

Recall: Groups

§ 1. Groups (LNGT)

e.g. $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$

$$e = 1$$

$a \backslash \bar{a}^{-1}$	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	8	7	4
7	7	5	1	7	4	2
8	8	7	5	4	2	1

	1	2	4	5	7	8
1	1					
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	8	7	4
7	7	5	1	7	4	2
8	8	7	5	4	2	1

$$(2 \cdot 4) \cdot 7 = 2 \cdot (4 \cdot 7)$$

1] Notations:

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

② Power: $a^n = \underbrace{a \cdot a \cdot \dots \cdot a}_{n\text{-times}}; a^0 = e$ $a^n = \begin{cases} a \cdot a^{n-1} \\ e \text{ if } n=0 \end{cases}$

③ negative power: $\bar{a}^n = (\bar{a}^{-1})^n$

④ Avoid juxtaposition and power notations

if the operation of the group is

denoted additively: $+$, $\oplus$, $\#$

$$\mathbb{Z}_9^*$$

$$2^3 \cdot 2^{-2}$$

$$= (2 \cdot 2 \cdot 2) \cdot (\bar{2}^{-1} \cdot \bar{2}^{-1})$$

$$= (2 \cdot \bar{2}^{-1}) \cdot (2 \cdot \bar{2}^{-1}) \cdot 2 = 2$$

e.g. for $a+a+a$, write $3a$ instead of a^3

2] Prop. (Cancellation Property)

let G be a group, and let $a, b, c \in G$

① if $ab = ac$ then $b=c$

② if $ac = bc$ then $a=b$

	a	b	c
↑		d	d
b			
c			

proof ①

$$ab = ac$$

$$\Rightarrow \bar{a}^{-1}(ab) = \bar{a}^{-1}(ac) \quad \text{by existence of inverse}$$

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

$$\Rightarrow e b = e c \quad \text{by def}^n \text{ of inverse}$$

$$\Rightarrow b = c \quad \text{by def}^n \text{ of identity}$$

3] Defⁿ. G is abelian (commutative) if $\forall a, b \in G, ab = ba$

e.g. $(\mathbb{Z}_{10}^*, \cdot)$ and $(\mathbb{Z}_5, +)$ are abelian groups

4] Defⁿ. a group G is finite if it contains a finite number of elements (n). In this case n is called the group order, denoted by $|G|$.

5] Defⁿ. let $a \in G$. if there is a positive integer n such that $a^n = e$, then the smallest such n is called the order of a . If there is no such positive integer, then a has an infinite order.

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

$$\text{ord}(5) = 2 \quad \text{for} \quad 5+5=0$$

$$\text{ord}(4) = 5 \quad \text{for} \quad 4+4+4+4+4=0$$

$$\text{ord}(3) = 10 \quad 3+3+\dots+3=$$

$(\mathbb{Z}_{10}^*, \cdot)$

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

$$\text{ord}(3) = 4$$

$$\text{for } 3 \cdot 3 \cdot 3 \cdot 3 = 1$$

$$\text{ord}(9) = 2$$

$$\text{for } 9 \cdot 9 = 1$$

$(\mathbb{Z}, +)$

$\text{ord}(2)$ is infinite