"the Class equation"

aka "Keys to the kingdom"

or "Path to total victory"

<u>Theorem (Cauchy's theorem)</u>

Suppose $p \mid |G|$ p prime. Then $\exists g \in G, o(g) = p$.

<u>Pf:</u> induct on $|G|$.

$|G| = p$ ✓

in general, $|G| = |Z(G)| + \sum_{i=1}^{m} [G : C_G(a_i)]$

if $p \mid |C_G(a_i)|$ done by induction since $C_G(a_i) \lneq G$.

$a_i \notin Z(G)$ by assumption.

if not the case, then

$p \nmid |C_G(a_i)|$ each a_i, $p \mid |G|$

$\Rightarrow p \mid [G : C_G(a_i)]$

$\Rightarrow p \mid |Z(G)| = |G| - \sum [G : C_G(a_i)]$

So WLOG, G is Abelian.

Now, choose $g \in G \setminus \{e\}$.

if $p \mid o(g)$ then, say $o(g) = p\ell \Rightarrow o(g^\ell) = p$

done.

if $p \nmid o(g)$ consider $G/\langle g \rangle$

by hyp, $\exists\ \bar{h} = h\langle g \rangle$ w/ $o(\bar{h}) = p$

$\Rightarrow p \mid o(h)$ (if not $h^s = e$ pts $\Rightarrow$

$\bar{h}^s = e$ pts $\Rightarrow$ ↯)

$\square$

<u>**Ex:**</u> Suppose $|G| = 20$. Then $\exists\ N \triangleleft G$ w/

$|N| = 5$

<u>Pf:</u> by Cauchy $\exists\ H < G$, $|H| = 5$.

Consider $G \circlearrowright G/H$ by left mult.

Gives $G \xrightarrow{\varphi} S_4$, $|G| = 20$, $|S_4| = 24$

So $G/\ker\varphi < S_4 \Rightarrow |\ker\varphi| = 5, 10, 20$

Now G/H is a single orbit

$\Rightarrow |\mathrm{Stab}_G(H)| = 5$

and $\ker\varphi < \mathrm{Stab}_G(H)$

$\Rightarrow |\ker\varphi| = 5$ D.

Good for big primes.

Consider $|H| = 2$ $H < G$ $|G| = 20$

Get $G \to S_{10}$ not helpful

HW 3.1 / 36

If $o(g) = p^2$

$$|G| = |Z(G)| + \sum_{i=1}^{m} [G : C_G(a_i)]$$

$p \mid [G : C_G(a_i)]$ each $i \Rightarrow p \mid |Z(G)|$.

So $|Z(G)| = p$ or p^2

if $|Z(G)| = p \Rightarrow |G/Z(G)| = p$ is cyclic

$\Rightarrow G$ Abelian $\Rightarrow Z(G) = G$.

<u>Thm</u> $|G| = p^n \Rightarrow Z(G) \neq (e)$.

<u>Symmetric groups</u>

Conjugacy classes $\longleftrightarrow$ cycle types $\longleftrightarrow$ partitions ex: S_4 classes

(e)	$1+1+1+1$	24	1
(ab)	$2+1+1$	4	6
$(ab)(cd)$	$2+2$	8	3
(abc)	$3+1$	3	8
$(abcd)$	4	4	6

$$C_{S_4}((12)) = S_2 \times S_2 = S_{\{1,2\}} \times S_{\{3,4\}}$$

$C_{S_4}((12)(34)) =$ same but can also switch (12) $\cancel{\&}$ (34)

$$C_{S_4}((12)(3,4)) \to S_{\{\{12\}\{34\}\}}$$

kernel $S_{\{12\}} \times S_{\{34\}}$

$$C_{S_4}((abc)) = C_3$$

$$C_{S_4}(1234) = C_4$$

The simplicity of A_5

Observation: In any finite group G, if $N \trianglelefteq G$ then N is a union of conjugacy classes.

$|A_5| = 60.$

What are the conjugacy classes?

even cycle types $(12)(34)$

(123)

(12345)

1

etc.

$$C_{S_5}((123)) = \langle (123) \rangle \cup \langle (123)(45) \rangle$$

$A_3 \times S_2$ so $C_{A_5}((123)) = \langle (123) \rangle$

$$C_{S_5}(\langle 12345 \rangle) = \langle (12345) \rangle = C_{A_5}(\langle 12345 \rangle)$$

So 20 conj.'s of (123)

12 conj.'s of (12345)

there are $5 \cdot 4 \cdot 3 / 3 = 20$ 3-cycles $\Rightarrow$ all conjugate.

There are $5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 / 5 = 24$ 5-cycles $\Rightarrow$ not all conj. (2 conj classes)

So far:

$$\left.\begin{array}{l} |Z(G)| = 1 \\ |\text{order } 3 \text{ class}| = 20 \\ |\text{order } 5 \text{ class } 1| = 12 \\ |\text{order } 5 \text{ class } 2| = 12 \end{array}\right\} 45 \text{ so far.}$$

all remaining elmts are order 2 (15 of them.

$C_{A_5}((12)(34))$ ends up as gen by $(12)(34)$ & $(13)(24)$

order 4

$(\{1, (14)(23)\})$

So ordr 4 $\Rightarrow$ all ordr 2 elmts are conjugate.

So if $N \triangleleft G$, $N = \{e\} \cup \bigcup$ subsets of orders

15, 20, 12, 12

and $|N| \mid |G| = 60$

impossible! $\square$.

<u>Some general facts</u>

- Correspondence thm

  let $N \triangleleft G$. Then $\exists$ a bijection

  corresp. $\{H < G \mid N \subset H\} \longleftrightarrow \{\overline{H} < G/N\}$

  $H \longmapsto H/N$

  $\{g \in G \mid gN \in \overline{H}\} \longleftarrow \overline{H}$

  and $H \triangleleft G \Leftrightarrow \overline{H} \triangleleft G/N$.

<u>Thing 2</u> How subgroups fit together to make a group.

Suppose $H, K < G$.

$HK = \{hk \mid h \in H, k \in K\}$.

when is $HK < G$?

Note $H < G \Rightarrow H^{-1} = \{h^{-1} \mid h \in H\} = H$

So $HK < G \Rightarrow \underset{\overset{\shortparallel}{HK}}{(HK)^{-1}} = K^{-1}H^{-1} = KH$

and for $H \subset G$, $H < G$ iff H closed i.e. $HH = H$

Now if $HK = KH$ then

$$(HK)(HK) = H(KH)K = H(HK)K$$
$$= (HH)(KK) = HK$$

$\Rightarrow HK < G$. <u>Prop</u> $HK < G \Leftrightarrow HK = KH$.

In fact it is clear that so long as $KH \subset HK$ we have

$$HK \subset HKHK \subset HHKK = HK \Rightarrow$$

$$HKHK = HK$$

$$\Rightarrow HK < G.$$

So <u>Prop</u> $HK < G \iff KH \subset HK$

$$\iff KH = HK!$$

<u>Cor</u> if $H < N_G(K)$ then $HK < G$

<u>Pf:</u> $H < N_G(K) \Rightarrow \forall h \in H,\ hK = Kh$

$\Rightarrow HK \subset KH \Rightarrow HK < G$.

<u>e.g.</u> works if $H \trianglelefteq G$.

How big is HK?

$$H \times K \xrightarrow{f} HK \qquad \text{set map}$$
$$(h,k) \longmapsto hk$$

$$f^{-1}(hk) = \{(h',k') \mid h'k' = hk\}$$
$$= \{(h',k') \mid h^{-1}h' = k(k')^{-1}\}$$

Have ~~a~~ maps $f^{-1}(hk) \longleftrightarrow H \cap K$

$$(h',k') \longmapsto h^{-1}h'$$
$$(hg, g^{-1}k) \longleftarrow\!\shortmid\ g$$

bijection.

So $|f^{-1}(hk)| = |H \cap K|$ all $hk \in HK$

$\Rightarrow$ (because multiplication)

$$|H \times K| = |H \cap K| \cdot |HK|$$

$$\overset{\shortparallel}{|H||K|} \qquad \Rightarrow \quad |HK| = \frac{|H||K|}{|H \cap K|}$$

Could also do orbit-stabilizer

$H \times K$ acts on HK via

$$(h,k)\, h'k' \equiv h h' k' k^{-1}$$

check: $(h_1,k_1)\underbrace{(h_2,k_2)\, h'k'} = (h_1,k_1)\, h_2 h' k' k_2^{-1}$

$$= h_1 h_2 h' k' k_2^{-1} k_1^{-1}$$

$$= (h_1 h_2) h' k' (k_1 k_2)^{-1}$$

$$= (h_1 h_2, k_1 k_2)\, h'k'.$$

$\mathrm{Stab}_{H \times K}(e) = \{(h,k) \mid hk^{-1} = e\} \leftrightarrow H \cap K.$

$\{(h,k) \mid h = k\}$

The Sylow theorems

Def Let G be finite, $|G| = p^\alpha m$ w/ $p \nmid m$.
We say $H < G$ is a p-Sylow subgroup if $|H| = p^\alpha$. We write $Syl_p(G) = \{p\text{-Sylow subgps}\}$

Theorem Let G be a finite group. Then $\forall p$,

1) $Syl_p(G) \neq \emptyset$
2) $\forall P, Q \in Syl_p(G)$, $\exists g \in G$ w/ $gPg^{-1} = Q$.

$2\frac{1}{2}$) $\forall P \in Syl_p(G)$, $H < G$ w/ $|H| = p^\beta$ $gHg^{-1} \subset P$ some g.

3) $|Syl_p(G)| \equiv_p 1$
($3\frac{1}{2}$) 4) $|Syl_p(G)| \,\big|\, |G|$

Pf strategy:
1) is from Class eqn.
for rest, will want to consider action of G & P's on $Sylp(G)$, count sizes of orbits/Stabs... $|P| = p^\beta$

1) Consider $|G| = |Z(G)| + \sum_{i=1}^{m} [G : C_G(g_i)]$

will induct on $|G|$.

Case 1: $p \nmid |G| \Rightarrow Syl_p(G) = \{(e)\}$ ✓

Case 2: $p \mid |Z(G)|$. Choose $g \in Z(G)$

$o(g) = p$. $\langle g \rangle \triangleleft G$ since g is central.

By induction $\exists \bar{P} \triangleleft G/\langle g \rangle$ order $p^{\alpha - 1}$

but $\bar{P} \longleftrightarrow P < G$ order p^{α} $\square$.

<u>Case 3</u>: $p \nmid |Z(G)|$. this $\Rightarrow p \nmid [G : C_G(g_i)]$
some g_i

$\Rightarrow p^m \mid |C_G(g_i)|$

but $C_G(g_i) \lneq G$ (since g_i not central)

and so by induction $\exists P < C_G(g_i) < G$

order p^m $\square$.

Reminders:

Consider $\mathrm{Syl}_p(G) \ni P$

and its orbit $P_1 = P, P_2, \dots, P_r$ under G.

Suppose $Q < G$, $|Q| = p^\beta$.

Then Q acts on $P_1, \dots, P_r$ by conj.

Suppose $P_1, \dots, P_s$ $\underbrace{\qquad X \qquad}$ are orbit of Q.

Then $s = \dfrac{|Q|}{|\mathrm{Stab}_Q P_1|}$ $\qquad \mathrm{Stab}_Q P_1 = Q \cap N_G(P)$

but $\quad Q \cap N_G(P) < Q$ is a p-gp

and $Q \cap N_G(P) < N_G(P) \implies$

$\big(Q \cap N_G(P)\big) P < G$ is also a p-gp

containg $P \Rightarrow = P$

$\implies Q \cap N_G(P) \subset P$. But $\Rightarrow Q \cap N_G(P) \supset Q \cap P$ so $=$.

So $\quad s = \dfrac{|Q|}{|Q \cap P|} = [Q : Q \cap P]$

For example, if $Q = P = P_1$ then we find $s = 1$

So orbit of P_1 under P_1 has one.

but all other orbits under P_1 have size $s = \dfrac{|P_i|}{|P_1 \cap P_i|}$

mult. of p.

$\Longrightarrow \quad |Syl_p(G)| \equiv_p 1. \qquad \Rightarrow 3).$

Now part $2\frac{1}{2}$: if $Q < G \quad |Q| = p^\beta$,

suppose $Q \not\leq P_i$ all i.

then size of orbit of P_i under Q is

a mult. of p $\left(= [Q : Q \cap P_i] \right)$

but $p \nmid |Syl_p G| \Rightarrow$ ⨳.

$\Rightarrow 2\frac{1}{2}$. but $2\frac{1}{2} \Rightarrow 2$.

Finally, we get $\mathrm{Syl}_p G$ is a single orbit under G

$$\Rightarrow |\mathrm{Syl}_p G| = \frac{|G|}{|\mathrm{Stab}_G(P)|} = [G : N_G(P)] \,\big|\, |G|.$$

in fact $\mid [G : P]$

but automatic.

Notation $n_p = n_p(G) = |\mathrm{Syl}_p(G)|$.

<u>Cor</u> $n_p = 1 \Longleftrightarrow P \trianglelefteq G$ P a Syl. p-subgp

P char G

elmts of order p gen a subgp.

<u>Note</u> K char $N \trianglelefteq G \Rightarrow K \trianglelefteq G$

<u>Pf:</u> $\forall g \in G$, $gNg^{-1} = N \Rightarrow \mathrm{inn}_g : N \to N$

is an aut. $\Rightarrow \mathrm{inn}_g(K) = K \Rightarrow gKg^{-1} = K$ ✓.

<u>Cor</u> if $P < N \trianglelefteq G$ P unique p-Sylow in $N \Rightarrow$

$P \trianglelefteq G$!

Suppose $|G| = 60$ then either

$P_5 \in Syl_5 G$ is normal or G is simple.

<u>Warmups</u>

$|G| = 2, 3, 4, 5, 6, 7, 8, \ldots$

$|G|$ prime $\Rightarrow$ cyclic, (simple)

$|G| = p^2 = $ Abelian

so have $N \triangleleft G$ order $|G/N| = p$.

how about pq?

e.g. $|G| = 6$ or 16.

for 6, $n_2 \equiv_1 2$, $n_2 | 6 \Rightarrow n_2 = 1, 3$

$n_3 \equiv_1 3$, $n_3 | 6 \Rightarrow \boxed{n_2 = 1}$

so $P_3 \triangleleft G$.

for 10 $n_2 \equiv_1 2$ $n_2 | 10 \Rightarrow n_2 = 1, 5$

$n_5 \equiv_1 5$ $n_5 | 10 \Rightarrow n_5 = 1$

or pq

$n_p \equiv_1 p \quad n_p | pq$. but $n_p \nmid p \Rightarrow$
$n_p | q$

but n_p is either
1 or $p+1$ or $2p+1 \ldots$

$\Rightarrow n_p = 1$ or $n_p > p$.

consequently, if $p > q \Rightarrow n_p | q \Rightarrow$
$n_p = 1$.

So $\boxed{|G| = pq, \ p > q \Rightarrow n_p = 1}$

$\boxed{P_p \triangleleft G.}$

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11,

order p^n ?

as we've seen $Z(G) \neq (e) \Rightarrow$ have
nontrivial normal $Z(G) \triangleleft G$ so can
express in terms of smaller.

Def G is solvable, if we can find subgps

$(e) = H_0 < H_1 < H_2 < \dots < H_m = G$ w/

$H_i \triangleleft H_{i+1}$ and H_{i+1}/H_i Abelian

($\Leftrightarrow$ can do w/ H_{i+1}/H_i cyclic)

So far, evrythg is solvable...

How about $|G| = 12$?

$n_2 \equiv_2 1$ and $n_2 | 3$ $\quad n_2 = 1, 3$

$n_3 \equiv_3 1$ and $n_3 | 4$ $\quad n_3 = 1, 4.$

Give up? no!! what if $n_2 = 3$.

3 is pretty small, and G acts on a set of 3 elmts w/ sylow orbit.

get nontrivial map

$$\begin{array}{ccc} G & \longrightarrow & S_3 \\ 12 & & 6 \end{array}$$

How big is kernel? kernel $\subset \mathrm{Stab}_G(P_2) = N_G P_2$

so kernel size 2 or 4.

order 4 ($= P_2$)

So have $N \triangleleft G$ order 2 or 4.

since $P_2 \ntriangleleft G$ by assumption have $N \triangleleft G$ order 2.

So either $P_2 \triangleleft G$ or have $N \triangleleft G$ order 2.

(and $n_2 = 3$ so get $N = P_2 \cap P_2' \cap P_2''$)

$|G/N| = 6$ solvable etc.

Let's move on

13, 14, 15, 16, 17, 18

$n_3 \equiv_1 3$, $n_3 \mid 2$ ✓

in general if $|G| = p^a q$ $p > q$ works $n_p = 1$

19, 20

$n_5 \equiv_5 1, \quad n_5 \mid 4 \Rightarrow n_5 = 1$

in general if $|G| = p^a q^b$ w/ $p > q^b$ then $n_p = 1$

21, 22, 23, 24

$n_2 \equiv_2 1, \quad n_2 \mid 3 \qquad n_2 = 1, 3$

$n_3 \equiv_3 1, \quad n_3 \mid 8 \qquad n_3 = 1, 4$

if $n_2 = 3$, get again

$G \xrightarrow{\varphi} S_3 \qquad \ker\varphi \subset \mathrm{Stab}\, P_2 = N_G(P_2)$

24 $\qquad$ 6

so $|\ker\varphi| = 4$ or $\cancel{8}$ $\qquad$ ord 8 $= P_2$

so $|\ker \varphi| = 4$ so $\exists\, N \trianglelefteq G$, $|N| = 4$

$N = P_2 \cap P_2' \cap P_2''$

25, 26, 27, 28, 29, 30

$n_2 \equiv_2 1 \quad n_2 \mid 15 \qquad n_2 = 1, 3, 5, 15$

$n_3 \equiv_3 1, \; n_3 \mid 10, \quad n_3 = 1, 10$

$n_5 \equiv_5 1, \; n_5 \mid 6, \quad n_5 = 1, 6$

<u>Let's count!</u> if $n_5 = 6$ & $n_3 = 10$ then

P_5's don't intersect except in (e) & sim P_3's.

each has 4 non id. elmts

each has 2 non-id elmts

$\Rightarrow \underbrace{6 \cdot 4}_{24}$ elmts order 5 $\qquad \underbrace{2 \cdot 10}_{20}$ elmts order 2

too many! can't both happen!

So either $\boxed{n_5 = 1 \text{ or } n_3 = 1}$

31, 32, 33, 34, 35, 36

$2^2 \cdot 3^2$

$n_2 \equiv_2 1 \quad n_2 \mid 9 \Rightarrow n_2 = 1, 3, 9$

$n_3 \equiv_3 1 \quad n_3 \mid 4 \Rightarrow n_3 = 1, 4$

Get $G \xrightarrow{\varphi} S_4 = S_{Syl_3 G}$

$\ker \varphi < N_G P_3 = P_3$

$\uparrow$ mod 9 $\Rightarrow$

and $\dfrac{|G|}{|\ker \varphi|} \mid |S_4| = 24$

$\dfrac{36}{|\ker \varphi|} \mid 12$ so $|\ker \varphi| = 3$ or $\cancel{9}$

$\Rightarrow \exists N \lhd G \ |N| = 3.$

37, 38, 39, 40

$2^3 \cdot 5$

$n_5 \equiv_5 1 \quad n_5 \mid 8 \implies n_5 = 1$ ✓

41, 42

$7 \cdot 6 \quad n_7 \equiv_7 1 \quad n_7 \mid 6 \implies n_7 = 1$

$|G| = p^a m \,, \quad p > m \implies n_p = 1.$

43, 44, 45

✓

$n_5 \equiv_5 1 \,, \quad n_5 \mid 9 \implies n_5 = 1.$

46, 47, 48

$2^4 \cdot 3 \quad n_2 \equiv_2 1 \,, \quad n_2 \mid 3$ so if $n_2 = 3$ then

$G \xrightarrow{\varphi} S_3$ w/ $\ker\varphi < N_G(P_2)$

$= P_2$ ord 16

$\frac{|48|}{|\ker\varphi|} \mid 6$ so $|\ker\varphi| = 8$

$\Rightarrow P_2 \cap P_2' \cap P_2'' = N \trianglelefteq G, |N| = 8.$

49, 50, 51, 52, 53, 54, 55, 56

$7 \cdot 8$

$n_7 \equiv_7 1 \quad n_7 | 8 \Rightarrow n_7 = 1, 8$

$n_2 \equiv_2 1 \quad n_2 | 7 \Rightarrow n_2 = 1, 7$

what if $n_7 = 8$? and $n_2 = 7$?

then get $\underbrace{6 \cdot 8}_{48}$ elmts order 7

and one identity. = 49 elmts.

there are exactly 7 elements left

Know $\exists P_2 < G$ order 8 and this has 7 elmts of order not 7. But therefore there is only one such subgroup $\Rightarrow n_2 = 1$.

57, 58, 59, 60

now it's interesting!

$n_5 \equiv_5 1$, $n_5 | 6$ $\Rightarrow$ $n_5 = 1$ or 6.

Suppose $n_5 = 6$.

<u>Claim:</u> G is simple.

Assume not, say $N \trianglelefteq G$.

we can't have $5 \mid |N|$ since this would say

$|N| = 5$ or 10 or 15 or 20 or 30

if $|N| = 5, 10, 15, 20 \Rightarrow n_5 = 1$. since P_5 chr $N \trianglelefteq G$.

if $|N| = 30$ and $P_5 \ntrianglelefteq N \Rightarrow P_3$ chr $N \trianglelefteq G$

and G/P_3 ord 20 so get $\overline{H} \trianglelefteq G/P_3$ ord 5

$\Rightarrow H \trianglelefteq G$ ord 15.

so $P_3 \ntrianglelefteq G$

But P_5 chr $H \trianglelefteq G \Rightarrow$ ~~$\Rightarrow$~~.

So $5 \nmid |N|$.

$\Rightarrow |N| = 2, 3, 4, 6, 12$.

if $|N| = 6$ then P_2 chr N

if $|N| = 12$ then P_2 chr N or

$\underbrace{P_2 \cap P_2' \cap P_2''}_{\text{ordr } 2}$ chr N

$\Rightarrow$ have normal w/

$|N| = 2, 3, 4$ in all cases.

but now G/N ordr 30 or 20 or 15

no since

$P_3 \ntriangleleft G$

So get $|N| = 2, 4$

now

if $|N| = 4 \Rightarrow |G/N| = 15 \Rightarrow \exists\ \bar{H} \triangleleft G/N$ ordr 5

$\Rightarrow |H| = 20$ w/ $H \triangleleft G$ done.

if $|N|=2$, $|G/N|=15 \Rightarrow \exists \bar{H} \triangleleft G/N$ ordr 5
or ordr 3

$\Rightarrow H \triangleleft G$ ordr 10 or 6

$\Downarrow$ $P_5 \triangleleft G$ $\Downarrow$ $P_3 \triangleleft G$ $\leadsto$ ⨯.

$\square$

Cor A_5 simple

Pf $\langle (12345) \rangle \neq \langle (13245) \rangle$.