Correspondence theorem

$G \qquad N \triangleleft G$

$$G \xrightarrow{\varphi} G/N$$
$$g \longmapsto gN$$

$\exists$ bijection

$$\{H < G \text{ w/ } N \subset H\} \longleftrightarrow \{\overline{H} < G/N\}$$
$$H \longmapsto H/N = \varphi(H)$$
$$\varphi^{-1}(\overline{H}) \longleftarrow \overline{H}$$
$$\text{normal} \longleftrightarrow \text{normal}$$
$$H \rightsquigarrow |H/N| = |H|/|N|$$

Counting: $H, K < G \qquad |HK|$

$$H \times K \longrightarrow G$$
$$(h,k) \longmapsto hk$$

$$(h', k') \longrightarrow hk$$
$$h^{-1}h' = kk'^{-1} \in H \cap K \ni a$$
$$(ha, a^{-1}k) \longrightarrow hk$$

$$\boxed{|HK| = \frac{|H||K|}{|H \cap K|}}$$

Sylow Stuff:

Recall: If G a finite gp $|G| = p^n m$ w/ p prime $p \nmid m$.

we say $P < G$ is a p-Sylow subgp if $|P| = p^n$

Def $Syl_p G = \{\text{Sylow } p \text{ subgps}\}$ $n_p = |Syl_p G|$

Part 1: $Syl_p G \neq \emptyset$

$X = \{\text{subsets of } G \text{ of order } p^n\}$

Pf: $|G| = |Z(G)| + \sum_i [G : C_G(a_i)]$

a_i distinct nontrivial conj classes.

Case 1: $p \mid |Z(G)|$

$a \in Z(G)$ $\langle a \rangle \triangleleft G$ $G/\langle a \rangle$ gp of order $p^{n-1}m$

choose Cauchy $o(a) = p$

by induction G has a subgp $\overline{P}$ of order p^{n-1}

but by corresp G has P of order p^n.

Case 2: $p \nmid |Z(G)|$

$\Rightarrow p \nmid [G : C_G(a_i)]$ some i

$$[G : C_G(a_i)] = |G| / |C_G(a_i)|$$

$\Rightarrow p^n \mid |C_G(a_i)|$

$C_G(a_i) \subsetneq G$

So by induction $\exists\, P < C_G(a) < G$

order p^n ✓.

Sylow conjugates

(p-group = gp of order p^n some n)

if $P < G$ any p-subgroup and $S < G$ Sylow p-subgp. then $\exists g \in G$ w/ $gSg^{-1} \supset P$.

Pf: note: $P \subset gSg^{-1} \Leftrightarrow PgSg^{-1} = gSg^{-1}$

$\Leftrightarrow PgS = gS$

Consider G/S $\quad P \circlearrowright G/S$ left translation.

G/S union of orbits under P but orbit-stab.

$\Rightarrow |\text{orbit}_{gS}| = \dfrac{|P|}{|\text{Stab}_{gS}|}$ p-powers. either size 1 or mult. of p.

not all mult. of p since G/S union of orbits not a mult. of p.

$|G/S| = m$
$p \nmid m$

So one orbit must be size $1 \Rightarrow$ ∎.

Aside: If P is a p-gp. consider action of $P \circlearrowright P$ via conj. again as above orbits are p-pow size.

$\Rightarrow$ either 1 or mult. of p

$\{e\}$ size 1.

$\Rightarrow$ at least p size 1 orbits $\Rightarrow p \mid |Z(G)|$

$Z(G) \neq (e)$.

$\Rightarrow$ P groups have nontrivial centers

Follows that elements of $\mathrm{Syl}_p G$ are conj. to each other (single orbit for G acting via conjugation).

$P_0, P_1 \in \mathrm{Syl}_p G$

$\mathrm{Stab}_{P_1} P_0 = P_0 \cap N_G P_1$

conj. action

$$\boxed{\begin{array}{l}\text{claim} \\ P_0 \cap N_G P_1 = P_0 \cap P_1\end{array}}$$

$\Rightarrow \underset{\text{under } P_0}{|\text{orbit of } P_1|} = \frac{|P_0|}{|P_0 \cap P_1|}$

need to show $P_0 \cap N_G P_1 \subset P_1$

$(P_0 \cap N_G P_1) P_1$ is a subgp

$P_0 \cap N_G P_1 \subset N_G P_1$

$$|(P_0 \cap N_G P_1) P_1| = \frac{|P_0 \cap N_G P_1| \, |P_1|}{|P_0 \cap N_G P_1 \cap P_1|}$$

is a p-power.

but P_1 = max'l p-power subgp $\Rightarrow (P_0 \cap N_G P_1) P_1 = P_1$

$\Rightarrow P_0 \cap N_G P_1 \subset P_1$ $\square$.

$n_p \equiv_p 1$ but in fact if $p^e \mid [P_0 : P_0 \cap P_1]$ all $P_0, P_1 \in \mathrm{Syl}_p$
then $n_p \equiv_{p^e} 1$

<u>Sylow divisibility</u>

$$n_p = \frac{|G|}{|N_G P|} \;\Big|\; \frac{|G|}{|P|} = [G : P]$$

$P \in \mathrm{Syl}_p G$

<u>Stupid example</u>:

$|G| = 360$

$n_3 \equiv 1 \pmod 3$

$n_3 \equiv_3 1 \quad n_3 \mid 40$

$n_3 = 1, 4, 10, 40$

if $n_3 = 4$ or $40 \Rightarrow n_3 \not\equiv_9 1$

$\Rightarrow \exists\, P, Q \in \mathrm{Syl}_3 G \quad |P \cap Q| = 3$

<u>Def</u> A group is simple if it is nonabelian and has no nontrivial normal subgroups

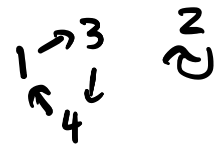
<u>Rem</u>: An Abelian group has no nontrivial normal subgps $\Leftrightarrow$ it has prime order ($\Rightarrow$ is cyclic)

"devissage"

Permutations (symmetric groups)

$S_n = S_{\{1,\dots,n\}}$ $\quad \sigma \in S_n \quad \begin{pmatrix} 1 & 2 & 3 & \cdots & \cdots \\ \sigma(1) & \sigma(2) & & & \end{pmatrix}$

$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} \qquad (134)\cancel{(2)}$



$\sigma \in S_n \qquad \langle \sigma \rangle \circlearrowright \{1,\dots,n\}$

disj. union of orbits

ordered orbits $\longleftrightarrow$ action of σ

orbit notation

given $\sigma \in S_n$ what is $cl(\sigma)$

$$\tau\sigma\tau^{-1}(\tau(i)) = \tau\sigma(i)$$

$$\sigma: \quad i \longmapsto \sigma(i)$$

$$\tau\sigma\tau^{-1}: \quad \tau(i) \longrightarrow \tau(\sigma(i))$$

$\sigma = (134)$ in S_4

τ anything $\quad \tau\sigma\tau^{-1} = (\tau(1)\,\tau(3)\,\tau(4))$

orbit description $\Longrightarrow$ permutations described by partitions of $\{1,\dots,n\}$

$\{1,\dots,5\} \qquad (13)(245) \longmapsto 2+3=5$

conj. classes $\Longleftrightarrow$ partition types $\Longleftrightarrow$ partitions of integers

S_5 conj. classes

$1+1+1+1+1$	(identity)
$2+1+1+1$	(ab)
$2+2+1$	$(ab)(cd)$
$3+1+1$	(abc)
$3+2$	$(abc)(de)$
$4+1$	$(abcd)$
5	$(abcde)$

Alternating groups

$S_n \circlearrowright \{1,\dots,n\}$ $\qquad S_n \circlearrowright \mathbb{R}^n$ permuting basis vectors

$$\sigma \in S_n \to GL_n(\mathbb{R}) \xrightarrow{\det} \mathbb{R}^*$$

$$GL_n(\mathbb{R}) = \{T \in M_n(\mathbb{R}) \mid \det T \neq 0\}$$

homomorphism of gps

$$S_n \xrightarrow{\operatorname{sgn}} \{\pm 1\}$$

$$(ab) \mapsto -1$$

$$\boxed{\text{def } \ker(\operatorname{sgn}) =: A_n}$$

Fact A_n simple for $n \geq 5$

ex: (12) odd. $\qquad (123) = (13)(12)$ even.

$$(12\dots k) = \begin{cases} \text{even if } k \text{ odd} \\ \text{odd if } k \text{ even.} \end{cases}$$

even # of even cycles to be even.
length

A_5 cycle types: (12)(34)
(123)
(12345)

$cl((12)(34)) = [A_5 : C_{A_5}((12)(34))]$

order 4 $\quad C_{A_5}((12)(34)) = \underbrace{C_{S_5}((12)(34)) \cap A_5}$

(12)(34)
(12)
(34)
(13)(24)
(14)(23)
(e)

$|A_5| = 60$

$cl((12)(34)) = \frac{60}{4} = 15$

$cl((123)) = \frac{60}{3} = 20$

(e)
(123)
(132)
~~(12)(45)~~
(13)(

$\left.\begin{matrix}\\\\\end{matrix}\right\} \begin{matrix} C_3 \\ \shortparallel \\ A_3 \end{matrix} \left.\right\} 3$

$cl((12345)) = \frac{60}{5} = 12$

centralizer = $\langle (12345) \rangle$
5

conj. classes of order

(e)	1
(12)(34)	15
(123)	20
(12345)	12