Note Title 07-09-2021

MA-222

Lec-17

G

Partition of G.

Defn: Let G be gp & H be a subgp of G. $a \in G$. Then the set

$$Ha = \{h * a \mid h \in H\}$$

is called right coset of H containing a.

Similarly $$aH = \{a * h \mid h \in H\}$$

left coset of H containing a.

$5\mathbb{Z} = \{0, \pm 5, \pm 10, \ldots\}$

$A_1 = \{\ldots, -9, -4, 1, 6, 11, \ldots\}$

$A_2 = \{\ldots, -8, -3, 2, 7, 12, \ldots\}$

A_3

A_4

$|A|$

$G = \mathbb{Z}$ $\quad$ $H = 5\mathbb{Z}$.

$a = 1$ $\quad$ $aH = \{ a * h \mid h \in H \}$

$= \{ 1 + n \mid n \in 5\mathbb{Z} \}$

$= \{ 1 + 5k \mid k \in \mathbb{Z} \} = A_1$

$a = 2$ then $\quad$ $2 + H = A_2$

$3 + H = A_3$

$4 + H = A_4$

$a = 7$

$a + 5\mathbb{Z} = \{ 7 + 5k \mid k \in \mathbb{Z} \}$

$= \{ 2 + 5k \mid k \in \mathbb{Z} \}$

$= A_2$

Notⁿ: aH for left coset & Ha for right coset } if the operation is not specified.

Remark: If G is Abelian then left cosets & right cosets are equal.

i.e. $\boxed{aH = Ha}$

If G is Abelian then "generally" the cosets are denoted with $+$.

i.e. $a+H$.

$\varphi : aH \longrightarrow bH.$

$Ha \longrightarrow Hb$

$\{a*h \mid h \in H\} \longrightarrow \{b*h \mid h \in H\}$

$ah \longmapsto bh$

$ha \quad hb$

one-one $\quad bh_1 = bh_2 \Rightarrow ah_1 = ah_2.$

onto. $\quad x \in bH \quad x = b*h$ for some $h \in H$.

then $a*h \in aH$.

$a = e$ then $\underline{eH = H = He}$

i.e. the subgp $\underline{H}$ is <u>also</u> a left coset, as well as right coset.

$f : \underline{aH} \longrightarrow \underline{bH}$.

y.

Given $y \in B$

$\exists!\, x \in A$ s.t.

$f(x) = y$.

$y \in bH \Rightarrow y = b * \underline{h}$ for some $h \in H$

& compute $\underline{a * h} \in aH$.

If G is a finite gp of order n.

Let $o(H) = d$.

then $\underline{|aH|} = \underline{\cancel{o(H)}}\ \underline{|H|} = o(H)$. $= |Ha|$

All such cosets form a <u>partition</u> of G.

$$\bigcup_{a \in G} aH = G \implies \underset{\text{disjoint cosets}}{\dot{\bigcup}} aH = G.$$

$$\dot{\bigcup}\, Ha = G.$$

$\underline{\sum |aH| = o(G)}$. where sum is over disjoint / distinct left cosets

$\sum |Ha| = o(G)$

say k such distinct left cosets are there.

$\underline{k \cdot o(H)} = \underline{o(G)}$. $\Longrightarrow$ $\boxed{\underline{k} = \dfrac{o(G)}{o(H)}}$

Thm: (Lagrange's thm)

Let G be finite gp & $H \leq G$. Then $o(H)$ divides $o(G)$.

Defn: No. of distinct left cosets of H is called **index** of H in G.

right

Notn: $[G : H]$

Remark: No. of left cosets = no of right cosets

$$|aH| = |Hb|$$
$$\parallel \qquad\qquad \parallel$$
$$o(H) \qquad o(H).$$

$$\varphi : \underline{\underline{aH}} \longrightarrow \underline{\underline{Ha}} \quad \text{gives a bijection.}$$
$$ah \longmapsto ha$$

$$G = \underline{\underline{\mathbb{Z}_{18}}} \qquad H = \langle 3 \rangle = \underline{\underline{\{0, 3, 6, 9, 12, 15\}}}.$$

$$7 + \langle 3 \rangle = 1 + H = \{1, 4, 7, 10, \cancel{6}\,13, 16\}.$$

$$2 + H = \{2, 5, 8, 11, 14, 17\}.$$

$G = \mathbb{Z}_{12}$.

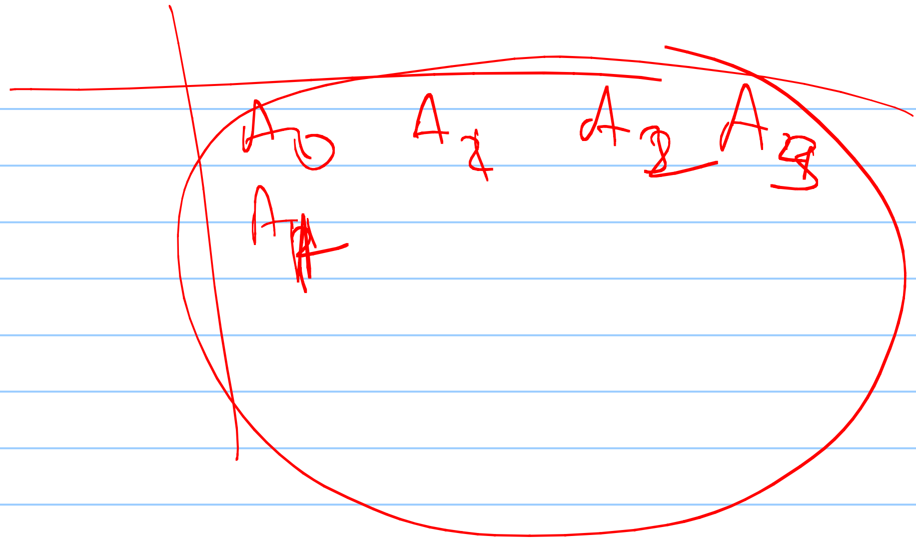
$H = \langle 4 \rangle = \{0, 4, 8\}$. A_0

$1 + \langle 4 \rangle = \{1, 5, 9\}$. A_1

$2 + \langle 4 \rangle = \{2, 6, 10\}$. A_2

$3 + \langle 4 \rangle = \{3, 7, 11\}$. A_3

	0	A_0 4	8	1	5	9	2	6	10	3	7	11
0	0	4	8	1	5	9						
4	4	A_0 8	0	5	A_1 9	1	6	A_2 10	2	7	A_3 11	3
8	8	0	4	9	1	5						
1	1											
5	5	A			–			–			–	
9	9											
2												
6		–			–			–			–	
10												
3												
7		–			–			–			–	
11												–


A_0 A_1 A_2 A_3
A_4

Coro: Let $a \in G$. then $o(a) \mid o(G)$.

$$o(a) = o(\underbrace{\langle a \rangle}_{H})$$

Coro: $a \in G$. $\boxed{a^{o(G)} = e}$.

$o(G) = o(a) \cdot n$ for some $n \in \mathbb{N}$.

$$a^{o(G)} = \left(a^{o(a)}\right)^{n} = e^{n} = e.$$

Cor: **Euler's thm**

$n \in \mathbb{N}$. $n \geq 2$. $a \in \mathbb{N}$ s.t. $(a, n) = 1$

then $\boxed{a^{\varphi(n)} \equiv 1 \pmod{n}}$.

Pf: take $G = \mathbb{Z}_n^*$.

then $o(G) = \varphi(n)$ & identity is 1.

$a^{\varphi(n)} \equiv 1 \pmod{n}$.

Fermat's Little thm

p: prime & $a \in \mathbb{N}$ s.t. $p \nmid a$.

then $$\boxed{a^{p-1} \equiv 1 \pmod{p}}$$

This gives a test to chk if n is prime

take a coprime to n.

& compute $a^{n-1} \pmod{n}$

If this is not 1 then n is composite.

If this is 1 then n is called pseudoprime wrt base a.

$p \nmid a \Rightarrow a^{p-1} \equiv 1 \pmod{p}$

$\boxed{a^p \equiv a \pmod{p}}$

$p \mid a \Rightarrow a \equiv 0 \pmod{p}$

$a^p \equiv 0 \equiv a \pmod{p}$

For any $a \in \mathbb{N}$, $\quad \underline{\underline{a^p \equiv a \pmod{p}}}$