TRANSITIVE & CONJUGATION

Consider $V_4 < A_4$ Consider

$\alpha : V_4 \times A_4 \to A_4 : (\sigma, \tau) \mapsto \sigma\tau\sigma^{-1}$

Recall: $(12)(34)(ijk)(34)(12) = (\quad)$

2& then $= (1)(2j$

then $(12)(34)(1jk)(34)(12) = (1)(2kj)$

So α sends $\{(ijk)\} \subseteq A_4$ to itself

i.e. $\mathrm{Orb}((123)) \subseteq \{(ijk)\}$

$\mathrm{Orb}((123)) \neq A_4$

There must be multiple orbits.

Def^n $\alpha : G \times X \to X$ is called <u>transitive</u> if $\mathrm{Orb}(x) = X$.

Def^n $\alpha : G \times X \to X : (g, x) \mapsto gxg^{-1}$ is called <u>action by conjugation</u>

We will apply this action to subgps:

Def^n Two subgps of G, H & K are called <u>conjugate</u> if $\exists g \in G$ s.t. $gH = Kg$ $(gHg^{-1} = K)$

Conjugacy is an equivalence relation:
equivalence classes are called <u>conjugacy classes</u>

$\boxed{\text{Eg}}$ $\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \, a,b,c,d \in \mathbb{Z}, \det = \pm 1 \right\}$

Complex Roots: $\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$

Rational Roots: $\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$ $m \geq 0$,

$\begin{pmatrix} -1 & -m \\ 0 & -1 \end{pmatrix}$ $m \geq 0$, $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, & $\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$

Irrational Roots: Infinitely many!
Related to approximation of quadratic irrationals

In particular: $R = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ $L = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$

each $\pm R^{\alpha_1} L^{\alpha_2} R^{\alpha_3} L^{\alpha_4} \cdots R^{\alpha_{2n-1}} L^{\alpha_{2n}}$
will have a distinct class for distinct sequences (α_i).

Notation: If H and K are conjugate in G, i.e. $\exists g$ s.t. $gHg^{-1} = K$ we write $H^g = K$ &

$H = K^{g^{-1}}$

$\boxed{\text{HW}}$ Let $H, K < G$ & $H^g = K$.
Prove $H \cong K$

Recall ~~that~~ $N \triangleleft K$ iff $gNg^{-1} = N$ $\forall g \in G$.
i.e. $N^g = N$ $\forall g \in G$

Remark: On cycle structure:

Theorem: Let σ & $\tau \in S_n$, some $n > 2$.
Then σ & $\tau\sigma\tau^{-1}$ have the same cycle structure.

Proof: $\forall 1 \leq i \leq n$, consider $\sigma(i) = j$, some $1 \leq j \leq n$
Then $(\tau\sigma\tau^{-1})(\tau(i)) = \tau\sigma(i) = \tau(j)$

So $\sigma : i \mapsto j$
$\tau\sigma\tau^{-1} : \tau(i) \mapsto \tau(j)$ $\square$

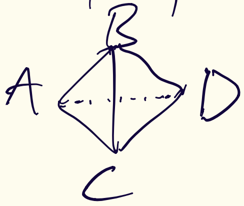
Corollary: $V_4 \triangleleft A_4$

Proof: All elts of V_4 (excl. e) are $(ij)(kl)$, so $gvg^{-1} \in V_4$ $\forall g \in A_4$ & $v \in V_4$ So $V_4 \triangleleft A_4$ $\square$

SYLOW'S THEOREMS

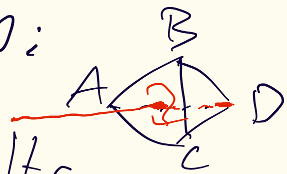
We are going to talk about subgp structure some more.
We have discussed $V_4 \triangleleft A_4 \triangleleft S_4$ — some examples
We have Lagrange's theorem — gives necessary conditions for a subgp to exist in finite gps.
If $H < G$ then $|G| = |H| \cdot k$, $k \in \mathbb{N}$
But this says nothing about existence.

$\boxed{\text{Eg}}$ Consider A_4, orientation preserving rotations of



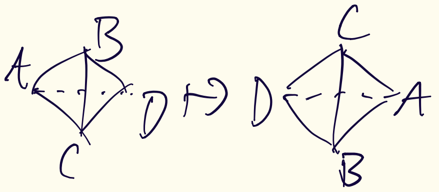
(12 elts).

Rotations of each face form a subgp:



$\langle (ABC) \rangle = \{e, (ABC), (ACB)\}$ - 3 elts

Rotations by π of an edge eg.



$\langle (AD)(BC) \rangle = \{e, (AD)(BC)\}$ - 2 elts
All such rotations together form a subgp.

$V_4 = \{e, (AD)(BC), (AC)(BD), (AB)(CD)\}$ - 4 elts

And that's it! No subgps of order 6.

Is there a simple statement that determines existence of subgps? Unfortunately not, but there is a theory guaranteeing the existence of <u>some</u> subgps.

Def Let p be prime and let G be a group s.t. every $g \in G$ has order a power of p. We call G a <u>p-group</u>.

[Here we skip all discussion of Normalisers, centralisers, class eqn]

Theorem (Sylow's First Theorem)
Let G be a finite group and let α be the largest power of the prime p in the order of G, i.e. $|G| = p^\alpha s$, $(p,s)=1$. Then for each $0 \leq \beta \leq \alpha$, $\exists$ a subgp of G of order p^β.

Def Such subgps of max. order p^α are called <u>Sylow p-subgps of G</u>.

Remark: Recall $\mathrm{ord}(g) \,|\, |G|$ $\forall g \in G$
So $|G| = p^\beta$ means $\mathrm{ord}(g)$ is a prime power.

$\boxed{HW}$ Prove or find a counterexample to:

$|G| = p^\alpha$ if and only if every elt of G has prime power.

<u>Theorem</u> (Sylow's Second & Third Theorems)

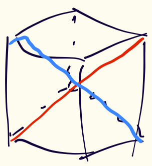
Let $|G| = p^\alpha s$, $(p,s)=1$, p prime. Let P be a Sylow p-subgp, i.e. $|P| = p^\alpha$. Then <u>every</u> Sylow p-subgps of G is conjugate to P. Moreover, if the number of conjugates is n_p then $n_p | s$ & $n_p \equiv 1 \pmod p$.

Remark. Conjugation shuffles all Sylow p-subgps around, i.e. Sylow p-subgps form an orbit of the action of conjugation on subgps.

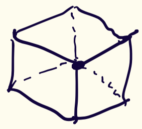
<u>Corollary</u>: Let $|G| = p^\alpha s$, $(p,s)=1$, & # of congruent p-Sylow subgps is 1. Then the p-Sylow subgp. is normal.

<u>Proof</u>: Conjugation permutes subgps. Let N be the p-Sylow subgp. Since there is only one conjugate, $gNg^{-1} = N$ $\forall g \in G$ i.e. $N \trianglelefteq G$.

Eg Cube rotational symmetries, S_4, $|S_4| = 4\cdot3\cdot2 = 3\cdot2^3$



Diagonal axis



3 rotations about this axis $\cong \mathbb{Z}_3$ (3-Sylow subgp)

# of 3-Sylow subgps is $n_3 \equiv 1 \bmod 3$ & $n_3 \mid 8$

$n_3 \in \{\underset{1 \bmod 3}{1}, \underset{2 \bmod 3}{\cancel{2}}, \underset{1 \bmod 3}{4}, \underset{2 \bmod 3}{\cancel{8}}\}$

4 pairs of diagonals gives 4 subgps of order 3.

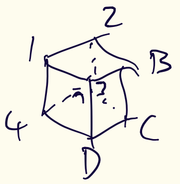
$n_p = 4$.

To check: distinct diagonals correspond to distinct subgps of S_4.

Let $H, K \leq S_4$ be 3-Sylow subgps of distinct diagonals

From Sylow's theorem, $gHg^{-1} = K$, some $g \in G$

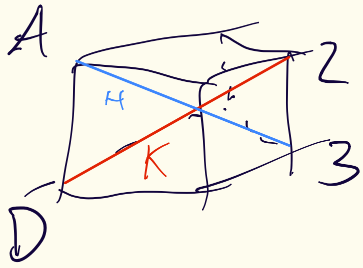
Consider a single $120°$ rotation ccw $R \in H$



It is clear no non-trivial rot. through another diag axis will fix A or 3. So gps are distinct.

So $n_3 = 4$.

For conjugacy: Let g take the diag. of H to K. Then $gHg^{-1} = K$

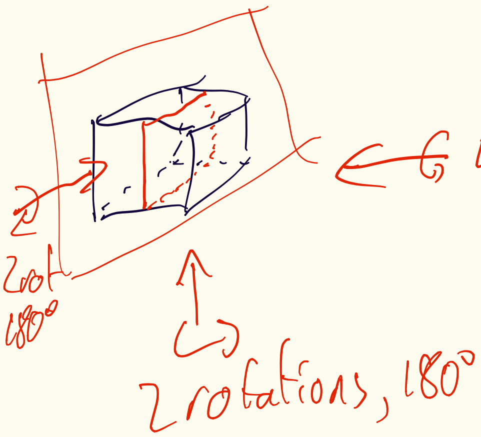


g^{-1} takes D2 to A3, H is some rotation about A3, g takes A3 to D2. So D2 is fixed, so $gHg^{-1} \subseteq K$.

Reversing the argument: $g^{-1}Kg \subseteq H$

Hence $gHg^{-1} = K$.

Now for 2-Sylow Subgps, i.e. $|H| = 8$



$\leftarrow$ 4 rotations ($R = 90°, R^2, R^3, R^4$)

So 8 rotation subgp fixing this plane. 3 planes, $n_2 = 3 \equiv 1 \bmod 2$