MATH 541 Lecture Notes

Pongsaphol Pongsawakul

Spring 2023

Contents

- Book: Dujmit Foote “Modern Algebra 3rd ed”
- Midterm 3/23 in class
- Final 5/8
- Homeworks: weekly
- Honors Credit: Extra sections + homeworks

1 Algebra

Operations often modeled: $+, \cdot$

composition: space of thing that you are looking at $\leftarrow$ alomst always not commutative

Groups: One operation $\cdot$

Rings: 2 operations: $+, \cdot$ that play nice

1.1 Axioms of Groups

By “operation” on S, I mean a function $\cdot S \times S \to S$

Instead of $\cdot(a, b)$, we write $a \cdot b$

A group is a set G with an operation $\cdot$ satisfying:

1. Associativity: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
2. There is an identity element: there is one special element $1 \in G$ so $1 \cdot a = a$ for any $a \in G$ and $a \cdot 1 = a$ for any $a \in G$
3. Inverses: For any $a \in G$, there is a $b \in G$ so $a \cdot b = b \cdot a = 1$

Note: $a \cdot b = b \cdot a$ is <u>not</u> an axiom.

If G satisfies this, we call it an abelian group

Example. $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$

1. 0 is the identity
2. inverses: $-a$ is the inverse of a

Example. $(\mathbb{Q} \setminus \{0\}, \cdot), (\mathbb{R} \setminus \{0\}, \cdot), (\mathbb{C} \setminus \{0\}, \cdot)$

1. 1 is the identity
2. Inverses: $\frac{1}{a}$ is the inverse of a

Note: $(\mathbb{Z} \setminus \{0\}, \cdot)$ is not a group

$(V, +)$ is a group

Example. For n, a natural number, $(\mathbb{Z}/n\mathbb{Z}, +)$ is a group

On $\mathbb{Z}$, we say a, b are (mod n) equivalent (written $a \equiv b (\text{mod } n)$) if n divides $a - b$

$\mathbb{Z}/n\mathbb{Z}$ is the set of equivalence classes mod n

Example. $n = 2$: (odds, evens) which is $\{0_{\text{mod } 2}, 1_{\text{mod } 2}\}$

$17_{\text{mod } 2} + 64_{\text{mod } 2} = 81_{\text{mod } 2} = 1_{\text{mod } 2}$

Example. $\mathbb{Z}/3\mathbb{Z} = \{0_{\text{mod } 3}, 1_{\text{mod } 3}, 2_{\text{mod } 3}\}$

Example. $(2\mathbb{Z}, +)$ is a group (even numbers)

Example. If $(G, \cdot_G)$ and $(H, \cdot_H)$ are groups, then $(G \times H, \cdot_G \times \cdot_H)$ is a group

- $(g_1, h_1) \cdot_{G \times H} (g_2, h_2) = (g_1 \cdot_G g_2, h_1 \cdot_H h_2)$
- Identity: $1_{G \times H} = (1_G, 1_H)$
- Inverse of (g, h): (g^{-1}, h^{-1})

1.1.1 Properties

- G has exactly 1 identity
- Each $g \in G$, there is exactly 1 inverse of g we write this g^{-1} (i.e. ${}^{-1} : G \to G$)
- $(g^{-1})^{-1} = g$
- $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$
- $(a_1 \cdot a_2 \cdot \ldots \cdot a_m)^{-1} = a_m^{-1} \cdot a_{m-1}^{-1} \cdot \ldots \cdot a_1^{-1}$

Proof.

- Suppose a, b are both identities in G. Then $a = a \cdot b = b$
- Suppose a, b are both inverses of g. i.e $a \cdot g = g \cdot a = 1$ and $b \cdot g = g \cdot b = 1$ Then $b = 1 \cdot b = (a \cdot g) \cdot b = a \cdot (g \cdot b) = a \cdot 1 = a$

- know $g \cdot g^{-1} = g^{-1} \cdot g = 1$ so $(g^{-1})^{-1} = g$
- $(a \cdot b)^{-1}$ satisfies: $x \cdot (a \cdot b) = (a \cdot b) \cdot x = 1$ we check $b^{-1}a^{-1}$ does this

  $(b^{-1}a^{-1}) \cdot (a \cdot b) = b^{-1}(a^{-1} \cdot a)b = b^{-1} \cdot 1 \cdot b = b^{-1}b = 1$

  $(ab)(b^{-1}a^{-1}) = a(b \cdot (b^{-1}) \cdot a^{-1} = a \cdot 1 \cdot a^{-1} = aa^{-1} = 1$

□

Theorem 1. In G, there is exactly 1 solution to the equation $ax = b$ for a fixed $a, b \in G$

Corollary. Cancellation laws:

$$ax = ay \implies x = y$$

$$xa = ya \implies x = y$$

Proof. If $a \cdot x = b$

$$\begin{aligned} a^{-1} \cdot a \cdot x &= a^{-1} \cdot b \\ (a^{-1} \cdot a) \cdot x &= \\ 1x = x &= \end{aligned}$$

□

Definition. For $x \in G$, the order of x, written $|x|$, is the least $n > 0$ so

$$x^n = \underbrace{x \cdot x \cdot \ldots \cdot x}_{n} = 1_G$$

If there is no such n, x has "infinite order"

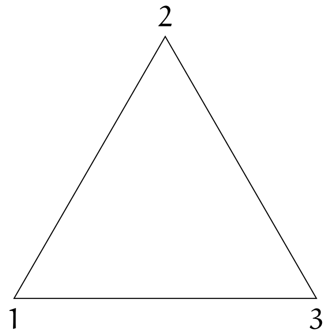
Example. In $(\mathbb{R} \setminus \{0\}, \cdot)$, $|5| = \infty$, $|-1| = 2$, $|1| = 1$

Example. $(\mathbb{Z}/6\mathbb{Z}, +)$, $|1_{\text{mod } 6}| = 6$, $|2_{\text{mod } 6}| = 3$, $|3_{\text{mod } 6}| = 2$, $|4_{\text{mod } 6}| = 3$, $|5_{\text{mod } 6}| = 2$

1.2 Dihedral Groups

1.2.1 Triangle

Look at the collection of symmetries of an equilateral Triangle



Rotation right

- $1 \to 2$
- $2 \to 3$
- $3 \to 1$

r

Rotation Left

- $1 \to 3$
- $2 \to 1$
- $3 \to 2$

r^2

Reflection around 2

- $1 \to 3$
- $2 \to 2$
- $3 \to 1$

$r^2 \circ s$

Reflection around 1

- $1 \to 1$
- $2 \to 3$
- $3 \to 2$

s

Reflection around 3

- $1 \to 2$
- $2 \to 1$
- $3 \to 3$

$r \circ s = s \circ r^2$

Identity

- $1 \to 1$
- $2 \to 2$
- $3 \to 3$

r^3, s^2

$$\begin{aligned} r^s &= r \cdot (r \cdot s) \\ &= (r \cdot s) \cdot r^{-1} \\ &= s \cdot (r^{-1} \cdot r^{-1}) \\ &= s \cdot (r^{-1})^2 \end{aligned}$$

(Symmetry of $\triangle, \circ) = D_6$

1.2.2 n-gon

Rotation right

- $k \to k+1$ (for $k < n$)
- $n \to 1$

$r, |r| = n$

Reflection around 1

- $k \to n+2-k$
- $1 \to 1$

$s, |r| = n$

My Symmetry

- $1 \to k$
- $2 \to k+1$

r^k

So, $\{r, s\}$ generates the group of sym of regular n-gon

(Symmetry of a regular n-gon, $\circ$) = D_{2n}

1.2.3 Definition

Rules of dihedral group multiplication in D_{2n} $\{r, s\}$

a) $r^n = 1$

b) $s^2 = 1$

c) $r \cdot s = s \cdot r^{-1}$

When you have generators S for G and can list R_1, R_2, R_3 <u>all</u> the rules you need to know to do multiplication in G Then $\langle S, R_1, R_2, R_3\rangle$ is a "presentation of the group G"

$D_{2n} = \langle r, s | r^n = 1, s^2 = 1, rs = sr^{-1}\rangle$

Fact: There is a finite set of rule $R_1, \ldots, R_{2000}$ so $\langle a, b | R_1, \ldots, R_{2000}\rangle$ "undecidable word problem"

1.3 Symmetric Group

Given Ω any set, S_Ω = The permutations of Ω = The bijections $f : \Omega \to \Omega$

Example 2. $\Omega = \{1, 2, 3\}$

$S_n = S_{\{1,2,\ldots,n\}}$ has $n!$ elements

$|S_3| = 6, |D_6| = 6, D_6 \subseteq S_3$

$|D_{2n}| = 2n$

$|S_n| = n!$

1.3.1 Cycle Decomposition

$1 \to 4, 2 \to 1, 3 \to 2, 4 \to 3, 5 \to 5$ can be written as $(1432)(5)$

$(a_1 \dots a_{m_1})(a_{m_1+1} \dots a_{m_2})$ with a_i is disjoint represents the function which satisfies

- a_i to a_{i+1} unless $i = m_j$ for some j
- a_{m_j} to $a_{m_{j-1}} + 1$ $j \neq 1$
- a_{m_1} to a_1

$(1)(2)(3)(4)(5)(6)(7) = 1$

$(1442) \circ (3421) = (124)$

$|(123)(45)| = 6$

Order of a product of disjoint cycles is the lcm(lengths of the cycles)