

$\text{Stab}(x) = \{g \in G : g \cdot x = x\}$ subgroup of G

$\text{Orb}(x) = \{g \cdot x : g \in G\}$

Orbit-Stabilizer Theorem

$$|\text{Orb}(x)| = [G : \text{Stab}(x)] = \frac{|G|}{|\text{Stab}(x)|}, \quad \sum_{\substack{\text{one } x \\ \text{from each} \\ \text{orbit}}} |\text{Orb}(x)| = |X|$$

Conjugation action

$G \curvearrowright G \quad (G \times G \rightarrow G)$

$$g \cdot h = ghg^{-1}$$

$$\text{Stab}(g) = \{h \in H : h^{-1}gh = g\}$$

$$= \{h \in H : gh = hg\}$$

$$= C_G(g)$$

$$\text{Orb}(g) = \{h^{-1}gh\} = \text{conjugacy class of } g$$

$$|\text{conj class}(g)| = [G : C_G(g)] = \frac{|G|}{|C_G(g)|}$$

center $\{g : gh = hg \forall h\}$

$$\sum_g |\text{conj class}(g)| = |G| \quad (\text{class equation})$$

$$|Z(G)| + \sum_g^{**} \frac{|G|}{|C_G(g)|} = |G|$$

G finite group, $X = \{(g, h) : gh = hg\}$

a)

Show $|X| = c|G|$, $c = \#$ conj classes

$$|X| = \sum_g |C_G(g)| = \sum_g \frac{|G|}{|\text{conj class}(g)|}$$

$$= |G| \cdot \sum_g \frac{1}{|\text{conj class}(g)|}$$

Each conjugacy class contributes 1 to the sum

$$= |G| \cdot c$$

b) Find $|X|$ for $G = S_5$.

Thm: Two permutations are conjugate in S_n

\iff they have the same cycle.

$$\left[\begin{array}{l} 1+1+1+1+1 \\ 2+1+1+1 \\ 3+1+1 \\ 4+1 \\ 5 \end{array} \right] \quad \left[\begin{array}{l} 2+2+1 \\ 2+3 \end{array} \right]$$

$$c = 7$$

$$|X| = 7 \cdot 5! = 7 \cdot 120 = 840.$$

$$|G| = n^k \cdot p^m$$

Sylow's Theorems. $|G| = p^k m, p \nmid m$

A Sylow p -subgroup is a subgroup of order p^k

I) Sylow p -subgroups exist (at least one)

II) Any two Sylow p -subgroups are conjugate

III) $n_p = \# \text{Sylow } p\text{-subgroups}$
 $n_p \equiv 1 \pmod{p}$
 $n_p \mid |G|$ (actually $n_p \mid m$)

$n_p = [G : N_G(P)] = |G| / |N_G(P)|, N_G(P) = \{g : gPg^{-1} = P\}$
 (orbit-stabilizer theorem)

$n_p = 1 \iff P$ is normal

Section
6.2
of
Dummit
& Foote

Show that if $|G| = 30$, then G has a cyclic subgroup of order 15.

n_2	n_3	n_5
$n_2 \mid 15$	$n_3 \mid 10$	$n_5 \mid 6$
$n_2 \equiv 1 \pmod{2}$	$n_3 \equiv 1 \pmod{3}$	$n_5 \equiv 1 \pmod{5}$
$n_2 = 1, 3, 5, 15$	$n_3 = 1, 10$	$n_5 = 1, 6$

We can rule out $n_3 = 10$ and $n_5 = 6$ occurring together



20 elements of order 3



24 elements of order 5

impossible since $20 + 24 > 30$

If $n_3 = 1$, then $P_3 \trianglelefteq G$ (normal)

$|G/P_3| = 10$

Sylow \Rightarrow has a subgroup of order 5

$|H/P_3| = 5 \Rightarrow |H| = 15$

So G has a subgroup H of order 15.

In H , $n_3 = 1, n_5 = 1$, so H

If $n_5 = 1$, then $P_5 \trianglelefteq G$ (normal)

$|G/P_5| = 6$

Sylow \Rightarrow has a subgroup of order 3.

$|H/P_5| = 3 \Rightarrow |H| = 15$

So G has a subgroup H of order 15.

In H , $n_3=1$, $n_5=1$, so H
has normal subgroups $P_3, P_5 \trianglelefteq H$

★ [Recognition theorem: If $H, K \trianglelefteq G$, $H \cap K = 1$, $|H| \cdot |K| = |G|$,
then $G \cong H \times K$.

So $H \cong P_3 \times P_5 \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/15\mathbb{Z}$ cyclic.
 $\uparrow \quad \uparrow$ CRT
 coprime

$H \leq G$ finite index $[G:H]=n$. Show G contains
a normal subgroup $N \trianglelefteq G$, $N \leq H$, $[G:N] \leq n!$

(One application: If $[G:H]=2$, then $H \trianglelefteq G$)

G acts on cosets of H by $g \cdot (g'H) = (gg')H$

$\varphi: G \rightarrow S_n$ a homomorphism

Set $N = \ker \varphi = \{g \in G : gg'H = g'H, \forall g'H\}$

$$= \bigcap_{g \in G} gHg^{-1}$$

$$g'^{-1}gg' \in H \quad \forall g'$$

$$g \in g'Hg'^{-1} \quad \forall g'$$

$N \trianglelefteq G$ since N is a kernel

$N \leq H$

$$[G : \ker \varphi] = |\text{im } \varphi| \leq |S_n| \quad (\text{so } \leq n!)$$

1) If G is nonabelian, then $G/Z(G)$ is not cyclic

Pf: If $G/Z(G) = \langle gZ(G) \rangle$

then any $hZ(G) = g^k Z(G)$

so $h = g^k \cdot z$ for some $z \in Z(G)$

$$\text{But } (g^j \cdot z)(g^k \cdot z') = (g^k \cdot z')(g^{j+k} \cdot z)$$

contradicts G nonabelian.

2) If $|G| = p^n$, show $|Z(G)| > 1$.

$$|G| = |Z(G)| + \sum_g \frac{|G|}{|C_G(g)|}$$

div by
 p (if $n \geq 1$)

$$\sum_g \frac{|G|}{|C_G(g)|}$$

$\frac{p^k}{p^k} = \text{power of } p,$
larger than 1

p (if $n \geq 1$)
So $p \mid |Z(G)|$

$p^n = \text{power}$
 \dots
 $\text{larger than } 1$
div by p

3) If $|G| = p^2$, then

$|Z(G)| = 1$
impossible
by (2)

or $|Z(G)| = p$
impossible
since then
 $|G/Z(G)| = p$
cyclic, contradicting (1)

or $|Z(G)| = p^2$
 G is
abelian