PMATH 347: Groups & Rings

Syed Mustafa Raza Rizvi

October 2, 2020

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 (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 2

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 3

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 4

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 5

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 6

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 7

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

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

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 8

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. $H \lhd G \iff N_G(H) = G$

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 9

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 $H, K \lhd G$ 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 $\gcd(m, n) = 1$

Appendix