A Brief Glimpse into Abstract Algebra

Jadon Jones

April 22, 2024

Abstract

This paper offers a relatively self contained look into the contents of an undergraduate course in abstract algebra. Definitions and main theorems are enriched with supplementary examples and propositions that

1 Preliminaries

Before we get to the good stuff we need to lay some groundwork in set theory and number theory. One of the most important objects of study in algebra is the humble function.

1.1 Functions

Definition 1. *Given sets A and B, a function f from A to B is a subset of $A \times B$ such that for each $a \in A$ we have $(a, b) \in f$ for some $b \in B$ and if $(a, b) \in f$ and $(a, c) \in f$ implies $b = c$.*

We tend to use the notation $f : A \to B$ to say that f is a function from A to B and we write $(a, b) \in f$ as $f(a) = b$.

Definition 2. *Given a function $f : A \to B$, and a set $C \subseteq A$, the image of C under f is $f[C] = \{f(c) : c \in C\}$.*

Definition 3. *Given a function $f : A \to B$, and a set $C \subseteq B$, the image of C under f is $f^{-1}[C] = \{c \in A : f(c) \in C\}$.*

Definition 4. *We call a function $f : A \to B$ onto if for each $b \in B$, there is an $ainA$ such that $f(a) = b$.*

Definition 5. *We call a function $f : A \to B$ one to one if $f(a) = f(b)$ implies $a = b$ for every $a, b \in A$.*

If a function is both one to one and onto, we say that the function is a bijection. This leads to some nice properties about function composition. Namely that the composition of bijections is again a bijection.

1.2 number theory

Definition 6. *Given two integers a and b, we say that a divides b or $a|b$ if $b = ak$ for some integer k.*

From this definition we can now define most terms used in elementary number theory.

Definition 7. *A prime number p is an integer whose only positive divisors are 1 and p.*

Definition 8. *The greatest common divisor of integers a and b, or $gcd(a, b)$ is the greatest integer that divides both a and b*

Definition 9. *The least common multiple of integers a and b, or $lcm(a, b)$ is the least positive number that is divisible by both a and b.*

Definition 10. *Two integers a and b are congruent modulo m, or $a \equiv b \pmod{m}$ if $m|(a - b)$.*

It is fairly straightforward to show that this relation defines an equivalence class on the integers. We call the set of the corresponding equivalence classes $\mathbb{Z}_m$.

2 Groups

Definition 11. *A binary operation on a set X is a function $\cdot : A \times A \to A$.*

We usually denote $\cdot(a, b) = a \cdot b$ or sometimes we get rid of the $\cdot$ entirely if the operation is clear by context.

With this in place, we can now define our first algebraic structure.

Definition 12. *A group $(G, \cdot)$ is a set G with a binary operation G that satisfies the following properties.*

- *There is an identity element e such that $e \cdot g = g \cdot e = a$ for all $g \in G$.*
- *For each $g \in G$ there is an inverse element g' such that $g \cdot g' = g' \cdot g = e$.*
- *The operation $\cdot$ is associative.*

If G is a group, we call $|G|$ the order of the group.

Example 1. *The following familiar objects are groups:*
$(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, *and* $(\mathbb{R} \setminus \{0\}, \cdot)$

Definition 13. *If a group G satisfies $g * h = h * g$ for all $h, g \in G$, then we say that G is abelian.*

We now prove some statements about groups

Proposition 1. *If G is a group of even order, prove that there is some $a \neq e$ in G such that $a * a = e$*

Proof. Let G be a group of even order. Now construct a sets $A = \{a_1, a_1, ..., a_k\}$ and $A' = \{a'_1, a'_1, ..., a'_k\}$ where none of the elements of A and A' are the identity and no pair of distinct elements in A are inverses. Since inverses are unique, no two distinct elements in A' are inverses. If A and A' are disjoint, that means that A, A', and $\{e\}$ form a partition of G. This would imply $|G| = |A| + |A'| + |\{e\}| = 2k + 1$. This contradicts the assumption that the order of G is even. Thus $A \cap A'$ must be nonempty. This means that there is some $a_n \in A'$. But since no two distinct elements in A' are inverses, this means that $a_n = a'_n$. This then implies that $a_n * a_n = e$ by the definition of inverses. □

Proposition 2. *Let $(G, \diamond)$ and $(H, \star)$ be groups. Prove that the set $\mathcal{G} = \{(g, h) \mid g \in G, h \in H\}$ is a group under the operation $(g_1, h_1) * (g_2, h_2) = (g_1 \diamond g_2, h_1 \star h_2)$.*

Proof. Let $(G, \diamond)$ and $(H, \star)$ be groups and let $\mathcal{G}$ and $*$ be defined as above.

First we need to check that $*$ is a binary operation on $\mathcal{G}$. To see that $\mathcal{G}$ is closed under $*$, take (g_1, h_1) and (g_2, h_2) to be elements of $\mathcal{G}$. Then we see that $(g_1, h_1) * (g_2, h_2) = (g_1 \diamond g_2, h_1 \star h_2)$ is an element of $\mathcal{G}$ since $g_1 \diamond g_2 \in G$ and $h_1 \star h_2 \in H$. To show that $*$ is well defined take (g_1, h_1), (g_2, h_2), (g_3, h_3), and (g_4, h_4) to be elements of $\mathcal{G}$ such that $(g_1, h_1) = (g_2, h_2)$ and $(g_3, h_3) = (g_4, h_4)$. Then $(g_1, h_1) * (g_2, h_2) = (g_1 \diamond g_2, h_1 \star h_2) = (g_3 \diamond g_4, h_3 \star h_4) = (g_3, h_3) * (g_4, h_4)$ since $\diamond$ and $\star$ are well defined operations.

[Associativity] Take (g_1, h_1), (g_2, h_2), (g_3, h_3) to be elements of $\mathcal{G}$. It follows that

$$\begin{aligned}(g_1, h_1) * ((g_2, h_2) * (g_3, h_3)) &= (g_1, h_1) * (g_2 \diamond g_3, h_2 \star h_3)\\ &= (g_1 \diamond (g_2 \diamond g_3), h_1 \star (h_2 \star h3))\\ &= ((g_1 \diamond g_2) \diamond g_3, (h_1 \star h_2) \star h3)\\ &= (g_1 \diamond g_2, h_1 \star h_2) * (g_3, h_3)\\ &= ((g_1, h_1) * (g_2, h_2)) * (g_3, h_3)\end{aligned}$$

by the associativity of G and H. Thus $\mathcal{G}$ is associative.

[Identity] Let $e = (e_G, e_H)$, where e_G and e_H are the identity elements of G and H respectively. Then for any $(g, h) \in \mathcal{G}$, it follows that $e * (g, h) = (e_G \diamond g, e_H \star h) = (g, h) = (g \diamond e_G, h \diamond e_H) = (g, h) * e$.

[Inverses] Let $a = (g, h) \in \mathcal{G}$ and define $a' = (g', h')$. Then we know that $a * a' = (g \diamond g', h \star h') = (e_G, e_H) = (g' \diamond g, h' \star h) = a' * a$. Thus each element in $\mathcal{G}$ has an inverse.

Therefore $(\mathcal{G}, *)$ is a group.

□

The group $\mathcal{G}$ is what we call the direct product of the groups G and H. We usually denote the group as $G \times H$.

3 Permutation Groups

Definition 14. *Given a set A, we call the set of bijections from A to A S_A the set of permutations of A.*

Theorem 1. *If A is a set, then S_A is a group under function composition.*

It is not too difficult to show this fact. Furthermore, if our set $A = \{1, 2, 3, ..., n\}$, we call the group S_n.

Proposition 3. *The order of S_n is $n!$*

Proof. We will prove this using a combinitorial argument. For a permutation $\sigma \in S_n$, σ can send 1 to any of the n natural numbers. Thus there are n choices for $\sigma(1)$. Since σ needs to be one to one, we only have $n - 1$ options for $\sigma(2)$. Similarly, we have $n - k + 1$ choices for $\sigma(k)$. To find the number of total possible permutations, we take the product of the number of possibilities for each number 1 to n. This gives $|S_n| = n(n-1)(n-1)...(2)(1) = n!$. □

For ease of discussing permutations, we need to develop some notation to talk about specific permutations. A cycle $\sigma \in S_n$ of length k is a permutation such that k is the least positive integer such that $\sigma^k = e$. We can describe a cycle as a list of the form $(a_1\ a_2\ ...\ a_k)$ where $a_1 = 1$ and $a_m = \sigma(a_{m-1})$. In general, we can write any permutation in S_n as a product of cycles.

Proposition 4. *Every $\sigma \in S_n$ where $n > 1$ can be written as a product of transpositions.*

Lemma 1. *Every n-cycle can be written as a product of transpositions.*

Proof of lemma. [By Induction on Cycle Length]

[Base Case] Any 1-cycle lets say (a) can be written as $(ab)(ab)$, where $b \neq a$. The fact that a and b need to be distinct is precisely the reason the theorem does not hold in S_1.

[Inductive Step] Suppose that any (n-1)-cycle can be written as a product of transpositions. Now consider the n-cycle $\sigma = (x_1 x_2 ... x_{n-1} x_n)$. We can then see that $(x_1 x_2 ... x_n) = (x_1 x_2 ... x_{n-1})(x_{n-1} x_n)$ since $x_1, x_2, ..., x_{n-2}$ are fixed by $(x_{n-1} x_n)$ and since x_n is fixed by $(x_1 x_2 ... x_n)$. But since $(x_1 x_2 ... x_{n-1})$ is an (n-1)-cycle, by the induction hypothesis we can write $(x_1 x_2 ... x_{n-1}) = \tau_1 \tau_2 ... \tau_k$ for some transpositions $\tau_1, \tau_2, ..., \tau_k$. Thus, we see $\sigma = \tau_1 \tau_2 ... \tau_k (x_{n-1}, x_n)$ can be written as a product of transpositions.

Therefore any n-cycle can be written as a product of transpositions.

□

Proof of Proposition. Let $\sigma \in S_n$. We can then write $\sigma = \sigma_1 \sigma_2 ... \sigma_n$ where each of the σ_i's are disjoint cycles. By our lemma, each of these cycles can be written as a product of transpositions. By substituting each σ_i for an equivalent product of transpositions, we see that we can write σ as a product of transpositions.

Note that this representation of σ is not unique. Since every transposition squares to the identity, you can add as many pairs of transpositions to this product without changing the value. □

Proposition 5. *If (ab) and (cd) are distinct transpositions in S_n, then (ab) and (cd) commute if and only if (ab) and (cd) are disjoint.*

Proof. Let (ab) and cd be distinct transpositions in S_n.

[$\Longrightarrow$](By Contrapositive) Suppose that (ab) and (cd) are not disjoint. Since the transpositions are distinct that means that the two transpositions share one letter. Without loss of generality, we will assume that $b = c$. It then follows that $(ab)(cd) = (ab)(bd) = (abd)$, but $(cd)(ab) = (bd)(ab) = (adb)$. Since $(abd) \neq (adb)$, we know that the two transpositions do not commute.

$[\Longleftarrow]$ Suppose that Suppose that (ab) and cd are disjoint. This implies that $a \neq c \neq b \neq d$. It then follows that

$$\begin{gathered}(ab) \circ (bc)(a) = b = (bc) \circ (ab)(a) \\ (ab) \circ (bc)(b) = a = (bc) \circ (ab)(a) \\ (ab) \circ (bc)(c) = d = (bc) \circ (ab)(c) \\ (ab) \circ (bc)(d) = c = (bc) \circ (ab)(d) \\ (ab) \circ (bc)(x) = x = (bc) \circ (ab)(x)\end{gathered}$$

for all $x \in \{1, 2, ..., n\}$ where $x \neq a, b, c, d$. Therefore $(ab)(cd) = (cd)(ab)$, or in other words, the two transpositions commute.

□

4 Subgroups and Cyclic Subgroups

Definition 15. *If G is a group and $H \subseteq G$ is also a group, then we say that H is a subgroup of G or $H \leq G$.*

Subgroups allow us to study the structure of groups by focusing our attention on pieces of the group at a time.

Proposition 6. *The intersection of two subgroups of the group G is also a subgroup.*

Proof. Let G be a group with subgroups H_1 and H_2. Consider the set $H_1 \cap H_2$. Let e be the identity of G. Since H_1 and H_2 are subgroups we know $e \in H_1$ and $e \in H_2$. This implies $e \in H_1 \cap H_2$. Suppose that $h_1, h_2 \in H_1 \cap H_2$. Since $h_1, h_2 \in H_1$, we know $h_1 h_2 \in H_1$. Similarly, since $h_1, h_2 \in H_2$, we know $h_1 h_2 \in H_2$. Thus, we can say $h_1 h_2 \in H_1 \cap H_2$. Suppose that $h \in H_1 \cap H_2$. Since $h \in H_1$, we know $h^{-1} \in H_1$. Likewise, since $h \in H_2$, we know $h^{-1} \in H_2$. Therefore, it follows that $h^{-1} \in H_1 \cap H_2$. Thus, we can say that $H_1 \cap H_2 \leq G$. □

We often wish to consider the "smallest" subgroup of G that contains the element g. Constructing this kind of group helps us understand the larger group.

Definition 16. *Given a group G with $g \in G$, we define the cyclic subgroup generated by g or $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$.*

We call the order of an element g in G to be the least positive integer n such that $g^n = e$ so long as such an n exists. If the order of g is finite then we can say that the order of g is equal to $|\langle g \rangle|$.

Proposition 7. *Let a be an element of the group G. Prove that the order of a is equal to the order of a^{-1}.*

Proof. Let G be a group and $a \in G$. Suppose that the order of a is k. That is k is the least positive integer such that $a^k = e$. By left multiplying a^{-k} on both sides of the equation, we see a^{-k} we see

$$\begin{aligned} a^{-k}a^k &= a^{-k}e \\ a^{-k+k} &= a^{-k} \\ a^0 &= (a^{-1})^k \\ e &= (a^{-1})^k. \end{aligned}$$

To show that k is the least power such that this holds, assume there is a smaller positive integer l such that $(a^{-1})^l = e$. We then get

$$\begin{aligned} (a^{-1})^l &= (a^{-1})^k \\ a^k a^{-l} &= a^k a^{-k} \\ a^{k-l} &= a^{k-k} = e. \end{aligned}$$

But $k - l$ is positive and less than k, so this contradicts the assumption that k is the order of a. Thus k is the order of a^{-1}. □

Proposition 8. *Let G be a group and let $a \in G$ have finite order. Prove that the order of a^k for $k \in \mathbb{Z}^+$ divides the order of a.*

Proof. Let G be a group and let $a \in G$ have finite order. Suppose the order of a is n. That is n is the least positive integer such that $a^n = e$. Let k be a positive integer and consider a^k. We know that the order of a^k is finite since $(a^k)^n = (a^n)^k = e^k = e$. Suppose that the order of a^k is l. By the division algorithm, there are integers q, r where $0 \leq r < l$, such that $n = lq + r$ or equivalently $n - r = lq$. It then follows that

$$\begin{aligned} (a^k)^{n-r} &= (a^k)^{lq} \\ a^{kn}((a^{-1})^k)^r &= (((a^k)^l)^q \\ (a^n)^k((a^{-1})^k)^r &= (e)^q \\ e^k((a^{-1})^k)^r &= e \\ (a^{-k})^r &= e. \end{aligned}$$

Since the order of a^{-k} is equal to the order of a^k and $r < l$, this implies that $r = 0$. This means that $l|k$. Therefore the order of a^k divides the order of a. □

5 Finite Cyclic Groups

We say that a group G is cyclic if $G = \langle g \rangle$ for some $g \in G$. An immediate consequence of this is that all cyclic groups are abelian. When we restrict our sights to finite cyclic groups, we find that they have very nice subgroup structure.

Theorem 2. *If G is a cyclic group and $H \leq G$, then H is also cyclic.*

Proposition 9. *Let G be a finite cyclic group and let k be a positive divisor of the order of G. Then there is a unique subgroup of G with order k.*

Proof. Let $G = \langle a \rangle$ with $|G| = m$. Since m is the order of G, we know that $|a| = m$ as well. Now suppose that k is a positive divisor of m. Then we can write $m = kl$ for some natural number l. Now consider the subgroup $H = \langle a^l \rangle$ of G. Since $(a^l)^k = a^{lk} = a^m = e$ and k is the smallest such natural number where that holds, we know $|a^l| = k$. Thus $|H| = k$, so we have found a subgroup of order k.

To show that H is unique, suppose that we have two subgroups H and H' of order k. Since G is cyclic, then so are H and H'. That means we can write $H = \langle a^i \rangle$ and $H' = \langle a^j \rangle$ for some $0 \leq i, j \leq m$. Since the order of both H and H' is k, we know that k is the least positive integer such that $a^{ik} = e = a^{jk}$. But in order for k to be the least positive integer where this holds, we need $ik = m = jk$, but this implies $i = j$. Thus $H = H'$. □

Proposition 10. *If H is a subgroup of the finite cyclic group G, then the order of H divides the order of G.*

Proof. Let G be a cyclic group of order m and let H be a subgroup of order k. Since G is cyclic, we know that H must also be cyclic. Suppose that a is a generator for G and a^l is a generator for H where $0 \leq l \leq m$. Since the order of G is m, then the order of a is also m. Similarly, the order of a^l must be k. By Proposition 8, this implies that k divides m. Thus the order of H divides the order of G. □

With these two propositions, we get a complete description of the subset structure of ever finite cyclic subgroup. Namely it turns the problem of finding all the subgroups of G into the problem of finding all divisors of $|G|$.

6 Group Homomorphisms

One of almost every mathematicians favorite hobbies is studying the structure preserving maps between the mathematical structures of their choice. In the case of groups, we deal with homomorphism and isomorphisms

Definition 17. *Given groups G and G', a homomorphism $\phi : G \to G'$ is a function such that $\phi(gh) = \phi(g)\phi(h)$ for all $g, h \in G$.*

If $\phi : G \to G'$ is a bijective homomorphism then we call ϕ an isomorphism and we say that G and G' are isomorphic or $G \cong G'$.

For the following propositions assume that $\phi : G \to G'$ is a homomorphism of groups.

Proposition 11. *If $H \leq G$, then $\phi[H] \leq G'$*

Proof. Let everything be defined as above. We want to show that $\phi[H]$ is a subgroup of G'. Obviously $\phi[H]$ is a subset of G'. To show closure take $x', y' \in \phi[H]$. That is $x' = \phi(x), y' = \phi(y)$ for some $x, y \in H$. Then $x'y' = \phi(x)\phi(y) = \phi(xy)$ is an element of the image of H by the closure of H. The identity e' is in $\phi[H]$ since $e \in H$ and $\phi(e) = e'$ by exercise 1. $(x')^{-1} \in \phi(H)$ since $x^{-1} \in H$ and $\phi(x)^{-1} = \phi(x^{-1})$ by exercise 2. Therefore $\phi[H] \leq G'$. □

Proposition 12. *If $K \leq G'$ prove that $\phi^{-1}[K] \leq G$.*

Proof. Let all be as above and $K \leq G'$. We want to show $\phi^{-1}[K] \leq G$. From the definition of pre-image, it is clear that $\phi^{-1}[K]$ is a subset of G. To see closure under multiplication, take $x, y \in \phi^{-1}[K]$, then note $\phi(x)\phi(y) = \phi(xy)$. thus $xy \in \phi^{-1}[K]$. Since $e' \in K$, we know that $e \in \phi^{-1}[K]$ since $\phi(e) = e'$. Suppose that $x \in \phi^{-1}[K]$. This implies $\phi(x) \in K$, but that means $\phi(x)^{-1} = \phi(x^{-1}) \in K$. This then implies that $x^{-1} \in \phi^{-1}[K]$. Therefore $\phi^{-1}[K]$ is a subgroup of G. □

An important corollary of this statement happens when we consider the preimage of the trivial group under ϕ. We call the resulting group the kernel of ϕ or $ker(\phi)$. It turns out this group has additional structure that causes it to play an important role later on.

Proposition 13. *Prove that $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic if and only if $gcd(m, n) = 1$.*

Proof. To prove this statement we need to first prove that if $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$, then $|(a, b)| = lcm(|a|, |b|)$. The order of (a, b) is the least positive integer k such that $k(a, b) = (ka, kb) = (0, 0)$. But this shows that the only condition on k

is that it is the least positive integer that divides the order of a as well as the order of b. However this is just the definition of $lcm(|a|, |b|)$.

[$\Longrightarrow$] We will prove the forward direction by contrapositive. Suppose that $gcd(m, n) > 1$. Now consider the element $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$. By our lemma, $|(a, b)| = lcm(|a|, |b|) \leq lcm(m, n) = \frac{mn}{gcd(m,n)} < mn$. Since the order of each element of $\mathbb{Z}_m \times Z_n$ is strictly less than the order of $\mathbb{Z}_m \times \mathbb{Z}_n$. No element of $\mathbb{Z}_m \times \mathbb{Z}_n$ generates the entire group. Thus $\mathbb{Z}_m \times \mathbb{Z}_n$ is not cyclic.

[$\Longleftarrow$] Now suppose that $gcd(m, n) = 1$. Consider the element $(1, 1)$ of $\mathbb{Z}_m \times \mathbb{Z}_n$. By our lemma, $|(1, 1)| = lcm(|1|, |1|) = lcm(m, n) = \frac{mn}{gcd(m,n)} = mn$. But $|\mathbb{Z}_m \times \mathbb{Z}_n| = mn$. Thus it must be the case that $\mathbb{Z}_m \times \mathbb{Z}_n = \langle(1, 1)\rangle$. Therefore $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic. □

An immediate corollary of this is that if $gcd(m, n) = 1$, then $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$.

7 Cosets and Lagrange's Theorem

If we want to study the subgroup structure of general finite groups, we need a new way of breaking up groups into manageable pieces. One way of doing this is by considering the cosets of a given subgroup of G

Definition 18. *If G is a group, $H \leq G$ and $g \in G$, then we call $gH = \{gh : h \in H\}$ the coset of H in G containing g.*

This is the definition of a left coset, we can define a right coset the same way, only with right multiplication by g. We call the set of right cosets of H in G G/H. It turns out that the cosets of H in G form a partition of G. Furthermore, it turns out that every coset of H has the same number of elements. This leads right into the next main theorem.

Definition 19. *Given a group G and subgroup H, the index of H in G or $(G : H)$ is the number of cosets of H in G.*

Theorem 3 (Lagrange)**.** *If G is a group and $H \leq G$, then $|G| = (G : H)|H|$.*

Proposition 14. *Let $K \leq H \leq G$. Prove that $(G : K) = (G : H)(H : K)$.*

Proof. Let $K \leq H \leq G$. By Lagrange's theorem, we know $|G| = (G : H)|H|$ and $|G| = (G : K)|K|$, since H and K are subgroups of G. This implies that $(G : K)|K| = (G : H)|H|$, or equivalently $(G : K) = (G : H)\frac{|H|}{|K|}$. Since K is also a subgroup of H, we know that $(H : K)|K| = |H|$, or $\frac{|H|}{|K|} = (H : K)$. It then follows that $(G : K) = (G : H)\frac{|H|}{|K|} = (G : H)(H : K)$. □

Proposition 15. *Every group of prime order is cyclic.*

Proof. Let G be a group with prime order p. Let x be a non-identity element of G. Now consider the subgraph $H = \langle x \rangle$. By Lagrange's theorem, the order of H must divide the order of G. Since The order of G is prime, then $|H|$ must either be 1 or p. However, since $x \neq e$, the order of H has to be p. But this implies $G = H$ and thus G is cyclic. □

8 Normal Subgroups and Factor Groups

A very important aspect of G/H is that it can be imbued with a group structure for certain subgroups H. We call these special subgroups Normal.

Definition 20. *If G is a group, we say that H is normal in G or $H \trianglelefteq G$ if for each $g \in G$, we have $gH = Hg$.*

An equivalent definition is that $H \trianglelefteq G$ if $g^{-1}hg \in H$ for all $g \in G$ and $h \in H$. With normal subgroups we can define quotient groups.

Proposition 16. *The intersection of any nonempty collection of normal subgroups is again normal.*

Proof. Let G be a group and $\mathcal{H}$ be a nonempty collection of normal subgroups of G. Consider $\bar{H} = \bigcap_{H \in \mathcal{H}} H$. By a generalization of Proposition 6, we can see that $\bar{H}$ is a group. Let $g \in G$ and $h \in \bar{H}$. Since each $H \in \mathcal{H}$ is normal, we know $g^{-1}hg \in H$ for each $H \in \mathcal{H}$. But this implies $g^{-1}hg \in \bar{H}$. Thus $\bar{H} \trianglelefteq G$. □

Theorem 4. *Let $H \trianglelefteq G$, then G/H is a group under the operation defined by $(gH)(g'H) = (gg')H$.*

Theorem 5. *If $\phi : G \to G'$ is a group homomorphism, then $ker(\phi) \trianglelefteq G$.*

Theorem 6 (Homomorphism Theorem)**.** *Given groups G and G' along with a group homomorphism $\phi : G \to G'$, then $G/ker(\phi) \cong \phi[G]$.*

Example 2. $(\mathbb{Z} \times \mathbb{Z})/\langle (0,2) \rangle \cong \mathbb{Z} \times \mathbb{Z}_2$

Proof. Define $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}_2$ given by $\phi(a,b) = (a, b \pmod 2)$. It is easy to show that ϕ is a group homomorphism. Then $ker(\phi) = \{(a,b) : \phi(a,b) = (0,0)\} = \{(0,2n) : n \in \mathbb{Z}\} = \langle (0,2) \rangle$. Thus $(\mathbb{Z} \times \mathbb{Z})/\langle (0,2) \rangle \cong \mathbb{Z} \times \mathbb{Z}_2$ by the homomorphism theorem. □

9 Rings

We have previously only considered sets with one well behaved operation. However, most basic examples have at least two natural operations defined, namely addition and multiplication. In most common examples of "number like" algebraic systems, addition forms a commutative group. Multiplication, however does not always exhibit a group structure under multiplication. To generalize this notion we define rings, domains, and fields.

Definition 21. *A ring is a set R with binary operations $+$ and $\cdot$ that satisfy*

- *$(R, +)$ is an abelian group.*
- *$\cdot$ is an associative operation*
- *$a(b+c) = ab + ac$ and $(a+b)c = ac + bc$ for all $a, b, c \in R$*

If R has a multiplicative identity, we say that R is a ring with unity. If $x \in R$ has a multiplicative inverse, we call x a unit of R. If every nonzero element of R is a unit, then we say that R is a division ring.

Proposition 17. *Let R be a ring with unity. Show that the unity is unique*

Proof. Let R be a ring and suppose that both 1 and $1'$ are unities of R. Then it follows that $1 = 1 \cdot 1' = 1'$. Thus the unity is unique. □

Proposition 18. *Let R be a division ring. Show that there are exactly two idempotent elements in R*

Proof. Let R be a division ring. Clearly, we know 0 is idempotent since $0^2 = 0 * 0 = 0$. Suppose a is a nonzero idempotent element of R. Since R is a division ring, it follows that $a^2 = a$ implies $a = 1$ by a cancellation law. Thus 0 and 1 are the only idempotent elements of R. □

Definition 22. *If R and R' are rings then we call a function $\phi : R \to R'$ that satisfies $\phi(x+y) = \phi(x) + \phi(y)$ and $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in R$ a ring homomorphism.*

Definition 23. *Given a ring R and $I \subseteq R$. We say that I is a subring if I is also a ring.*

Definition 24. *Given a ring R and a subring I, we call I an ideal if $xI \subseteq I$ for every $x \in R$.*

Theorem 7. *Given a ring R with ideal I, then R/I is a subgroup under the operations $(a+I) + (b+I) = (a+b) + I$ and $(a+I)(b+I) = ab + I$.*

Proposition 19. *Show that if $I \subseteq R$ is an ideal, then there exists a homomorphism with a kernel equal to I.*

Proof. Let $I \subseteq R$ be an ideal of the ring R. Now define $\phi : R \to R/I$ by $\phi(x) = x + I$. ϕ is a homomorphisim since, for $x, y \in I$, we know $\phi(x+y) = x+y+I = x+I+y+I = \phi(x)\phi(y)$ and $\phi(xy) = xy+I = (x+I)(y+I) = \phi(x)\phi(y)$. Now notice that

$$ker(\phi) = \{x \in R : \phi(x) = 0 + I\} = \{x \in R : x + I = I\} = \{x \in R : x \in I\} = I.$$

□

10 Polynomial Rings

One of the main objects of study in an algebra or pre-calculus class are polynomials. It turns out that polynomials have nice algebraic structure when their coefficients come from rings.

Definition 25. *Let R be a commutative ring. We can define the set of polynomials over R with indeterminate x or*

$$R[x] = \left\{ \sum_{n=0}^{\infty} a_n x^n : a_n \in R, \text{ only a finite number of } a_i\text{'s are nonzero} \right\}.$$

Where addition is defined component-wise and multiplication is performed using the distributive law and multiplication in R.

With this definition, it can be easily shown that $R[x]$ is a ring. A more compact definition of addition and multiplication are given below

Definition 26. *Let R be a commutative ring, and $f = \sum_{n=0}^{\infty} a_n x^n, g = \sum_{n=0}^{\infty} b_n x^n \in R[x]$. Then*

$$f + g = \sum_{n=0}^{\infty} (a_n + b_n) x^n$$

$$fg = \sum_{n=0}^{\infty} d_n x^n$$

where $d_n = \sum_{i+j=n} a_i b_j$.

We often need to talk about the highest power of a polynomial with a nonzero coefficient, we call this the degree of the polynomial.

Example 3. *How many polynomials of degree less than or equal to 2 are in $\mathbb{Z}_2[x]$?*

answer.

$$\begin{array}{cccc} 0, & x, & x^2, & x+x^2 \\ 1, & 1+x, & 1+x^2, & 1+x+x^2. \end{array}$$

□

The degree of polynomials happen to have some nice properties relating to multiplication and addition.

Theorem 8. *Let $f, g \in R[x]$ where R has no zero divisors. Suppose that $deg(f) = n$ and $deg(g) = m$ then $deg(fg) = m + n$ and $deg(f + g) = max(m, n)$ so long as $m \neq n$ or $a_n \neq -b_m$.*

Proposition 20. *If R is a ring and $R \subset S \subseteq R[x]$ is a subring, then there is no element of S with maximum degree.*

Proof. Let R be an integral domain with $R \subset S \subseteq R[x]$ is a subring of $R[x]$. Suppose that f has the maximum degree of a polynomial in S, lets say $def(f) = m$. Since $R \subset S$ S must contain an element of degree greater than zero. Thus $m \neq 0$. However $deg(f * f) = m + m = 2m \geq m$. This leads to a contradiction, thus there is no polynomial of maximum degree in S. □

11 Group Actions

The proof of Lagrange's theorem involved partitioning the group G into nice subsets which allowed us to use a counting argument. The main idea of considering group actions is twofold, first, they allow us to turn some group theory problems into counting problems, second, they can help us understand how to deal with "symmetries" in counting problems.

Definition 27. *Let G be a group and X be a set. We say an action of G on X is a map $* : G \times X \to X$ such that*

1. *$e * x = x$ for all $x \in X$*

2. *$(g_1 g_2) * x = g_1 * (g_2 * x)$ for all $g_1, g_2 \in G$ and $x \in X$.*

Example 4. *Every group G acts on itself via left multiplication.*

Proof. Let G be a group with $g_1, g_2, g_3 \in G$. Then clearly $e(g_1) = g_1$ by the definition of identity and $(g_1 g_2) g_3 = g_1(g_2 g_3)$ by associativity. Thus G acts on itself via left multiplication. □

Example 5. *If G is a group and $H \trianglelefteq G$, then G acts on G by conjugation.*

Proof. Let G be a group. Then for $x \in G$ and $g_1, g_2 \in G$ we have $e^{-1}xe = ex = x$. We also have $(g_1g_2)^{-1}xg_1g_2 = g_2^{-1}g_1^{-1}xg_1g_2 = g_2^{-1}(g_1^{-1}xg_1)g_2$. Thus G acts on G via conjugation. □

With the basic definition in place, we can define some useful sets and properties relating to group actions.

Definition 28. *Given a group G that acts on the set X, we call the set $G_x = \{g \in G : g(x) = x\}$ the stabilizer subgroup of $x \in X$ and the set $X_g = \{x \in X : g(x) = x\}$ the fixed point set under $g \in G$.*

The next theorem is easily verified.

Theorem 9. *For a group G that acts on a set X, G_x is a group for each $x \in X$.*

We next discuss the idea of orbits. These describe how a group action partitions the sets that are acted upon.

Theorem 10. *If G acts on the set X. For $x_1, x_2 \in X$ if is the relation defined by $x_1 \sim x_2$ iff there is a $g \in G$ such that $gx_1 = x_2$, then $\sim$ is an equivalence relation.*

Proof. [reflexive] Suppose $x \in X$ then $ex = x$, thus x x.

[symmetric] Suppose $x_1 \sim x_2$. Then $x_1 = gx_2$ for some $g \in G$. Then $g^{-1}x_1 = g^{-1}gx_2 = ex_2 = x_2$. Thus $x_2 \sim x_1$.

[transitive] Suppose $x_1 \sim x_2$ and $x_2 \sim x_3$. Then $x_1 = g_1x_2$ and $x_2 = g_2x_3$ for some $g_1, g_2 \in G$. But then $x_1 = g_1(g_2x_3) = (g_1g_2)x_3$. Thus $g_1 \sim g_3$. □

This equivalence relation creates a partition of X. We the equivalence class containing x the orbit of x under G, or more compactly $\mathcal{O}_x = \{gx : g \in G\}$.

Theorem 11. *If X is a G-set and $x \in X$, then $|\mathcal{O}_x| = (G : G_x)$.*

Proof. Let X be a G-set and $x \in X$. We want to construct a bijection between the orbit under x and G/G_x. Let $\phi : \mathcal{O}_x \to G/G_x$ be a function defined by $\phi(gx) = gG_x$. This function is well defined since if $gx = g'x$ then clearly $g = (g'h)$ for some $h \in G_x$, thus, we see $gG_x = g'hG_x = g'G_x$.

To show that ϕ is one-to-one, suppose $gG_x = g'G_x$. This implies that $g = g'h$ for some $h \in G_x$. Thus $gx = g'hx = g'x$.

To show that ϕ is onto take $gG_x \in G/G_x$. Then $\phi(gx) = gG_x$. Therefore ϕ is a bijection and $|\mathcal{O}_x| = |G/G_x| = (G : G_x)$. □

We now consider different properties that group actions can have.

Definition 29. *A group G acts transitively on a set X if for every $x_1, x_2 \in X$, we get $x_1 = gx_2$ for some $g \in G$.*

Proposition 21. *G acts transitively on X iff there is only one orbit.*

Proof. Let X be a G-set. Suppose that G acts transitively on X. That is for each $x_1, x_2 \in X$, we have $x_1 = gx_2$ for some $g \in G$. But by definition this tells us that $x_1 \sim x_2$ and thus they are in the same orbit.

Conversely, suppose that there is only one orbit. That means that for any $x, x' \in X$ we have $x' \in \mathcal{O}_x$. Thus $x' = gx$. Thus G acts transitively. □

Definition 30. *G acts faithfully on a G-set X if the identity is the only element which fixes all $x \in X$*

This definition is equivalent to saying that $X_g \subset X$ for all $g \in G$ where $g \neq e$.

Example 6. *The action of G on itself by left multiplication is faithful.*

Proof. Let G be a group. Suppose that $g \in G$ that fixes all elements of G. Then that would imply $gg = g$. However by left cancellation, this implies $g = e$. Thus G acts faithfully on G via left multiplication. □

12 Burnside's Theorem

In this section we use group actions to derive Burnside's theorem. This theorem can be used to count arrangements where some configurations are considered equivalent under a group of symmetries and it can be used to form counting arguments to prove theorems about groups.

Theorem 12 (Burnside)**.** *If G is a finite group and X a finite G-set where r is the number of orbits in X under G, then*

$$r|G| = \sum_{g \in G} |X_g|.$$

Proof. Let $S = \{(g, x) \in G \times X : gx = x\}$. If we pick some $g \in G$, then the set of $x \in X$ such that $(g, x) \in S$ is simply X_s. Thus, we see

$$|S| = \sum_{g \in G} |X_g|$$

If we instead pick a $x \in X$, then the set $g \in G$ such that $(g, s) \in S$ is G_x. Thus, we also have

$$|S| = \sum_{x \in X} |G_x|$$

We have previously shown that $|\mathcal{O}_x| = (G : G_x) = \frac{|G|}{|G_x|}$. This then implies that $|G_x| = \frac{|G|}{|\mathcal{O}_x|}$. Therefore

$$|S| = \sum_{x \in X} \frac{|G|}{|\mathcal{O}_x|} = |G| \sum_{x \in X} \frac{1}{|\mathcal{O}_x|}$$

Within each orbit, $|\mathcal{O}_x|$ is constant, so we can say

$$|S| = |G| \sum_{\text{orbit } \mathcal{O}} \sum_{x \in \mathcal{O}} \frac{1}{|\mathcal{O}_x|} = |G| \sum_{\text{orbit } \mathcal{O}} 1 = |G| r.$$

Putting everything together we get that

$$r|G| = |S| = \sum_{g \in G} |X_g|.$$

□

An immediate corollary if this is that

$$\# \text{ of orbits } = \frac{1}{|G|} \sum_{g \in G} |X_g|.$$

This form is useful in counting with respect to some group of symmetries. For example, if the G-Set represents some labels you can assign to a geometric object that has some symmetry and you wish to count the distinct ways of assigning labels, then the orbits become the distinct assignments the group G represents the symmetries of the object. This provides a bit more systematic way to count configurations in these types of problems.

We can also apply Burnside's formula to see some other familiar results.

Example 7. *Let G be a group and $H \leq G$ and let H act on G via left multiplication. Apply Burnside's theorem to this action.*

solution. Let G be a group and $H \leq G$ and let H act on G via left multiplication. For $x \in G$, we see $\mathcal{O}_x = \{hx | h \in H\} = Hg$. Under this action, the orbits are simply right cosets, thus the number of orbits is simply $(G : H)$. Now notice that for $h \in H$ $X_h = \{g \in G : hg = g\}$ However, this set is empty unless $h = e$ and in that case $X_e = \{g \in G : eg = g\} = G$. Therefore by Burnside's theorem, we see

$$(G : H)|H| = \sum_{h \in H} |X_h| = |X_e| = G$$

. □

This previous result is exactly the statement of Lagrange's theorem. This just gives a glimpse into how group actions can be used in group theory. In fact, with a little bit more work and a dash of induction, you use these sorts of methods to prove the existence and classification of so-called Sylow p-subgroups. This however is slightly beyond the scope of this paper.