Subgroups

Monday, October 6, 2025 9:10 AM

Recall groups

Quiz 2
500 # 2, 12, 14
19, 26, 29

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.
Given $(\mathbb{Z}_{10}, +)$, find a subgroup of:

① size 5.

Sol^r $H = \{0, 2, 4, 6, 8\}$

② size 2.

$H = \{0, 5\}$

③ Size 10.

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

④ size 1.

$H = \{0\}$

⑤ size 4. No subgroup by Lagrange

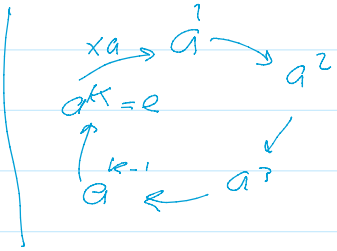
13] Prop. (our observation)
Let $H \subseteq G$, then H is a subgroup of G iff:

① $\forall a, b \in H$, we have $ab \in H$ (closure)
② $e \in H$, and (identity)
③ $\forall a \in H$, $a^{-1} \in H$ (inverse)

14] Lagrange Theorem:

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

$|H|$ divides $|G|$



15] Prop. Let $n = |G|$, then for all $a \in G$

① $\text{ord}(a) \mid n$

② $a^n = e$

16] Def^n. (Euler's Phi-function) $\phi(n)$ or $\varphi(n)$

The totient of a positive integer n, denoted $\phi(n)$, is the number of integers $< n$ and co-prime to n.

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

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

$\gcd(0, 1) = 1$

e.g. $\mathbb{Z}_3^* = \{1, 2\} \Rightarrow \phi(3) = 2$

$\mathbb{Z}_6^* = \{1, 5\} \Rightarrow \phi(6) = 2$

$\mathbb{Z}_{11}^* = \{1, \dots, 10\} \Rightarrow \phi(11) = 10$

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

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

17] Algorithm : To compute $\varphi(n)$

① $\phi(1) = 1$

② if p is prime, $\phi(p^k) = (p-1)\,p^{k-1}$

③ if $\gcd(m,n) = 1$, $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$

18] e.g. $\phi(17) = 16$

$\phi(15) = \phi(3)\,\phi(5) = 2 \cdot 4 = 8$

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

$\phi(25) = \phi(5^2) = 4(5^1) = 20$

$\phi(100) = \phi(10)\,\phi(10)$ ✗ $= 81$

$= \phi(2^2 \cdot 5^2) = (1 \cdot 2^1)(4 \cdot 5^1) = 40$

19] Euler's Theorem :

In $\mathbb{Z}_n^*$, the group order $|\mathbb{Z}_n^*| = \phi(n)$

$\therefore \forall\, a \in \mathbb{Z}_n^*$, we have

$a^{\phi(n)} = e$ by [15-2]

Hence if $k \equiv j \pmod{\phi(n)}$ then

$a^k \equiv a^j \pmod{n}$

20] e.g. in $\mathbb{Z}_{15}^*$

$17^{46} \pmod{15}$

mod 15 ↓ ; mod 8 ↓

$\equiv 2^6$

$\equiv 64 \equiv 4 \pmod{15}$

$\phi(15) = 8$

2] Exer :

① $463^{91} \pmod{15}$

$\equiv 13^{3}$

$\equiv (-2)^{3}$

$\equiv -8$

$\equiv 7 \pmod{15}$

Exer

① $33^{71} + 285^{43} \pmod{7}$

$\equiv (-2)^{5} + 5^{1}$

$\equiv -32$

$\equiv 3 + 5$

$\equiv 1 \pmod{7}$

$\Phi(7) = 6$

7	
14	13
21	26
28	39
35	52
42	