PMATH 347: Groups & Rings

Syed Mustafa Raza Rizvi

October 29, 2020

These are my notes for my 2nd year course Groups & Rings (PMATH 347) at the University of Waterloo. They are pretty similar to the content you may see in the course notes provided by Professor Ross Willard.
You will find that these aren't very useful as notes, in the sense that they are not significantly shorter than the content in the course notes, these notes are really just a way for me to type down and absorb the content I am learning. Also, I won't be including the proofs, it's best to read the course notes for that.
Reference text: Abstract Algebra, David S. Dummit, Richard M. Foote.

If the university or staff feel that I should take down this document, please feel free to contact me on github (https://github.com/meowstafa)

Contents

Part I

Group Theory

Chapter 1

Dihedral Symmetries and Permutations

Let C_n denote a regular n-gon for $n \geq 3$ (in $\mathbb{R}^3$). **A dihedral symmetry** of C_n is any "rigid motion" that moves C_n back to itself (so that it looks unchanged).
For example, the dihedral symmetries of C_6 include; Rotations (by multiples of 60 deg), "flips" (**reflections**) along an axis, and the "identity" symmetry (which does nothing)

Definition. D_{2n} = the set of all dihedral symmetries of C_n Note. In geometry the set is called D_n

Definition. Let X be any non-empty set.

- A **permutation** of X is a bijection $\sigma : X \to X$
- S_X is the set of all permutations of X
- If $X = \{1, 2, 3, \ldots, n\}$ then we denote S_X by S_n

Special notation, terminology.

- id denotes the identity permutation in S_X ($\mathrm{id}(x) = x$ for all $x \in X$)
- The cycle notation for id is () or just .
- Given $\sigma \in S_X$, the **support** of σ is the set

$$supp(\sigma) = \{x \in X : \sigma(x) \neq x\}$$

  That is, the supp(σ) is the set of elements in the cycle notation of σ
- σ, τ are **disjoint** if supp(σ) $\cap$ supp(τ)= $\emptyset$

Chapter 3

Definition of a Group

Definition. Let A be a non-empty set. A **binary operation on** A is a function $* : A \times A \to A$
Notice that a binary operation requires closure by definition

Definition. A **group** is an ordered pair $(G, *)$ where

- G is a non-empty set
- $*$ is a binary operation on G;

which jointly satisfy the following further conditions

1. $*$ is **associative**: $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$
2. There exists an **identity** element $e \in G : a * e = e * a = a$ for all $a \in G$
3. Every $a \in G$ has a 2-sided **inverse**, i.e., an element $a' \in G$ which satisfies $a * a' = a' * a = e$ (where e is the identity element from 2)

Note: A group, G, is called **abelian** (or **commutative**) if any $a, b \in G$ satisfy the equation $a * b = b * a$
Note that 2 ensures that a group is always non-empty

Notation: when discussing generic groups

- We often denote a group $(G, *)$ by just G. Unless we want to distinguish the group from its underlying set, e.g. then group is denoted by $\mathbb{G}$ and the set by just G
- We pften write ab or $a \cdot b$ for $a * b$
- Denote the identity element e of G by 1, often.
- Denote the inverse a' of an element a by a^{-1}, often
- The **order** of a group G, denoted $|G|$, is the number of its elements

Definition. In any group G, if $a \in G$ then define $a^0 = 1$ and $a^{n+1} = a \cdot a^n$ for $n \geq 0$. Also define $a^{-n} = (a^n)^{-1}$ for $n \geq 2$. This notation satisifes the usual rules of exponents.

Lemma 3.2. Let $(G, \cdot)$ be a group, $a \in G$, and $m, n \in \mathbb{Z}$

1. $a^1 = a$
2. $a^m \cdot a^n = a^{m+n}$
3. $(a^m)^n = a^{mn}$

Warning: in general $(ab)^n = a^n b^n$ is not true, since $(ab)^2 = abab$ and we need commutativity to get $a^2 b^2$.
Also, *additive notation* is used for operations involving the symbol $+$. Since for groups like $(\mathbb{R}, +)$, writing $a^n = a + \cdots + a$ is awkward.
Additive Notation. When the group operation is denoted by $+$ (or whenever the operation is being thought of as something "like addition") we may

- Denote the identity element by 0 (instead of 1)
- Denote the inverses by $-a$ (instead of a^{-1})
- Denote $a + \cdots + a$ (n times) by na (instead of a^n), for any $n \geq 1$

This notation is seldom used for non-abelian groups

Definition. For a group G and element $a \in G$, the **order** of a (denoted $|a|$ or $\circ(a)$) is the least integer $n > 0$ such that $a^n = 1$, if it exists. If no such n exists (this requires G to be infinite), then the order of a is defined to be ∞ **Remark.** The word has been used in two different ways

- of a *group* (the number of elements of the group) or
- of an *element* of a group (the least positive exponent giving the identity element)

Proposition 3.3. Suppose G is a group, $a \in G$, and $\circ(a) = n < \infty$. Then for all $k \in \mathbb{Z}$, $a^k = 1 \iff n|k$

Chapter 4

Elementary Properties of Groups

Proposition 4.1. Let G be a group and $a, b, u, v \in G$

1. Left and right cancellation:
   (a) if $au = av$, then $u = v$
   (b) If $ub = vb$, then $u = v$
2. the equations $ax = b$ and $ya = b$ have unique solutions for $x, y \in G$

Corollary 4.2. In any group G, the identity element is unique

Proposition 4.3. Suppose G is a group

1. Each $a \in G$ has a unique inverse a^{-1}
2. $(a^{-1})^{-1} = a$ for all $a \in G$
3. $(ab)^{-1} = (b^{-1})(a^{-1})$ for all $a, b \in G$

Some terminology:

1. G is **abelian** if $ab = ba$ for all $a, b \in G$
2. If $a \in G$ then $\langle a \rangle$ denotes the set $\{a^n : n \in \mathbb{Z}\}$. Thus $\langle a \rangle \subseteq G$
3. G is **cyclic** if there exists $a \in G$ such that $G = \langle a \rangle$
   In this case we call a a **generator** of G
   Note: A cyclic group can have more than one generator

Chapter 5

Isomorphisms

The most fundamental relation between groups is that of *isomorphism*

Definition. Let $\mathbb{G} = (G, \star)$ and $(\mathbb{H}, \diamond)$ be groups. A function $\varphi : G \to H$ is an **isomorphism from $\mathbb{G}$ to $\mathbb{H}$** if φ is a bijection and

$$\varphi(x \star y) = \varphi(x) \diamond \varphi(y) \qquad \textit{for all } x, y \in G$$

Theology:

1. If φ is an isomorphism from $\mathbb{G}$ to $\mathbb{H}$, then the operation tables for $\mathbb{G}$ and $\mathbb{H}$ are "the same" (modulo the translation given by φ)
2. If the operation tables for $\mathbb{G}$ and $\mathbb{H}$ are "the same" in this sense, then $\mathbb{G}$ and $\mathbb{H}$ are "essentially the same group"

Definition. We say that groups $\mathbb{G}$ and $\mathbb{H}$ are **isomorphic** and write $\mathbb{G} \cong \mathbb{H}$ if ther exists an isomorphism $\varphi : G \to H$

Chapter 6

Subgroups

Definition. Let $\mathbb{G} = (G, \cdot)$ be a group. A **subgroup** of $\mathbb{G}$ is a subset $H \subseteq G$ satisfying

1. $H \neq \emptyset$
2. H is closed under products; i.e. $a, b \in H$ implies $ab \in H$
3. H is closed under inverses; i.e. $a \in H$ implies $a^{-1} \in H$

Proposition 6.2. If $\mathbb{G} = (G, \cdot)$ is a group and H is a subgroup of $\mathbb{G}$, then $\mathbb{H} = (H, \cdot \restriction_H)$ is a group in its own right. ($\cdot \restriction_H$ is the restriction of the operation $\cdot$ to pairs from H)

Conventions.

1. In light of Proposition 6.2, we will return to beign lazy and not distinguish between $\mathbb{H}$ and H.
2. We will no longer write $(H, \cdot \restriction_H)$ and instead just write $(H, \cdot)$
3. We write $H \leq G$ or $\mathbb{H} \leq \mathbb{G}$ to mean H is a subgroup of $\mathbb{G}$

Claim. For $a \in G$, $\langle a \rangle \leq G$

Definition. If G is a group and $a \in G$, then $\langle a \rangle$ is called the **cyclic subgroup** of G **generated by** a

Cyclic subgroups are important and are the easiest subgroups to find. Note that if G is a group and $a \in G$, then $\langle a \rangle$ is the *smallest* subgroup of G containing a. Furthermore, any subgroup that contains a must also contain $\langle a \rangle$.

Proposition 6.6. Let G be a group and $a \in G$

1. If $\circ(a) = \infty$ then $a^i \neq a^j$ for all $i \neq j$ and $\langle a \rangle \cong (\mathbb{Z}, +)$

2. If $\circ(a) = n$, then $\langle a \rangle = \{a^0, a^1, \ldots, a^{n-1}\}$ and $\langle a \rangle \cong (\mathbb{Z}_n, +)$

Corollary 6.7. If G is a group and $a \in G$, then $\circ(a) = |\langle a \rangle|$. That is, the orders of an element and the cyclic subgroup generated by that element are the same

Chapter 7

Cosets and Lagrange's Theorem

Definition. Suppose G is a group, $H \leq G$, and $a \in G$. The **left coset of H determined by a** is the set

$$aH := \{ah : h \in H\}$$

E.g. $1H = H$.
Warning: aH is generally *not* a subgroup of G.
Note: When using additive notation, we write $a + H$ instead of aH

Lemma 7.2. For all $a \in G, |aH| = |H|$. Hence all left cosets of H have the same size as H
Caution: It can happen that $aH = bH$ even if $a \neq b$

Proposition 7.3. Suppose $H \leq G$. The set of left cosets of H partition G; that is

1. $\cup\{aH : a \in G\} = G$
2. If $aH \neq bH$ then $aH \cap bH = \emptyset$

Theorem 7.4. (Lagrange's Theorem). Suppose G is a finite group and $H \leq G$. Then $|H|$ divides $|G|$

Corollary 7.5. Suppose G is a finite group and $a \in G$. Then $\circ(a)$ divides $|G|$

Corollary 7.6. If G is a finite group and $|G| = n$, then $x^n = 1$ for all $x \in G$

Corollary 7.7. If G is a finite group and $|G| = p$ is prime, then G is cyclic
Note: the proof of the previous corollary shows that if $|G|$ is prime then *every* non-identity element of G is a generator

Chapter 8

Cosets (continued), Normal Subgroups

The number of left and right cosets of a subgroup are the same, however, they aren't always the same. This is because there is a bijection between the collection of left cosets and right cosets of H

Definition. If G is a group and $H \leq G$, the **index** of H in G, denoted $[G : H]$, is the number of distinct left (or right) cosets of H.
If G is *finite*, then

$$[G : H] = \frac{|G|}{|H|}$$

Definition. Suppsose $H \leq G$. We say that H is **normal**, or is a **normal subgroup** and write $H \triangleleft G$, if $aH = Ha$ for all $a \in G$

Note that this definition does not talk about commutivity, it talks about the left and right cosets being equal
Of course if G is abelian then every subgroup is normal. It is generally tedious to check whether a subgroup is normal or not.
Notation: Generalizing the notation used for cosets: If A, B are nonempty subsets of a group G and $g \in G$ then

$$gA := \{ga : a \in A\}$$
$$Ag := \{ag : a \in A\}$$
$$AB := \{ab : a \in A \text{ and } b \in B\}$$
$$A^{-1} := \{a^{-1} : a \in A\}$$

With this notation we can "multiply" and "invert" nonempty sets as well as elements of G. The notation obeys the associative property of multiplication $(Ag)B = A(gB)$, so we

can just write AgB, law of inverses $(AB)^{-1} = B^{-1}A^{-1}$ and $(gA)^{-1} = A^{-1}g^{-1}$. However, *cancellation laws do not work in this context, set cancellation is not a thing*, e.g. for any $a, b \in G$ it is true that $aG = bG$, but this does not imply that $a = b$ as the only thing the equation conveys is that the two sets generated are equal. Similarly, it is not true that $AA^{-1} = 1$ (or $\{1\}$). Inverses of sets are not true inverses

The notation shortens the definition of a subgroup;

Fact: If G is a group and $\varnothing \neq H \subseteq G$, then the following are equivalent

1. $H \leq G$
2. $HH \subseteq H$ and $H^{-1} \subseteq H$
3. $HH = H$ and $H^{-1} = H$

This is since $HH \subseteq H \iff H$ is closed under products, $H^{-1} \subseteq H \iff H$ is closed under inverses

Chapter 9

Applications of Normality

Proposition 9.1. Suppose $H \leq G$. The following are equivalent (TFAE):

1. $H \triangleleft G$
2. $aHa^{-1} = H$ for all $a \in G$
3. $aHa^{-1} \subseteq H$ for all $a \in G$
4. If $h \in H$, then $aha^{-1} \in H$ for all $a \in G$

Lemma 9.2. Suppose $H, K \triangleleft G$ and $H \cap K = \{1\}$. Then $hk = kh$ for all $h \in H, k \in K$

Useful trick: For $a, b \in G$, their **commutator** is $[a, b] = a^{-1}b^{-1}ab$. This makes it easy to show $ab = ba \iff [a, b] = 1$ by using prop 9.1. and showing the expression is in the intersection

If we have that H, K are two subgroups of G, then $H \subseteq HK$ (since $1 \in K$) and $K \subseteq HK$ (because $1 \in H$), but HK does not need to be a subgroup.

Proposition 9.3. Suppose G is a group and $H, K \leq G$. If either $H \triangleleft G$ or $K \triangleleft G$, then $HK \leq G$
Proof sketch:
Sub-claim: $HK = KH$. Proof: assume H is normal, since $HK = \cup_{k \in K} Hk = \cup_{k \in K} kH = KH$
Show that $(HK)(HK) \subseteq HK$ and $(HK)^{-1} \subseteq HK$, by making use of $HH = H = H^{-1}$

Definition. Suppose G is a group and $H \leq G$. The **normalizer** of H, denoted $N_G(H)$, is the set

$$N_G(H) = \{a \in G : aH = Ha\}$$

Normalizers are useful in many contexts, a couple of them are

1. $N_G(H) \leq G$
2. $H \triangleleft G \iff N_G(H) = G$

Corollary 9.4. Suppose G is a group and $H, K \leq G$. If $K \subseteq N_G(H)$ (or $H \subseteq N_G(K)$) then $HK \leq G$

Chapter 10

Direct Products

Definition. Let $(G_1, \star)$ and $(G_2, \diamond)$ be groups. Their **direct product** is $(G_1 \times G_2, *)$ where

$$(a_1, a_2) * (b_1, b_2) = (a_1 \star b_1, a_2 \diamond b_2)$$

More clarification: We are defining $(G_1 \times G_2, *)$, which means there is some new binary operation $*$ on the set of all the ordered pairs (tuple), i.e. of all cartesian products, of elements from G_1 and G_2. Whereby, applying the binary operation on elements from $(G_1 \times G_2, *)$ means that we evaluate individual entries/components with respect to the binary operation associated with the group they come from.
E.g. letting $G_1 = G_2 = \mathbb{R}$ would give us the euclidean plane ($\mathbb{R}^2$) with the appropriate restrictions.

Fact: If G_1, G_2 are groups, then $G_1 \times G_2$ is also a group

Notation:

- If both $\star$ and $\diamond$ are written as $+$ then we may also write $*$ as $+$
- Products of more factors are defined analogously. $G^n = \underbrace{G \times \cdots \times G}_{n}$

Theorem 10.1. Let G be a group. Suppose there exists $H, K \triangleleft G$ satisfying

1. $H \cap K = \{1\}$
2. $HK = G$

Then $G \cong H \times K$

Corollary 10.3. $(\mathbb{Z}_{mn}, +) \cong (\mathbb{Z}_m, +) \times (\mathbb{Z}_n, +)$ provided $\gcd(m, n) = 1$

Chapter 11

Homomorphisms

Definition. Let $G = (G, \star)$ and $H = (H, \diamond)$ be groups. A function $\varphi : G \to H$ is a **homomorphism** if

$$\varphi(x \star y) = \varphi(x) \diamond \varphi(y) \qquad \forall x, y \in G$$

Any isomorphism is a homomorphism

Definition. Let $\varphi : G \to H$ be a homomorphism

1. $\text{im}(\varphi)$ denotes the **image** (or **range**) of φ. That is, $\text{im}(\varphi) = \{\varphi(x) : x \in G\}$.
2. The **kernel** of φ, $\ker(\varphi)$, is the set

$$\{x \in G : \varphi(x) = 1\}$$

Proposition 11.2. Let $\varphi : G \to H$ be a homomorphism

1. $\varphi(1_G) = 1_H$
2. $\varphi(g^{-1}) = (\varphi(g))^{-1}$ for all $g \in G$
3. More generally, $\varphi(g^n) = (\varphi(g))^n$ for all $n \in \mathbb{Z}$
4. $\ker \varphi \leq G$ and $\text{im}(\varphi) \leq H$

Proposition 11.3. Let $\varphi : G \to H$ be a homomorphism. Then $\ker \varphi \triangleleft G$

Chapter 12

Quotient Groups

Definition. Suppose G is a group and $H \leq G$. Then G/H denotes the set of all left cosets of H

Examples:

1. If $G = (\mathbb{Z}, +)$ and $H = \langle 5 \rangle = 5\mathbb{Z}$, then
   $G/H = \mathbb{Z}/5\mathbb{Z} = \{5\mathbb{Z}, 1 + 5\mathbb{Z}, 2 + 5\mathbb{Z}, 3 + 5\mathbb{Z}, 4 + 5\mathbb{Z}\}$
2. If $G = (\mathbb{C}^\times, \cdot)$ and $H = S = \{z : |z| = 1\}$, then $G/H = \mathbb{C}^\times/S = \{$all circles centered at $0\}$

We want to define an operation $\cdot$ on G/H. That for any given left cosets of C, D of H, we want to define another left coset $C \cdot D$. Which would be

$$C \cdot D \stackrel{df}{=} CD = \{cd : c \in C, d \in D\}$$

or equivalently $(aH) \cdot (bH) = (aH)(bH)$. But this $(aH)(bH)$ might not be a left coset of H, however, this issue will be solved if H is *normal*

Proposition 12.1. If $N \triangleleft G$, then $(aN)(bN) = (ab)N \in G/N$, $\forall a, b \in G$

Definition. If $N \triangleleft G$, then $\cdot$ is defined on G/N by $(aN) \cdot (bN) \stackrel{df}{=} (aN)(bN) = (ab)N$

Notation: When the operation on G is denoted by $+$ we switch to the additive notation $(a + N) + (b + N) = (a + b) + N \in G/N$, $\forall a, b \in G$

Proposition 12.4. Suppose $N \triangleleft G$. Then $(G/N, \cdot)$ is a group

Definition. Suppose $N \triangleleft G$. The group $(G/N, \cdot)$ is called the **quotient group of** G **by** N (or the quotient group of G **modulo** N)

Examples:

1. $\mathbb{Z}/5\mathbb{Z}$. Its elements are the 5 cosets of $5\mathbb{Z}$, this quotient group is easily seen to be isomorphic to $\mathbb{Z}_5$. The suitable isomorphism being $\mathbb{Z}_5 \to \mathbb{Z}/5\mathbb{Z}$ which sends $a \mapsto a + 5\mathbb{Z}$ ($\mathbb{Z}_5$ is often defined to be $\mathbb{Z}/5\mathbb{Z}$)
2. $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$
3. $\mathbb{C}^\times/S \cong (\mathbb{R}^{>0}, \cdot)$

Chapter 13

1st Isomorphism Theorem

Definition. Suppose $N \triangleleft G$. Define $\pi_N : G \to G/N$ by $\pi_N(g) = gN$
π_N is called the "mod N projection map"

Lemma 13.1. If $N \triangleleft G$, then $\pi_N : G \to G/N$ is a homomorphism and $\ker \pi_N = N$

If we consider an arbitrary homomorphism $\varphi : G \to H$. Generally, we cannot assume that φ is surjective or injective. Let $N = \ker \varphi$ and $H_0 = \text{im}(\varphi)$. Recall that $N \triangleleft G$ and $H_0 \leq H$.
For each $h \in H_0$, the preimage $\varphi^{-1}(h) = \{g \in G : \varphi(g) = h\}$ is called the **fiber** of φ above h. This notation of $\varphi^{-1}(h)$ here is only symbolic, it is not claiming that φ is invertible, it is just representing a set.
Note: the fiber of 1_H is $\ker(\varphi) = Ns$

Proposition 13.2. Suppose $\varphi : G \to H$ is a homomorphism and $N = \ker \varphi$. The fibers of φ are precisely the left (= right) cosets of N

We observe that φ is injective iff each of its fibers consists of just one element. By Prop 13.2 and Lemma 7.2, this holds *iff* $|\ker \varphi| = |N| = 1$. We thus get

Corollary 13.3. A homomorphism $\varphi : G \to H$ is injective $\iff \ker \varphi = \{1_G\}$

Theorem 13.4. (1st Isomorphism Theorem). Suppose $\varphi : G \to H$ is a surjective homomorphism. Then $G/\ker \varphi \cong H$

Chapter 14

2nd and 3rd Isomorphism Theorem

For the proof of the 1st Isomorphism theorem we used a function that satisified
$\overline{\varphi}(aN) = \varphi(a),\ \forall a \in G$
Which is equivalent to $\overline{\varphi(\pi_N(a))} = \varphi(a),\ \forall a \in G$. And equivalently $\overline{\varphi} \circ \pi_N = \varphi$
We say that φ **factors through** π_N via $\overline{\varphi}$

Theorem 14.1. (2nd Isomorphism Theorem). Suppose G is a group and $H, N \leq G$ with $N \triangleleft G$. Then $(H \cap N) \triangleleft H$ and $HN/N \cong H/(H \cap N)$

Theorem 14.2. (3rd Isomorphism Theorem). Suppose G is a group and $N, K \triangleleft G$ with $N \leq K$. Then $K/N \triangleleft G/N$ and $G/K \cong (G/N)/(K/N)$

Chapter 15

Group Actions

Definition. Let G be a group and X a non-empty set. An **action of G on X** is a mapping which assigns to each $g \in G$ a permutation π_g of X, and which moreover satisfies

$$\pi_{gh} = \pi_g \circ \pi_h \qquad \forall g, h \in G$$

The mapping is $\pi : G \to S_X$

Definition. Alternative Definition.
Let G be a group and X a non-empty set. An **action of G on X** is a homomorphism $\pi : G \to S_X$
Example:

1. $G = GL_n(\mathbb{R}), X = \mathbb{R}^n$. Assign each $A \in GL_n(\mathbb{R})$ to L_A where $(L_A : \mathbb{R}^n \to \mathbb{R}^n, L_A(\vec{x}) = A\vec{x})$
   Since A is invertible $\implies$ L_A is an isomorphism $\implies$ L_A is a bijection so it is a permutation of $\mathbb{R}^n$
   So $L : GL_n(\mathbb{R}) \to S_{\mathbb{R}^n}$ this function sends $A \mapsto L_A$
   This function satisifes the homomorphism property $L_{AB} = L_A \circ L_B$. So L is an action of $GL_n(\mathbb{R})$ on $\mathbb{R}^n$
2. G naturally acts on itself in a number of ways. One way is that for each $g \in G$ let $\psi_g : G \to G$ given by $\psi_g(x) = gxg^{-1}$. ψ_g is an automorphism of G so is a permutation of G. And for any $g, h \in G$

   $$\psi_{gh}(x) = (gh)x(gh)^{-1} = ghxh^{-1}g^{-1} = g\psi_h(x)g^{-1} = \psi_g(\psi_h(x)) = (\psi_g \circ \psi_h)(x)$$

   This is true for all $x \in G$, so $\psi_{gh} = \psi_g \circ \psi_h$. So the map $g \mapsto \psi_g$ is a homomorphism $\psi : G \to S_G$

Notation: If π is an action of G on X, and $g \in G$ and $a, b \in X$, then $\pi_a = b$ by writing $g \cdot a = b$ and say that *g moves a to b*. Note; $\pi_{gh} = \pi_g \circ \pi_h$ which is $(gh) \cdot a = g \cdot (h \cdot a)$ for all $a \in X$. $\pi_1 = \text{id}$, which translates to $1 \cdot a = a$ for all $a \in X$

Definition. Let π be an action of G on X

1. The **kernel** of the action is the kernel of π as a homomorphism $G \to S_X$
2. The action is **faithful** if its kernel is $\{1\}$ (equivalently, if π is injective)
3. Given $a \in X$, the **orbit** of a is the set $G \cdot a = \{g \cdot a : g \in G\}$ of elements of X to which a gets moved by the elements of G

Another way to say an action is faithful is saying that the identity of G is assigned the identity permutation of S_X
Note: If G acts faithfully on X, then G is isomorphic to a subgroup of S_X. (π is the isomorphism)
Warning: $G \cdot a$ is *not* a coset of G. (It is not even a subset of G)

Proposition 15.2. Suppose G acts on X. The orbits of the action partition X
Note: Clearly, the union of all orbits of X is equal to X, since G has the identity

Definition. An action of G on X is **transitive** if it has only one orbit (X itself)

Definition. Let π be an action of G on X. Given $a \in X$, the **stabilizer** of a is the set

$$G_a := \{g \in G : g \cdot a = a\}$$

Proposition 15.4. [Orbit-Stabilizer theorem]
Suppose G acts on X. For every $a \in X$:

1. $G_a \leq G$
2. $|G \cdot a| = [G : G_a]$

Hence if G is finite, then every orbit has size dividing $|G|$

Example: Scalar multiplication on a vector space $\mathbf{V}$ by the multiplicative group $\mathbb{F}^\times$ is a group action. In the case $\mathbf{V} = \mathbb{R}^n$, $\mathbb{F} = \mathbb{R}$. Then the group action of $\alpha \in \mathbb{F}^\times$ on V is given by $\alpha(x_1, \ldots, x_2) = (\alpha x_1, \ldots, \alpha x_n)$

Chapter 16

Permutation Representations and Cayley's Theorem

Definition. Let G be a group. Given $g \in G$, define $\lambda_g : G \to G$ by

$$\lambda_g(a) = ga \text{ for } a \in G$$

Each λ_g is a permutation of G
Thus we get a mapping $\lambda : G \to S_G$, namely, $g \mapsto \lambda_g$
This mapping is called the **left-regular action** of G on itself.

Claim: The left-regular action of G is an action of G on itself.
Given $g, h \in G$, $\lambda_{gh}(a) = gh(a) = g\lambda_h(a) = \lambda_g(\lambda_h(a)) = (\lambda_g \circ \lambda_h)(a)$ this is true for all $a \in G$. Then as functions $\lambda_{gh} = \lambda_g \circ \lambda_h$
What is $G \cdot 1$?, $G \cdot 1 = G$ so there is only one orbit. The action is transitive.
$\ker \lambda = \{g \in G : \lambda_g = \text{id}\} \iff g \cdot a = a, \forall a \in G \iff g = 1 \iff \ker \lambda = \{1\}$.
So this action is faithful and $\lambda : G \to S_G$ is injective $\implies \lambda : G \cong \text{im}(\lambda) \leq S_G$

Theorem 16.1. [Cayley's Theorem]
Every group is isomorphic to a subgroup of a permutation group. If $|G| = n$, then G is isomorphic to a subgroup of S_n

Example 16.2: Suppose $H \leq G$. G also acts on G/H (here this is not necessarily a quotient group since H is not necessarily normal) by left multiplication: $\lambda_g(aH) = gaH$
λ is an action. λ is transitive (since g spanning over G will cause the orbit to have all the left cosets of H). λ need not be faithful
Let $N = \ker \lambda = \{g \in G : \lambda_g = \text{id}\}$. $g \in N \iff \lambda_g(aH) = aH, \forall aH \in G/H \iff$

$gaH = aH, \forall a \in G$

This must be true for $a = 1$ so $\implies gH = H \iff g \in H$. So in summary $g \in N \implies g \in H$

Hence $N \subseteq H$. We already have $N \triangleleft G$

So if we chose H to be such a set that has only the identity subgroup as a normal subgroup. Then in this case, from the scheme above, we get that $N = \ker \lambda = \{1\} \implies \lambda$ is injective/faithful $\implies \lambda : G \cong \text{im}(\lambda) \leq S_{G/H}$

From this example we get the following proposition

Proposition 16.3. Suppose G is a finite group, $H < G$, and G has no normal subgroups contained in H except $\{1\}$

Then G is isomorphic to a subgroup of S_m where $m = [G : H]$

Proof: Building on the previous example we get that $\lambda : G \cong \text{im}(\lambda) \leq S_{G/H} \cong S_m$ since $|G/H| = [G : H] = m$

Fact: If $H \leq G$ and $[G : H] = 2$, then $H \triangleleft G$

Proof: Left cosets of H are H and $H^c = G \backslash H$. Right cosets of H are H and $H^c = G \backslash H$

Proposition 16.4. Suppose G is a finite group, $H \leq G, [G : H] = p$ (prime) *and* p is the smallest prime divisor of $|G|$. Then $H \triangleleft G$

Chapter 17

Class Equation and Cauchy's Theorem

Let G be a group that acts on itself by **conjugation**: the action $\psi : G \to S_G$ is given by $\psi_g(x) = gxg^{-1}$, or equivalently by $g \cdot a = gag^{-1}$. We now explore the properties of this action.

Definition. The set $\{gag^{-1} : g \in G\}$ is called the **conjugacy class** of a and is denoted by $\text{Conj}(a)$

Proposition 17.2. Let G be a group

1. G is partitioned by its conjugacy class
2. For any $a \in G$, define $C_G(a) = \{x \in G : xa = ax\}$. Then $C_G(x) \leq G$ and $|\,\text{Conj}(a)| = [G : C_G(a)]$

That is, $|\,\text{Conj}(a)|$ divides $|G|$ when G is finite

Notation: The subgroup $C_G(a)$ is called the **centralizer** of a in G

Note: the conjugacy class and centralizer of $a \in G$ are the orbit and stabilizer of a under the action of conjugation, so they are just special names.

Definition. Recall that the **center** of a group G is the set $Z(G) = \{x \in G : xa = ax,\ \forall a \in G\}$ which is a subgroup of G.

We agree to call a conjugacy class **trivial** if it is a 1-element orbit and **nontrivial** otherwise. We then see that

$$\text{Conj}(a) = \{a\} \iff |\,\text{Conj}(a)| = 1 \iff [G : C_G(a)] = 1 \iff C_G(a) = G$$

$$\iff ga = ag,\ \forall g \in G \iff a \in Z(G)$$

Since these statements are all equivalent, $Z(G)$ is the union of the trivial conjugacy classes, which with Prop 17.2 proves:

Proposition 17.2. [Class Equation]
Every group G is the disjoint union of $Z(G)$ and the group's nontrivial conjugacy classes

Theorem 17.4. If p is a prime and $|G| = p^n$, then $Z(G) \neq \{1\}$

Theorem 17.5. [Cauchy's Theorem]
Suppose G is a finite group. If p is prime and p divides $|G|$, then there exists an element of order p

Chapter 18

Finite Abelian Groups

Lemma 18.1. Suppose G is an abelian group and $m \in \mathbb{Z}$. Define $G^{(m)} = \{a \in G : a^m = 1\}$ then $G^{(m)} \leq G$

Lemma 18.2. Suppose G is finite abelian and $|G| = mk$ with $\gcd(m, k) = 1$. Then

1. $G \cong G^{(m)} \times G^{(k)}$
2. $|G^{(m)}| = m$ and $|G^{(k)}| = k$

Corollary 18.3. Suppose G is finite abelian and $|G| = n = p_1^{n_1} \dots p_k^{n_k}$ where $p_1, \dots, p_k$ are distinct primes

1. $G \cong G^{(p_1^{n_1})} \times \cdots \times G^{(p_k^{n_k})}$
2. $|G^{p_i^{n_i}}| = p_i^{n_i}$ for each i

The equation in Corollary 18.3(1) is called the **primary decomposition** of G

Definition. Fix a prime p. A finite group is a p-**group** if $|G| = p^n$ for some $n \geq 1$

In Corollary 18.3 we saw that every finite group can be factored as a direct product of finite abelian p-groups, where p varies over the prime divisors of $|G|$. We will now see how to further factor finite abelian p-groups

Definition. Let G be an abelian group. A **basis** of G is a sequence $a_1, \dots, a_t \in G$ satisfying

1. $a_i \neq 1$ for all i
2. $G = \langle a_1 \rangle \langle a_2 \rangle \dots \langle a_t \rangle$
3. For all $i = 1, 2, \dots, t-1$, if $H_i = \langle a_1 \rangle \langle a_2 \rangle \dots \langle a_i \rangle$ then $H_i \cap \langle a_{i+1} \rangle = \{1\}$

Let $a_1, \ldots, a_t$ be a basis of G. Let $N_i = \langle a_i \rangle$ for each i. Accoridng to (3) $H_i \cap N_{i+1} = \{1\}$ for $i < t$. Note that $H_i N_{i+1} = H_{i+1}$. Since G is abelian we have that $H_i, N_{i+1} \triangleleft H_{i+1}$. Hence by Theorem 10.1 $H_{i+1} \cong H_i \times N_{i+1}$ for each $i < t$

$$G = H_t \cong H_{t-1} \times N_t \cong H_{t-2} \times N_{t-1} \times N_t \cong \ldots \cong N_1 \times \ldots N_t$$

So we have

Proposition 19.1. If G is abelian and G has a basis, then G is isomorphic to a direct product of cyclic groups

Theorem 19.2. Every finite abelian p-group has a basis

Theorem A. Every abelian p-group (p is prime) is isomorphic to a direct product of one or more cyclic p-groups

Lemma B. Suppose G is a finite group, $N \triangleleft G$ and $a \in G$

1. $\circ(aN) | \circ(a)$
2. If $N \cap \langle a \rangle = \{1\}$, then $\circ(aN) = \circ(a)$

Lemma C. [Correspondence Theorem]
Suppose G is a group and $N \triangleleft G$

1. If $H \leq G$ with $N \subseteq H$, then $N \triangleleft H$ and $H/N \leq G/N$
2. Every subgroup of G/N is of the form H/N with H as in (1)

Lemma D. Suppose G is a finite, abelian, non-cyclic p-group (p is a prime), and $a \in G$ is an element of maximum order. There exists $b \in G$ with $\circ(b) = p$ and $\langle a \rangle \cap \langle b \rangle = \{1\}$

Proposition E. Suppose G is a finite abelian p-group (p is a prime). Let $a \in G$ be an element of maximum order. There exists $H \leq G$ with $\langle a \rangle \cap H = \{1\}$ and $\langle a \rangle H = G$

Theorem 19.3. Every finite abelian group is isomorphic to a direct product of cyclic groups (whose orders are powers of primes)

Definitions and Results from Assignments and Tests

Appendix

Parity of a Permitation

Proposition 1. Every $\sigma \in S_n$ can be written as a product of 2-cycles

Proof. We claim that each cycle $(a_1 a_2 \dots a_k)$ can be rewritten as

$$(\star) \quad (a_1\, a_2 \dots\, a_k) = (a_1\, a_k) \circ (a_1\, a_{k-1}) \circ \cdots \circ (a_1\, a_3) \circ (a_1\, a_2)$$

One can check that this works. □

The decompositions are not unique, there can even be decompositions with less or more 2 cycle products.

Definition. (Invented for PMATH 347). Let $\sigma \in S_n$

1. A product of 2-cycles equalling σ is called **canonical** if it is obtained from the cycle notation for σ by replacing each cycle with a product of 2-cycles following the recipe in $(\star)$
2. The **canonical number** of σ, denoted by $\text{can}_{\#}(\sigma)$ is the number of 2-cycles in any canonical product for σ

Consider $\sigma \in S_n$, $\sigma = \overbrace{\sigma_1 \dots \sigma_n}^{\text{k cycles (non-trivial)}} = \underbrace{(\dots)}_{m_1\text{cycle}} \circ \underbrace{(\dots)}_{m_2\text{cycle}} \circ \cdots \circ \underbrace{(\dots)}_{m_k\text{cycle}}$ Each of these m_i cycles decompose into $m_i - 1$ many 2-cycles by the recipe $(\star)$
$\text{can}_{\#}(\sigma) = \sum_{i=1}^{k} m_i - k$. $m :=$ sum of lengths of non-trivial cycles
So $\text{can}_{\#}(\sigma) = m - k$
Let $r =$ number of 1-cycles(trivial) of σ then $m + r = n$
So we also have that $\text{can}_{\#}(\sigma) = n - (k + r)$

Proposition 2. Given $\sigma \in S_n$, let
$k =$ the number of nontrivial cycles of σ
$m =$ the sum of the lengths of the nontrivial cycles

$r =$ the number of trivial cycles of σ
Then, $\text{can}_{\#}(\sigma) = m - k = n - (k + r)$

Proposition 3. Suppose $\sigma \in S_n$ and $\tau = (a\, b)$ is a 2-cycle. Then

$$\text{can}_{\#}(\tau\sigma) = \text{can}_{\#}(\sigma) + 1 \text{ or } \text{can}_{\#}(\sigma) - 1$$

The proof breaks into two cases. Case 1: a, b are in two different cycles in σ and Case2: a, b are in the same cycle in σ. In the first case we find that $\text{can}_{\#}(\tau\sigma) = \text{can}_{\#}(\sigma) + 1$ and in the second case we find that $\text{can}_{\#}(\tau\sigma) = \text{can}_{\#}(\sigma) - 1$
So we have from Proposition 3: $\text{can}_{\#}(\tau\sigma) = \text{can}_{\#}(\sigma) \pm 1$

Corollary 4. Suppose $\sigma \in S_n$ and $\tau_1, \ldots, \tau_k$ are 2-cycles

1. $\text{can}_{\#}(\tau\sigma) \equiv \text{can}_{\#}(\sigma) + 1 \mod 2$
2. $\text{can}_{\#}(\tau_1\tau_2 \ldots \tau_k\sigma) \equiv \text{can}_{\#}(\sigma) + k \mod 2$

Proposition 5. For all $\sigma, \rho \in S_n$

$$\text{can}_{\#}(\rho\sigma) \equiv \text{can}_{\#}(\rho) + \text{can}_{\#}(\sigma) \mod 2$$

Definition. We define the **parity** of a permutation $\sigma \in S_n$ as

$$\begin{cases} \textbf{even} & \text{if } \text{can}_{\#}(\sigma) \equiv 0 \mod 2 \\ \textbf{odd} & \text{if } \text{can}_{\#}(\sigma) \equiv 1 \mod 2 \end{cases}$$

We can define a homomorphism $\varphi : S_n \to \mathbb{Z}_2$ by the rule $\varphi(\sigma) = \begin{cases} 0 & \text{if } \sigma \text{ is even} \\ 1 & \text{if } \sigma \text{ is odd} \end{cases}$ We see that φ is a homomorphism by the fact $\varphi(\sigma\rho) = \varphi(\sigma) \underbrace{+}_{\text{mod } 2} \varphi(\rho)$

Definition. The **alternating subgroup** of S_n is

$$A_n := \ker \varphi = \{\text{even permutations in } S_n\} \triangleleft S_n$$

This is for the φ defined just above. And A_n is normal since it is the kernel of φ so it is normal to its domain

By definition $G_A = \{M \in GL_2(\mathbb{R}) : MAM^{-1} = A\} = \{M \in GL_2(\mathbb{R}) : MA = AM\}$

Let $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$

$$\begin{aligned} & MA = AM \\ \iff & \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \\ \implies & \begin{bmatrix} a & 2b \\ c & 2d \end{bmatrix} = \begin{bmatrix} a & b \\ 2c & 2d \end{bmatrix} \\ \implies & b = c = 0 \text{ and } a, d \in \mathbb{R} \setminus \{0\} \end{aligned}$$

The restriction of $a, d \neq 0$ as $M \in GL_2(\mathbb{R})$

So we get that $G_A = \{M \in GL_2(\mathbb{R}) : MA = AM\} = \left\{ \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} : a, d \in \mathbb{R} \setminus \{0\} \right\}$

Similarly for G_B we find the form of $M \in GL_2(\mathbb{R}) : MB = BM$

$$\begin{aligned} & MB = BM \\ \iff & \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \\ \implies & \begin{bmatrix} 2a & 3b \\ 2c & 3d \end{bmatrix} = \begin{bmatrix} 2a & 2b \\ 3c & 3d \end{bmatrix} \\ \implies & b = c = 0 \text{ and } a, d \in \mathbb{R} \setminus \{0\} \end{aligned}$$

So $G_B = \{M \in GL_2(\mathbb{R}) : MB = BM\} = \left\{ \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} : a, d \in \mathbb{R} \setminus \{0\} \right\}$

Hence we see that G_A, G_B are the same set by definition. $G_A = G_B$