CLASSIFICATION OF FINITE GROUPS

YANNIS WU-YIP

Abstract. We introduce group actions and prove the four Sylow Theorems. We then introduce direct products and prove the main theorem of finitely generated abelian groups. We use the Sylow Theorems and the fundamental theorem of finitely generated abelian groups to examine classification problems of finite groups. Some knowledge of group theory is assumed.

Contents

1. Introduction

We assume basic knowledge in group theory. In particular, we assume that the reader is familiar with notions like subgroups, orders, (left) cosets, normal groups, and conjugates. Here we provide the statements of important theorems and propositions that are assumed for the paper. The proofs of these statements can be found in chapters 4, 5, and 7 of [2].

Proposition 1.1 (Subgroup Test)**.** *Let G be a group. Then H is a subgroup of G if and only if H satisfies the following conditions:*

(1) $e_G \in H$.
(2) If $x, y \in H$, then $xy^{-1} \in H$.

Theorem 1.2 (Lagrange Theorem)**.** *Let G be a group with a finite number of elements and H be a subgroup of G. Then the number of distinct left cosets of H in G is $|G : H| = \frac{|G|}{|H|}$. In particular, $|H|\big||G|$ and $|G : H|\big||G|$.*

Definition 1.3. Let A and B be subgroups of G. Then AB is the set of elements of the form ab, with $a \in A$ and $b \in B$.

Corollary 1.4. *Let A and B be finite subgroups of G. Then $|AB| = \frac{|A||B|}{|A \cap B|}$.*

Definition 1.5. Let A and B be subgroups of G. Then $\langle A, B\rangle$ is the set of elements that are in the span of A and B. In this case, $\langle A, B\rangle = A \cup B \cup AB \cup BA$.

Proposition 1.6. *Let N be a normal subgroup of G and H be a subgroup of G. Then $\langle N, H\rangle = NH$ and $HN = NH$.*

Proposition 1.7. *Conjugate elements have the same order.*

Theorem 1.8 (Fourth Isomorphism Theorem)**.** *Let N be a normal subgroup of G. Then every subgroup of G/N is of the form H/N for some subgroup H of G with N also a subgroup of H. Conversely, if H is a subgroup of G and H contains N, then H/N is a subgroup of G/N.*

Thus there is a bijection between subgroups of G/N and subgroups of G containing N. Moreover, the correspondence between the normal subgroups of G/N and the normal subgroups of G containing N is also a bijection.

The majority of statements and proofs in Sections 1-3 and 6 follow from [2] and those in Sections 4-5 follow from [1].

2. Group Actions and the Orbit-Stabilizer Theorem

Definition 2.1. Let G be a group and X be a set. A *(left) group action* is a map $\cdot : G \times X \to X$ satisfying the following properties:

(1) For all $x \in X$, $e_G \cdot x = x$.
(2) For all $g_1, g_2 \in G$ and any $x \in X$, $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$.

In this case, we say that G acts on X from the left and that X is a *G-set*.

Example 2.2. Here we consider two examples of group actions which will appear again in later proofs:

(1) Let X be the set of all subsets of G and $H \in X$ be some subset of G. For some $g \in G$, we define $g \cdot H = gH$, so that g and H are mapped to the set gH in X. We can easily check the properties in Definition 2.1 to verify that this is a group action.
(2) Let X be the set of all subgroups of G. For any $H \in X$ and $g \in G$, we define $g \cdot H = gHg^{-1}$, so that g conjugates H. Again, one can verify that the conjugation action is indeed a group action.

Definition 2.3. Let X be a G-set. For any element $x \in X$, the *stabilizer* G_x is the set of elements $g \in G$ that fix x under the group action:

$$G_x = \{g \in G : g \cdot x = x\}.$$

By applying the subgroup test (Proposition 1.1), it can be easily shown that the stabilizer set G_x is in fact a subgroup of G.

Example 2.4. Continuing from Example 2.2, we examine the stabilizers of each group action.

(1) In order for $g \cdot H = gH = H$ to be true, we must have that $g \in H$. So the stabilizer of H is the set $\{g \in G : gH = H\}$. In the special case that H is a subgroup of G, we have that $G_H = H$.
(2) In the case of the conjugation action on a subgroup of G, the stabilizer is called the normalizer, which we define as follows:

Definition 2.5. The *normalizer* $N_G(H)$ is defined by the set $\{g \in G : gHg^{-1} = H\}$ or equivalently, $\{g \in G : gH = Hg\}$.

From this definition three important facts follow:

(1) $N_G(H)$ is a subgroup of G.
(2) $N_G(H) \supseteq H$.
(3) $H \trianglelefteq G$ if and only if $N_G(H) = G$.

Given a group G and an element $x \in X$, it is natural to ask about the properties of the set consisting of elements of the form $g \cdot x$, which we call the orbit of x. To formally introduce the concept of an orbit, we must first consider the following proposition.

Proposition 2.6. *Let G be a group and X be a G-set. For $x, y \in X$, define the relation xRy if and only if there exists $g \in G$ such that $y = g \cdot x$. Then R is an equivalence relation.*

Proof. We can show that R is an equivalence relation by checking that it is (1) reflexive, (2) symmetric, and (3) transitive.

(1) By the first property of Definition 2.1, we have that $e_G \cdot x = x$, so xRx.
(2) Suppose that xRy. Then $y = g \cdot x$ for some $g \in G$. Using the second property of Definition 2.1, we have that $g^{-1} \cdot y = g^{-1} \cdot (g \cdot x) = x$ and thus yRx.
(3) Finally, suppose that xRy and yRz, so that $y = g \cdot x$ and $z = h \cdot y$, respectively, for some $g, h \in G$. By substitution, we can write $z = h \cdot (g \cdot x) = hg \cdot x$ and xRz as required.

□

Using the fact that a group action induces an equivalence relation, we can formulate our definition of an orbit.

Definition 2.7. Let G be a group and X be a G-set. Then the equivalence class of $x \in X$ under relation R, as described above, is called the *orbit of x*. That is, $\text{orb}(x) = \{g \cdot x : g \in G\}$.

Now we ask how the orbit of an element relates to the stabilizer group for that given element. To that end, we have the following result:

Theorem 2.8 (Orbit-Stabilizer Theorem)**.** *Let G be a group and X be a G-set. Then, for every $x \in X$, $|orb(x)| = |G : G_x|$.*

Proof. The proof for this theorem consists of showing that a map between the orbit of x and the set of left cosets of G_x in G is well-defined and bijective.

Let $x \in X$ be given. We define a map ϕ that maps elements of the orbit of x to left cosets of G_x in G. In particular, let $\phi(g \cdot x) = gG_x$.

First we will show that ϕ is well-defined. Suppose $g \cdot x = h \cdot x$ for some $g, h \in G$. Then $h^{-1}g \cdot x = h^{-1}h \cdot x = x$, so $h^{-1}g \in G_x$. This implies that $gG_x = hG_x$, as needed.

Next we show that ϕ is injective. Suppose that $\phi(g \cdot x) = \phi(h \cdot x)$ for some $g, h \in G$. By the definition of ϕ, we can write $gG_x = hG_x$ so that $g_2^{-1}g_1 \in G_x$. But by the definition of stabilizer, this implies that $x = h^{-1}g \cdot x$ and thus $g \cdot x = h \cdot x$, as required.

Finally, we note that every left coset of the form gG_x is equal to $\phi(g \cdot x)$ by definition, so ϕ is surjective as well. Since ϕ is a bijection between the orbit of x and the set of left cosets of G_x in G, we conclude that their cardinalities are equal. □

Remark 2.9. Note that if we apply the Orbit-Stabilizer Theorem on the first example of Example 2.2, we find that for a subgroup H of G, the number of distinct left cosets of H in G is equal to $|G : H|$. Thus the Lagrange Theorem is a special case of the Orbit-Stabilizer Theorem.

3. Sylow Theorems

The Fundamental Theorem of Arithmetic tells us that every positive integer is a unique product of prime numbers. The Sylow Theorems allow us to classify any finite group G, by considering subgroups of G of maximal prime power order. In this section, we will assume that all groups are of finite order.

Definition 3.1. Let p be a prime number, n be a positive integer, and k be a positive integer such that p does not divide k. Let G be a group with $|G| = kp^n$. A *p-Sylow subgroup* is a subgroup of G with p^n elements.

We begin with a short lemma.

Lemma 3.2. *Let p be a prime and k be a positive integer such that p does not divide k. The number of ways to select a subset with p^n elements from a set with kp^n elements is congruent to $k \pmod p$.*

Proof. Using generating functions, we can see that the number of ways of selecting a subset with p^n elements from a set with kp^n elements is equal to the coefficient of x^{p^n} in $(1+x)^{p^n k} = \left((1+x)^{p^n}\right)^k$. But, $(1+x)^{p^n} \equiv 1 + x^{p^n} \pmod p$ since all other coefficients of powers of x in the binomial expansion are divisible by p. Thus, the coefficient of x^{p^n} that we wish to find is congruent to the coefficient of x^{p^n} in $\left((1+x)^{p^n}\right)^k$, which we see to be $k \pmod p$. □

Using the Orbit-Stabilizer Theorem and the previous lemma, we can prove the first of the four Sylow Theorems.

Theorem 3.3 (First Sylow Theorem)**.** *Let p be a prime number and G be a finite group of order $p^n k$ with k not divisible by p. Then G has at least one p-Sylow subgroup.*

Proof. Let $\mathbb{S}$ be the set of all subsets of G with p^n elements. Lemma 3.2 gives us that $|\mathbb{S}| \equiv k \pmod p$. We make $\mathbb{S}$ a G-set by defining, for every $S \in \mathbb{S}$ and every $g \in G$, the group action $g \cdot S = gS$. Let $S_1, S_2, \ldots, S_r$ be representatives of orbits of $\mathbb{S}$ under this action. Since the orbits partition $\mathbb{S}$, we can write $\mathbb{S}$ as the disjoint union of all the orbits.

$$\mathbb{S} = \operatorname{orb}(S_1) \cup \operatorname{orb}(S_2) \cup \cdots \cup \operatorname{orb}(S_r) \tag{3.4}$$

Suppose that for every $1 \leq i \leq r$, p divides $|\operatorname{orb}(S_i)|$. Then (3.4) implies that $p \big| |\mathbb{S}|$, which contradicts Lemma 3.2. Thus there exists at least one orbit, WLOG $\operatorname{orb}(S_1)$, such that $|\operatorname{orb}(S_1)| = m$ with $p \nmid m$.

By the Orbit-Stabilizer Theorem, the order of the stabilizer G_{S_1} is $|G|/|\operatorname{orb}(S_1)| = kp^n/m$. But since p does not divide m, we have that $|G_{S_1}| = tp^n$ for some t also not

divisible by p. Furthermore, for any $g \in G_{S_1}$, we have $gS_1 = S_1$. So for any $s \in S_1$, we also have $gs \in S_1$ and the coset $G_{S_1}s \subseteq S_1$. Considering their cardinalities, we have that $|G_{S_1}| = |G_{S_1}s| \leq |S_1| = p^n$. But $|G_{S_1}| = tp^n \leq p^n$, thus $|G_{S_1}| = p^n$, and we have shown that there exists a p-Sylow subgroup of G and $G_{S_1}s = S_1$. □

Theorem 3.5 (Second Sylow Theorem)**.** *The number of p-Sylow subgroups in a finite group G is congruent to* $1 \pmod{p}$.

Proof. Again, let G be a finite group with $|G| = p^n k$ and $\mathbb{S}$ be the set of all subsets of G with p^n elements, as in the proof of Theorem 3.4. Let $S \in \mathbb{S}$ be a subset of G with p^n elements. By the First Sylow Theorem, if $p \nmid |\text{orb}(S)|$, then for all $s \in S$, we have that $G_S s = S$. Then, $G_S = Ss^{-1}$ is a p-Sylow subgroup of G. Additionally, since G_S is a subgroup of G, its conjugate $s^{-1}(G_S)s$ is also a subgroup of G with $|s^{-1}(G_S)s| = |G_S| = p^n$. Then $s^{-1}(G_S)s = s^{-1}(Ss^{-1})s = s^{-1}S$ is a p-Sylow subgroup in $\text{orb}(S)$. Note that by the Orbit-Stabilizer Theorem, $\text{orb}(s^{-1}(G_S)s) = \text{orb}(S)$ has k elements, where k is not divisible by p. Thus, if the orbit's cardinality is not divisible by p, the orbit contains a p-Sylow subgroup and the cardinality of the orbit is k.

Conversely, suppose that $\text{orb}(S)$ contains a p-Sylow subgroup, say P. If $g \in G_P$, then $gP = P$. Clearly, $g = g1 \in P$, so $G_P \subseteq P$. On the other hand, $P \subseteq G_P$, so $G_P = P$. By Orbit-Stabilizer, it follows that $|\text{orb}(P)|$ is not divisible by p and in fact has cardinality k. Thus, we have shown that every orbit that contains a p-Sylow subgroup has cardinality k, where k is not divisible by p, and that every orbit of cardinality not divisible by p contains a p-Sylow subgroup.

Consider the following claim: Distinct p-Sylow subgroups are contained in distinct orbits.

Let P_1 and P_2 be p-Sylow subgroups of G. Suppose that $P_1, P_2 \in \text{orb}(S)$. Then $P_1 = gP_2$ for some $g \in G$, which implies that $1 \in P_2 \cap gP_2$. Since cosets partition G and are thus either equal or disjoint, we have that $P_2 = gP_2 = P_1$.

Now let n_P denote the number of p-Sylow subgroups of G. Since every orbit that does not have a p-Sylow subgroup has cardinality divisible by p, $|\mathbb{S}| \equiv kn_P \pmod{p}$. But by Lemma 3.2, $k \equiv kn_P \pmod{p}$ and it follows that $n_P \equiv 1 \pmod{p}$. □

Before we introduce the Third Sylow Theorem, we must introduce the notion of a p-group.

Definition 3.6. Let p be a prime number. A *p-group* is a group where every element has order a power of p.

If G is a finite p-group, the First Sylow Theorem gives that the number of elements in G is a power of p. Conversely, if a finite group has order a power of p, by Lagrange's Theorem, it follows that the group is a p-group. Thus G is a p-group if and only if $|G| = p^n$.

Proposition 3.7. *Let P be a p-Sylow subgroup of a finite group G. Then any p-subgroup of $N_G(P)$ is a subset of P. In particular, P is the unique p-Sylow subgroup of $N_G(P)$.*

Proof. Let Q be a p-subgroup of $N_G(P)$. Suppose $|Q| = p^m$ and $|P| = p^n$. Since P is a p-Sylow subgroup, we must have that $n \geq m$. Since $P \trianglelefteq N_G(P)$, it follows from Proposition 1.6 that $\langle P, Q\rangle = PQ$ is a subgroup of G. Furthermore, by Corollary 1.4, $|PQ| = p^{n+m-s}$, where $|P \cap Q| = p^s$. Since p^n is the highest power of p dividing

$|G|$, we must have $m \leq s$. Noting that the intersection of two subgroups, $P \cap Q$, is also a subgroup of G, we have that $s \leq m$. Thus $m = s$ and $P \cap Q = Q$. So, $Q \subseteq P$; in particular, if Q is a p-Sylow subgroup of $N_G(P)$, then $Q = P$. □

Theorem 3.8 (Third Sylow Theorem)**.** *Let P be a p-Sylow subgroup of a finite group G and Q be any p-group of G. Then Q is contained in a conjugate of P.*

Proof. Let $\mathbb{P}$ be the set of distinct G-conjugates of P, that is $\mathbb{P} = \{gPg^{-1} : g \in G\}$. We consider the orbits of $\mathbb{P}$ under conjugation by P, that is elements of the form $p(gPg^{-1})p^{-1}$ for all $p \in P$. In particular, note that if $g = e$, then $\text{orb}(P) = \{P\}$.

We claim that P is the only element of $\mathbb{P}$ with orbit of cardinality 1. Suppose gPg^{-1} has exactly one element in its orbit; clearly $gPg^{-1} \in \text{orb}(gPg^{-1})$. Then for all $x \in P$, $x(gPg^{-1})x^{-1} = gPg^{-1}$ so that $(g^{-1}xg)P(g^{-1}xg)^{-1} = P$ and $g^{-1}pg \in N_G(P)$. By Proposition 1.7, $g^{-1}xg$ and x have the same order. Thus $g^{-1}Pg$ is a p-subgroup of $N_G(P)$. Furthermore, $g^{-1}Pg$ is a p-Sylow subgroup of $N_G(P)$ since P and $g^{-1}Pg$ have the same number of elements. But by Proposition 3.7, it follows that $g^1Pg = P$ is the unique p-Sylow subgroup of $N_G(P)$ and P is the only element of $\mathbb{P}$ with orbit size 1.

Then, for all $g \notin P$, the cardinality of orbits of gPg^{-1} under conjugation by elements of P is greater than 1. In fact, Orbit-Stabilizer tells us that the cardinalities of their orbits are congruent to 0 (mod p). Summing over cardinalities of orbits, we find that $|\mathbb{P}| \equiv 1 \pmod{p}$.

Now we consider the orbits of $\mathbb{P}$ under conjugation by elements of Q. Since every orbit's cardinality is a power of p and we have that $|\mathbb{P}| \equiv 1 \pmod{p}$, there exists at least one orbit with cardinality 1. Then, there exists $g \in G$ such that for all $x \in Q$, $x(gPg^{-1})x^{-1} = gPg^{-1}$. Following a similar argument as above, we find that $g^{-1}Qg \subseteq N_G(P)$. By Proposition 3.7, it follows that $g^{-1}Qg \subseteq P$ and $Q \subseteq gPg^{-1}$. □

Corollary 3.9 (Fourth Sylow Theorem)**.** *All the p-Sylow subgroups of a finite group G are conjugate, so the number of p-Sylow subgroups divides $|G|$, i.e. $n_P \big| |G|$.*

Proof. This result follows from the Third Sylow Theorem. Let P and Q be p-Sylow subgroups of G. Then $|P| = |Q|$. But the Third Sylow Theorem gives us that $Q \subseteq gPg^{-1}$ for some $g \in G$, and it follows that $Q = gPg^{-1}$, that is p-Sylow subgroups are conjugate. Furthermore, under the conjugation action, Orbit-Stabilizer gives us that the number of conjugates of P is equal to $|G : N_G(P)|$. Finally, Lagrange Theorem tells us that the number of p-Sylow subgroups of G, n_P, divides $|G|$, as required. □

We end with a short proposition that often assists us in classification problems.

Proposition 3.10. *Let G be a finite group and n_P be the number of p-Sylow subgroups of G. Then $n_P = 1$ if and only if G has a normal p-Sylow subgroup.*

Proof. We will first prove the forward direction. Let H be a p-Sylow subgroup of G. Then the conjugate of H is also a subgroup with $|H| = |gHg^{-1}|$. But the conjugate of a p-Sylow subgroup is also a p-Sylow subgroup and is in fact the same as the original one. Thus we have $gHg^{-1} = H$ and H is normal.

For the reverse direction, let P be a normal p-Sylow subgroup. The Third Sylow Theorem gives us that $P \subseteq gPg^{-1}$ for some $g \in G$. It follows that there is only one p-Sylow subgroup and we have established equivalence. □

4. Direct Products

Definition 4.1. Let G and H be groups. The *direct product* $G \times H$ is the set of ordered pairs (g, h), where $g \in G$ and $h \in H$, under the multiplication rule $(g, h)(g', h') = (gg', hh') \in G \times H$.

Note that associativity of multiplication follows from associativity in G and H. Furthermore, the ordered pair (e_G, e_H) is the identity element $e_{G\times H}$ and the inverse of (g, h) is (g^{-1}, h^{-1}). Thus $G \times H$ forms a group.

We will prove two propositions regarding direct products.

Proposition 4.2. *Let m and n be positive integers. Then $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is cyclic if and only if $\gcd(m, n) = 1$.*

Proof. We will first prove the reverse direction. Let k be the order of $(1, 1) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Then we have $(k \pmod m, k \pmod n) = (0, 0)$ and it follows that $m|k$ and $n|k$. But $\gcd(m, n) = 1$, so that $mn|k$. Furthermore, since k is the order of $(1, 1)$, k must be the least non-zero multiple of mn and thus $k = mn$. Thus we have shown that $(1, 1)$ generates $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$. In particular, $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/(mn)\mathbb{Z}$.

For the forward direction, we will prove the contrapositive. Suppose $d = \gcd(m, n)$ with $d > 1$. We wish to show that $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is not cyclic. Let $m' = \frac{m}{d}$ and $n' = \frac{n}{d}$. For $(x, y) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, we have

$$\begin{aligned} m'n'd(x, y) &= (m'n'dx \pmod m, m'n'dy \pmod n) \\ &= (mn'x \pmod m, m'ny \pmod n) \\ &= (0, 0). \end{aligned}$$

Thus the order of (x, y) is at most $m'n'd$, which is strictly less than mn. Thus $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ does not contain an element of mn and is not cyclic. □

Proposition 4.3. *Let H and K be subgroups of G such that $HK = G$, $H \cap K = \{e_G\}$, and $hk = kh$ for all $h \in H$ and $k \in K$. Then $G \cong H \times K$.*

Proof. To show that G is isomorphic to $H \times K$, we will show that a map between them is a bijective homomorphism. We define such a map $\phi : H \times K \to G$ by $\phi(x, y) = xy$ for all $x \in H$ and $y \in K$. Observe that

$$\begin{aligned} \phi\left((x, y), (x', y')\right) &= \phi(xx', yy') \\ &= xx'yy' \\ &= xyx'y' \\ &= \phi(x, y)\phi(x', y') \end{aligned}$$

So, ϕ is a homomorphism.

To show ϕ is injective, suppose $\phi(x, y) = \phi(x', y')$. Then $xy = x'y'$ and $(x')^{-1}x = y'y^{-1}$. Since $(x')^{-1}x \in H$ and $y'y^{-1} \in K$, it follows that $(x')^{-1}x = y'y^{-1} \in H \cap K = \{e_G\}$. Thus $x = x'$ and $y = y'$, as required.

Lastly, to show ϕ is surjective, we note that for any $g \in G$, we have that $g = xy$ for some $x \in H$ and $y \in K$, and we are done. □

5. The Fundamental Theorem of Finitely Generated Abelian Groups

Although the main goal of this paper is to examine several finite groups, in this section we will prove a more general result about abelian groups. Section 6 will make use of Corollary 5.4.

Definition 5.1. A group is *finitely generated* if it has a finite number of generators.

Theorem 5.2 (Fundamental Theorem of Finitely Generated Abelian Groups)**.** *Any finitely generated abelian group is isomorphic to a direct product of cyclic groups:*

$$\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z} \times \mathbb{Z}^r,$$

where $m_i | m_{i+1}$ *for all* $1 \leq i \leq k-1$.

To complete our proof, we require two additional definitions.

Definitions 5.3. Let G be a finitely generated abelian group and $x_1, \ldots, x_r$ be distinct elements that together generate G.

(1) If no set of $r-1$ elements can generate G, then $x_1, \ldots, x_r$ is called a *minimal set of generators*.
(2) An expression of the form $e = x_1^{n_1} x_2^{n_2} \cdots x_r^{n_r}$ is called a *relation between generators*, where e is the identity element in G.

Note that if $x_1, \ldots, x_r$ form a minimal set of generators, for $m \in \mathbb{Z}$, $x_1 x_2^m, x_2, \ldots, x_r$ also form a minimal set of generators. This is because for any $g \in G$

$$g = x_1^{n_1} x_2^{n_2} \cdots x_r^{n_r} = (x_1 x_2^m)^{n_1} x_2^{n_2 - m n_1} x_3^{n_3} \cdots x_r^{n_r}.$$

Now we will prove Theorem 5.2.

Proof. We have two cases for G in terms of relations: there is only the trivial relation or there exists some non-trivial relation. We will first consider the case with only the trivial relation. Suppose that G has a minimal set of generators $x_1, \ldots, x_k$ where the only relation requires that $e = x_1^0 \cdots x_k^0$. Then for any $g \in G$, the expression $g = x_1^{n_1} \cdots x_k^{n_k}$ is unique and the correspondence $g \to (n_1, \ldots, n_k)$ is an isomorphism $G \cong Z^k$.

Now we consider the general case, where regardless how we select a minimal set of generators for G, there is some non-trivial relation. Over all relations of every possible minimal set of generators, there is a smallest possible exponent, say m_1, so that WLOG we have the relation $e = x_1^{m_1} x_2^{n_2} \cdots x_k^{n_k}$ between generators $x_1, \ldots, x_k$.

We claim that $m_1 | n_2$. Otherwise, if $n_2 = q_2 m_1 + u$, where $0 < u < m_1$, then

$$e = x_1^{m_1} x_2^{q_2 m_1 + u} x_3^{n_3} \cdots x_k^{n_k} = (x_1 x_2^{q_2})^{m_1} x_2^u x_3^{n_3} \cdots x_k^{n_k},$$

which contradicts the fact that m_1 is the smallest possible exponent. Thus we write $n_2 = q_2 m_1$. A similar argument follows for each of $n_3, \ldots, n_k$ so that $n_i = q_i m_1$ for $3 \leq i \leq k$.

Consider the new set of generators $z_1, x_2, \ldots, x_k$, where $z_1 = x_1 x_2^{q_2} x_3^{q_3} \cdots x_k^{n_k}$ so that $e = z_1^{m_1}$. Since m_1 was chosen to be the smallest possible exponent for the relation to hold, it follows that m_1 is equal to the order of $\langle z_1 \rangle$. Let $H = \langle z_1 \rangle$ and G_1 be the subgroup of G generated by $x_2, \ldots, x_k$. We can easily see that $HG_1 = G$ and $H \cap G_1 = \{e_G\}$. Then by Proposition 4.3, it follows that $G \cong H \times G \cong \mathbb{Z}/m_1\mathbb{Z} \times G_1$.

Repeating the procedure of the proof so far for G_1, we have two cases: $G_1 \cong \mathbb{Z}^{k-1}$ or $G_1 \cong \mathbb{Z}/m_2\mathbb{Z} \times G_2$, where G_2 is a subgroup generated by $x_3, \ldots, x_k$. Then it follows that $G \cong \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}^{k-1}$ or $\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times G_2$. Continuing with $G_2, \ldots$ and reducing the number of generators by one in each step, we eventually come to the result that $G \cong \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z} \times \mathbb{Z}^r$, for some r and $m_1 | m_2 | \cdots | m_k$. □

More relevant to this paper, we will make use of the following corollary.

Corollary 5.4. *Any finite abelian group is isomorphic to a direct product of cyclic groups* $\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}$ *where* $m_i | m_{i+1}$ *for all* $1 \leq i \leq k-1$.

Proof. Let G be a finite abelian group. By Theorem 5.2, we know that $G \cong \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z} \times \mathbb{Z}^r$, where $m_i | m_{i+1}$ for all $1 \leq i \leq k-1$. Suppose that $r > 0$, then the element $(0, 0, \ldots, 0, 1)$ has infinite order, which contradicts the finiteness of G. Thus $r = 0$ and the result follows. □

In the next section, we will simply refer to this theorem and its corollary as classification theorems.

Though we did not see the use of Proposition 4.2 in the proof of the Fundamental Theorem itself or its corollary, we can use it to rewrite direct products of cyclic groups into the standard form given by the Fundamental Theorem as in the following example.

Example 5.5. Consider the direct product $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$. We can easily see that $6 \nmid 15$. Using Proposition 4.2, we can write

$$\begin{aligned} \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z} &\cong (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \\ &\cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z} \end{aligned}$$

so that $3 \mid 30$, as needed.

6. Classification Problems

Both the Sylow Theorems and the classification theorem are powerful tools in classifying groups of finite order. However, depending on the order of a group, one theorem may give a more complete classification. To that end, we consider two examples of classification problems: groups of order 4 and groups of order 30.

6.1. Groups of Order 4.

Let G be a group of order 4. We may first attempt to apply the Second and Fourth Sylow Theorems (Theorem 3.5 and Corollary 3.9, respectively). Here, we find that the number of 2-Sylow subgroups is of the form $n_2 \equiv 1 \pmod 2$ (so that n_2 is odd) and n_2 divides 4. But we can easily see that the only odd number that divides 4 is $n_2 = 1$. By Proposition 3.10, it follows that this 2-Sylow subgroup, call it P, is normal. Now, take $y \in G \setminus P$. So $yPy^{-1} = P$. But, we know that $P = \langle x \rangle$ where x has order 2. Thus we either have $yxy^{-1} = e_G$, which contradicts that P is a 2-Sylow subgroup, or $yxy^{-1} = x$, which tells us that G is abelian.

Though we are unable to proceed with the Sylow Theorems, the classification theorem tells us that $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $G \cong \mathbb{Z}/4\mathbb{Z}$. That is, groups of order 4 are either isomorphic to the Klein four-group or cyclic.

6.2. Groups of Order 30.

If we approach this problem directly with the classification theorem, we find that we restrict ourselves to the case where G is abelian, which may not always be the case. Furthermore, in this case, since the prime factorization of 30 is $2 \cdot 3 \cdot 5$, we only have that $G \cong \mathbb{Z}/30\mathbb{Z}$.

Before we begin our discussion on groups of order 30 using the Sylow Theorems, we will make a brief comment on groups of order $2p$, where p is prime. Applying the Second and Fourth Sylow Theorems, we find that there is a unique p-Sylow subgroup. Furthermore, Proposition 3.10 tells us that this p-Sylow subgroup is normal. We will use this fact when we work with quotient groups of order $2p$.

Proposition 6.1. *Let G be a group of order 30. Then G has a cyclic, normal subgroup of order 15.*

Proof. We will begin by applying the Second and Fourth Sylow Theorems to find that the number of 3-Sylow subgroups is $n_3 \in \{1, 10\}$ and the number of 5-Sylow subgroups is $n_5 \in \{1, 6\}$.

If $n_3 = 1$, then Proposition 3.10 tells us that the 3-Sylow subgroup, say P, is unique and normal. We then form G/P with order 10. Using that $10 = 2 \cdot 5$ and the discussion about groups of order $2p$, we can see that there exists a normal 5-Sylow subgroup, say N/P, of G/P. Furthermore, the Fourth Isomorphism Theorem gives us that N is a normal subgroup of G and the order of N is 15.

Applying the Second and Fourth Sylow Theorems again to N, we find that $n_3' = 1$ and $n_5' = 1$. Counting the number of elements by their order, we have the identity element, two order 3 elements, and four order 5 elements, leaving eight elements. But by Lagrange's Theorem we know that the order of an element must be 1, 3, 5, or 15. Thus, the remaining eight elements must have order 15 and N is a cyclic group.

Suppose now that $n_3 = 10$ so that $P_1, P_2, \ldots, P_{10}$ are distinct 3-Sylow subgroups. Then by Lagrange's Theorem, for each $i, j \in \{1, 2, \ldots, 10\}$ with $i \neq j$, the order of the subgroup $P_i \cap P_j$ divides $|P_i| = 3$. Since each 3-Sylow subgroup is distinct, we have that their intersection is the identity element. Then each distinct 3-Sylow subgroup contains two elements of order 3 that do not appear in any other 3-Sylow subgroup and thus G has 20 distinct order 3 elements. Furthermore, by counting the number of elements by their order, we find that there are 9 elements of G with order neither 1 nor 3. If G also contained six 5-Sylow subgroups, then we would find 24 elements of order 5. But there were only 9 uncounted elements, leading to a contradiction. It follows that in this case, $n_5 = 1$. By a similar argument as in the $n_3 = 1$ case, we find that G has a cyclic, normal subgroup of order 15. □

Proposition 6.2. *Let G be a group of order 30. Then G is either cyclic, dihedral, or isomorphic to one of the following:*

$$\langle x, y : x^{15} = 1 = y^2,\ yxy^{-1} = x^4 \rangle \text{ or} \tag{6.3}$$

$$\langle x, y : x^{15} = 1 = y^2,\ yxy^{-1} = x^{11} \rangle. \tag{6.4}$$

Proof. From Proposition 6.1, we have that G has a normal cyclic subgroup N of order 15. Let x be a generator for N and y be a generator for some 2-Sylow subgroup. Since N is normal, we have that $yxy^{-1} = x^i$ for some i. Noting that $y^2 = 1$, we write $x = y^2xy^{-2} = y(yxy^{-1})y^{-1} = yx^iy^{-1} = x^{i^2}$. Then $i^2 - 1 \equiv 0 \pmod{15}$ and by exhaustion we have that $i \in \{1, 4, 11, 14\}$. If $i = 1$, then we have that $yxy^{-1} = x$ and $yx = xy$ so that G is abelian. This is the only case where the classification theorem would have been applicable. If $i = 14 \equiv -1 \pmod{15}$, then $yx^{-1}y^{-1} = x$ or $x^{-1} = yxy$ so that G is dihedral. If i is 4 or 11, then we have (6.3) or (6.4), respectively. □

6.3. **Conclusion.** As we saw in the first example, after we found that groups of order 4 are abelian, the classification theorem was a very powerful tool in completing the classification. On the other hand, in the second example, only one of the four cases was found to be abelian and thus the Sylow Theorems proved to be much more effective. All in all, the Sylow Theorems are always applicable in

classification problems but often require more work to classify a group. Meanwhile, the classification theorem only works under the condition that the group is abelian but often gives an immediate result.

Acknowledgments

I would like to thank my mentor, Andreea Iorga, for her assistance in the learning and writing process. Though I had minimal knowledge of group theory prior to this REU, Andreea guided me through concepts and proofs that I found confusing on my own. I would also like to thank Professor Peter May for organizing and running the 2020 Math REU remotely, despite the difficulties caused by the ongoing pandemic. I am incredibly grateful for this experience to enjoy math in a research-based context.

References

[1] M. A. Armstrong. Groups and Symmetry. Springer-Verlag. 1988
[2] John F. Humphreys. A Course in Group Theory. Oxford University Press. 1996.