GROUP ACTIONS

RYAN C. SPIELER

Abstract. In this paper, we examine group actions. Groups, the simplest objects in Algebra, are sets with a single operation. We will begin by defining them more carefully and exploring some key definitions related to groups. We will then define group actions and several important concepts that relate to them. The remainder of the paper explores two important types of action and uses them to explore the structure of finite groups. The first is the coset. In examining cosets, we will prove Lagrange's Theorem, a major result in Finite Group Theory. The second type of action which we will examine is conjugation. Using our knowledge of conjugation, we will prove Sylow's Thoerems - a set of statements which provide knowledge of the internal structure of a finite group.

Contents

1. A Little Bit About Groups

Before we discuss group actions, we will need to know something about groups. In this section, we explore basic concepts in group theory that will be of use to us later. Our survey will not be exhaustive, and interested readers are invited to peruse [1], [2], or [3] for more results.

Definition 1.1. A **group** is an ordered pair $(G, \cdot)$, where G is a set and $\cdot$ is a binary operation (often referred to as multiplication) such that:
(i) For all $a, b, c \in G$, $(a \cdot (b \cdot c) = (a \cdot b) \cdot c)$
(ii) There exists $1 \in G$ such that for all $g \in G, 1 \cdot g = g$
(iii) For each $g \in G$, there exists $g^{-1} \in G$ such that $g \cdot g^{-1} = g^{-1} \cdot g = 1$

Examples 1.2. $(\mathbb{R}, +), (\mathbb{C}, +), (\mathbb{Q}, +)$ are all groups.

Other interesting examples of groups occur in geometry. An example is D_3, the dihedral group on three elements (the vertices of the triangle), which contains all of the symmetries of an equilateral triangle. Another is the points on a circle with

Date: AUGUST 28, 2017.

the operation of rotation, which is easy to draw and which obviously satisfies the above axioms. We also have a natural notion of the size of a group.

Definition 1.3. Let $(G, \cdot)$ be a group. The **order** of G, denoted $|G|$, is the number of elements in the set G.

Remark 1.4. When there is no risk of confusion regarding the operation with which G is a group, I will often refer to G as the group.

Note that our operation need not be commutative. For instance, many sets of matrices form groups with respect to matrix multiplication, which is generally noncommutative. This leads to our next definition.

Definition 1.5. A group $(G, \cdot)$ is **Abelian** if $\cdot$ is commutative.

Examples 1.6. The groups listed in Example 1.2 are all Abelian.

Looking at the examples listed, the reader might notice something; $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ and all of these sets are groups with respect to addition. This notion is encapsulated in the following defintion.

Definition 1.7. A **subgroup** $H \leqslant G$ is a set $H \subseteq G$ that is a group under the same operation under which G is a group.

We will prove several results in this paper that help us determine subgroups of a group. The following is the first of these results, though it only works of one knows that a group contains certain subgroups. Other results will not need us to have this knowledge.

Proposition 1.8. *If $\{H_i\}$ are subgroups of G, then their intersection is a subgroup of G.*

Proof. The identity is obviously in the intersection of H_i. Since associativity and inverses hold by hypothesis for elements in any H_i, they hold for elements in the intersection. □

Proposition 1.9 enables us to make the following definiton:

Definition 1.9. Let A be a subset of a group G and let H_i be subgroups of G such that $A \subseteq H_i$. $\langle A \rangle = \cap_i H_i$ is called the **subgroup of G generated by A**.

An important special case follows:

Definition 1.10. A group generated by a single element, call it x, is called a **cyclic group** and is denoted $\langle x \rangle$.

For the intuition behing the term cylcic, one need only look at the rotations of a circle. Cyclic groups allow us to assign an order to an element of a group if the element generates a cyclic group. The order is simply the order of the cyclic group the element generates.

We have now examined groups. It is natural to next ask what maps are of interest. The answer is the maps that preserve group structure.

Definition 1.11. Let G and H be groups. A map $\varphi : G \to H$ is a **homomorphism** if, given $g_1, g_2 \in G$, $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$.

Remark 1.12. : There are really two operations in the above definition. The first is the binary operation in G and the second is the one in H.

There are some special homomorphisims to which we will refer by name.

Definitions 1.13. : A homomorphism that is injective is a **monomorphism**. A homomorphism that is surjective is an **epimorphism**. A homomorphism that is bijective is an **isomorphism**.

The most important of the above to recognize is isomorphism. If two groups have an isomorphism between them, they are, as far as algebraists care, the same. They do not need to have the same elements; algebraists seldom care about the elements of groups. Rather, the groups have the same structure - namely binary operations that satisfy the axioms in Definition 1.1. Two groups with an isomorphism between them are said to be *isomorphic*.

2. Actions

In this section, we introduce actions. Intuitively, an action is simply the way a group acts on a set (often the group itself) in a way with some intersting properties. In what follows, we clarify the prior remark and introduce related definitions that will allow us to utilize actions in future proofs.

Definition 2.1. Let G be a group and S be a set. An action of G on S is a map $\varpi : G \times S \to S$ (often written gs for some $s \in S$) such that
(i) For all $g_1, g_2 \in G$ and for all $s \in S$, $g_1(g_2 s) = (g_1 g_2)s$
(ii) For all $s \in S$, $1s = s$

Definition 2.2. Let G be a group and S a set. The **kernal** of an action ϖ of G on S is:

$$ker(\varpi) = \{g \in G : \forall s \in S, gs = s\}$$

Definition 2.3. An action ϖ such that $ker(\varphi) = \{1\}$ is called **faithful**.

There are some important notions that accompany actions that will be of use to us later.

Definition 2.4. If G is a group acting on S and $s \in S$, the **stabilizer** of s in G is:

$$Stab_G(s) = \{g \in G : gs = s\}$$

Proposition 2.5. $Stab_G(s) \leqslant G$.

Proof. By definition, if $g \in Stab_G(s)$, then $g \in G$. We need only show that $Stab_G(s)$ is closed under multiplication and taking inverses. For $g, h \in Stab_G(s)$, $(hg)s = h(gs) = hs = s$ and $g^{-1}s = g^{-1}(gs) = (g^{-1}g)s = 1s = s$. □

Definition 2.6. If G is a group acting on S, the **orbit** of $s \in S$ under G is:

$$Orb_G(s) = \{gs : g \in G\}$$

In words, Orbits are the points in S to which s is mapped by a group action. Orbits are important for many proofs that follow because they partition S into equivalence classes, as we show now.

Proposition 2.7. *The relation $y \sim x$ if and only if $y \in Orb_G(x)$ is an equivalence relation.*

Proof. We must check that the relation is reflexive, symmetric and transitive.

• Taking $1 \in G$, we see that $x = 1x \in Orb_G(x)$. Thus, $x \sim x$ and the relation is reflexive.

• To establish our relation is symmetric, let $y \in Orb_G(x)$. We need to show that $x \in Orb_G(y)$. Since $y \in Orb_G(x)$, there exists $h \in G$ such that $y = hx$. Since elements of groups have inverses, there exists $h^{-1} \in G$ such that $h^{-1}y = h^{-1}hx = 1x = x$. Thus, $x \in Orb_G(y)$.

• Let $y \in Orb_G(x)$ and $z \in Orb_G(y)$. To show that our relation is transitive, we must show that $z \in Orb_G(x)$. Since $y \in Orb_G(x)$, there exists $h \in G$ such that $y = hx$. Since $z \in Orb_G(y)$, there exists $h' \in G$ such that $z = h'y$. But, since $y = hx$, $z = h'y = h'hx$. Thus, since groups are closed under multiplication, $h'h \in G$ and $z \in Orb_G(x)$ as needed. □

The fact that actions partition sets into orbits will be the crux of many future proofs, as we will see when we use two types of actions, left multiplication and conjugation, to investigate the structure of groups.

3. Cosets and Lagrange's Theorem

We begin by examining another example of an action - left multiplcation. This will lend us to the concept of cosets and to Lagrange's theorem, an important result in finite group theory.

Proposition 3.1. *Let G be a group. Left multiplication - defined by ga for $g, a \in G$ - is an action.*

Proof. We already have our map. Associativity and multiplication by 1 follow from the definition of a group. □

Definition 3.2. Let $H \leqslant G$ and $a, b \in G$. a is **congruent to b mod H** if $b^{-1}a \in H$. If this is so, we write $a \equiv b \mod H$

Since left multiplication is an action, the orbits of any element of H by a fixed element of G form equivalence classes. We can partition G into these equivalence classes.

Definition 3.3. The equivalence classes mentioned above are called **left cosets** of H containing a, where a is the fixed element of G called a representative of the coset. We write them aH The collection of all cosets of H in G is denoted G/H.

The following provides a way to determine when two cosets are equal.

Proposition 3.4. *Let G be a group and let $H \leqslant G$. For all $a, b \in G$, $aH = bH$ if and only if $b^{-1}a \in N$ in particular, if and only if a and b are representatives of the same coset.*

Proof. Since cosets partition G, G is the union of products of the form gH. We need to show that distinct left cosets do not intersect. Suppose that $aH \cap bH \neq \emptyset$. Let $c \in aH \cap bH$. For some $h, h' \in H$, $c = ah = bh'$ so $a = ch^{-1} = bh'h^{-1} = bh''$ where $h'' \in H$. Now any $am \in aH$ ($m \in H$) is of the form $am = bh''m \in bH$, showing that $aH \subseteq bH$. The same argument reversing the roles of a and b yields $aH \supseteq bH$, so $aH = bH$. Since H is closed under products, this is equivalent to saying a and b represent the same coset. □

Definition 3.5. The cardinality of G/H is called the **index** of H in G and is written $[G : H]$.

Theorem 3.6. ***Lagrange's Theorem*** *Let G be a finite group and let $H \leqslant G$. Then $|G| = |H|[G : H]$.*

Proof. The map $h \mapsto ah$ is obviously a bijection. Thus, $|H| = |aH|$. Hence, since the cosets are equivelence classes, G is partitioned into $[G : H]$ of them, each with $|H|$ elements. □

In short, Lagrange's theorem says that the order of a subgroup of G divides the order of G. It gives a natural way of calculating the size of a group given a coset collection and vice versa. We will use it extensively in future proofs. Here's a snapshot of what it is capable of.

Proposition 3.7. *Let G be a finite group acting on a set S and let $s \in S$. Then $|G| = |Stab_G(s)|\sharp Orb_G(s)$.*

Proof. Since $Stab_G(s) \leqslant G$, we may find its cosets. They are given (fixing $h \in G$) by $h(gs) = hs$ i.e the orbits of S. Using Lagrange's Theorem, the result follows. □

By a simple application of Lagrange's Theorem we have a way of determining group size based on actions. Is there more we can learn about group structure using actions? Absolutely. In the next section, we will see how we can obtain detailed information about the internal structure of a finite group using group actions.

4. Conjugation and Sylow's Theorems

In this section, we introduce another important action - conjugation. We show several important application of conjugation and use conjugation and its applications to prove Sylow's Theorems, which are a sort of partial converse to Lagrange's theorem. Whereas Lagranges Theorem gives an equation for the order of a group in terms of a subgroup and cosets with it, Sylow's Theorems provide detailed information about certain special subgroups of a group. These subgroups are called p-Sylow subgroups and are a sort of maximal prime subgroup. We then move to some applications of Sylow's Theorems and will even get to glance at one of the crowned jewels of twentieth century mathematics. We begin with some definitions.

Definitions 4.1. Let $p \in \mathbb{Z}$ be prime and $k \in \mathbb{N}$. A group L such that $|L| = p^k$ is called a **p-group**. A subgroup $H \leqslant G$ is a **p-subgroup** if $|H| = p^k$.

Definition 4.2. Let $H \leqslant G$ be a p-subgroup of order p^k, with $k \in \mathbb{N}$. If k is the largest integer for which p^k divides $|G|$, H is a **p-Sylow subgroup**.

To prove Sylow's Theorems, we will need a type of action called a conjugation, which takes an element of a group to its conjugate.

Definition 4.3. Let G be a group and consider $a, b \in G$. The **conjugate** of a by b is $a^b = b^{-1}ab$.

Definition 4.4. Let G be a group and $a, b \in G$ The conjugation of a by b is a map $\varpi : G \times G \to G$ such that $\varpi(a, b) = b^{-1}ab$.

Proposition 4.5. *Conjugation as defined above is an action of G on itself.*

Proof. That we have a map from $G \times G$ to G is evident from the definition of conjugation. We need to show that the map obeys the axioms of definition 2.1.

• Let $a, b, c \in G$. $a^{(b^c)} = c^{-1}b^{-1}abc = c^{-1}(b^{-1}ab)c = (a^b)^c$ so the map is associative.

• Let $a, 1 \in G$. By the definition of identities in groups, $1a = a$. □

Proposition 4.6. *The conjugation of G by an element of G is an isomorphism.*

Proof. Recall that an isomorphism is a homomorphism that is both injective and surjective. Let $a, b, g \in G$. Denote the map that conjugates an element in G by g by φ_g.

• $\varphi_g(ab) = g^{-1}abg = g^{-1}a(gg^{-1})bg = \varphi_g(a)\varphi_g(b)$ so φ_g is a homomorphism.

• Let $\varphi_g(a) = \varphi_g(a')$. By definition of conjugation, $g^{-1}ag = g^{-1}bg$. Left multiplying both sides by g and right multiplying both sides by g^{-1} yields $a = b$ so φ_g is injective.

• Consider $h \in G$. For φ_g to be surjective, there must be $h' \in G$ such that $h' = ghg^{-1}$, causing $\varphi_g(h') = h$. Since G is closed under multiplication, there is such an element, so φ is surjective. □

Definition 4.7. Since conjugations are an action, the orbits of elements G under conjugation partition a group into equivalence classes. These equivalence classes are called **conjugacy classes**.

As with cosets, we have a natural notion of a representative of a conjugacy class. This time, the representative is an element of the group that is being conjugated.

We can extend the definiton of Conjugation to any subset of G. All of the above propositions hold and the proofs are identical. We now give some important results obtained using cojugations.

As a first application of conjugation, we will now establish a remarkable theorem due to Cauchy that *guarantees* the existence of a type of subgroup of G under certain circumstances.

Theorem 4.8. ***Cauchy's Theorem*** *Let G be a finite group and let $p \in \mathbb{Z}$ be a prime number such that p divides $|G|$. G has an element, call it x, of order p.*

Proof. Consider elements $(x_1, ..., x_p) \in G \times ... \times G$ (the p-fold Cartesian product of G) such that $x_1x_2...x_p = 1$. Define C to be the set of all above Cartesian products except for $(1, ..., 1)$. Note that $x_p = (x_1...x_{p-1})^{-1}$, so by the fundamental counting principle, the cardinality of C is $|G|^{p-1} - 1$ and is not divisible by p. Define $Z = \langle z \rangle$ (with no necessary relationship to G) to be a cyclic group of order p. Specifying $z(x_1, x_2, ..., x_p) = (x_2, ..., x_p, x_1)$ amounts to conjugating $x_1...x_p$ by x_1 and therefore defines an action. Since $|Z| = p$, by Proposition 3.7, every orbit of Z in C has either 1 or p elements. If all of the orbits had p elements, p would divide C, so one orbit must have one element. Because of the way we defined our action on C, this element must of the form $(x, ..., x)$ for some $x \in G$. Thus, $x^p = 1$ and x is of order p. □

Remark 4.9. It follows from applying Lagrange's Theorem to a group of prime order that any subgroup $H \leqslant G$ of prime order must be generated by a single element.

Definition 4.10. The **center** of G, written $Z(G)$, is the kernal of the conjugation action.

Definition 4.11. The **centralizer** of b in G, written $C_G(b)$ is the stablilzer of the conjugation action on b.

Definitions 4.12. Let G be a group, $a \in G$ and $H \in G$. The **normalizer** of H in G is:

$$N_G(H) = \{g \in G : a^{-1}Ha = H\}$$

Let $N \leqslant G$. N is called a **normal subgroup** of G if $N_G(N) = G$ and we say $N \trianglelefteq G$ if N is a normal subgroup of G.

The next proposition gives an important application of normal subgroups.

Proposition 4.13. *Let G and N be groups such that $N \leqslant G$. Multiplication of left cosets, defined by:*

$$(aN)(bN) = (ab)N$$

is well defined if and only if $N \trianglelefteq G$.

Proof. Suppose $abN = a'b'N$. We need to show that N is normal in G i.e. $g^{-1}Ng = N$. Let $g \in G$ and $n \in N$. Setting $1 = a$, $n = a'$ and $b = b' = g$, we find that $1gN = ngN$ so $gN = ngN$. Since $a \in N$, $ng1 \in gnN$ hence, there exists $n' \in N$ such that $g^{-1}Ng = n' \in N$ as needed.

Conversely, suppose $g^{-1}Ng = N$. Let $a, a' \in aN$ and $b, b' \in bN$. For some $n, n' \in N$, we know $a' = an$ and $b' = bn'$. We need to show $a'b' \in abN$.

$$a'b' = (an)(bn') = a(bb^{-1})(nbn') = (ab)(b^{-1}nb)n'$$

. By assumption, $b^{-1}nb \in N$ and, since N is closed under products, the entire product is in N. Thus, $abN = a'b'N$ as needed. □

Corollary 4.14. *Let $N \trianglelefteq G$ and $g, 1 \in G$. G/N is a group with the identity $1N$ and the inverse $(gN)^{-1} = g^{-1}N$.*

Definition 4.15. The group constructed in Corollary 4.11 is called the **quotient group** of G by N.

Definition 4.16. A group G is **simple** if its only normal subgroups are G and $\{1\}$.

Proposition 4.17. ***The Class Equation*** *Let G be a finite group and let b_i be representatives of conjugacy classes of G not contained in $Z(G)$.*

$$|G| = |Z(G)| + \sum_i [G : C_G(b_i)]$$

Proof. The conjugacy classes form the equivalence classes that partition G. Either they land in the center of G or they do not. Thus, the proposition will be correct if the conjugacy classes are the cosets of the centralizer of the b_i in G. We need to show this is so. In the course of proving the Proposition 3.7, we found that the orbit of the stabilizer of the action is the orbit of the element in the group. The result follows. □

We are now ready to proceed to Sylow's Theorems.

Theorem 4.18. ***Sylow's First Theorem*** *Let G be a finite group and let $p \in \mathbb{Z}$ be a prime such that p divides $|G|$. Then G has a p-Sylow subgroup.*

Proof. Induct on $|G|$. For $|G| = 1$, the theorem is vacuously true. Suppose that $|G| = N$ and if $|G| < N$, G has a p-Sylow subgroup. We can divide the remainder of the proof into two complementary cases.

• For the first case, assume G has a proper subgroup $H < G$ such that p does not divide $[G : H]$. By the inductive hypothesis, H has a p-Sylow subgroup $P_1 \leqslant H$. By Lagrange's theorem since p does not divide the index of G with H but divides $|H|$, P_1 is p-Sylow in G.

• For the second case, assume p divides $[G : H]$ for all $H < G$. Note that since $C_G(H)$ is the stabilizer of an action, $C_G(H) < G$. Therefore, p divides $C_G(H)$. By the class equation, $|G| = |Z(G)| + [G : C_G(H)]$, so p divides $Z(G)$. Since it does, Cauchy's theorem guarentees an $x \in Z(G)$ of order p. Since the cyclic subgroup generated by x is in the normalizer of G, $\langle x\rangle \triangleleft G$. Using the above result, $G/\langle x\rangle$ is of order $p^{k-1}m < p^k m = N$, where $k \in \mathbb{N}$ is the largest power of p that divides $|G|$, so $G/\langle x\rangle$ has a p-Sylow subgroup K. Since $\langle x\rangle$ is normal, $K = \dfrac{K_1}{\langle x\rangle}$ for some $K_1 \leqslant G$. By Lagrange's theorem, $|K_1| = |K||\langle x\rangle| = p^k$, so K_1 is a p-Sylow subgroup of G. □

In proving Sylow's second theorem, we will need the following lemma:

Lemma 4.19. *Let G be a finite group. Let $p \in \mathbb{Z}$ be prime and let $H \leqslant G$ be a p-subgroup. Let P be a p-Sylow subgroup of G. $H \cap N_G(P) = H \cap P$.*

Proof. Let $K = H \cap N_G(P)$. By the Isomorphism Theorem (see the appendix), $KP/P \cong K/(K \cap P)$. Thus, $[KP : P] = [K : (K \cap P)] = p^k$ ($k \in \mathbb{N}$), where $p^k \leqslant |H|$, with the last equality following from the fact that $K \leqslant H$ is a p group. By the preceding set of equalities and Lagrange's Theorem, KP is a p group. Look at KP. Taking $1 \in K$, we see that $P \leqslant KP$. However, since P is p-Sylow in G, $|P| \geqslant |KP|$, so $P = KP$. Since this is so, $K = K \cap P$. Further, since $K = H \cap N_G(P)$, the prior equality implies $H \cap N_G(P) = H \cap N_G(P) \cap P = H \cap P$, with the last equality following from the fact that $N_G(P) \cap P = P$. □

We now proceed to Sylow's next theorem.

Theorem 4.20. ***Sylow's Second Theorem*** *Let G be a finite group, $p \in \mathbb{Z}$ be prime and $P \leqslant G$ be a p-Sylow subgroup of G. Suppose H is a p group. Then there exists $x \in G$ such that $H \leqslant P^x$. In particular, all p-Sylow subgoups are conjugates of one another.*

Proof. Let S be the set of all G conjugates of P given by $S = \{P^{y_i} : y_i \in G\}$. Since P is p-Sylow and each p^{y_i} is the conjugate of P by y, each is isomorphic to P and is therefore p-Sylow. We examine the action of H on S by conjugation. By definition, the stabilizer of this action is $N_H(S) = \cup_i N_H(P^{y_i})$. Using the above lemma, $N_H(S) = \cup_i N_H(P^{y_i}) = \cup_i (H \cap N_G(P^{y_i})) = \cup_i H \cap P^{y_i} = H \cap S$. By Proposition 3.7, $|S| = [G : N_G(P^y)]$. Since $P \leqslant N_G(P)$ and P is p-Sylow, and since p divides G and $N_G(P)$, p does not divide $|S|$, as the factors of p cancel in applying Lagrange's Theorem. Let y_i be the distinct elements of G. By the class equation, we may also write $|S| = \sum_i [H : H \cap P^{y_i}]$ since the orbits of S under conjugation by partition S into conjugacy classes $[H : H \cap P^{y_i}]$. Since H is a p group, $[H : H \cap P^{y_i}] = p^k$ for some $k \in \mathbb{N}$. Note that $p \leqslant N_G(P)$ and therefore $N_G(P)$ contains all of the powers of P in the order of G. Thus, by Lagrange's Theorem, p does not divide the order of the stabilizer. Hence, for some of these y_i, call them y_j, $[H : H \cap P^{y_j}] = 1$, since p cannot divide the order of the stabilizer. Therefore, we have j such that $H \cap P^{y_j} = H$ so $H \leqslant P^x$ as needed. □

Theorem 4.21. ***Sylow's Third Theorem*** *If G is a finite group and $p \in \mathbb{Z}$ is prime, the number of p-Sylow subgroups of G is congruent to 1 modulo p.*

Proof. Let $H = P$. We need to find the size of $\sum_j [P : P \cap P^{y_j}]$ (with the y_j from the previous proof). We know $\{P\}$ is an orbit of P^y under conjugation and is of order 1. By Lagrange's Theorem, p must divide the order of all other orbits. The result follows. □

Now, we see the information Sylow's theorems do indeed contain. They guarantee the existence of p-Sylow subgroups, tell us how to get from one p-Sylow subgroup to another, and how many distinct p-Sylow subgroups there are. One of the ways this is useful is in showing which groups are not simple. We explore this now.

Proposition 4.22. *Let G be a finite group and $p \in \mathbb{Z}$ be prime. Suppose P is the unique p-Sylow subgroup of G. $P \trianglelefteq G$.*

Proof. If P is the unique p-Sylow subgroup in P, the conjugate of P by any of its elements is in P by Sylow's Second Theorem. Thus, P is normal. □

For an example of how this type of thinking progresses, consider a group of order $56 = (2^3)(7)$. By Sylow's first theorem, there are 2-Sylow subgroups and 7-sylow subgroups. The number of 7-Sylow subgroups is either 1 or 8. If there is one, it is normal and our group is not simple. If there are 8 7-sylow subgroups, then there are 8 $(56 - 8 \cdot 6)$ elements in the group not included in those 8. These constitute a 2-Sylow subgroup which must be unique and therefore normal. Hence, a group of order 56 cannot be simple. It is interesting to ask which groups are simple. That question was answered in the twentieth century by the **Classification Theorem of Finite Groups**. The theorem states that all finite simple groups fall into just a few classes. There are cyclic groups of prime order, alternating groups (even permutations) and simple finite Lie Groups that act as matrices over finite fields. The most interesting, however, are the sporatic groups, which don't fit into any of the aforementioned classes. Remarkably, these can get quite large. The largest of them, the Fischer-Greiss Group, is of order 808017424794512875886459904961710757005754368000000000. It is often (appropriately) referred to as the Monster.

5. Appendix: The Isomorphism Theorem and Notation

We state the Isomorphism Theorem here, which we used in proving Sylow's Second Theorem. We will not prove it here, but a proof can be found in [1] or [2].

Theorem 5.1. ***The Isomorphism Theorem*** *Suppose H, K are subgroups of G and that K is a subgroup of $N_G(H)$. Then, $KH = HK \leqslant G$, $H \trianglelefteq KH$, $K \cap H \trianglelefteq K$, and $KH/H \cong K/K \cap H$.*

Where $a \cong b$ means that a is isomorphic to b.

Since I use the notation KH (K and H groups) in proofs, I should note here that it is simply the set of all products kh, where $k \in K$ and $h \in H$.

6. Acknowledgements and References

This paper was written for the Mathematics REU program at the University of Chicago in the summer of 2017. It simply wouldn't be possible without the wonderful program and without the help of my amazing mentor - Peter Morfe. I would also like to thank Professor Laci Babai for the excellent apprentice course on Linear Algebra and applications (or, as he puts it, all of Mathematics) and, of course, Professor Peter May for making the program possible and for allowing me to participate in it.

References

[1] Larry C. Grove, *Algebra*, Dover Publications, 2010.
[2] Richard S. Dummit and Robert M. Foote, *Abstract Algebra*, Prentice Hall Inc., 1991.
[3] Charles C. Pinter, *A Book of Abstract Algebra*, Dover Publications, 2010.
[4] Martin W. Liebeck, The Classification Theorem for Finite Simple Groups. *The Princeton Companion to Mathematics*, Princeton University Press, 2008.
[5] Timothy Gowers, The Monster Group. *The Princeton Companion to Mathematics*, Princeton University Press, 2008.