Groups
Wednesday, February 17, 2021 8:34 AM

Lecture Notes on Group Theory (LNGT)

§1. Groups and Subgroups

1] Def^n. Let $*$ be a binary operator. Then the operator $*$ is said to be on a set A if $*$ is a function from $A \times A$ to A.

$$*: A \times A \longrightarrow A$$

Here, A is said to be closed under the $*$ operation

2] Def^n. a group $(G, \cdot)$ is a nonempty set G together with a binary operation $\cdot$ on G such that:

① Closure: $\forall\, a, b \in G$, $a \cdot b \in G$

② Associativity; $\forall\, a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

③ Identity: $\exists\, e \in G$, $\forall\, a \in G$, $a \cdot e = a = e \cdot a$

④ Inverse: $\forall\, a \in G$, $\exists\, \bar{a}^{-1} \in G$, $a \cdot \bar{a}^{-1} = \bar{a}^{-1} \cdot a = e$

3] e.g. $(\mathbb{Z}_{12}, +)$ + is in (mod 12)

additive group

$\mathbb{Z}_{10} = \{0, 1, 2, \ldots, 11\}$

$9 + 5 = 2$

$e = 0$

inverse of 9 is 3

Note: $-9 \equiv 3 \pmod{12}$

$\mathbb{Z}$: all integers

$\mathbb{Z}^+$: positive int. $\{1, 2, 3, \ldots\}$

$\mathbb{Z}^-$: negative int. $\{-1, -2, -3, \ldots\}$

$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$

$\mathbb{Z}_p^* = \{1, 2, 3, \ldots, p-1\}$ for prime p.

e.g. $(\mathbb{Z}_5^*, \cdot)$ ... Multiplicative group

for prime p.

e.g. $(\mathbb{Z}_5^*, \cdot)$ multiplicative group

$\mathbb{Z}_5^* = \{1, 2, 3, 4\}$

$e = 1$

a	a^{-1}
1	1
2	3
3	2
4	4

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

4] Notations:

① Juxtaposition: ab for $a \cdot b$

② Power (superscript): $a^n = \underbrace{a\,a\,a\,\cdots\,a}_{n\text{-times}}$

$$a^n = \begin{cases} a\,a^{n-1} & \text{if } n > 0 \\ e & \text{if } n = 0 \end{cases}$$

$a^3 = a\,a^2 = a(aa^1)$
$= a\,a(aa^0)$
$= a\,a(ae)$
$= aaa$

③ negative power:

$$a^{-n} = (a^{-1})^n$$

④ Avoid juxtaposition and superscript if the group operator is denoted additively. $(\mathbb{Z}_{10}, +)$

use $n(a)$ instead of a^n

e.g. $3(5) = 5 + 5 + 5$

5] Prop. (Cancellation Property)

Let G be a group, $a, b, c \in G$.

① if $ab = ac$, then $b = c$

② if $ac = bc$, then $a = b$

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

7] e.g. $\mathbb{Z}_{10}$ and $\mathbb{Z}_5^*$ are abelian

$(\mathbb{Z}, +)$ is also an abelian group

8] Def^n. the order of the group G is $|G|$ = number of element in G if G is finite.

e.g.

$|\mathbb{Z}_{10}| = 10$

$|\mathbb{Z}_5^*| = 4$

$(\mathbb{Z}, +)$ has infinite order

9] Def^n. for $a \in G$, the order of a is the smallest $n > 0$ such that $a^n = e$. If there is no such n then a has infinite order.

10] e.g. $(\mathbb{Z}_5^*, \cdot)$

$\text{ord}(3) = 4$ for $3^4 = 1$

$\text{ord}(2) = 4$ for $2^4 = 1$

$\text{ord}(4) = 2$ for $4^2 = 1$

$\text{ord}(2) = 4$ for $2^4 = 1$

$\text{ord}(4) = 2$ for $4^2 = 1$

$\text{ord}(1) = 1$

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

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

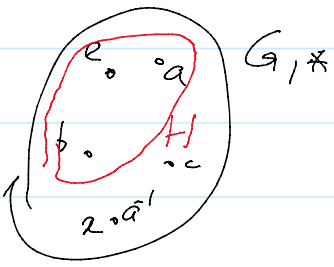
$\text{ord}(4) = 5$ for $5(4) = 4+4+4+4+4 = 0$

Feb 22

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

$\text{ord}(4) = 3$ for $4^3 = 1$

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



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

$H_1 = \{0, 4, 6, 2, 8\}$

$H_2 = \{0, 3, 6, 9, 2, 8, 7, 1, 4, 5\}$

$H_3 = \{0, 5\}$

$H_4 = \{0\}$

14] Thm (Lagrange Theorem)

if H is a subgroup of a finite group G, then

if H is a subgroup of a finite group G, then $|H|$ divides $|G|$

13] Prop: Let G be a group with identity e.
and $H \subseteq G$. Then H is a subgroup of G iff

① $e \in H$

② if $a \in H$ then $a^{-1} \in H$, $\forall a \in G$.

③ $\forall a, b \in H$, $ab \in H$

15] Prop. Let $|G| = n$, $\forall a \in G$.

(a) $\text{ord}(a) \mid n$

(b) $a^n = e$

16] Def^n. (The Euler's Phi function)

The totient of a positive integer n, denoted by $\phi(n)$, is defined as follows:

$$\phi(n) = |\mathbb{Z}_n^*|$$

where $\mathbb{Z}_n^* = \{x \mid 0 \leq x < n \text{ and } \gcd(x, n) = 1\}$

e.g.

$\phi(5) = 4$ $\quad \mathbb{Z}_5^* = \{1, 2, 3, 4\}$

$\phi(4) = 2$ $\quad \mathbb{Z}_4^* = \{1, 3\}$

$\phi(3) = 2$ $\quad \mathbb{Z}_3^* = \{1, 2\}$

$\phi(2) = 1$ $\quad \mathbb{Z}_2^* = \{1\}$

$\phi(1) = 1$ $\quad \mathbb{Z}_1^* = \{0\}$

$\phi(100) = 40$ $\quad \mathbb{Z}_{100}^* = \{0$ ~~5 15 25 ... 95 99~~ $\}$

17] Algorithm: $\phi(n)$ can be computed recursively using the following theorems.

1. $\phi(1) = 1$
2. $n = p^e$, for prime p, $\phi(p^e) = (p-1)p^{e-1}$
3. if $\gcd(m,n) = 1$, then $\phi(mn) = \phi(m) \cdot \phi(n)$

e.g. $\phi(25) = \phi(5^2) = 4 \cdot 5^1 = 20$

$\phi(100) = \phi(25)\phi(4) = 20 \cdot 2 = 40$

Quiz Setups

Feb 24

① Blackboard.

② Phone camera
15 - 200 cm. left.

③ Room:
- quite
- desk facing blank wall.

$\gcd(24, 15)$

$24 = 1 \cdot 15 + 9$
$15 = 1 \cdot 9 + 6$
$9 = 1 \cdot 6 + 3$
$6 = 2 \cdot 3 + 0$

$24 = 1 \cdot 15 + 9$
$15 = 1 \cdot 9 + 6$
$\vdots$
$9 = 1 \cdot 6 + 3$
$6 = 2 \cdot 3 + 0$
So $\gcd = 3$

Recall $\phi(n) = |\mathbb{Z}_n^*|$

18] e.g.

$\phi(17) = 16$
$\phi(16) = \phi(2^4) = (2-1)2^{4-1} = 1 \cdot 2^3 = 8$
$\phi(20) = \phi(4 \cdot 5) = 2 \cdot 4 = 8$
$\phi(6) = \phi(2 \cdot 3) = 1 \cdot 2 = 2$
$\phi(36) = \phi(4 \cdot 9) = 2 \cdot (2 \cdot 3) = 12$

$\mathbb{Z}_{16}^* = \{1, 3, \ldots 13, 15\}$
8 odds

$\mathbb{Z}_6^* = \{1, 5\}$

$\phi(36) = \phi(4 \cdot 9) = 2 \cdot (2 \cdot 3) = 12$

$\phi(105) = \phi(3 \cdot 5 \cdot 7) = 2 \cdot 4 \cdot 6 = 48$

$\phi(55) = \phi(5 \cdot 11) = 40$

$\phi(200) = \phi(2^3 \cdot 5^2) = (1 \cdot 2^2)(4 \cdot 5^1) = 80$

$\phi(1024) = \phi(2^{10}) = 1 \cdot 2^9 = 512$

19] Thm (Euler's Theorem):

In $\mathbb{Z}_n^*$, $|\mathbb{Z}_n^*| = \phi(n)$, therefore $\forall a \in \mathbb{Z}_n^*$, $a^{\phi(n)} = 1$

if $k \equiv j \pmod{\phi(n)}$, then $a^k \equiv a^j \pmod{n}$

20] e.g. in $\mathbb{Z}_7^*$

$2^{26} \equiv (2^6)^4 \cdot 2^2 \equiv 1 \cdot 4 \equiv 4 \pmod 7$

e.g. $2^{73} \equiv 2^1 \equiv 2 \pmod 5$

i	3^i	$\mathbb{Z}_7^*$
1	3	
2	2	
3	6	
4	4	
5	5	
$\phi(7)$ → 6	1	
7	3	
8	2	
9	6	
10	4	
11	5	
$2\phi(7)$ 12	1	
13	3	

21] e.g. Compute

(a) $14^{52} \pmod{11}$

$\equiv 3^2$

$14^{52} \equiv 3^2 \pmod{11}$ (mod $\phi(11)$)

(b) $463^{91} \pmod{15}$ → mod 8

$\equiv 13^3$

$\equiv (-2)^3$

$\equiv (-8) \equiv 7 \pmod{15}$

e.g.

e.g.

$$15^{1234500} \cdot 14^{1234520} \pmod{19}$$

HW