Algebra I Lecture 7/18: Conjugation

loo

· Moving Exam? Ask them

$G \circlearrowright G$ by **conjugation**: $g \cdot h = ghg^{-1}$

orbits $\rightsquigarrow$ conjugacy classes.

Ex: · Conj. classes of $S_n \longleftrightarrow$ partitions of n.

· Conj. classes of $GL_n(\mathbb{C}) \longleftrightarrow$ Jordan normal form

$G \circlearrowright 2^G$ by conj. Orbit-stabilizer:

$\#$ of conj. of $S = [G : N_G(S)]$ (already saw on a HW)

e.g. $\#$ of conj. of $g \in G = [G : C_G(g)]$.

Thm (Class Eqn): $|G| < \infty$, conj. classes of elts. not in the center: $G \cdot g_1, \dots, G \cdot g_k$

~~the ones not in the center~~

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

Pf: $g \in Z(G) \Longleftrightarrow$ conj. class of $g = \{g\}$.

As the orbits partition G,

$$G = \dot{\bigcup} \text{ conj classes} = Z(G) \;\dot{\cup} \bigcup_{1 \le i \le k} G \cdot g_i \quad \text{size } [G : C_G(g_i)]$$

$$\Rightarrow |G| = |Z(G)| + \sum_{1 \le i \le k} [G : C_G(g_i)].$$

Ex: A **p-gp.** is a gp of order p^k, p prime.

Any p-gp. G has a non-trivial center, as

$$|G| \equiv 0 \equiv |Z(G)| + \sum 0 \mod p \quad \left(\frac{|G|}{|C_G(g)|} \,\Big|\, p^k, \neq p^0\right)$$

$$\Rightarrow p \,\big|\, |Z(G)|,\ Z(G) \ni e \Rightarrow |Z| \neq 0.$$

Cor: $|G| = p^2 \Rightarrow G \cong \mathbb{Z}/p^2$ or $\mathbb{Z}/p \times \mathbb{Z}/p$.

Pf: $Z(G) \neq 1 \Rightarrow G/Z(G)$ is cyclic (size 1 or p).

HW problem $\Rightarrow$ G is abelian.

If G has elt. of order $p^2 \Rightarrow G \cong \mathbb{Z}/p^2$.

If not, every non-ident. elt. has order p.

Pick any such ~~$g \in G \setminus \{e\}$. $g \neq g' \in G \setminus \{e\}$~~. $g \in G \setminus \{e\}$, and any $g' \in G \setminus \langle g \rangle$.

Then $|\langle g, g' \rangle| > |g| = p$

$\Rightarrow \langle g, g' \rangle = G \Rightarrow G \cong \mathbb{Z}/p \times \mathbb{Z}/p$.

Classes in S_n; $\sigma \in S_n \rightsquigarrow$ cycle decomposition

~~$\sigma = (n_1, \dots, n_k)(n_2$~~

e.g. $\sigma = (1372)(46)(5)(8)(9)$.

$\rightsquigarrow$ cycle type $4^1 2^1 1^3 \rightsquigarrow$ partition $4+2+1+1+1 = 9$.

of 9

Lemma: Conj preserves cycle type.

Pf: $\sigma = (a_1, \dots, a_{k_1})(b_1, \dots, b_{k_2}) \cdots$

$\tau \sigma \tau^{-1} = (\tau(a_1) \cdots \tau(a_{k_1}))(\tau(b_1) \cdots \tau(b_{k_2}))$

as if $\sigma(i) = j$, $\quad \tau \sigma \tau^{-1}(\tau(i)) = \tau(\sigma(i)) = \tau(j)$.

so $\tau \sigma \tau^{-1}: \tau(i) \longmapsto \tau(j)$.

so if ij appears in cycle decomp. of σ,

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

Prop: σ_1, σ_2 are conjugate iff same cycle type.

Pf: $\Rightarrow$ above

$\Leftarrow$: If σ_1, σ_2 have same cycle types.

Order in non-increasing length, including 1-cycles.

Ex: $\sigma_1 = (1372)(46)(5)(8)(9)$

$\sigma_2 = (4539)(12)(6)(7)(8)$.

Define τ: i^{th} int. in list of ints in σ_1 cycle decomp.

$\longmapsto i^{th}$ " " " σ_2 " "

Ex: $\tau: \begin{pmatrix} 1 & 3 & 7 & 2 & 4 & 6 & 5 & 8 & 9 \\ 4 & 5 & 3 & 9 & 1 & 2 & 6 & 7 & 8 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 9 & 5 & 1 & 6 & 2 & 3 & 7 & 8 \end{pmatrix} = (14)(2987356)$

Then $\tau \sigma_1 \tau^{-1} = \sigma_2$. Ex: $\tau \sigma_1 \tau^{-1}$: $5 \xrightarrow{\tau^{-1}} 3 \xrightarrow{\sigma_1} 7 \xrightarrow{\tau} 3 = \sigma_2(5)$

(2): $2 \rightarrow 6 \rightarrow 4 \rightarrow 1, = \sigma_2(2)$.

More interesting: conjugacy classes in A_n : (splitting --- partitions into odd distinct pts)

Sylow Theory: Partial Converses to Lagrange.

Powerful tool in finite gp. theory.

All the techniques come together! ~~All~~ All sorts of gp actions! [follow book, not Conrad.]

Lemma: G a p-gp. acts on X.

$|X| \equiv \#$ fixed pts mod p.

$(g \cdot x = x \ \forall g \in G)$.

all comes down to this!

Pf: $X = \dot{\bigcup}$ Orbits, rep. by $x_1, \dots, x_k$

$\Rightarrow |X| = \sum_i \frac{|G|}{|G_{x_i}|} \equiv$ # fixed pts. (p)

stab. $\equiv \begin{cases} 0 \bmod p & |G_{x_i}| < |G| \\ 1 \ \text{stab mod } p \ \text{~~Stab~~} & |G_{x_i}| = |G| \end{cases}$

[Make big table of actions on board]

Th^m (Sylow I):

Any finite gp. G of order n, $p^k \| n$ (exactly divides) has a subgp. of order p^k. Any such subgp. is called a p-Sylow subgp.

[all $\cong$, + in a particular way...]

Sylow II: All p-sylow gps. are conjugate.

Sylow III: If $n_p = \#$ of Sylow p-subgps, $|G| = p^k m$, then $(p^k \| |G|)$.

$n_p \equiv 1 \bmod p$, $n_p \mid m$. [knows about p and the rest! ~~Strong!~~]

Sylow III*: $n_p = [G : N_G(P)]$ P any Sylow p-subs. (Check: orbit-stab)

Pf: I: Do better: Show $\exists$ subgp. of order p^i $0 \le i \le k$.

(true for any p-gp). Given $|H| = p^i$ $i < k$ as things before. (conjugacy)

build a new subgp. $H' \supseteq H$. $[H' : H] = p$.

$\to$ chain $\{e\} = H_0 \overset{p}{\subseteq} H_1 \overset{p}{\subseteq} H_2 \subseteq \dots$

$H \circlearrowright G/H$ by left mult.
(not nec. a gp).

By lemma, H is a p gp.
$\Rightarrow |G/H| \equiv |\mathrm{Fix}_H(G/H)| \pmod p$

Now $gH \in \mathrm{Fix}_H(G/H) \Leftrightarrow hgH = gH \ \forall h \in H$
$\Leftrightarrow g^{-1}hgH = H \ \forall h$
$\Leftrightarrow g^{-1}hg \in H \ \forall h$
$\Leftrightarrow g^{-1}Hg \subseteq H$
$\Leftrightarrow g^{-1}Hg = H$ (as $|g^{-1}Hg| = |H|$)
$\Leftrightarrow g \in N_G(H)$.

$\Rightarrow \mathrm{Fix}_H(G/H) = \{gH \mid g \in N(H)\} = N(H)/H$
$\Rightarrow [G:H] \equiv [N(H):H] \bmod p$.

Now $H \trianglelefteq N(H) \Rightarrow N(H)/H$ is a gp.
As $|H| = p^i$, $i < k$, $p \mid [G:H] \Rightarrow p \mid [N(H):H] \Rightarrow N(H)/H$ has a subgp of order p (by Cauchy). By the correspondence theorem,

$\exists$ subgp. H' of $N(H)$ containing H,
$[H':H] = p \Rightarrow |H'| = p \cdot |H| = p^{i+1}$

(trans. action) Sylow II: Let $P, Q \in \mathrm{Syl}_p(G)$. To show: They are conj.

$Q \circlearrowright G/P$ by left. mult. Q is a p-group.

So lemma $\Rightarrow |G/P| \equiv |\mathrm{Fix}_Q(G/P)| \pmod p$

$\not\equiv 0 \bmod p$ as $|P| \,\|\, |G| \Rightarrow |\mathrm{Fix}_Q(G/P)| \neq 0$.
has no p-powers left

Take a fixed pt gP in G/P. Thus, $qgP = gP \ \forall q \in Q$
$\Rightarrow qg \in gP \ \forall q \Rightarrow Q \leq gPg^{-1} \Rightarrow Q = gPg^{-1}$ as they have the same size.

Sylow III:

Show: $n_p = |Syl_p^{(G)}| \equiv 1 \mod p$ | Pick any $P \in$ ...

$P \circlearrowright Syl_p(G)$ by conjugation | Want to use our Lemma.

Lemma $\Rightarrow$ $n_p \equiv$ {# fixed pts mod p.

(you know the trick)

Fixed pts are $Q \in Syl_p$ s.t. $gQg^{-1} = Q$ $\forall g \in P$.

Ex: P is a fixed pt.

For any such Q, $P \subseteq N_G(Q)$

Also, $Q \subseteq N(Q) \Rightarrow P, Q$ are p-sylow in $N_G(Q)$.

By Sylow ~~III~~ II, P, Q are conjugate in $N(Q)$.

As $Q \trianglelefteq N(Q)$, the only subgp of $N(Q)$ conj. to Q is Q itself.

$\Rightarrow P = Q$. Thus the only fixed pt. is P

$\Rightarrow$ # fixed pts $= 1$

$\Rightarrow n_p \equiv 1 \mod p$.

Show: $n_p | m$.

$G \circlearrowright Syl_p(G)$ by conj.

Sylow II $\Rightarrow$ all sylows are conjugate

$\Rightarrow$ one orbit (transitive)

$\Rightarrow n_p \,|\, |G|$ (as $|Syl_p| = |orbit(P)| = \left|\frac{G}{Stab(P)}\right| \,\Big|\, |G|$).

As $n_p \equiv 1 \mod p$, $(n_p, p) = 1 \Rightarrow \boxed{n_p | m}$

Sylow III*: $P \in Syl_p(G)$ $G \circlearrowright Syl_p(G)$ by conj.

orbit-stabilizer $\Rightarrow n_p = |Syl_p(G)| = [G : Stab_{\{P\}}]$.

(size orbit)

But: $Stab_{\{P\}} = \{g \in G \,|\, gPg^{-1} = P\} = N_G(P) \Rightarrow n_p = [G : N(P)]$.

Still catching up from storm

N.B. The book gives different pfs. I followed Conrad. (nicer pf).

To here

$\boxed{\text{Recall Sylow Th}^{ms}.}$

~~Ex~~: $A_4 = 6$. Why the culminator about actions! $|G| = 12 = 2^2 \cdot 3$

$\boxed{\begin{array}{l}\cdot \text{ Ask about HW 4} \\ \cdot \text{ 2 Exam date changes...}\end{array}}$

$\underline{n_3}$.

Get to have some recall for now!

Subgps of size 3: 3-cycles are even. 3's gen by these.

$\boxed{\text{New Exam Dates: Oct 5, Nov. 14.}}$

$\binom{4}{3}$ $\frac{4 \cdot 3 \cdot 2}{3} = 8$ 3-cycles, each is paired w another in a cyclic subg.

$\boxed{\text{Mention Conrad's pf.}}$

$\rightsquigarrow n_3 = 4$.

explicitly: $Syl_3(A_4) = \{\{(1),(123),(132)\}, \{1,(124),(142)\}, \{1,(134),(143)\}, \{(1),(234),(243)\}\}$.

check: $n_3 \equiv 1 \bmod 3$ ✓

$n_3 \mid 4$ ✓

All conjugate; we saw ~~conjuga~~ same cycle type $\Rightarrow$ conj. in S_n

$\Rightarrow$ $\sigma = (123), (124), (134), \text{ or } (234)$

σ' is another choice,

not all conj. in A_4, but close $\exists\ \tau \in S_4$ s.t. $\tau\sigma\tau^{-1} = \sigma'$. Not Enough.

By our proof before: ~~$\sigma = (ijk)$~~ ~~$\sigma' = (l,m,n)$~~ say $\sigma' = (ijl)$ or (jil) (at least $2 =$)

~~τ~~ τ: ~~$\tau = (kl) = (l)$ if $k = l$~~

Say $\sigma = (123)$

$(123)(4)$, $(124)(3)$, $\tau = (34)$ odd ✗

$(123)(4)$, $(134)(2)$, (234) even ✓

$(123)(4)$, $(234)(1)$, (1234) odd ✗

Conjugator

~~$\tau = (123)(34)$~~ Do instead: $(123)(4)$, $(124)(3)$, $(143)(123)(134)$ even! $= (142)$.

$(123)(4)$, $(142)(3)$, $\tau = (243)$ even.

$(123)(4)$, $(243)(1)$, $\tau = (124)$ even

So σ can be conjugated in A_4 to get a generator of any of the other gps. Now $(\tau\sigma\tau^{-1})^2 = \tau\sigma^2\tau^{-1}$ So we see directly all Sylow 3-subgps are conj.

Now ~~try~~ take $P = \{(1), (123), (132)\}$.

$N_{A_4}(P) = P$

as $P \leq N_{A_4}(P)$, if ~~$\sigma \notin P$~~ $\sigma \in A_4 \setminus P$, ~~take or~~ σ or $(i4)$

then σ has a decomposition $\sigma = (i4) \cdot \sigma'$,

σ' no 4s.

(count through them)

<u>But</u> $(i4)(123)(i4)$ $\boxed{\text{forgot } \sigma' \text{ no 4s}}$

$4 \to i \to \neq i,4 \xrightarrow{\text{fixed}} \neq i,4$

So 4 is <u>not</u> fixed $\rightsquigarrow$ conj. goes outside P.

$\therefore [A_4 : N_{A_4}(P)] = 12/3 = 4 = n_3$ ✓

~~n_2~~ $= Syl_2 = \{$subgps of size 4$\}$.

Can't have a 3-cycle. Can't have 4 cycles not even

has to be the unique one of order 4

gen. by ~~(12)(34)~~ (products of disjoint transp. $\cup \{1\}$).

$\{1, (12)(34), (13)(24), (14)(23)\}$.

$\Rightarrow n_2 = 1$.

$n_2 \equiv 1 \ (2)$ ✓

$n_2 | 3$ ✓

all conjugate? ~~yes!~~ $\boxed{\text{Tip: use Sylow here instead of checking it!}}$

Sylow II $\Rightarrow$ all conjugate $\Rightarrow gPg^{-1} = P \ \forall g \in G$

$\Rightarrow P \trianglelefteq A_4$

common trick!

$\Rightarrow [A_4 : N(P)] = [A_4 : A_4] = 1 = n_2$ ✓

(really just checking consistent

$\Rightarrow$ Sylow II