Group Theory

Wednesday, February 25, 2026 9:12 PM

Recall: Modular Arithmetic

Lecture Notes on Group Theory (LNGT)

§1. Groups and Subgroups

1] Def^n. The binary operation $*$ is said to be on a set A if $*$ is a function from $A \times A$ to A.

i.e. $* : A \times A \to A$

Here, A is closed under the $*$ operation

2] Def^n. a group $(G, \cdot)$ is a nonempty set G with a binary operator $\cdot$ on G, such that the following conditions hold.

(i) *Closure:* For all $a, b \in G$ the element $a \cdot b$ is a uniquely defined element of G

(ii) *Associativity:* For all $a, b, c \in G$, we have

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

(iii) *Identity:* There exists an *identity element* $e \in G$ such that for all $a \in G$

$$e \cdot a = a \qquad \text{and} \qquad a \cdot e = a$$

(iv) *Inverses:* For each $a \in G$ there exists an *inverse* element $a^{-1} \in G$ such that

$$a \cdot a^{-1} = e \qquad \text{and} \qquad a^{-1} \cdot a = e$$

3] e.g. $(\mathbb{Z}_7, +)$ the additive group modulo 7

$\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$

① closure $\forall a, b$, $a + b \pmod 7 \in \mathbb{Z}_7$

② Assoc. ✓

③ Identity: $e = 0$

④ Inverse: then inverse of $x = -x \pmod 7$

a	0	1	2	3	4	5	6
a^{-1}	0	6	5	4	3	2	1

e.g. $(\mathbb{Z}_{10}^*, \cdot)$ the multiplicative group modulo 10

$\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$

① closure

② Assco.

③ $e = 1$

④ inverse

a	1	3	7	9
a^{-1}	1	7	3	9

·	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

4] Notations:

① Juxtaposition: write ab for $a \cdot b$

② Power (superscript): $a^n = \underbrace{a \cdot a \cdot \dots \cdot a}_{n\text{- times}}$; $a^0 = e$

③ Nagative power: $a^{-n} = (a^{-1})^n$

④ Avoid these notations if the operation of the group is denoted additively. e.g $+$, $\oplus$

use $3(a)$ for $a+a+a$

5] Prop. (Cancellation Properties)

① if $ab = ac$, then $b = c$

② if $ac = bc$, then $a = b$

Proof ①

let $ab = ac$

$\Rightarrow a^{-1}(ab) = a^{-1}(ac)$ by inverse

$\Rightarrow (a^{-1}a)b = (a^{-1}a)c$ by associativity

$\Rightarrow (e)b = (e)e$ by def^n inverse.

$\Rightarrow b = c$ by identity $\square$

6] Def^n. a group G is *abelian* (or commutative) if $\forall a, b \in G$, $ab = ba$.

7] e.g. $(\mathbb{Z}_7, +)$, $(\mathbb{Z}_{10}^*, \cdot)$ are abelian

8] Def^n. a group G is *finite* if it contains a finite number of elements (called the group order, denoted by $|G|$)

9] Def^n. the order of an element, $a \in G$; ord(a)

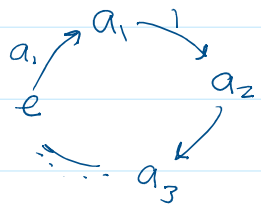
[9] Definition. Let a be an element of the group G. If there exists a positive integer n such that $a^n = e$, then a is said to have a ***finite order***, and the smallest such positive integer is called the ***order*** of a, denoted by ord(a). If there is no such a positive integer n such that $a^n = e$, then a is said to have an ***infinite order***.

10] e.g.

$(\mathbb{Z}_5^*, \cdot)$

$3 \cdot 3 \cdot 3 \cdot 3 = 1 = e$

$\therefore$ ord$(3) = 4$



$(\mathbb{Z}, +)$

$3 + 3 + 3 + \cdots \Rightarrow$ ord(3) is infinite

11] Def^n. Let $H \subseteq G$. Then H is a subgroup of G if H is a group under the operation induced by G.

e.g. $(\mathbb{Z}_{10}, +)$

$H = \{0, 2, 4, 6, 8\}$ is a subgroup.