circ \pi : D_{2n} \to \mathbb{C} \) and \( \phi_2 = \overline{\phi}_2 \circ \pi : D_{2n} \to \mathbb{C} \) are representations of \( D_{2n} \). These are given by

\[
\phi_1 : D_{2n} \to \mathbb{C} \\
\quad r \mapsto 1 \\
\quad s \mapsto 1
\]

\[
\phi_2 : D_{2n} \to \mathbb{C} \\
\quad r \mapsto 1 \\
\quad s \mapsto -1
\]

Corollary 3.3.3. If \( n \) is even, then \( D_{2n} \) has four degree 1 (irreducible) representations.

Proof. Let \( H = D_{2n}' = \langle r^2 \rangle \). By lemma 2 we know that \( D_{2n}/H \) is an abelian group of order 4. In fact \( D_{2n}/H = \{H, rH, sH, srH\} \). Since \( (srH)^2 = r^2H = H, (sH)^2 = s^2H = H \), and \( (srH)^2 = srsrH = ssr^{-1}rH = H \) we see that \( D_{2n}/H \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \). We find the following four representations of \( D_{2n}/H \):

\[
\bar{\phi}_1 : D_{2n}/H \to \mathbb{C} \\
\quad rH \mapsto 1 \\
\quad sH \mapsto 1
\]

\[
\bar{\phi}_2 : D_{2n}/H \to \mathbb{C} \\
\quad rH \mapsto 1 \\
\quad sH \mapsto -1
\]

\[
\bar{\phi}_3 : D_{2n}/H \to \mathbb{C} \\
\quad rH \mapsto -1 \\
\quad sH \mapsto 1
\]

\[
\bar{\phi}_4 : D_{2n}/H \to \mathbb{C} \\
\quad rH \mapsto -1 \\
\quad sH \mapsto -1
\]

Proceeding as we did in the example of \( D_8 \) in Section 2.3, we get the following degree 1 representations of \( D_{2n} \):

\[
\phi_1 : D_{2n} \to \mathbb{C} \\
\quad r \mapsto 1 \\
\quad s \mapsto 1
\]

\[
\phi_2 : D_{2n} \to \mathbb{C} \\
\quad r \mapsto 1 \\
\quad s \mapsto -1
\]

\[
\phi_3 : D_{2n} \to \mathbb{C} \\
\quad r \mapsto -1 \\
\quad s \mapsto 1
\]

\[
\phi_4 : D_{2n} \to \mathbb{C} \\
\quad r \mapsto -1 \\
\quad s \mapsto -1
\]
3.4 Irreducible Representations of $D_{2n}$

The goal of this last section, and indeed of this thesis is to prove the following theorem, and its analogue for when $n$ is odd:

**Theorem 3.4.1.** Let $D_{2n} = \langle r, s \vert r^n = s^2 = 1, rs = sr^{-1} \rangle$ such that $n = 2k, n \in \mathbb{Z}^+, k \geq 2$. Then the irreducible representations of $D_{2n}$ are given by the following:

\[ \phi_1 : D_{2n} \to \mathbb{C} \quad \phi_2 : D_{2n} \to \mathbb{C} \]
\[ r \mapsto 1 \quad r \mapsto 1 \]
\[ s \mapsto 1 \quad s \mapsto -1 \]

\[ \phi_3 : D_{2n} \to \mathbb{C} \quad \phi_4 : D_{2n} \to \mathbb{C} \]
\[ r \mapsto -1 \quad r \mapsto -1 \]
\[ s \mapsto 1 \quad s \mapsto -1 \]

and for all $1 \leq m \leq k - 1$

\[ \rho_m : D_{2n} \to GL_2(\mathbb{C}) \]
\[ r \mapsto \begin{pmatrix} e^{\frac{2m\pi i}{n}} & 0 \\ 0 & e^{-\frac{2m\pi i}{n}} \end{pmatrix} \]
\[ s \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \]

**Proof.** Note $\phi_1, \phi_2, \phi_3, \phi_4$ come from our analysis of commutator subgroup of $D_{2n}$ in the prior section. If we can show that all the $\rho_m$'s are irreducible and inequivalent then by Theorem 2.3.1 and Thereom 3.2.1 we have a list of $k + 3$ irreducible and inequivalent representations which means we have found them all since $D_{2n}$ has $k + 3$ conjugacy classes when $n$ is even. First we will show that $\rho_m$, for all $1 \leq m \leq k - 1$, is irreducible. We will use character theory to prove this. Let $\chi_m : D_{2n} \to \mathbb{C}$ be the character afforded by $\rho_m$. If we can show that $||\chi_m|| = 1$ then $\rho_m$ is irreducible by Proposition 2.4.3. We know that $e^{\frac{2m\pi i}{n}}$ and $e^{-\frac{2m\pi i}{n}}$ are $n^{th}$ roots of unity for all $1 \leq m \leq k - 1$ since
Let $\omega_m = e^{\frac{-2\pi i}{n}}$ and note that $\overline{\omega_m} \neq 1 \forall 1 \leq m \leq k - 1$. Before we proceed with the rest of this proof let us prove the following lemma.

**Lemma 3.4.1.** If $\omega \neq 1$ is an $n$th root of unity then $\omega^{n-1} + \cdots + \omega + 1 = \sum_{i=0}^{n-1} \omega^i = 0$.

**Proof.** For any $n$th root of unity $\omega$, we have the following:

$$\omega^n - 1 = 0 \Rightarrow (\omega - 1)(\omega^{n-1} + \cdots + \omega + 1) = 0.$$ 

Since $\omega \neq 1$ this implies that $\omega^{n-1} + \cdots + \omega + 1 = 0$. \hfill \Box

Since none of the $\omega_m$’s are equal to 1 then $\sum_{i=0}^{n-1} \omega_m^i = 0$. Also since $\omega_m^2 \neq 1 \Rightarrow \sum_{i=0}^{n-1} \omega^{2i} = 0$ for all $1 \leq m \leq k - 1$. We should also note that for all $1 \leq t \leq k$ we have that $\overline{\omega_m^t} = \omega_m^{n-t}$, and in particular $\overline{\omega_m^k} = \omega_m^k$.

Now let us examine the values of $\chi_m$ on the conjugacy classes of $D_{2n}$ by looking at the following table. The sizes of each class and the classes come from the Theorem 3.2.3.

<table>
<thead>
<tr>
<th>Conjugacy Class [a]</th>
<th>Size of Conj. Class</th>
<th>$\chi_m(a)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>[1]</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>[r]</td>
<td>2</td>
<td>$\omega_m + \overline{\omega_m}$</td>
</tr>
<tr>
<td>[r^2]</td>
<td>2</td>
<td>$\omega_m^2 + \overline{\omega_m^2}$</td>
</tr>
<tr>
<td>:</td>
<td>:</td>
<td>:</td>
</tr>
<tr>
<td>[r^{k-1}]</td>
<td>2</td>
<td>$\omega_m^{k-1} + \overline{\omega_m^{k-1}}$</td>
</tr>
<tr>
<td>[r^k]</td>
<td>1</td>
<td>$\omega_m^k + \overline{\omega_m^k}$</td>
</tr>
<tr>
<td>[s]</td>
<td>k</td>
<td>0</td>
</tr>
<tr>
<td>[sr]</td>
<td>k</td>
<td>0</td>
</tr>
</tbody>
</table>

The computations for $\chi_m(a)$ are simplified since the matrices associated to $r$ are diagonal. Let $d_i$ denote the size of the conjugacy class $[r^i] \forall 0 \leq i \leq k$. Computing the norm of $\chi_m$ we get
\[(\chi_m, \chi_m) = \frac{1}{2n} \left[ \sum_{j=0}^{k} (d_j \chi_m(r^j)^2) + k\chi_m(s)^2 + k\chi_m(sr)^2 \right] \]

\[= \frac{1}{2n} \left[ 2^2 + 2 \sum_{j=1}^{k-1} (\omega_m^j + \omega_m^{-j})^2 + \left( \omega_m^k + \omega_m^{-k} \right)^2 \right] \]

\[= \frac{1}{2n} \left[ 4 + 2 \sum_{j=1}^{k-1} (\omega_m^{2j} + \omega_m^{-2(n-j)}) + 2 \sum_{j=1}^{k-1} 2 + 4\omega_m^{2k} \right] \]

\[= \frac{1}{2n} \left[ 4 + 4(k-1) + 2 \sum_{j=1}^{k-1} \omega_m^{2j} + 2 \sum_{j=k+1}^{n-1} \omega_m^{2j} + 2 + 2\omega_m^{2k} \right] \]

\[= \frac{1}{2n} \left[ 4k + 2 \sum_{j=0}^{n-1} \omega_m^{2j} \right] \]

\[= \frac{1}{4k} (4k + 0) \]

\[= 1. \]

Thus, \( \rho_m \) is irreducible for all \( 1 \leq m \leq k-1 \). Finally, let us to show these representations are inequivalent. We know two representations are equivalent if and only if their characters are the same. Note that for all \( 1 \leq m \leq k-1 \).

\[\chi_m(r) = \omega_m + \omega_m^{-1} = e^{\frac{2mi\pi}{k}} + e^{-\frac{2mi\pi}{k}} = \cos\left(\frac{m\pi}{k}\right) + i\sin\left(\frac{m\pi}{k}\right) + \cos\left(\frac{m\pi}{k}\right) - i\sin\left(\frac{m\pi}{k}\right) = 2\cos\left(\frac{m\pi}{k}\right).\]

Since \( 1 \leq m \leq k-1 \) then \( 0 \leq \frac{\pi}{k} \leq \frac{m\pi}{k} \leq \frac{(k-1)\pi}{k} \leq \pi \) and since \( \cos x \) is one-to-one on the interval \((0, 2\pi)\) \( \Rightarrow \chi_m(r) \neq \chi_l(r) \) whenever \( m \neq l \) with \( 1 \leq m, l \leq k-1 \). Hence each of the \( \rho_m \)'s are inequivalent. This concludes the proof of our theorem.

\[\square\]

We state and now prove the case when \( n \) is odd.

**Theorem 3.4.2.** Let \( D_{2n} = \langle r, s \rangle | r^n = s^2 = 1, rs = sr^{-1} \rangle \) such that \( n = 2k + 1, n \in \mathbb{Z}^+, k \geq 1 \). Then the irreducible representations of \( D_{2n} \) are given by the following:
\[ \phi_1 : \ D_{2n} \to \mathbb{C} \quad \phi_2 : \ D_{2n} \to \mathbb{C} \]
\[ r \mapsto 1 \quad r \mapsto 1 \]
\[ s \mapsto 1 \quad s \mapsto -1 \]

and for all \( 1 \leq m \leq k \)

\[ \rho_m : \ D_{2n} \to GL_2(\mathbb{C}) \]
\[ r \mapsto \begin{pmatrix} e^{\frac{2m\pi i}{n}} & 0 \\ 0 & e^{-\frac{2m\pi i}{n}} \end{pmatrix} \]
\[ s \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \]

Proof. Again \( \phi_1, \phi_2 \) come from our analysis of commutator subgroup of \( D_{2n} \) in section 3.3. If we can show that all the \( \rho_m \)'s are irreducible and inequivalent then by Theorem 2.3.1 we have a list of \( k + 2 \) irreducible and inequivalent representations which means we have found them all since \( D_{2n} \) has \( k + 2 \) conjugacy classes when \( n \) is odd. First we will show that \( \rho_m \) is irreducible for all \( 1 \leq m \leq k \). Again we create a table that contains the conjugacy classes, sizes of conjugacy classes, and the value of \( \chi_m \), where \( \chi_m \) is the character associated to \( \rho_m \).

<table>
<thead>
<tr>
<th>Conjugacy Class</th>
<th>Size of Conj.</th>
<th>( \chi_m(a) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>([a])</td>
<td></td>
<td></td>
</tr>
<tr>
<td>([1])</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>([r])</td>
<td>2</td>
<td>( \omega_m + \overline{\omega}_m )</td>
</tr>
<tr>
<td>([r^2])</td>
<td>2</td>
<td>( \omega_m^2 + \overline{\omega}_m^2 )</td>
</tr>
<tr>
<td>(\vdots)</td>
<td>(\vdots)</td>
<td>(\vdots)</td>
</tr>
<tr>
<td>([r^k])</td>
<td>2</td>
<td>( \omega_m^k + \overline{\omega}_m^k )</td>
</tr>
<tr>
<td>([s])</td>
<td>(n)</td>
<td>0</td>
</tr>
</tbody>
</table>
Computing the norm of $\chi_m$ we get the following:

\[
(\chi_m, \chi_m) = \frac{1}{2n} \left[ \sum_{j=0}^{k} (d_j \chi_m(r_j)^2) + n\chi_m(s)^2 \right]
\]

\[
= \frac{1}{2n} \left[ \sum_{j=1}^{k} (\omega_m^j + \omega_m^{n-j})^2 \right]
\]

\[
= \frac{1}{2n} \left[ \sum_{j=1}^{k} (\omega_m^j + \omega_m^{n-j})^2 \right]
\]

\[
= \frac{1}{2n} \left[ 4 + 2 \sum_{j=1}^{k} (2 + 2\omega_m^{2j} + \omega_m^{2(n-j)}) \right]
\]

\[
= \frac{1}{2n} \left[ 4 + 4k + 2 \sum_{j=1}^{n-1} \omega_m^{2j} \right]
\]

\[
= \frac{1}{4k + 2} \left[ 4k + 2 + 2 \sum_{j=0}^{n-1} \omega_m^{2j} \right]
\]

Thus, $\rho_m$ is irreducible for all $1 \leq m \leq k$. Finally note again that for all $1 \leq m \leq k$.

\[
\chi_m(r) = 2 \cos(\frac{m\pi}{k}).
\]

Since $1 \leq m \leq k$ then $0 \leq \frac{m\pi}{k} \leq \frac{k\pi}{k} \leq \pi$ and since $\cos x$ is one-to-one on the interval $(0, 2\pi)$ $\Rightarrow \chi_m(r) \neq \chi_l(r)$ whenever $m \neq l$ with $1 \leq m, l \leq k$. Hence each of the $\rho_m$'s are inequivalent. \qed
Chapter 4

Conclusion

Having completed this project I am now interested in the representation theory over \( \mathbb{C} \) of other well known non-abelian groups that I have been introduced to in my studies. For example, the quaternion group defined by \( Q = \langle x, y : x^4 = 1, x^2 = y^2, y^{-1}xy = x^{-1} \rangle \), would be another relatively easy non-abelian group that I can study. I would probably start by finding the conjugacy classes in \( Q \) and the commutator of \( Q \) to mimic what I have learned from computing the representation theory of \( D_n \). I am also interested in finding the representation theory of \( S_n \), the symmetric group on a set of \( n \) elements. If \( A = \{1, 2, \ldots, n\} \) then the group \( S_n \) contains all the possible permutations of the set \( A \). We have results that describe the conjugacy classes of \( S_n \) and again I would try to compute the commutator subgroup of \( S_n \). In both of these examples I hope to be able to use character theory so that I can better understand its uses.

Yet another possibility would be to study the representations of these groups over other fields, especially finite fields. I would need to understand these fields and their algebraic closure to be able to use many of the results that I know thus far. Finally, I am interested in the applications of representation theory to other branches of learning.
Bibliography
