Legendve's Theorem

If $H \subset G$ subgroup, G finite $\Rightarrow |H| \mid |G|$

Cor. 2 : $\text{ord}(a) \mid |G|$ for any $a \in G$

Cor. 3 : $|G| = p$ prime $\Rightarrow \exists\, a \in G$ s.t. $G = \langle a \rangle$ cyclic

(Recall: in this case G is isomorphic to $\mathbb{Z}_p$)

$\Rightarrow$ we have classified all groups of order p, up to isomophism]

proof. let $a \in G$, $a \neq e$ consider the subgroup $\langle a \rangle \subset G$

- $|\langle a \rangle| > 1$
- $|\langle a \rangle| \mid |G| = p$ by legendve's Theorem

p prime $\Rightarrow |\langle a \rangle| = p \Rightarrow \langle a \rangle = G$.

Cor. 4 $a^{|G|} = e$ for all $a \in G$, G finite

proof. $n = \text{ord}(a) \mid |G|$ by Cor. 2 $\Rightarrow |G| = nk$

$\Rightarrow a^{|G|} = a^{nk} = (a^n)^k = e^k = e$

Cor. 5 (Fermat's Little Theorem)

Let $k \in \mathbb{Z}$, p a prime $\Rightarrow k^p \bmod p = k$

(e.g. $5^{23} \bmod 23 = 5$)

proof. **case 1:** $p \mid k \Rightarrow p \mid k^p$

$\Rightarrow k^p \bmod p = 0 = k \bmod p$

case 2: $p \nmid k \Rightarrow \gcd(k, p) = 1$

$\Rightarrow k \bmod p$ is in $\mathcal{U}(p) = \{1, 2, 3, \ldots, p-1\}$

$|\mathcal{U}(p)| = p-1 \Rightarrow k^{p-1} \bmod p = 1$ ← identity elem. of $\mathcal{U}(p)$

(← $|\mathcal{U}(p)|$)

Cor. 4

multiply previous line by k. → $\Rightarrow k^p \bmod p = k$

Remark: For encryption, one considers $\mathcal{U}(pq)$ where p and q are large primes

$|\mathcal{U}(pq)| = (p-1)(q-1)$.

Remark: The idea of the proof of Lagrange's theorem was to just count the number r of cosets of H in G

$$\Rightarrow |G| = r|H|$$

This idea can be used even if G is infinite

Def. The index $[G:H]$ of a subgroup $H \subset G$ is the number of left cosets of H

Cor. 1 If G is finite. $\Rightarrow |G:H| = \frac{|G|}{|H|}$ follows from $|G| = r|H|$ solve for r !

Cor 2: $[\mathbb{Z} : 2\mathbb{Z}] = 2$

because $\mathbb{Z} = 2\mathbb{Z} \cup (1+2\mathbb{Z})$

even numbers, odd numbers

Remark: have seen: if $G = \langle a \rangle$ cyclic, $d \mid |G| = \text{ord}(a)$

$\Rightarrow$ can find subgroup H with $|H| = d$

namely $H = \langle a^{|G|/d} \rangle$

Question: Is this true for arbitrary groups G?

i.e. if $d \mid |G|$ can we find subgroup $H \subset G$ with $|H| = d$

Answer: not always!

Example: Consider A_4 even permutations in S_4

$$|A_4| = \frac{4!}{2} = \frac{24}{2} = 12$$

Recall: A_4 had 8 3-cycles (123), (132), (124), (142) ....

3 elem. of order 2 (12)(34), (13)(24), (14)(23)

all elem. with 2 commuting 2-cycles

claim: A_4 does not have a subgroup H with 6 elements

proof by contradiction.

assume we have $H \subset A_4$, $|H| = 6$

$\exists$ 3-cycles in A_4 $\Rightarrow$ there exists 3-cycle $a \notin H$

$\Rightarrow aH \neq H$

$A_4 = H \cup aH$

Question: in which coset is a^2 ?

- $a^2 \in H$?

$a = a^4 = (a^2)(a^2) \in H$ ↯ $a \notin H$

(a: $\text{ord}(a) = 3$; a^2: H, H)

- $a^2 \in aH$? $\Rightarrow a^2 = ah$ for some $h \in H$

$\Rightarrow a = h \in H$ ↯ $a \notin H$

(left cancellation)

$\Rightarrow$ no $H \subset A_4$ with $|H| = 6$

Remark: have seen: if $|G|=p \Rightarrow G \cong \mathbb{Z}_p$

what about, say $|G|=2p$ p odd prime ?

in this case we have: **Theorem:** $G \cong \mathbb{Z}_{2p}$ or $G \cong D_p$ dihedral group

Chapter 9 Normal Subgroups

have seen: left cosets may not always be right cosets

e.g. $H = \langle (12) \rangle \subset S_3$

$(13)H \neq H(13)$

Def A subgroup $H \subset G$ is called a normal subgroup, $H \trianglelefteq G$ if $aH = Ha$ for all $a \in G$ (i.e. left cosets same as right cosets)

Examples: ① If G is abelian, any subgroup $H \subset G$ is normal: because $aH = Ha$

② $\langle (12) \rangle \subset S_3$ is NOT normal

Theorem: Assume $[G:H] = 2 \Rightarrow H \trianglelefteq G$

proof $[G:H] = 2 \Rightarrow G = H \cup aH$ for $a \notin H$

and $G = H \cup \underbrace{Ha}_{\neq H}$

If $a \in H \Rightarrow aH = H = Ha$ ✓

If $a \notin H \Rightarrow aH = G \setminus H = \{g \in G,\ g \notin H\}$

$\| $

$Ha = G \setminus H$

$\Rightarrow aH = Ha$ for all $a \in G$ ✓

Example: Have seen $|A_n| = \frac{n!}{2} = \frac{|S_n|}{2}$

$\Rightarrow [S_n : A_n] = 2$ by Legendre's theorem.

$\Rightarrow A_n \trianglelefteq S_n$.

Remark: This shows that we can have normal subgroups also in non-abelian groups.