Burnside's Theorem

Julie Linman, Oregon State University
Advisor: Holly Swisher

April 2010

Contents

Chapter 1

Introduction

Just as prime numbers can be thought of as the building blocks of the natural numbers, in a similar fashion, simple groups may be considered the building blocks of finite groups. More precisely, every group G has a *composition series*, which is a series of subgroups

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_k = G,$$

such that G_{i+1}/G_i is simple for all $0 \leq i \leq k-1$, and the Jordan-Hölder Theorem states that any two composition series of a group G are equivalent. Therefore, the following goals naturally emerged in finite group theory:

1. Classify all finite simple groups.

2. Find all ways to construct other groups out of simple groups.

Toward the end of the 19th century, much of the research in finite group theory was related to the search for simple groups. Following the work of German mathematician Otto Hölder [15] and American mathematician Frank Nelson Cole [7], in 1895 English mathematician William Burnside found all simple groups of order less than or equal to 1092 [3]. However, it was Hölder's result, stating that a group whose order is the product of two or three primes is solvable [15], that prompted Burnside to consider the following questions:

1. Do there exist non-abelian simple groups of odd order?

2. Do there exist non-abelian simple groups whose orders are divisible by fewer than three distinct primes?

In 1904, Burnside answered question 2 when he used representation theory to prove that groups whose orders have exactly two prime divisors are solvable[4]. His proof is a clever application of representation theory, and while purely group-theoretic proofs do exist, they are longer and more difficult than Burnside's original proof. For more information on Burnside's work see [19]. The goal of this paper is to present a representation theoretic proof of Burnside's Theorem, providing sufficient background information in group theory and the representation theory of finite groups first, and then give a brief outline of a group theoretic proof.

In this paper we begin by reviewing some definitions and theorems from group theory in Chapter 2. In particular, we prove Lagrange's Theorem, the Class Equation, and the Isomorphism Theorems in Sections 2.2.1 and 2.2.2, which are necessary for the proofs of the results concerning solvable groups given in Section 2.2.3. In Chapter 3 we give an introduction to the representation theory of finite groups, beginning with a brief discussion of linear algebra and modules in Sections 3.1 and 3.2. Next, in Section 3.3 we define and give examples of representations of finite groups and prove that every representation can be decomposed uniquely into a direct sum of irreducible representations. In Section 3.4 we introduce characters and prove some results about characters that allow us to determine the specific irreducible representations of a group and the decomposition of a general representation into a direct sum of these irreducible representations. Moreover, we prove that the set of characters of irreducible representations of a finite group G form an orthonormal basis for the set of class functions on G. We will then present two proofs of Burnside's Theorem in Chapter 4. In Section 4.1 we give a proof that relies on results stated in Section 3.4, and in Section 4.2 we outline a purely group theoretic proof. We finish with some consequences of Burnside's Theorem in Chapter 5.

Chapter 2

Group Theory Background

2.1 Definitions

In this section we begin by reviewing some definitions and results from group theory. See [8] and [9] for an in-depth introduction to abstract algebra. Recall that a *group* is a nonempty set G with a binary operation $\cdot : G \times G \to G$ such that

1. $(g \cdot h) \cdot k = g \cdot (h \cdot k)$, for all $g, h, k \in G$.
2. There exists an element $1 \in G$, called the *identity* of G, which satisfies $g \cdot 1 = 1 \cdot g = g$, for all $g \in G$.
3. For each $g \in G$ there exists an element $g^{-1} \in G$, called the *inverse* of g, such that $g \cdot g^{-1} = g^{-1} \cdot g = 1$.

Moreover, a group G is called *abelian* if $g \cdot h = h \cdot g$, for all $g, h \in G$. The *order* of a group G, denoted $|G|$, is the cardinality of the set G, and a group is called *finite* is it has finite order. Note that when discussing an abstract group G, it is common to use juxtaposition to indicate the group's operation. Furthermore, if a group G has the operation $+$, we use the conventional notation of 0 for the identity element and $-g$ for the inverse of $g \in G$.

You are probably already familiar with several groups. For example, $\mathbb{Z}$, $\mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ are all groups under addition. These sets, however, are not groups under multiplication because the identity 0 does not have a multiplicative inverse. Yet, all nonzero elements in $\mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ have multiplicative inverses, so we can conclude that $\mathbb{Q} \setminus \{0\}, \mathbb{R} \setminus \{0\}$, and $\mathbb{C} \setminus \{0\}$ are groups under multiplication. In fact, all of the above examples of groups are abelian.

Example 2.1.1. For an example of a non-abelian group consider the set of all bijections of $\{1, \ldots, n\}$ to itself, where the *cycle* $(a_1 \ldots a_m)$ of length $m \leq n$ denotes the permutation that takes a_i to a_{i+1} for all $1 \leq i \leq m-1$, takes a_m to a_1, and fixes a_j for all $m+1 \leq j \leq n$. This set, denoted S_n, is a group of order $n!$ under function composition and is called the *symmetric group of degree* n. To see that S_n is not an abelian group for all $n > 2$, consider the permutations $(12), (23) \in S_n$. We see that $(12)(13) = (132)$, but $(13)(12) = (123) \neq (132)$.

A cycle of length 2 is called a *transposition*, and it turns out that every element of S_n can be written as a product of transpositions. Although this product might not be unique, the parity of the number of transpositions is, and therefore we say that $g \in S_n$ is an *odd* permutation if g is a product of an odd number of transpositions and an *even* permutation if g is a product of an even number of transpositions. Moreover, we define the *sign* of a permutation $g \in S_n$ to be

$$\operatorname{sgn}(g) = \begin{cases} -1 & \text{if g is an odd permutation} \\ 1 & \text{if g is an even permutation.} \end{cases}$$

A *subgroup* of a group G is a nonempty subset $H \subseteq G$ such that for all $h, k \in H$, $hk \in H$ and $h^{-1} \in H$, often denoted $H \leq G$. In fact, to determine whether a nonempty subset $H \subseteq G$ is a subgroup of G, it suffices to show that $gh^{-1} \in H$ for all $g, h \in H$. This is referred to as the *Subgroup Criterion* and it is an easy exercise to show that these two definitions of a subgroup are equivalent.

Example 2.1.2. For any $n \in \mathbb{N}$, consider the subset

$$n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\} \subseteq \mathbb{Z}.$$

Take any elements $x, y \in n\mathbb{Z}$. There exist $a, b \in \mathbb{Z}$ such that $x = na$ and $y = nb$. Therefore, $x - y = na - nb = n(a - b) \in n\mathbb{Z}$. Hence, by the Subgroup Criterion, $n\mathbb{Z} \leq \mathbb{Z}$.

A proper subgroup M of G is called *maximal* if the only subgroups of G containing M are M and G. A subgroup N of G is called *normal*, denoted $N \trianglelefteq G$, if for all $n \in N$, $g \in G$, we have that $gng^{-1} \in N$. Equivalently, $N \trianglelefteq G$ if

$$gNg^{-1} = N,$$

for all $g \in G$. Note that if G is abelian, then each subgroup of G is normal. However, while every group G has both itself and $\{1\}$ as normal subgroups, which are referred to as *trivial* subgroups, it is not necessarily true that G has any other normal subgroups. A group which has no nontrivial normal subgroups is called *simple*.

Example 2.1.3. The *alternating group of degree n*, denoted A_n, is the set of all even permutations in S_n. It turns out that A_n is a simple group for all $n \geq 5$ and A_5 is the smallest non-abelian simple group.

Several important subgroups can be generated given a nonempty subset A of a group G.

1. The *normalizer* of A in G is the subgroup of G defined by

$$N_G(A) = \{g \in G \mid gag^{-1} \in A, \text{ for all } a \in A\}.$$

2. The *centralizer* of a A in G is the subgroup

$$C_G(A) = \{g \in G \mid ga = ag, \text{ for all } a \in A\}.$$

3. Similarly, the *center* of G is the subgroup

$$Z(G) = \{g \in G \mid gx = xg, \text{ for all } x \in G\}.$$

Notice that $Z(G) = C_G(G)$ and $Z(G) \trianglelefteq G$.

4. Moreover, for every subset $A \subseteq G$, there exists a unique smallest subgroup of G containing A, namely the *subgroup of G generated by A*, defined by

$$\langle A \rangle = \bigcap_{\substack{A \subseteq H \\ H \leq G}} H,$$

or equivalently,

$$\langle A \rangle = \{a_1^{\epsilon_1} a_2^{\epsilon_2} \cdots a_n^{\epsilon_n} \mid n \in \mathbb{N}, a_i \in A, \epsilon_i = \pm 1\}.$$

A subgroup $H \leq G$ which is generated by a single element $g \in G$ is called *cyclic* and is written

$$H = \langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}.$$

The *order* of an element $g \in G$, denoted $|g|$, is the smallest positive integer n such that $g^n = 1$. If no such integer exists, then we say g has infinite order. As a consequence of the division algorithm, it is easy to see that if H is a cyclic group generated by $g \in G$, then $|H| = |g|$.

A group of order p^n, where $p \in \mathbb{N}$ is a prime and $n \in \mathbb{N}$, is called a *p-group*. Similarly, a subgroup of a group G which is itself a p-group is called a *p-subgroup*. Suppose G is a group of order $p^a m$, where p is a prime that does not divide m and $a \in \mathbb{N}$. A *Sylow p-subgroup* of G is a subgroup of order p^a. In fact, there exists at least one Sylow p-subgroup of G for each prime $p \in \mathbb{N}$ dividing $|G|$. A proof of this will be given in the following section.

Example 2.1.4. Consider the group S_3, which has order 6. S_3 has three Sylow 2-subgroups, $\langle(12)\rangle, \langle(23)\rangle$, and $\langle(13)\rangle$, and one Sylow 3-subgroup, $\langle(123)\rangle$.

For any subgroup N of G and any element $g \in G$, the set

$$gN = \{gn \mid n \in N\}$$

is called a *left coset* of N in G. We use G/N to denote the set of all left cosets of N in G, and the *index* of N in G, denoted $|G : N|$, is equal to the cardinality of G/N. We will see in the next section that the set of left cosets of N in G partition G and two cosets gN, $hN \in G/N$ are equal if and only if $h^{-1}g \in N$.

If N is a normal subgroup of G, then G/N forms a group called the *quotient group*, with the operation

$$gN \cdot hN = (gh)N.$$

Example 2.1.5. Consider the group $(\mathbb{Z}, +)$. Since this is an abelian group, all of its subgroups are normal. Therefore, for each $n \in \mathbb{N}, \mathbb{Z}/n\mathbb{Z}$ is a group. Let $g + n\mathbb{Z}$ and $h + n\mathbb{Z}$ be cosets in $\mathbb{Z}/n\mathbb{Z}$ such that $g + n\mathbb{Z} = h + n\mathbb{Z}$. Then it must hold that $g - h \in n\mathbb{Z}$, or in other words, $g \equiv h \pmod{n}$. Hence, $\mathbb{Z}/n\mathbb{Z}$ is the group of *integers modulo n* containing n distinct left cosets. In fact, $\mathbb{Z}/n\mathbb{Z}$ is cyclic and equal to $\langle 1 + n\mathbb{Z}\rangle$.

Let G and H be groups. A *(group) homomorphism* is a map $\phi : G \to H$ such that for all $g, h \in G$,

$$\phi(gh) = \phi(g)\phi(h).$$

The *kernel* of the map ϕ is the set

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

and the *image* of ϕ is the set

$$\phi(G) = \{h \in H \mid h = \phi(g) \text{ for some } g \in G\}.$$

A bijective homomorphism between two groups is called a *(group) isomorphism*. If the map $\phi : G \to H$ is an isomorphism, then G and H are said to be *isomorphic*, denoted $G \cong H$. In other words, G and H are the same group, up to relabeling of elements.

Example 2.1.6. Recall the groups $\mathbb{Z}$ and $n\mathbb{Z}$ under addition. For a fixed $n \in \mathbb{N}$, the map $\phi : \mathbb{Z} \to n\mathbb{Z}$ defined by $\phi(k) = nk$ is an isomorphism. The map $\psi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ defined by $\psi(k) = k + n\mathbb{Z}$ is also a homomorphism. However, ψ is not an isomorphism, since it is clearly not injective. Note that it is not necessary for two isomorphic groups to have the same operation. For example, the map $f : (\mathbb{R}, +) \to (\mathbb{R}^+, \times)$ defined by $f(x) = e^x$ is an isomorphism, since for all $x, y \in \mathbb{R}$, $e^{x+y} = e^x e^y$.

2.2 Important Results

Here we prove some important results from group theory, which are necessary for the proofs of Burnside's Theorem presented in Chapter 4.

2.2.1 Lagrange's Theorem and Consequences

We begin by proving Lagrange's Theorem, Cauchy's Theorem, and the Class Equation, which give us information about the order of a group and its subgroups. We will then use these results to prove the existence of Sylow p-subgroups, as mentioned in the previous section, and show that $Z(P)$ is nontrivial for all p-groups P. These results are all needed for the representation theoretic proof of Burnside's Theorem given in Section 4.1.

Theorem 2.2.1. *(Lagrange's Theorem) Let G be a finite group and $H \leq G$. Then $|H|$ divides $|G|$ and*

$$|G : H| = \frac{|G|}{|H|}.$$

Proof. Let G be a finite group and let $H \leq G$ such that $|H| = m$ and $|G : H| = k$. For any $g \in G$, define a map $\phi_g : H \to gH$ by $\phi_g(h) = gh$. This map is clearly surjective. Furthermore, for any distinct $h_1 \neq h_2 \in H$, we have that $gh_1 \neq gh_2$. Thus ϕ_g is a bijection, so $|gH| = |H| = m$.

It is easy to see that the set of left cosets of H in G form a partition of G. First note that for any $g \in G$, $g \in gH$. Thus, $G \subseteq \bigcup_{g \in G} gH$, and clearly $\bigcup_{g \in G} gH \subseteq G$. Therefore,

$$G = \bigcup_{g \in G} gH.$$

To show that left cosets are disjoint, suppose that for distinct cosets $g_1H \neq g_2H \in G/H$, there exists an element $x \in g_1H \cap g_2H$. Then there exist elements $h_1, h_2 \in H$ such that $x = g_1h_1 = g_2h_2$. Therefore, $g_1 = g_2h_2h_1^{-1}$, so for any $g_1h \in g_1H$,

$$g_1h = (g_2h_2h_1^{-1})h = g_2(h_2h_1^{-1}h) \in g_2H.$$

Hence, $g_1H \subseteq g_2H$. But we have seen that $|g_1H| = |g_2H|$, so $g_1H = g_2H$, which is a contradiction. Thus, the k left cosets of H in G are in fact disjoint and, hence, partition G. Since each has cardinality m, it follows that $|G| = km$. Therefore $|H|$ divides $|G|$ and $\frac{|G|}{|H|} = k$. $\square$

Corollary 2.2.2. *(Cauchy's Theorem) Let G be a finite abelian group, and let $p \in \mathbb{N}$ be a prime dividing $|G|$. Then G has an element of order p.*

Proof. We will perform induction of $|G|$. Take any nonidentity element $g \in G$. If $|G| = p$, then by Lagrange's Theorem, g has order p. Now assume that $|G| > p$ and that all subgroups of order less than $|G|$ whose orders are divisible by p have an element of order p.

First consider the case where p divides the order of g. Then we can write $|g| = np$, for some $n \in \mathbb{N}$. Thus, $1 = g^{np} = (g^n)^p$, so the order of g^n must divide p. But p is prime, so $|g^n| = p$.

So we now consider the case where p does not divide the order of g. Let $H = \langle g \rangle$, which is a normal subgroup of G, since G is abelian. By Lagrange's Theorem, $|G/H| < |G|$, since H is nontrivial. Moreover, it must hold that p divides $|G/H|$, because p divides $|G|$, but does not divide $|H|$. Hence, by induction, G/H contains an element of order p, say xH. We have that $x^p \in H$, but $x \notin H$, so $\langle x^p \rangle \neq \langle x \rangle$, giving that $|x^p| < |x|$. By Lagrange's Theorem, we find that $|x^p|$ divides $|x|$, so we have that p divides $|x|$. This brings us back to the previous case. So, by induction, G has an element of order p. $\square$

Let G be a group and X a set. A *group action* of G on X is a map $\cdot : G \times X \to X$ such that

1. $g \cdot (h \cdot x) = (gh) \cdot x$, for all $g, h \in G$, $x \in X$,
2. $1 \cdot x = x$, for all $x \in X$.

In fact, the action of a group G on a set X induces an equivalence relation $\sim$ on X, where we say that $x \sim y$ if there exists $g \in G$ such that $x = g \cdot y$. For $x \in X$, the *orbit* of G containing x is the equivalence class

$$[x] = \{g \cdot x \mid g \in G\}.$$

We can define a group action of G on itself by conjugation, i.e. for all $g, x \in G$,

$$g \cdot x = gxg^{-1}.$$

It is easy to check that this action satisfies the conditions above to be a group action. Moreover, the orbits of G with respect to this action are called the *conjugacy classes* of G.

Theorem 2.2.3. *(The Class Equation) Let G be a finite group, and let $g_1, g_2, \dots, g_n$ be representatives of the distinct conjugacy classes of G that are not contained in $Z(G)$. Then,*

$$|G| = |Z(G)| + \sum_{i=1}^{n} |G : C_G(g_i)|.$$

Proof. Let G be a finite group. By definition, if $z \in Z(G)$, then $gzg^{-1} = z$ for all $g \in G$, so $\{z\}$ is a conjugacy class of G containing a single element. Write $Z(G) = \{1, z_2, \dots, z_k\}$, and let $K_1, \dots, K_n$ denote the distinct conjugacy classes of G not contained in $Z(G)$ with respective representatives $g_1, g_2, \dots, g_n$. Since conjugation is a group action of G on itself, and thus induces an equivalence relation on G, the conjugacy classes partition G. Hence we have

$$|G| = \sum_{i=1}^{k} 1 + \sum_{i=1}^{n} |K_i| = |Z(G)| + \sum_{i=1}^{n} |K_i|.$$

For each $1 \leq i \leq n$, define a map $\phi_i : K_i \to G/C_G(g_i)$ by

$$\phi_i(gg_ig^{-1}) = gC_G(g_i).$$

Suppose that for some $g, h \in G$, $gg_ig^{-1} = hg_ih^{-1}$. Then $h^{-1}gg_ig^{-1}h = g_i$, so we have that $h^{-1}g \in C_G(g_i)$, which implies that $gC_G(g_i) = hC_G(g_i)$. Therefore, ϕ_i is well-defined. Now take any distinct elements $gg_ig^{-1} \neq hg_ih^{-1} \in K_i$. Then $h^{-1}gg_i \neq g_ih^{-1}g$, so $h^{-1}g \notin C_G(g_i)$. Thus, $gC_G(g_i) \neq hC_G(g_i)$, so we have that ϕ_i is injective. We can easily see that ϕ_i is also surjective, so $|K_i| = |G/C_G(g_i)| = |G : C_G(g_i)|$. Hence,

$$|G| = |Z(G)| + \sum_{i=1}^{n} |G : C_G(g_i)|.$$

□

Corollary 2.2.4. *(Sylow's Theorem) Let G be a group of order $p^a m$, where $a \in \mathbb{N}$ and $p \in \mathbb{N}$ is a prime that does not divide m. Then there exists a Sylow p-subgroup of G.*

Proof. We will perform induction on $|G|$. If $|G| = 1$, the result is trivial. Assume that Sylow p-subgroups exist for all groups of order less than $|G|$. First consider the case where p divides $|Z(G)|$. Since $Z(G)$ is an abelian group, then by Cauchy's Theorem, $Z(G)$ has a cyclic subgroup, N, of order p. So by Lagrange's Theorem, $|G/N| = p^{a-1}m$. Therefore, by induction, G/N has a Sylow p-subgroup, $\overline{P}$, of order p^{a-1}. By the Fourth Isomorphism

Theorem (given in the following section), there exists a subgroup $P \leq G$ containing N such that $\overline{P} = P/N$. Hence, by Lagrange's Theorem, $|P| = p^a$, so P is a Sylow p-subgroup of G.

Now consider the case where p does not divide $|Z(G)|$. By the Class Equation, we have that

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

where $g_1, g_2, \ldots, g_n$ are representatives of the distinct conjugacy classes of G that are not contained in $Z(G)$. It must hold that for some $1 \leq i \leq n$, $p \nmid |G : C_G(g_i)|$, so we have that $|C_G(g_i)| = p^a k$, for some $k \in \mathbb{N}$ with $p \nmid k$. Moreover, since $g_i \notin Z(G)$, then $C_G(g_i) \neq G$, so $|C_G(g_i)| < |G|$. Therefore, by induction, $C_G(g_i)$ has a Sylow p-subgroup, P, of order p^a, which is also a subgroup of G. Thus, P is a Sylow p-subgroup of G. $\square$

Corollary 2.2.5. *Let $p \in \mathbb{N}$ be prime and $a \in \mathbb{N}$. If P is a group of order p^a, then $Z(P) \neq 1$.*

Proof. Let P be a finite group of order p^a, where $p \in \mathbb{N}$ is prime and $a \in \mathbb{N}$. Let $g_1, g_2, \ldots, g_n$ be representatives of the distinct conjugacy classes of P that are not contained in $Z(P)$. By the Class Equation, we have that

$$|P| = |Z(P)| + \sum_{i=1}^{n} |P : C_P(g_i)|.$$

For each $1 \leq i \leq n, g_i \notin Z(P)$. Thus, $C_P(g_i) \neq P$, so $|P : C_P(g_i)| \neq 1$. By Lagrange's Theorem, p must divide $|P : C_P(g_i)|$. Therefore, p divides $\sum_{i=1}^{n} |P : C_P(g_i)|$, and since p divides $|P|$, then it must hold that p divides $|Z(P)|$. Therefore, $Z(P) \neq 1$. $\square$

2.2.2 The Isomorphism Theorems

In this section we will prove the Isomorphism Theorems for groups. These are fundamental results in group theory, which help us characterize the relationships between quotient groups and subgroups of a group G.

Theorem 2.2.6. *(The First Isomorphism Theorem) Let $\phi : G \to H$ be a group homomorphism, and let $K = \ker(\phi)$. Then*

$$G/K \cong \phi(G).$$

Proof. Let $\phi : G \to H$ be a group homomorphism, and let $K = \ker(\phi)$. For any $g \in G$ and $k \in K$, $gkg^{-1} \in K$, since

$$\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g^{-1}) = \phi(g)\phi(g^{-1}) = \phi(gg^{-1}) = \phi(1) = 1.$$

Thus, $K \trianglelefteq G$.

Define a map $\Phi : G/K \to \phi(G)$ by $\Phi(gK) = \phi(g)$. Take any cosets $gK, hK \in G/K$ such that $gK = hK$. Then $h^{-1}g \in K$, so $\phi(h^{-1}g) = 1$. Since ϕ is a homomorphism, then

$$\phi(h) = \phi(h)\phi(h^{-1}g) = \phi(h)\phi(h^{-1})\phi(g) = \phi(hh^{-1})\phi(g) = \phi(g).$$

Hence, $\Phi(gK) = \Phi(hK)$, so Φ is well-defined.

Take any cosets $gK, hK \in G/K$. Then, since ϕ is a homomorphism,

$$\Phi(gK \cdot hK) = \Phi(ghK) = \phi(gh) = \phi(g)\phi(h) = \Phi(gK)\Phi(hK).$$

Therefore, Φ is a homomorphism.

Now suppose that $\Phi(gK) = \Phi(hK)$ for some cosets $gK, hK \in G/K$. Then $\phi(g) = \phi(h)$. So, by a similar argument as above, $h^{-1}g \in K$, which implies that $gK = hK$. Thus, Φ is injective, and it is easy to see that Φ is surjective. Therefore, we can conclude that Φ is an isomorphism, so

$$G/K \cong \phi(G).$$

□

Theorem 2.2.7. *(The Second Isomorphism Theorem) Let A and B be subgroups of a group G, such that $A \leq N_G(B)$. Then $AB \leq G$, $B \trianglelefteq AB$, $A \cap B \trianglelefteq A$, and*

$$AB/B \cong A/(A \cap B).$$

Proof. Let A and B be subgroups of a group G, such that $A \leq N_G(B)$. Take any $a \in A$, $b \in B$. Since $A \leq N_G(B)$, then $aba^{-1} \in B$, so $ab = (aba^{-1})a \in BA$. Thus $AB \subseteq BA$. Likewise, we see that $ba = a(a^{-1}ba) \in AB$. Hence, $AB = BA$.

Now take any $x, y \in AB$, where $x = a_1b_1$ and $y = a_2b_2$, for some $a_1, a_2 \in A$, $b_1, b_2 \in B$. Then $xy^{-1} = a_1b_1b_2^{-1}a_2^{-1}$. Since $AB = BA$, then we have that $(b_1b_2^{-1})a_2^{-1} = a_3b_3$, for some $a_3 \in A$, $b_3 \in B$, so $xy^{-1} = a_1a_3b_3 \in AB$. Therefore, by the Subgroup Criterion, $AB \leq G$. Since A and B are both subgroups of $N_G(B)$, this argument can be used to show that $AB \leq N_G(B)$. Hence, $B \trianglelefteq AB$.

Define a map $\phi : A \to AB/B$ by $\phi(a) = aB$. The fact that ϕ is a homomorphism follows from the definition of the group operation in AB/B, and it is also easy to see that ϕ is surjective. Moreover, we see that $\ker(\phi) = \{a \in A \mid aB = B\} = A \cap B$. Thus, by the First Isomorphism Theorem, we have that $A \cap B \trianglelefteq A$ and

$$AB/B \cong A/(A \cap B).$$

□

Theorem 2.2.8. *(The Third Isomorphism Theorem) Let H and K be normal subgroups of a group G such that $H \leq K$. Then $K/H \trianglelefteq G/H$ and*

$$(G/H)/(K/H) \cong G/K.$$

Proof. Let H and K be normal subgroups of a group G such that $H \leq K$. Take any cosets $kH \in K/H$, $gH \in G/H$. Then $gH \cdot kH \cdot (gH)^{-1} = gkg^{-1}H \in K/H$, since $K \trianglelefteq G$. Therefore, $K/H \trianglelefteq G/H$.

Define a map $\phi : G/H \to G/K$ by $\phi(gH) = gK$. Take any cosets $g_1H, g_2H \in G/H$ such that $g_1H = g_2H$. Then $g_2^{-1}g_1 \in H$. Since $H \leq K$, then $g_2^{-1}g_1 \in K$. Hence, $g_1K = g_2K$, so ϕ is well-defined. It is easy to see that ϕ is a surjective homomorphism. Note that

$$\begin{aligned}
\ker(\phi) &= \{gH \in G/H \mid \phi(gH) = K\} \\
&= \{gH \in G/H \mid gK = K\} \\
&= \{gH \in G/H \mid g \in K\} \\
&= K/H.
\end{aligned}$$

So, by the First Isomorphism Theorem,

$$(G/H)/(K/H) \cong G/K.$$

□

Theorem 2.2.9. *(The Fourth Isomorphism Theorem) Let $N \trianglelefteq G$. Then there is a bijection between the set of subgroups A of G containing N and the set of subgroups A/N of G/N. Moreover, for all subgroups A, B of G containing N,*

1. *$A \leq B$ if and only if $A/N \leq B/N$.*
2. *If $A \leq B$, then $|B : A| = |B/N : A/N|$.*
3. *$\langle A, B\rangle/N = \langle A/N, B/N\rangle$.*
4. *$(A \cap B)/N = (A/N) \cap (B/N)$.*
5. *$A \trianglelefteq G$ if and only if $A/N \trianglelefteq G/N$.*

Proof. Let $N \trianglelefteq G$. Define a map $\phi : G \to G/N$ by $\phi(g) = gN$. Note that ϕ is clearly a homomorphism as a consequence of the definition of the group operation in G/N.

Let $A/N \leq G/N$. If we take any $a \in A$, then $\phi(a) = aN \in A/N$, so $A \subseteq \phi^{-1}(A/N)$. Similarly, if we take any $g \in \phi^{-1}(A/N)$, then $\phi(g) \in A/N$, so $g \in A$. Thus, $A = \phi^{-1}(A/N)$. Take any elements $g, h \in \phi^{-1}(A/N)$. Then

$$\phi(gh^{-1}) = \phi(g)\phi(h^{-1}) = \phi(g)(\phi(h))^{-1} \in A/N,$$

since $\phi(g), \phi(h) \in A/N$, so $gh^{-1} \in \phi^{-1}(A/N)$. Hence, by the Subgroup Criterion, $A \leq G$.

Conversely, let A be a subgroup of G containing N, and take any cosets $gN, hN \in \phi(A)$. Then

$$gN \cdot (hN)^{-1} = gN \cdot h^{-1}N = gh^{-1}N \in \phi(A),$$

since $gh^{-1} \in A$. Moreover, it is easy to see that $\phi(A) = A/N$. Thus, by the Subgroup Criterion, $A/N \leq G/N$.

Therefore, we can conclude that there is a bijection between the set of subgroups A of G containing N and the set of subgroups A/N of G/N. The remaining results follow directly as a consequence of this bijection, so their proofs will be omitted. □

2.2.3 Solvability

Burnside's Theorem tells us that a group whose order has exactly two prime divisors is solvable. Hence, in this section we will prove some results concerning solvable groups.

Definition 2.2.10. *A group G is* solvable *if it has a chain of subgroups*

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_k = G,$$

such that G_{i+1}/G_i is abelian for all $0 \leq i \leq k-1$.

Proposition 2.2.11. *Let G be a group and $N \trianglelefteq G$. If N and G/N are solvable, then G is solvable.*

Proof. Let G be a group and $N \trianglelefteq G$ such that N and G/N are solvable. Then there exist respective series of subgroups

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_k = N$$

and

$$1 = \overline{G_0} \trianglelefteq \overline{G_1} \trianglelefteq \cdots \trianglelefteq \overline{G_m} = G/N,$$

such that N_{j+1}/N_j and $\overline{G_{i+1}}/\overline{G_i}$ are abelian for all $0 \leq j \leq k-1$ and $0 \leq i \leq m-1$. By the Fourth Isomorphism Theorem, for each $\overline{G_i}$ there exists $G_i \leq G$ such that $N \trianglelefteq G_i$ and $\overline{G_i} = G_i/N$. Moreover,

$$\overline{G_i} \trianglelefteq \overline{G_{i+1}} \Leftrightarrow G_i \trianglelefteq G_{i+1},$$

for all $0 \leq i \leq m-1$, and by the Third Isomorphism Theorem,

$$\overline{G_{i+1}}/\overline{G_i} = (G_{i+1}/N)/(G_i/N) \cong G_{i+1}/G_i.$$

Therefore, G has the following chain of subgroups

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_k = N = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_m = G,$$

such that each quotient factor is abelian. Therefore, G is solvable. □

Corollary 2.2.12. *All p-groups are solvable.*

Proof. Let P be a p-group. We will induct on n, where $|P| = p^n$. If $|P| = p$, then P is cyclic. Therefore, P is abelian and, hence, solvable. Suppose that for all $1 \leq k < n$, groups of order p^k are solvable. Let $|P| = p^n$. By Corollary 2.2.5, $Z(P) \neq 1$. Thus, $|P/Z(P)| = p^k$ for some $k < n$. So, by the inductive hypothesis, $P/Z(P)$ is solvable. Since $Z(P)$ is abelian, then $Z(P)$ is solvable. Thus, by Lemma 2.2.11, P is solvable. Therefore, by induction, all p-groups are solvable. □

Chapter 3

Introduction to the Representation Theory of Finite Groups

Although Burnside's Theorem is group theoretic in nature, the proof presented in Section 4.1 uses results from representation theory. Over 50 years after this representation theoretic proof was given, proofs of the theorem that do not use representation theory were discovered, one of which we will outline in Section 4.2. Yet, as we will see, these group theoretic proofs are much more difficult, in the sense that they are longer and require a much stronger background in finite group theory. Thus, we will provide a brief introduction to the representation theory of finite groups in this chapter. See [8], [12], and [17] for a more complete introduction to this area.

3.1 Preliminary Definitions

First we will review some definitions. Recall that a *ring* is an additive abelian group $(R, +)$ with a multiplicative binary operation (often denoted by juxtaposition) such that

1. $r(st) = (rs)t$, for all $r, s, t \in R$.
2. $r(s + t) = rs + rt$, for all $r, s, t \in R$.

Moreover, a ring R is *commutative* if $rs = sr$, for all $r, s \in R$. If there exists an element $1 \in R$ such that $1r = r1 = r$, for all $r \in R$, then R is called a ring with *identity.* Note that in the context of rings, 0 is used to indicate the ring's additive identity, and for an element $r \in R$, the additive inverse is denoted $-r$.

Many of the examples of groups given in Section 2.1 are in fact rings. For example, $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are all commutative rings with identity. Additionally, given a ring R, it is possible to construct other rings from it.

Example 3.1.1. For any ring R and any $n \in \mathbb{N}$, the set of $n \times n$ matrices with entries in R forms a ring under matrix addition and multiplication, denoted $M_n(R)$. Note that if R is nontrivial, then $M_n(R)$ is not a commutative ring for any $n \geq 2$. However, if R has an identity element, then so does $M_n(R)$. The set of all invertible matrices in $M_n(R)$ is a subring of $M_n(R)$ called the *general linear group* of degree n over R and is denoted $GL_n(R)$.

Example 3.1.2. Let R be a ring with identity such that $0 \neq 1$, and let $G = \{g_1, \dots, g_n\}$ be any finite group. Then we can define the *group ring*

$$RG = \{a_1 g_1 + \ldots + a_n g_n \mid a_i \in R\}.$$

Here, addition is defined componentwise and multiplication is defined using distributive laws. The group ring RG is commutative if and only if G is abelian.

A *field* $\mathbb{F}$ is a commutative ring with identity such that each nonzero $x \in \mathbb{F}$ has a multiplicative inverse $x^{-1} \in \mathbb{F}$. Since $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$, and $\mathbb{C} \setminus \{0\}$ are all groups under multiplication, it is easy to see that in fact $\mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ are fields. Our other example, $\mathbb{Z}/n\mathbb{Z}$, is a field if and only if n is a prime number. For instance, the coset $2 + 4\mathbb{Z}$ does not have a multiplicative inverse in $\mathbb{Z}/4\mathbb{Z}$, so $\mathbb{Z}/4\mathbb{Z}$ is not a field.

Given a field $\mathbb{F}$, recall that a *vector space* V over $\mathbb{F}$ is an abelian group $(V, +)$ with scalar multiplication $\mathbb{F} \times V \to V$ such that

1. $(a + b)v = av + bv$, for all $a, b \in \mathbb{F}$, $v \in V$.

2. $(ab)v = a(bv)$, for all $a, b \in \mathbb{F}$, $v \in V$.

3. $a(v + w) = av + aw$, for all $a \in \mathbb{F}$, $v, w \in V$.

4. $1v = v$, for all $v \in V$.

A *basis* of a vector space V is a minimal spanning set for V, and the *dimension* of V, denoted $\dim(V)$, is defined to be the number of elements in a basis of V. See [14] for a proof of the Dimension Theorem, which states that the dimension of a vector space V is independent of the choice of basis for V.

Example 3.1.3. For example, if $\mathbb{F}$ is any field, then for all $n \in \mathbb{N}$,

$$\mathbb{F}^n = \{(a_1, \dots, a_n) \mid a_i \in \mathbb{F}\}$$

is an n-dimensional vector space over $\mathbb{F}$ with basis $\{e_1, \dots, e_n\}$, where $e_i = (0, \dots, 0, 1, 0, \dots, 0)$ is the element of $\mathbb{F}^n$ with the identity in the i^{th} component and zeros elsewhere.

Example 3.1.4. Not all vector spaces are finite dimensional. The set

$$\mathbb{F}[x] = \{a_n x^n + \ldots + a_1 x + a_0 \mid n \in \mathbb{N}, a_i \in \mathbb{F}\}$$

is an infinite dimensional vector space over $\mathbb{F}$. To see this, suppose that $\dim(\mathbb{F}[x]) < \infty$. Then $\mathbb{F}[x]$ has a finite basis, so there is an element in this basis of highest degree, say n. However, any polynomial of degree $n + 1$ can not be written in terms of this basis, which is a contradiction. Thus, we must have that $\dim(\mathbb{F}[x]) = \infty$.

Let V and W be any vector spaces over $\mathbb{F}$. A function $T : V \to W$ is called a *linear transformation* provided that

1. $T(v + w) = T(v) + T(w)$, for all $v, w \in V$.

2. $T(av) = aT(v)$, for all $v \in V$, $a \in \mathbb{F}$.

If V and W are both finite dimensional, say $\dim(V) = n$ and $\dim(W) = m$, then there exists a matrix $A \in M_{m\times n}(\mathbb{F})$ such that $T(v) = Av$, for all $v \in V$. Such a matrix A is called a *matrix representation* of the linear transformation T and depends on the bases chosen for V and W.

Now let V be a finite dimensional vector space. We define the *trace* of a linear transformation $T : V \to V$ to be the trace of any matrix representation of T. Recall that the trace of a square matrix is the sum of the elements on the diagonal and that similar matrices have the same trace.

An *eigenvalue* of a linear transformation $T : V \to V$ is a scalar $\lambda \in \mathbb{F}$ such that $T(v) = \lambda v$, for some nonzero $v \in V$. Such an element $v \in V$ is called an *eigenvector* of T corresponding to λ. The *characteristic polynomial* of T is the monic polynomial

$$f(x) = \det(xI - T),$$

where the determinant of a linear transformation T is defined to be the determinant of any matrix representation of T. Thus, the roots of the characteristic polynomial of T are the eigenvalues of T. Moreover, the *minimal polynomial* of T is the unique polynomial $p(x)$ satisfying

1. $p(x)$ is monic.

2. $p(T)$ is the 0 map.

3. If $f(T) = 0$ for some polynomial $f(x)$, then $p(x) \mid f(x)$.

Let V be an n-dimensional vector space and $T : V \to V$ be a linear transformation. If T has n distinct eigenvalues or, equivalently, if the minimal polynomial of T has n distinct roots, then there exists a basis of V such that the matrix representation of T is a diagonal matrix with these distinct eigenvalues on the diagonal. As a consequence, the trace of T is the sum of the eigenvalues of T. See [14] for a more in-depth discussion of diagonalizable matrices.

Example 3.1.5. We use $\mathrm{Hom}(V, W)$ to denote the set of all linear transformations from V to W. It is easy to check that $\mathrm{Hom}(V, W)$ is also a vector space over $\mathbb{F}$. If V and W are both finite dimensional, with $\dim(V) = n$ and $\dim(W) = m$, then we can define a map $\phi : \mathrm{Hom}(V, W) \to M_{m\times n}(\mathbb{F})$ taking a linear transformation to its matrix representation in terms of some fixed bases. The map ϕ is in fact an isomorphism, so we have that

$$\dim(\mathrm{Hom}(V, W)) = (\dim(V))(\dim(W)).$$

Example 3.1.6. Given a vector space V over $\mathbb{F}$, the *dual space* of V, denoted V^*, is the space $\mathrm{Hom}(V, \mathbb{F})$ and elements of V^* are called *linear functionals*. By the above argument, we have that

$$\dim(V^*) = \dim(V).$$

Moreover, if V is finite dimensional, then given a basis $\{v_1, \dots v_n\}$ of V we can define the *dual basis* $\{v_1^*, \dots, v_n^*\}$ of V^* by

$$v_i^*(v_j) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j. \end{cases}$$

Hence, there is a natural pairing between V and V^*, denoted $\langle \ , \ \rangle$, where $\langle v^*, w\rangle = v^*(w)$, for all $w \in V$, $v^* \in V^*$.

The dual space V^* will be useful in proving some results in the following sections.

3.2 Modules and Tensor Products

Before beginning our discussion of representations, it is necessary to introduce modules and tensor products.

Definition 3.2.1. *Similar to a vector space, given a ring R, a* left R-module *is an abelian group $(M, +)$ with an action $R \times M \to M$ such that*

1. *$(r + s)m = rm + sm$, for all $r, s \in R$, $m \in M$.*
2. *$(rs)m = r(sm)$, for all $r, s \in R$, $m \in M$.*
3. *$r(m + n) = rm + rn$, for all $r \in R$, $m, n \in M$.*
4. *If R has identity, then $1m = m$, for all $m \in M$.*

A *right R-module* is defined in a similar fashion, with the action $M \times R \to M$ defined by $m \cdot r := rm$. If R is commutative, then any left R-module is also a right R-module, and therefore we just refer to it as an R-module.

Example 3.2.2. Let G be any additive abelian group. Then we can think of G as a $\mathbb{Z}$-module by defining for any $n \in \mathbb{Z}$, $g \in G$,

$$ng = \begin{cases} g + g + \cdots + g (n \text{ times}) & \text{if } n > 0 \\ 0 & \text{if } n = 0 \\ -g - g - \cdots - g(-n \text{ times}) & \text{if } n < 0. \end{cases}$$

Example 3.2.3. An R-module F is called *free* on a subset $A \subseteq F$ if for all nonzero elements $x \in F$ there exist unique $a_1, \dots a_n \in A$ and unique $r_1, \dots r_n \in R \backslash \{0\}$ such that $x = \sum_{i=1}^n r_i a_i$, for some $n \in \mathbb{N}$. The set A is called a *basis* for F, and $|A|$ is called the *rank* of F. In fact, given any set A there exists a free R-module on A, denoted $F(A)$, consisting of all finite R-linear combinations of elements of A.

Example 3.2.4. If R is any ring with identity, then for all $n \in \mathbb{N}$,

$$R^n = \{(r_1, \ldots, r_n) \mid r_i \in R\}$$

is an R-module. In fact, R^n is a free R-module of rank n with basis $\{e_1, \ldots, e_n\}$, where $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ is the element of R^n with the identity in the i^{th} component and zeros elsewhere.

Definition 3.2.5. *Let R be any ring, M be a right R-module, N be a left R-module, and $F(M \times N)$ be the free $\mathbb{Z}$-module on $M \times N$. Define H to be the normal subgroup of $F(M \times N)$ generated by all elements of the form*

1. $(m_1 + m_2, n) - (m_1, n) - (m_2, n)$,
2. $(m, n_1 + n_2) - (m, n_1) - (m, n_2)$, *and*
3. $(mr, n) - (m, rn)$,

for $m, m_i \in M, n, n_i \in N, r \in R$. The tensor product *of M and N over R is the quotient group*

$$M \otimes_R N := F(M \times N)/H.$$

Elements of $M \otimes_R N$ of the form $m \otimes n = (m, n) + H$ are called simple tensors*, and in fact, each element of $M \otimes_R N$ can be written as a finite sum of simple tensors.*

As a direct consequence of the definition of $M \otimes_R N$, we have the following properties of tensors:

1. $(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n$,
2. $m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2$,
3. $mr \otimes n = m \otimes rn$, and

for all $m, m_i \in M, n, n_i \in N, r \in R$.

Example 3.2.6. Let $m, n \in \mathbb{N}$ with $d = \gcd(m, n)$. Then, we have that

$$\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/d\mathbb{Z}.$$

First, notice that $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}$ is a cyclic group generated by $1 \otimes 1$, since for any element $a \otimes b \in \mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}$, we can write

$$\begin{aligned} a \otimes b &= a \otimes (b \cdot 1) \\ &= ab \otimes 1 \\ &= ab \cdot 1 \otimes 1 \\ &= ab(1 \otimes 1). \end{aligned}$$

Moreover, the order of $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}$ divides d, since $m(1 \otimes 1) = m \otimes 1 = 0 \otimes 1 = 0$ and $n(1 \otimes 1) = 1 \otimes n = 1 \otimes 0 = 0$, implying that $d(1 \otimes 1) = 0$. Now define a map $\phi : \mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ by

$$\phi(a \otimes b) = ab \pmod{d},$$

and extend linearly to sums of simple tensors. Therefore, ϕ is a homomorphism. We have that $\phi(1 \otimes 1) = 1 \in \mathbb{Z}/d\mathbb{Z}$, which has order d, so $1 \otimes 1 \in \mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}$ has order at least d, giving that $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}$ has order at least d. Therefore, $|\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}| = d$, so ϕ is an isomorphism, i.e.

$$\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/d\mathbb{Z}.$$

Example 3.2.7. Let V and W vector spaces. Define a map $\phi : V^* \otimes W \to \mathrm{Hom}(V, W)$ by

$$\phi(v^* \otimes w) = f_{v^*,w},$$

where $f_{v^*,w}$ is the linear transformation $V \to W$ defined by $f_{v^*,w}(u) = v^*(u)w$. Since each element of $V \otimes W$ can be written as a sum of simple tensors, ϕ is clearly a homomorphism. Furthermore, suppose $v^* \otimes w \in \ker(\phi)$. Then, $f_{v^*,w}(u) = v^*(u)w = 0$ for all $u \in V$. If v^* is the 0-map, then $v^* \otimes w = 0 \otimes w = 0$. Now suppose $v^* \not\equiv 0$. Then, there is some $u \in V$ such that $v^*(u) \neq 0$. Hence, we must have that $w = 0$, so $v^* \otimes w = v^* \otimes 0 = 0$. Thus, $\ker(\phi) = 0$, so ϕ is injective. Since, $\dim(\mathrm{Hom}(V, W)) = \dim(V^* \otimes W)$, then we have that

$$\mathrm{Hom}(V, W) \cong V^* \otimes W.$$

3.3 Representations and Complete Reducibility

In this section we define a representation of a finite group. A representation associates each element of a group with an invertible matrix so that the group operation may be viewed as matrix multiplication. Studying group representations is motivated by the fact that it enables us to examine the structure of a group in the context of linear algebra. Note that all groups considered in the following sections are finite and that all vector spaces are over $\mathbb{C}$.

Definition 3.3.1. *Let G be a finite group and V be a finite dimensional vector space over $\mathbb{C}$. A* representation *of G on V is a homomorphism $\rho : G \to GL(V)$. For each $g \in G$, $\rho_g := \rho(g)$ is a linear transformation from V to V.*

Equivalently, $\rho : G \to GL(V)$ is a representation of G on V if and only if

$$g \cdot v := \rho_g(v)$$

defines a group action of G on V. Therefore, it is common to refer to V as a representation of G. Moreover, this makes V into a $\mathbb{C}[G]$-module with the action

$$\left(\sum z_i g_i\right) \cdot v = \sum z_i (g_i \cdot v),$$

for all $\sum z_i g_i \in \mathbb{C}[G]$, $v \in V$.

A *subrepresentation* of V is a subspace $W \subseteq V$ such that $g \cdot w \in W$, for all $g \in G$, $w \in W$, and a representation is called *irreducible* if it does not have any proper, nontrivial subrepresentations. Moreover, a linear transformation $\phi : V \to W$ is called a *G-linear map* provided that $\phi(gv) = g\phi(v)$, for all $g \in G$, $v \in V$.

Given representations V and W of a group G, we can use them to generate other representations of G. For instance, the *direct sum*

$$V \oplus W = \{v + w \mid v \in V, w \in W\}$$

and the tensor product $V \otimes W$ are representations of G with the respective actions

$$g \cdot (v + w) = gv + gw$$

and

$$g \cdot (v \otimes w) = gv \otimes gw,$$

for all $g \in G, v \in V, w \in W$. Additionally, V^* is a representation of G. To see this, define the dual representation of $\rho : G \to GL(V)$ to be $\rho^* : G \to GL(V^*)$ with

$$\rho_g^* = (\rho_{g^{-1}})^t,$$

for all $g \in G$. Note that this preserves the pairing described in Example 3.1.6, i.e.

$$\langle \rho_g^*(v^*), \rho_g(v)\rangle = \langle v^*, v\rangle.$$

Thus, as a consequence of Example 3.2.7, we have that $\operatorname{Hom}(V, W)$ is a representation of G, with the action

$$(g \cdot \phi)(v) = g\phi(g^{-1}v),$$

for all $g \in G, \phi \in \operatorname{Hom}(V, W)$.

Example 3.3.2. Let $U = \mathbb{C}$ and let G act trivially on U, i.e. $g \cdot u = u$ for all $g \in G, u \in U$. Then U is called the *trivial representation* of G and is clearly irreducible. The *regular representation* R of G is defined to be the vector space over $\mathbb{C}$ with basis $\{v_g \mid g \in G\}$, where G acts on R by

$$h \cdot \sum_{g \in G} z_g v_g = \sum_{g \in G} z_g v_{hg},$$

for all $h \in G, \sum_{g \in G} z_g v_g \in R$.

Example 3.3.3. Consider the *dihedral group* $D_8 = \{1, r, r^2, r^3, s, rs, rs^2, rs^3\}$, which is the group of symmetries of a square, where r denotes a counterclockwise rotation of $90°$ and s denotes a reflection across a line of symmetry. Therefore, D_8 has the following relations: $r^4 = 1, s^2 = 1$, and $(rs)^2 = 1$. Define matrices

$$R = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ and } S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

and define a function $\rho : D_8 \to GL_2(\mathbb{C})$ by

$$\rho(r^i s^j) = R^i S^j,$$

for $0 \leq i \leq 3, 0 \leq j \leq 2$. It is easy to check that ρ is a homomorphism and also that $R^4 = S^2 = (RS)^2 = I$. Thus, it follows that ρ is a 2-dimensional representation of D_8.

Proposition 3.3.4. *Let V be a representation of a group G, and let W be a subrepresentation of V. Then there exists a subrepresentation $W' \subseteq V$ such that $V = W \oplus W'$.*

Proof. Let V be a representation of G and W a subrepresentation of V. Then W is a subspace of the vector space V. Let $B_W = \{w_1, \ldots, w_r\}$ be a basis for W, and let $\dim(V) = n$. Then we know from linear algebra that B_W can be extended to a basis for V by adding on appropriate linearly independent vectors $\{u_1, \ldots, u_{n-r}\}$. Then $U = \text{span}\{u_1, \ldots, u_{n-r}\}$ is a subspace of V such that $V = W \oplus U$. See [14] for more on extending bases of vector spaces.

Let $\pi_0 : V \to W$ be the projection of V onto W, i.e. for any $v = w + u \in V$ written uniquely with $w \in W, u \in U$, we define

$$\pi_0(v) = w.$$

It is easily checked that π_0 is a linear transformation. Define a map $\pi : V \to W$ by

$$\pi(v) = \sum_{g \in G} g(\pi_0(g^{-1}v)).$$

Since π_0 is a linear transformation, then it follows from the properties of group actions that π is also a linear transformation. We claim that, in fact, π is a G-linear map. Take any $h \in G, v \in V$. Then by definition,

$$\pi(hv) = \sum_{g \in G} g(\pi_0(g^{-1}(hv))) = \sum_{g \in G} g(\pi_0(g^{-1}hv)).$$

Let $x = h^{-1}g$. Then $x^{-1} = g^{-1}h$ and $g = hx$. By recognizing that summing over all $x \in G$ is equivalent of summing over all $g \in G$, we see that

$$\pi(hv) = \sum_{x \in G} hx(\pi_0(x^{-1}v)) = h \sum_{x \in G} x(\pi_0(x^{-1}v)) = h\pi(v).$$

Therefore, π is G-linear. Moreover, for any $w \in W$,

$$\pi(w) = \sum_{g \in G} g(g^{-1}w) = \sum_{g \in G} w = |G|w.$$

Thus, $\pi\left(\frac{1}{|G|}w\right) = w$, so π is surjective.

Now let $W' = \ker(\pi)$, which is a subspace of V that is invariant under the action of G since π is G-linear. Therefore, by definition, W' is a subrepresentation of V. Furthermore, $W \cap W' = \{0\}$, so we can conclude that $V = W \oplus W'$. $\square$

Lemma 3.3.5. *(Schur's Lemma) Let V and W be irreducible representations of a group G, and let $\phi : V \to W$ be a G-linear map. Then*

1. *Either ϕ is an isomorphism or $\phi = 0$.*

2. *If $V = W$, then $\phi = zI$, for some $z \in \mathbb{C}$.*

Proof. For 1, let V and W be irreducible representations of G, and let $\phi : V \to W$ be a G-linear map. For any $g \in G$ and $v \in \ker(\phi)$, we have $gv \in \ker(\phi)$, since

$$\phi(gv) = g\phi(v) = g \cdot 0 = 0.$$

Therefore $\ker(\phi)$ is a subrepresentation of G, and since V is irreducible, either $\ker(\phi) = 0$ or $\ker(\phi) = V$. Similarly, $\phi(V)$ is a subrepresentation of W. Thus, either $\phi(V) = W$ or $\phi(V) = 0$. Therefore, either ϕ is an isomorphism or $\phi = 0$.

For 2, note that $\mathbb{C}$ is *algebraically closed*, i.e. every non-constant polynomial of one variable with coefficients in $\mathbb{C}$ has a root in $\mathbb{C}$. In particular, the characteristic polynomial of ϕ has roots in $\mathbb{C}$, so there exists $z \in \mathbb{C}$ such that $\ker(\phi - zI) \neq 0$. Therefore, by 1, $\ker(\phi - zI) = V$, so $\phi = zI$. □

Theorem 3.3.6. *(Complete Reducibility) Let V be a representation of a group G. Then V can be decomposed into a direct sum*

$$V = V_1^{\oplus a_1} \oplus \cdots \oplus V_k^{\oplus a_k},$$

such that each V_i is a distinct irreducible representation of G. This decomposition into k factors is unique, along with the V_i and their respective multiplicities a_i.

Proof. As a result of Proposition 3.3.4, any representation V of a group G can be written as a direct sum of irreducible representations. Let $V = V_1^{\oplus a_1} \oplus \cdots \oplus V_k^{\oplus a_k}$ be a decomposition of V into irreducible representations and suppose W is another representation of G with decomposition into irreducible representations $W = W_1^{\oplus b_1} \oplus \cdots \oplus W_m^{\oplus b_m}$.

Let $T : V \to W$ be a G-module homomorphism such that T is nonzero on the irreducible representation V_i. Then by Schur's Lemma, $T|_{V_i}(V) = W_j$ for some $1 \leq j \leq m$. Hence, $V_i \cong W_j$ and $a_i = b_j$. Now let $T : V \to V$ be the identity map. Then, by the above argument, the decomposition of V into irreducible representations must be unique. □

Complete reducibility should not be taken for granted, because it does not hold in general. In particular, this property fails when considering representations on vector spaces over finite fields. Since we have complete reducibility in the case of representations of finite groups on vector spaces over $\mathbb{C}$, then we can thoroughly understand the representation theory by understanding the irreducible representations. Hence, our goals are to:

1. Determine all of the irreducible representations of G.

2. Determine the multiplicities a_i in the decomposition $V = V_1^{\oplus a_1} \oplus \cdots \oplus V_k^{\oplus a_k}$ of an arbitrary representation V of G.

Example 3.3.7. Consider the group S_3. We know that the trivial representation U is an irreducible representation of S_3. However, this is not the only 1-dimensional irreducible representation of S_3. The *alternating representation* is the 1-dimensional vector space $U' = \mathbb{C}$ with the action

$$g \cdot u = \operatorname{sgn}(g)u,$$

for all $g \in S_3$, $u \in U'$. Recall that, as mentioned in Example 2.1.1,

$$\operatorname{sgn}(g) = \begin{cases} -1 & \text{if g is an odd permutation} \\ 1 & \text{if g is an even permutation.} \end{cases}$$

Consider the 3-dimensional vector space $\mathbb{C}^3$ with the action

$$g \cdot (z_1, z_2, z_3) = (z_{g^{-1}(1)}, z_{g^{-1}(2)}, z_{g^{-1}(3)}),$$

for all $g \in S_3, (z_1, z_2, z_3) \in \mathbb{C}^3$. This is called the *permutation representation* of S_3 and is not an irreducible representation, since it has $W = \operatorname{span}\{(1, 1, 1)\}$ as a subrepresentation. Define the 2-dimensional subspace V of $\mathbb{C}^3$ by

$$V = \{(z_1, z_2, z_3) \mid z_1 + z_2 + z_3 = 0\}.$$

Since V is invariant under the action of S_3, V is a subrepresentation of $\mathbb{C}^3$. Moreover, notice that $W \cap V = \{0\}$ and $\dim(\mathbb{C}^3) = \dim(W) + \dim(V)$, so $\mathbb{C}^3 = W \oplus V$. By Schur's Lemma, $W \cong U$, so in fact, $\mathbb{C}^3 = U \oplus V$. We will see in the next section that U, U', and V are the only irreducible representations of S_3.

3.4 Characters

One way to determine the structure of a representation ρ of a group G is to compute the eigenvalues of ρ_g for each $g \in G$. This, however, can be a long process, even for groups as small as S_3. In this section we will discuss a useful tool for describing all of the irreducible representations of a finite group and finding the decomposition of a representation into irreducible representations.

Definition 3.4.1. *Let $\rho : G \to GL(V)$ be a representation of G. The* character *of V is the function $\chi_V : G \to \mathbb{C}$ defined by $\chi_V(g) = \operatorname{tr}(\rho_g)$.*

A *class function* is a function on a group G that is constant on the conjugacy classes of G. Therefore, by properties of similar matrices, the character χ_V is a class function. Furthermore, since $1 \in G$ acts trivially on all elements of a representation V, then we have that $\chi_V(1) = \dim(V)$.

Proposition 3.4.2. *Let V be a representation of a group G. Then for all $g \in G$, $\chi_V(g)$ is a sum of $\chi_V(1)$ roots of unity.*

Proof. Let V be a representation of G with character χ_V. Fix an element $g \in G$. Since G is finite, then $|g| = k$, for some $k \in \mathbb{N}$. Hence, $(\rho_g)^k = \rho_{g^k} = \rho_1$, which is the identity map. Therefore, the minimal polynomial of ρ_g divides the polynomial $x^k - 1$, so the roots of the minimal polynomial of ρ_g are distinct kth roots of unity. Therefore, there is a basis of V such that the matrix representation of ρ_g is diagonal with kth roots of unity on the diagonal. Hence, $\chi_V(g)$ is the sum of $\chi_V(1)$ roots of unity. □

Proposition 3.4.3. *If V and W are representations of G, then*

1. $\chi_{V \oplus W} = \chi_V + \chi_W$.
2. $\chi_{V \otimes W} = \chi_V \chi_W$.
3. $\chi_{V^*} = \overline{\chi_V}$*, where the bar denotes complex conjugation.*

Proof. Fix an element $g \in G$. Let $\{\lambda_i\}$ and $\{\mu_j\}$ be the eigenvalues of the action of g on V and W, respectively. Suppose λ is an eigenvalue of the action of g on $V \oplus W$ with corresponding eigenvector $v + w$. Then

$$gv + gw = g \cdot (v + w) = \lambda(v + w) = \lambda v + \lambda w.$$

Hence, $gv = \lambda v$ and $gw = \lambda w$. It follows that either

1. $w = 0$ and $\lambda \in \{\lambda_i\}$,
2. $v = 0$ and $\lambda \in \{\mu_j\}$, or
3. $\lambda \in \{\lambda_i\} \cap \{\mu_j\}$.

Thus the eigenvalues of the action of g on $V \oplus W$ are $\{\lambda_i\} \cup \{\mu_j\}$. Similarly, the eigenvalues of the action of g on $V \otimes W$ are $\{\lambda_i \cdot \mu_j\}$

It follows from the pairing described in Example 3.1.6, that the eigenvalues of the action of g on V^* are $\{-\lambda_i\}$. However, since the eigenvalues $\{\lambda_i\}$ are all *nth* roots of unity, where $|g| = n$, then for each i, $-\lambda_i = \overline{\lambda_i}$.

The above formulas follow from the fact that the trace of a linear transformation is equal to the sum of its eigenvalues. □

Definition 3.4.4. *Let G be a group with irreducible representations $V_1, \ldots, V_k$ and let $g_1, \ldots, g_n$ be representatives of the distinct conjugacy classes of G. The* character table *of G is the table with the V_i along the left, the g_j across the top (with the number of elements in the respective conjugacy class $[g_j]$ above), and the boxes filled in with the values $\chi_{V_i}(g_j)$.*

Example 3.4.5. Consider the group S_3. Since the trivial representation U associates each group element with the 1×1 identity matrix, then the character χ_U takes the value 1 on all elements of S_3. Moreover, since $\dim(U') = 1$ and $\dim(V) = 2$, then $\chi_{U'}(1) = 1$ and $\chi_V(1) = 2$. Also, $\chi_{U'}((12)) = -1$ and $\chi_{U'}((123)) = 1$, because (12) and (123) are odd and even permutations, respectively. It remains to calculate the values of $\chi_V((12))$ and $\chi_V((123))$.

Recall the permutation representation $\mathbb{C}^3 = U \oplus V$. In terms of the standard bases, the linear transformation $\rho_{(12)} : \mathbb{C}^3 \to \mathbb{C}^3$ has matrix representation

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

so we see that $\chi_{\mathbb{C}^3}((12)) = 1$. Similarly, $\rho_{(123)} : \mathbb{C}^3 \to \mathbb{C}^3$ has matrix representation

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

and thus $\chi_{\mathbb{C}^3}((123)) = 0$. We know that $\chi_V = \chi_{\mathbb{C}^3} - \chi_U$, so it is easy to calculate that $\chi_V((12)) = 1 - 1 = 0$ and $\chi_V((123)) = 0 - 1 = -1$. Therefore, the character table of S_3 is:

	1	3	2
S_3	1	(12)	(123)
U	1	1	1
U'	1	-1	1
V	2	0	-1

Once we know the irreducible representations of a group, our next goal is to be able to describe every representation of the group as a direct sum of these irreducible representations. In order to accomplish this, we define an inner product on $\mathbb{C}_{class}(G)$, the set of class functions on G, by

$$\langle f, g \rangle = \frac{1}{|G|} \sum_{x \in G} \overline{f(x)} g(x).$$

This inner product is very useful, because it can be used to establish whether or not a representation is irreducible and to find the multiplicities a_i in the decomposition $V = V_1^{\oplus a_1} \oplus \cdots \oplus V_k^{\oplus a_k}$.

For any representations V and W of a group G, let $\mathrm{Hom_G}(V, W)$ denote the set of all G-linear maps $V \to W$. Moreover, define the set

$$V^G = \{v \in V \mid g \cdot v = v, \text{ for all } g \in G\}.$$

Note that if the decomposition of V into irreducible representations contains m copies of the trivial representation U, then $V^G = U^{\oplus m}$.

Lemma 3.4.6. *Let V and W be representations of a group G. Then*

$$\mathrm{Hom}(V, W)^G = \mathrm{Hom_G}(V, W),$$

and

$$\dim(\mathrm{Hom_G}(V, W)) = \begin{cases} 1 & \text{if } V \cong W \\ 0 & \text{if } V \ncong W. \end{cases}$$

Proof. Take any map $\phi \in \mathrm{Hom_G}(V, W)$ and any element $g \in G$. Since ϕ is G-linear, then for all $v \in V$,

$$\begin{aligned}(g \cdot \phi)(v) &= g\phi(g^{-1}v) \\ &= \phi(g(g^{-1}v)) \\ &= \phi((gg^{-1})v) \\ &= \phi(v).\end{aligned}$$

Therefore, $\phi \in \mathrm{Hom}(V, W)^G$, so $\mathrm{Hom_G}(V, W) \subseteq \mathrm{Hom}(V, W)^G$.

Now take any $\phi \in \mathrm{Hom}(V, W)^G$. Since ϕ is fixed under the action of G, then $g \cdot \phi = \phi$ for all $g \in G$. So for any $g \in G$,

$$\begin{aligned}g\phi(v) &= g\phi((g^{-1}g)v) \\ &= g\phi(g^{-1}(gv)) \\ &= g \cdot \phi(gv) \\ &= \phi(gv).\end{aligned}$$

Thus, $\phi \in \mathrm{Hom_G}(V, W)$, so we have that $\mathrm{Hom}(V, W)^G \subseteq \mathrm{Hom_G}(V, W)$. Therefore, $\mathrm{Hom}(V, W)^G = \mathrm{Hom_G}(V, W)$.

Now let V be an irreducible representation of G. If $\phi \in \mathrm{Hom}(V, W)^G$, then $\phi(V)$ is an irreducible subrepresentation of W. Therefore, by Schur's Lemma, the dimension of $\mathrm{Hom}(V, W)^G$ is equal to the multiplicity of V in W. Likewise, if W is an irreducible representation of G, then the dimension of $\mathrm{Hom}(V, W)^G$ is equal to the multiplicity of W in V. Hence, if V and W are both irreducible, then

$$\dim(\mathrm{Hom_G}(V, W)) = \begin{cases} 1 & \text{if } V \cong W \\ 0 & \text{if } V \ncong W. \end{cases}$$

□

Theorem 3.4.7. *Let V and W be irreducible representations of a group G. Then, in terms of the above inner product,*

$$\langle \chi_V, \chi_W \rangle = \begin{cases} 1 & \text{if } V \cong W \\ 0 & \text{if } V \ncong W. \end{cases}$$

Proof. Let V be an irreducible representation of G and define a map $\phi : V \to V^G$ by

$$\phi(v) = \frac{1}{|G|} \sum_{g \in G} g \cdot v.$$

By properties of group actions, ϕ is linear. Moreover, for any $h \in G$,

$$\phi(hv) = \frac{1}{|G|} \sum_{g \in G} g(hv) = \frac{1}{|G|} \sum_{g \in G} hgh^{-1}(hv) = \frac{1}{|G|} \sum_{g \in G} hg(h^{-1}hv) = h\frac{1}{|G|} \sum_{g \in G} g(v) = h\phi(v).$$

Thus, ϕ is G-linear.

Furthermore, take any $v \in \phi(V)$. Then there is some $w \in V$ such that

$$v = \phi(w) = \frac{1}{|G|} \sum_{g \in G} g(w).$$

. Then for any $h \in G$,

$$hv = \frac{1}{|G|} \sum_{g \in G} h(gw) = \frac{1}{|G|} \sum_{g \in G} hg(w) = \frac{1}{|G|} \sum_{g \in G} g(w) = v.$$

Therefore, $\phi(V) \subseteq V^G$. Moreover, for any $v \in V^G$,

$$\phi(v) = \frac{1}{|G|} \sum_{g \in G} v = v.$$

Thus, $\phi(V) = V^G$, so ϕ is a projection of V onto V^G.

Therefore, since the dimension of V^G is equal to the number of copies of the trivial representation U in the decomposition of V,

$$\dim(V^G) = \mathrm{tr}(\phi) = \frac{1}{|G|} \sum_{g \in G} \chi_V(g).$$

So, by Example 3.2.7 and Lemma 3.4.6,

$$\begin{aligned}
\dim(\mathrm{Hom_G}(V, W)) &= \dim(\mathrm{Hom}(V, W)^G) \\
&= \frac{1}{|G|} \sum_{g \in G} \chi_{\mathrm{Hom}(V,W)}(g) \\
&= \frac{1}{|G|} \sum_{g \in G} \chi_{V^* \otimes W}(g) \\
&= \frac{1}{|G|} \sum_{g \in G} \chi_{V^*}(g) \chi_W(g) \\
&= \frac{1}{|G|} \sum_{g \in G} \overline{\chi_V(g)} \chi_W(g) \\
&= \langle \chi_V, \chi_W \rangle.
\end{aligned}$$

Hence, if V and W are irreducible representations of G, then we can conclude that

$$\langle \chi_V, \chi_W \rangle = \begin{cases} 1 & \text{if } V \cong W \\ 0 & \text{if } V \ncong W. \end{cases}$$

□

As a consequence, a representation is uniquely determined by its character, because if $V = V_1^{\oplus a_1} \oplus \cdots \oplus V_k^{\oplus a_k}$ is the decomposition of V into irreducible representations, then $\chi_{V_1}, \ldots, \chi_{V_k}$ are linearly independent and $\chi_V = \sum_{i=1}^k a_i \chi_{V_i}$. Hence, the number of irreducible representations of a group G is less than or equal to the number of conjugacy classes of G. We also have the following results:

Corollary 3.4.8. *A representation V of a group G is irreducible if and only if $\langle \chi_V, \chi_V \rangle = 1$.*

Proof. Let $V = V_1^{\oplus a_1} \oplus \cdots \oplus V_k^{\oplus a_k}$ be the decomposition of V into irreducible representations of G. Then by Theorem 3.4.7,

$$\langle \chi_V, \chi_V \rangle = \left\langle \sum_{i=1}^k a_i \chi_{V_i}, \sum_{j=1}^k a_j \chi_{V_j} \right\rangle = \sum_{i=1}^k \sum_{j=1}^k a_i a_j \langle \chi_{V_i}, \chi_{V_j} \rangle = \sum_{i=1}^k a_i^2.$$

($\Rightarrow$) Suppose V is an irreducible representation of G. Then $V = V_i$ for some $1 \leq i \leq k$. So $\langle \chi_V, \chi_V \rangle = \langle \chi_{V_i}, \chi_{V_i} \rangle = 1$.

($\Leftarrow$) Conversely, suppose that $\langle \chi_V, \chi_V \rangle = 1$. Then, $a_i = 1$ for some $1 \leq i \leq k$, and $a_j = 0$ for all $j \neq i$. Hence, $V = V_i$ is irreducible. □

Corollary 3.4.9. *Let V be an irreducible representation of a group G. Then V^* is also an irreducible representation of G.*

Proof. By Proposition 3.4.3,

$$\begin{aligned} \langle V^*, V^* \rangle &= \frac{1}{|G|} \sum_{g \in G} \overline{\chi_{V^*}(g)} \chi_{V^*}(g) \\ &= \frac{1}{|G|} \sum_{g \in G} \chi_V(g) \overline{\chi_V(g)} \\ &= \frac{1}{|G|} \sum_{g \in G} \overline{\chi_V(g)} \chi_V(g) \\ &= \langle \chi_V, \chi_V \rangle \\ &= 1. \end{aligned}$$

Thus, by Corollary 3.4.8, V^* is irreducible. □

Example 3.4.10. Therefore, we can check that the representations U, U', and V of S_3 that we discussed earlier this section are in fact irreducible and distinct. From the character table of S_3 given in Example 3.4.5, we see that

$$\begin{aligned}
\langle \chi_U, \chi_U \rangle &= \frac{1}{6}(1 \cdot 1^2 + 3 \cdot 1^2 + 2 \cdot 1^2) = 1, \\
\langle \chi_{U'}, \chi_{U'} \rangle &= \frac{1}{6}(1 \cdot 1^2 + 3 \cdot (-1)^2 + 2 \cdot 1^2) = 1, \\
\langle \chi_V, \chi_V \rangle &= \frac{1}{6}(1 \cdot 2^2 + 3 \cdot 0^2 + 2 \cdot (-1)^2) = 1, \\
\langle \chi_U, \chi_{U'} \rangle &= \frac{1}{6}(1 \cdot 1 \cdot 1 + 3 \cdot 1 \cdot (-1) + 2 \cdot 1 \cdot 1) = 0, \\
\langle \chi_{U'}, \chi_V \rangle &= \frac{1}{6}(1 \cdot 1 \cdot 2 + 3 \cdot (-1) \cdot 0 + 2 \cdot 1 \cdot (-1)) = 0, \\
\langle \chi_U, \chi_V \rangle &= \frac{1}{6}(1 \cdot 1 \cdot 2 + 3 \cdot 1 \cdot 0 + 2 \cdot 1 \cdot (-1)) = 0.
\end{aligned}$$

So, U, U', and V are distinct irreducible representations, and since S_3 has three conjugacy classes, then these are the only irreducible representations of S_3.

Now that we can determine the irreducible representations of a group G, this next corollary gives us a way to compute the multiplicity a_i of an irreducible representation V_i in the decomposition $V = V_1^{\oplus a_1} \oplus \cdots \oplus V_k^{\oplus a_k}$.

Corollary 3.4.11. *Let V be a representation of a group G such that $V = V_1^{\oplus a_1} \oplus \cdots \oplus V_k^{\oplus a_k}$, where the V_i are distinct irreducible representations. Then*

$$\langle \chi_V, \chi_{V_i} \rangle = a_i,$$

for each $1 \leq i \leq k$.

Proof. Let $V = V_1^{\oplus a_1} \oplus \cdots \oplus V_k^{\oplus a_k}$ be a representation of G, where the V_i are distinct irreducible representations. Then, by Theorem 3.4.7,

$$\begin{aligned}
\langle \chi_V, \chi_{V_i} \rangle &= \frac{1}{|G|} \sum_{g \in G} \overline{\chi_V(g)} \chi_{V_i}(g) \\
&= \frac{1}{|G|} \sum_{g \in G} \overline{\left(\sum_{j=1}^{k} a_j \chi_{V_j}(g) \right)} \chi_{V_i}(g) \\
&= \frac{1}{|G|} \sum_{g \in G} \left(\sum_{j=1}^{k} a_j \overline{\chi_{V_j}(g)} \right) \chi_{V_i}(g) \\
&= \sum_{j=1}^{k} a_j \left(\frac{1}{|G|} \sum_{g \in G} \overline{\chi_{V_j}(g)} \chi_{V_i}(g) \right) \\
&= \sum_{j=1}^{k} a_j \langle \chi_{V_j}, \chi_{V_i} \rangle \\
&= a_i \langle \chi_{V_i}, \chi_{V_i} \rangle \\
&= a_i.
\end{aligned}$$

$\square$

Theorem 3.4.12. *Let $V_1, \dots, V_k$ be all of the irreducible representations of a group G. Then the characters $\{\chi_{V_1}, \dots, \chi_{V_k}\}$ form an orthonormal basis for $\mathbb{C}_{class}(G)$. Therefore, the number of irreducible representations of G is equal to the number of conjugacy classes of G.*

Proof. We already know that $\{\chi_{V_1}, \dots, \chi_{V_k}\}$ are linearly independent in $\mathbb{C}_{\text{class}}(G)$, so it remains to show that they span $\mathbb{C}_{\text{class}}(G)$. Suppose $\alpha \in \mathbb{C}_{\text{class}}(G)$ is such that $\langle \alpha, \chi_{V_i} \rangle = 0$ for all $1 \le i \le k$. Fix an irreducible representation V_i and define a map $\phi_{\alpha,V_i} : V_i \to V_i$ by

$$\phi_{\alpha,V_i} = \sum_{g \in G} \alpha(g) g.$$

Take any $h \in G$. Then, by substituting hgh^{-1} for g in the definition of $\phi_{\alpha,V_i}(hv)$, using properties of groups actions, and using the fact that α is a class function, we see that

$$\begin{aligned}
\phi_{\alpha,V_i}(hv) &= \sum_{g \in G} \alpha(g) g(hv) \\
&= \sum_{g \in G} \alpha(hgh^{-1}) hgh^{-1}(hv) \\
&= \sum_{g \in G} \alpha(hgh^{-1}) hg(h^{-1}hv) \\
&= h \sum_{g \in G} \alpha(hgh^{-1}) g(v) \\
&= h \sum_{g \in G} \alpha(g) g(v) \\
&= h\phi_{\alpha,V_i}(v).
\end{aligned}$$

Thus, ϕ_{α,V_i} is a G-linear map. Therefore, by Schur's Lemma, $\phi_{\alpha,V_i} = zI$ for some $z \in \mathbb{C}$. If we write $\dim(V_i) = n$, then $\operatorname{tr}(\phi_{\alpha,V_i}) = nz$, and since V^* is irreducible by Corollary 3.4.9, then

$$
\begin{aligned}
z &= \frac{1}{n}\operatorname{tr}(\phi_{\alpha,V_i}) \\
&= \frac{1}{n}\left(\sum_{g\in G}\alpha(g)\chi_{V_i}(g)\right) \\
&= \frac{1}{n}\left(\overline{\sum_{g\in G}\overline{\alpha(g)}\overline{\chi_{V_i}}(g)}\right) \\
&= \frac{1}{n}\left(\overline{\sum_{g\in G}\overline{\alpha(g)}\chi_{V_i^*}(g)}\right) \\
&= \frac{|G|}{n}\overline{\langle\alpha,\chi_{V_i^*}(g)\rangle} \\
&= \frac{|G|}{n}\cdot\overline{0} \\
&= 0.
\end{aligned}
$$

Therefore, ϕ_{α,V_i} is the 0-map for all irreducible representations V_i of G.

Recall the regular representation R with basis $\{v_g \mid g \in G\}$. We have that

$$
0 = \phi_{\alpha,V_i}(v_1) = \sum_{g\in G}\alpha(g)g\cdot v_1 = \sum_{g\in G}\alpha(g)v_g,
$$

so by the linear independence of the basis elements, $\alpha(g) = 0$ for all $g \in G$. So α is the 0-map, which implies that $\{\chi_{V_1},\ldots,\chi_{V_k}\}$ span $\mathbb{C}_{\text{class}}(G)$ and, therefore, form an orthonormal basis for $\mathbb{C}_{\text{class}}(G)$. □

Example 3.4.13. Note that the identity element of $1 \in G$ fixes all elements of the regular representation R, however no elements of R are fixed under the action of any nonidentity element of G. Therefore,

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

So, by Corollary 3.4.8, if G is a nontrivial group, then R is not an irreducible representation of G.

Proposition 3.4.14. *Let $V_1,\ldots,V_k$ be all of the distinct irreducible representations of a group G, and let R be the regular representation of G. Then*

$$
R = V_1^{\oplus \dim V_1} \oplus \cdots \oplus V_k^{\oplus \dim V_k}.
$$

Proof. By Corollary 3.4.11 and Example 3.4.13, if $R = V_1^{\oplus a_1} \oplus \cdots \oplus V_k^{\oplus a_k}$, then

$$\begin{aligned} a_i &= \langle \chi_R, \chi_{V_i} \rangle \\ &= \frac{1}{|G|} \sum_{g \in G} \overline{\chi_R(g)} \chi_{V_i}(g) \\ &= \frac{1}{|G|} \overline{\chi_R(1)} \chi_{V_i}(1) \\ &= \frac{1}{|G|} |G| \chi_{V_i}(1) \\ &= \chi_{V_i}(1) \\ &= \dim(V_i). \end{aligned}$$

Therefore any irreducible representation V_i of G appears in the decomposition of R $\dim(V_i)$ times, so

$$R = V_1^{\oplus \dim V_1} \oplus \cdots \oplus V_k^{\oplus \dim V_k}.$$

□

Example 3.4.15. Let R be the regular representation of the group S_3. By Example 3.4.10 we know that the irreducible representations of S_3 are U, U', and V. Thus, by Proposition 3.4.14,

$$R = U \oplus U' \oplus V \oplus V.$$

Corollary 3.4.16. *Let $V_1, \ldots, V_k$ be all of the distinct irreducible representations of a group G. Then*

$$|G| = \sum_{i=1}^{k} \dim(V_i)^2.$$

Proof. By Example 3.4.13 and Proposition 3.4.14,

$$|G| = \chi_R(1) = \sum_{i=1}^{k} \dim(V_i) \chi_{V_i}(1) = \sum_{i=1}^{k} \dim(V_i)^2.$$

□

Corollary 3.4.17. *For any nonidentity element $g \in G$,*

$$\sum_{i=1}^{k} \chi_{V_i}(1) \chi_{V_i}(g) = 0.$$

Proof. By Propositions 3.4.13 and 3.4.14, we have that

$$0 = \chi_R(g) = \sum_{i=1}^{k} \dim(V_i) \chi_{V_i}(g) = \sum_{i=1}^{k} \chi_{V_i}(1) \chi_{V_i}(g).$$

□

This Corollary will be used in the proof of Burnside's Theorem presented in the following section.

Chapter 4

Proofs of Burnside's Theorem

In this chapter we demonstrate two proofs of Burnside's Theorem:

Theorem. *Let $p, q \in \mathbb{N}$ be prime, and let a and b be nonnegative integers. If G is a group of order $p^a q^b$, then G is solvable.*

Burnside's Theorem was first proved by English mathematician William Burnside in 1904 [4]. While he is mainly known for his contributions to group theory, Burnside began his work in other areas of math, including elliptic functions and hydrodynamics. It was in 1893, as a Professor at the Royal Naval College in Greenwich, that Burnside published his first paper on group theory [2], and in 1897 he published the first edition of his book *Theory of Groups of Finite Order* [5].

As mentioned in the introduction, there were several mathematicians involved in the search for simple groups around this time, and many results about the orders of solvable groups emerged as a consequence. In 1892, German mathematician Otto Hölder showed that groups whose orders are the product of two or three distinct primes are solvable [15]. Soon after, German mathematician Ferdinand Georg Frobenius proved that groups whose orders are square-free are solvable. Additionally, he proved that for primes $p, q \in \mathbb{N}$ and nonnegative $a, b \in \mathbb{Z}$, groups of order $p^4 q^b$, where $p < q$, are solvable, and groups of order $p^a q$ are solvable [10].

Burnside was also producing similar results concerning solvable groups at this time. In 1897 he proved that groups of order $p^a q^2$ are solvable. Moreover, he showed that if G is a group of order $p^a q^b$ such that $a < 2m$, where $m \equiv \operatorname{ord}(p) \pmod{q}$, then G is solvable [5]. In 1902, Frobenius proved a similar result with the condition $a < 2m$ replaced by $a \leq 2m$ [11]. Then in 1904, Burnside published his representation theoretic proof of Lemma 4.1.2 [4], from which it easily follows that all groups of order $p^a q^b$ are solvable.

After decades of work, purely group theoretic proofs of Burnside's Theorem were discovered by American mathematician David Goldschmidt in 1970 [13], German mathematician Helmut Bender in 1972 [1], and Japanese mathematician Hiroshi Matsuyama in 1973 [18]. However, these proofs are significantly longer than Burnside's proof and require a much stronger background in the theory of finite groups. Therefore, we will simply give an outline of a group theoretic proof of Burnside's Theorem in Section 4.2. See [16] for a complete proof.

4.1 A Representation Theoretic Proof of Burnside's Theorem

For the first step in proving Burnside's Theorem, we give the following lemmas.

Lemma 4.1.1. *Let G be any group with a conjugacy class K and an irreducible representation $\rho : G \to GL(V)$ such that* $\gcd(|K|, \chi_V(1)) = 1$. *Then for all $g \in K$, either $\chi_V(g) = 0$ or $\rho_g = zI$, for some $z \in \mathbb{C}$.*

Proof. Let G be any group with a conjugacy class K and an n-dimensional irreducible representation $\rho : G \to GL(V)$ such that $\gcd(|K|, \chi_V(1)) = 1$. Then from elementary number theory, we know there exist $s, t \in \mathbb{Z}$ such that $s|K| + t\chi_V(1) = 1$. Take any $g \in K$. Multiplying both sides of this equations by $\chi_V(g)$ and dividing by $\chi_V(1)$ gives

$$\frac{s|K|\chi_V(g)}{\chi_V(1)} + t\chi_V(g) = \frac{\chi_V(g)}{\chi_V(1)}.$$

By Proposition 3.4.2, $\chi_V(g)$ is the sum of $\chi_V(1)$ roots of unity and is, thus, an *algebraic integer*, i.e. it is the root of a monic polynomial in $\mathbb{Z}$. Moreover, we claim that $\frac{|K|\chi_V(g)}{\chi_V(1)}$ is also an algebraic integer. See [8] for a proof of this and for more information on algebraic integers. As a consequence, we have that $\frac{\chi_V(g)}{\chi_V(1)}$ is an algebraic integer, call it α_1, and let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the *conjugates* of α_1 over $\mathbb{Q}$, i.e. the distinct roots of the minimal polynomial of α_1 over $\mathbb{Q}$. For each $1 \leq i \leq n$, α_i is the sum of $\chi_V(1)$ roots of unity divided by $\chi_V(1)$, so $|\alpha_i| \leq 1$. The constant term in the minimal polynomial of α_1 is $\pm \prod_{i=1}^n \alpha_i \in \mathbb{Z}$, so since each $|\alpha_i| \leq 1$, we have that

$$\left| \prod_{i=1}^n \alpha_i \right| = \prod_{i=1}^n |\alpha_i| \leq 1.$$

Thus, this product must be either 0 or ± 1. If $\prod_{i=1}^n \alpha_i = 0$, then we have that $\alpha_1 = 0$, so $\chi_V(g) = 0$.

Therefore, suppose that $\prod_{i=1}^n \alpha_i = \pm 1$. In this case we have that $|\alpha_1| = 1$. Thus, $|\chi_V(g)| = \chi_V(1) = n$. Since the minimal polynomial of ρ_g has n distinct roots, then there exists a basis B of V such that the matrix representation of ρ_g is a diagonal matrix

$$[T]_B = \begin{pmatrix} z_1 & & & \\ & z_2 & & \\ & & \ddots & \\ & & & z_n \end{pmatrix}.$$

Hence, we have that $\chi_V(g) = \sum_{i=1}^n z_i$. If $z_i \neq z_j$ for all $i \neq j$, then by the triangle inequality $|\chi_V(g)| = |\sum_{i=1}^n z_i| < \sum_{i=1}^n |z_i| = n = \chi_V(1)$. This is a contradiction, so it must hold that $z = z_i$ for all $1 \leq i \leq n$, and hence $\rho_g = zI$. □

Lemma 4.1.2. *Let G be a group with a nonidentity conjugacy class K such that $|K| = p^a$ for some prime $p \in \mathbb{N}$. Then G is not a non-abelian simple group.*

Proof. Suppose G is a non-abelian simple group with a nonidentity conjugacy class K such that $|K| = p^a$ for some prime $p \in \mathbb{N}$. Then, there exists a nonidentity element $g \in K$. If $a = 0$ then $K = \{g\}$ is a conjugacy class consisting of a single element. Therefore, for all $h \in G, hgh^{-1} = g$, so $g \in Z(G)$. This is a contradiction, since $Z(G) \trianglelefteq G$ and we assumed that G was non-abelian and simple. Therefore, we may assume that $a > 0$.

Let $\chi_1, \ldots, \chi_k$ be the characters of all of the distinct irreducible representations of G, such that χ_1 is the character of the trivial representation. By Proposition 3.4.17, we know that

$$0 = \sum_{i=1}^{k} \chi_i(1)\chi_i(g) = 1 + \sum_{i=2}^{k} \chi_i(1)\chi_i(g).$$

If $p|\chi_j(1)$ for all $j > 1$ such that $\chi_j(g) \neq 0$, then write $\chi_j(1) = pd_j$ to get that

$$0 = 1 + p \sum_{\substack{j>1 \\ \chi_j(g)\neq 0}} d_j\chi_j(g).$$

Therefore, $\sum_j d_j\chi_j(g) = -\frac{1}{p}$ is an algebraic integer, and is hence in $\mathbb{Z}$, which is a contradiction. So there exists some $2 \leq j \leq k$ such that $p \nmid \chi_j(1)$ and $\chi_j(g) \neq 0$.

Let $\rho : G \to GL(V)$ be the representation with character χ_j. Since $\gcd(|K|, \chi_j(1)) = 1$ and $\chi_j(g) \neq 0$, then by Lemma 4.1.1, $\rho_g = zI$, for some $z \in \mathbb{C}$. Thus, $\rho_g \in Z(\rho(G))$. Moreover, since we assumed that G is simple, $\ker(\rho)$ must be trivial. Therefore, ρ is injective. So for all $h \in G$,

$$\begin{aligned} & \rho_h\rho_g\rho_{h^{-1}} = \rho_g \\ \Rightarrow\ & \rho_{hgh^{-1}} = \rho_g \\ \Rightarrow\ & hgh^{-1} = g \\ \Rightarrow\ & g \in Z(G). \end{aligned}$$

This is a contradiction to G being a non-abelian simple group, so it must hold that G is not a non-abelian simple group. □

Now we are ready to prove Burnside's Theorem.

Proof. Let G be a group of order p^aq^b, where $p, q \in \mathbb{N}$ are prime and a and b are nonnegative integers. If $p = q$ or if either a or b is zero, then G is a p-group and is solvable by Corollary 2.2.12. So we can assume that $p \neq q$ and $a, b \in \mathbb{N}$.

Suppose G is of minimal order such that G is not solvable. If G is not a simple group, then G has a nontrivial normal subgroup N. However, by induction, both N and G/N are solvable, since their orders divide and are strictly less than $|G|$. Thus, by Lemma 2.2.11, G is solvable. Therefore, we may also assume that G is a non-abelian simple group.

Let P be a Sylow p-subgroup of G. Then $|P| = p^a$ and by Corollary 2.2.5, $Z(P) \neq 1$. Thus, there exists a nonidentity element $g \in Z(P)$, which implies that P is a subgroup of $C_G(g)$. As discussed in the proof of Theorem 2.2.3, the order of the conjugacy class of g is given by $|G : C_G(g)|$. However, since $p^a = |P| \leq |C_G(g)|$, then the order of the conjugacy class of g must be a power of q. This is a contradiction to Lemma 4.1.2. Therefore, G is solvable. □

4.2 A Group Theoretic Proof of Burnside's Theorem

The goal of this section is to give an outline of a group theoretic proof of Burnside's Theorem, so as to contrast it with the simplicity of the representation theoretic proof that was given in the previous section. This proof relies on a sequence of lemmas which, as mentioned in the beginning of this chapter, require a strong background in finite group theory. Therefore, we will omit the proofs of these lemmas, but they can be found in [16].

Proof. This proof begins in the same manner as the representation theoretic proof. Let G be a finite group of order $p^a q^b$, where $p, q \in \mathbb{N}$ are prime and a and b are nonnegative integers. As shown in the previous section, we can assume that $p \neq q$, $a, b \in \mathbb{N}$, and that G is simple. Now suppose that G is of minimal order such that G is not solvable. The first step in the proof is to prove the following lemma.

Lemma 4.2.1. *If P is a Sylow p-subgroup of G, then P does not normalize any nontrivial q-subgroup of G.*

Before proceeding, we need a few more definitions. Let G by any group. Define subgroups $Z_0(G) = 1$ and $Z_1(G) = Z(G)$, and then inductively define $Z_{i+1}(G)$ to be the subgroup of G containing $Z_i(G)$, such that $Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$. The group G is called *nilpotent* if $Z_k(G) = G$ for some $k \in \mathbb{N}$. The *Fitting subgroup* of G, denoted $F(G)$, is the unique largest normal nilpotent subgroup of G. Lemma 4.2.1 is used to prove the following result about the Fitting subgroup of a maximal subgroup of G.

Lemma 4.2.2. *If M is a maximal subgroup of G, then $F(M)$ is of prime-power order.*

As a consequence, we get this next result.

Lemma 4.2.3. *If P is a Sylow p-subgroup and $x \in Z(P)\backslash\{1\}$, then x does not normalize any nontrivial q-subgroup of G.*

Again, it is necessary to give some more definitions. Let G be any finite group and let $p \in \mathbb{N}$ be prime. The *p-core* of G, denoted $O_p(G)$, is the largest normal p-subgroup of G. Now let P be any p-group. Then $\Omega_1(P)$ is defined to be the subgroup of P generated by all elements of P of order dividing p. As a result of Lemmas 4.2.2 and 4.2.3, the subsequent lemmas follow.

Lemma 4.2.4.

1. *$|G|$ is odd.*
2. *If B is a p-subgroup of G, then $O_q(N_G(B)) = 1$ and $O_q(C_G(B)) = 1$.*
3. *If B is a nonidentity p-subgroup of G, then $C_G(\Omega_1(Z(O_p(C_G(B)))))$ is a p-group.*

Lemma 4.2.5. *Suppose $q < p$. If D is a nonidentity q-subgroup of G, the Sylow p-subgroups of $N_G(D)$ are cyclic.*

Now let $p \in \mathbb{N}$ be prime and let G be an abelian group such that every nonidentity element of G has order p. Then G is called an *elementary abelian* group. Let P be any p-group. Then, $J_e(P)$ is defined to be the subgroup of P generated by all elementary abelian subgroups of P which are of order as large as possible. As a consequence of the preceding lemma, we get the following result about the subgroup $J_e(P)$.

Lemma 4.2.6. *Suppose M is a maximal subgroup of G, $O_q(M) = 1$, and P is a Sylow p-subgroup of M. Then $M = N_G(J_e(P))$ and P is a Sylow p-subgroup of G.*

For any element $g \in G$ and any subgroup H of G, define $H^g = gHg^{-1}$. By Lemmas 4.2.3 and 4.2.6, we obtain these last two results necessary for the proof.

Lemma 4.2.7. *Let M be a maximal subgroup of G. If $O_q(M) = 1$, then $M \cap M^g$ is a q-group for any $g \in G \backslash M$.*

Lemma 4.2.8. *If P is a Sylow p-subgroup of G, then $|P|^2 \leq |G|$.*

By our hypotheses, $|G| = p^a q^b$, where $p, q \in \mathbb{N}$ are distinct primes and $a, b \in \mathbb{N}$. Let P be a Sylow p-subgroup of G, and let Q be a Sylow q-subgroup of G. Then $|P| = p^a$ and $|Q| = q^b$. Without loss of generality, suppose $p^a < q^b$. Then,

$$|G| = p^a q^b < (q^b)^2 = |Q|^2.$$

This contradicts Lemma 4.2.8, so it must hold that G is solvable. $\square$

Chapter 5

Conclusion

Burnside's Theorem played a significant role in the classification of finite simple groups, which was a huge project involving hundreds of mathematicians that took over three decades. The classification was completed in 1980, when the following result, often referred to as the "enormous theorem," was proved.

Theorem. *Every finite simple group is one of the following (up to isomorphism):*

1. *A cyclic group of prime order.*
2. *An alternating group of degree greater than or equal to 5.*
3. *In one of the 16 families of groups of Lie type.*
4. *One of 26 sporadic simple groups.*

All together, the papers comprising the proof of this theorem total over 5,000 pages. The reason that Burnside's Theorem was important in the classification of finite simple groups is because of the following corollary.

Corollary. *Let G be a non-abelian finite simple group. Then $|G|$ is divisible by at least three distinct primes.*

As a consequence, in the second edition of his book *Theory of Groups of Finite Order*, Burnside made the following conjecture [6].

Conjecture. *Let G be a non-abelian finite simple group. Then $|G|$ is even.*

Over 50 years later, this conjecture was eventually proved in 1963 by American mathematicians Walter Feit and John Griggs Thompson when they proved the celebrated Feit-Thompson Theorem [20].

Theorem. *(Feit-Thompson Theorem) Let G be a finite group of odd order. Then G is solvable.*

The proof of this theorem is 255 pages and very complicated. It was a significant step in the classification of finite simple groups and established several new techniques that were later used in the classification.

Bibliography

[1] H. Bender, A group theoretic proof of the $p^\alpha q^\beta$ theorem. *Math. Z.*, 126 (1972), 327-338.

[2] W. Burnside, Notes on the theory of groups of finite order, *Proc. London Math. Soc.*, 25 (1893-94), 9-18.

[3] W. Burnside, Notes on the theory of groups of finite order, *Proc. London Math. Soc.*, 26 (1894-95), 325-338.

[4] W. Burnside, On groups of order $p^\alpha q^\beta$, *Proc. London Math Soc.* (2), 1 (1904), 388-391.

[5] W. Burnside, *Theory of Groups of Finite Order*, Cambridge University Press, 1897.

[6] W. Burnside, *Theory of Groups of Finite Order*, Second Edition, Cambridge University Press, 1911; reprinted by Dover Publications, New York, NY, 1955.

[7] F.N. Cole, Simple groups as far as order 660, *Amer. J. Math.*, 15 (1893), 303-315.

[8] D.S. Dummit and R.M. Foote, *Abstract Algebra, Third Edition*, Jonh Wiley and Sons, Inc., Hoboken, NJ, 2004.

[9] J.B. Fraleigh, *A First Course in Abstract Algebra, Third Edition*, Addison-Wesley Publishing Company, Inc., Menlo Park, CA, 1982.

[10] G. Frobenius, Über auflösbare Gruppen, *Sitzungsber. Kön. Preuss. Akad. Wiss. Berlin*, (1893), 337-345.

[11] G. Frobenius, Über Gruppen der Ordnung $p^\alpha q^\beta$, *Acta Math.*, 26 (1902), 189-198.

[12] W. Fulton and J. Harris, *Representation Theory, A First Course*, Springer Science+Business Media, LLC., New York, NY, 2004.

[13] D. Goldschmidt, A group-theoretic proof of the $p^a q^b$ theorem for odd primes, *Math. Z.*, 113 (1970), 373-375.

[14] K. Hoffman and R. Kunze, *Linear Algebra*, Prentice-Hall, Inc., Englewood Cliff, NJ, 1971.

[15] O. Hölder, Die einfachen Gruppen im ersten und zweiten Hundert der Ordnungszahlen, *Math. Annalen*, 40 (1892), 55-88.

[16] B. Huppert and N. Blackburn, *Finite Groups III*, Springer-Verlag, New York, 1982.

[17] G. James and M. Liebeck, *Representations and Characters of Groups, Second Edition*, Cambridge University Press, New York, NY, 2001.

[18] H. Matsuyama, Solvability of groups of order $2^a q^b$, *Osaka J. Math.*, 10 (1973), 375-378.

[19] P.M. Neumann, A.J.S. Mann, and J.C. Tompson, *The Collected Papers of William Burnside, Volume I*, Oxford University Press, Inc., New York, NY, 2004.

[20] J.G. Thompson and W. Feit, Solvablity of groups of odd order, *Pacific Journal of Mathematics*, 13 (1963), 775-1029.