Groups

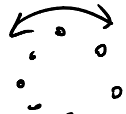
Monday, August 7, 2023

Subgroups $H \leq G$

$$[G:H] = \#\text{ of cosets } gH = \frac{|G|}{|H|}$$

Examples:

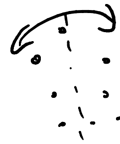
Cyclic, $\mathbb{Z}/n\mathbb{Z}$



rotations of n points

$|C_n| = n$

Dihedral



$\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$

rotations, reflections of n points

$|D_n| = 2n$

Symmetric

permutations of n points

$|S_n| = n!$

Alternating

$S_n \to \{\pm 1\}$

even/odd permutation

Even permutations form A_n

$|A_n| = \frac{n!}{2}$

Matrix

Ex. $SL(3,5)$ means 3×3 matrices, entries mod 5, determinant 1

Quaternion Group

$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$

$i^2 = j^2 = k^2 = -1$

$ij = k$

Cyclic group of order n

$\mathbb{Z}/n\mathbb{Z}$

$\#$ of generators $= \varphi(n) = \#$ of $1 \leq k \leq n$ coprime to n

Ex: $\mathbb{Z}/10\mathbb{Z}$ generated by 1 or 3, 7, 9

$\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$

If $|G| = n$, if for each $d \mid n$, there is at most one subgroup of order d, then G is cyclic.

At most one cyclic subgroup of order d

Cyclic subgroup of order d $\longrightarrow$ $\varphi(d)$ elements of order d

An element of order d $\longrightarrow$ Cyclic subgroup of order d

So $\leq \varphi(d)$ elements of order d.

order d

So $\leq \varphi(d)$ elements of order d.

So $\leq \sum'_{d|n} \varphi(d)$ elements total.

So $n = |G| \leq \sum'_{d|n} \varphi(d) = n$ — Think about C_n. It has exactly $\varphi(d)$ elements of order d.

So G must have exactly $\varphi(d)$ element of each order $d|n$.

So G has an element of order n

So G is cyclic.

Alternate: Sylow $\Rightarrow G = P_1 \times \cdots \times P_k$
so reduce to case where $|G| = p^k$,
at most subgroup of order p^{k-1},
and any element outside will generate G.

Orbit-Stabilizer

G acting on a set X $\left\{ \begin{array}{l} g \cdot x \in X \\ 1 \cdot x = x \\ (gh) \cdot x = g \cdot (h \cdot x) \end{array} \right.$

- $\mathrm{Orb}(x) = \{g \cdot x : g \in G\}$ ← these orbits partition X.
- $\mathrm{Stab}(x) = \{g \in G : g \cdot x = x\}$

$|\mathrm{Orb}(x)| = [G : \mathrm{Stab}(x)] = \dfrac{|G|}{|\mathrm{Stab}(x)|}$

$(g\,\mathrm{Stab}(x) \longleftrightarrow g \cdot x)$

G acts on itself by conjugation $g \cdot h := ghg^{-1}$

$\mathrm{Orb}(g) = \{hgh^{-1} : h \in G\} = $ conjugacy class of g

$\mathrm{Stab}(g) = \{h \in G : hgh^{-1} = g\} = \{h \in G : hg = gh\} = C_G(g)$

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

Class equation: $|G| = \sum' |\text{conj classes}| = \sum' \dfrac{|G|}{|C_G(g)|}$

Class equation: $|G| = \sum' |\text{conj classes}| = \sum' \frac{|G|}{|C_G(g)|}$

$Z(G) = \{g \in G : \forall h,\ gh = hg\}$ $= |Z(G)| + \sum_{\text{rest}}' \frac{|G|}{|C_G(g)|}$

$= \{g : C_G(g) = G\}$

$= \{g : |\text{conj class}| = 1\}$

If G finite group,

$X = \{gh = hg\} \subseteq G \times G$

then $|X| = c|G|$, where $c = \#\text{conj classes}$

$$|X| = \sum_{g \in G}' |\{h \in G : gh = hg\}| = \sum_{g \in G}' |C_G(g)|$$

$$= \sum_{g \in G} \frac{|G|}{|\text{conj class}(g)|}$$

$$= |G| \sum_{g \in G} \frac{1}{|\text{conj class}(g)|}$$

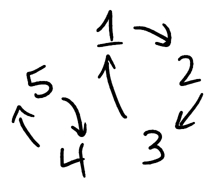
$$= |G| \cdot c.$$

If a conj class has size k, it will contribute $\frac{1}{k}$ k times, so 1 total.

Compute $|X|$ for $G = S_5$ (permutations of 5 letters)

How many conjugacy classes does S_5 have?

cycle decomposition



has cycle type $2+3$

Theorem: Two permutations in S_n are conjugate $\iff$ they have the same cycle type.

sometimes called partitions of 5

$1+1+1+1+1$
$1+1+1+2$
$1+2+2$
$1+1+3$
$2+3$
$1+4$

7 total, $c = 7$, $|X| = 7|G| = 7 \cdot 120 = 840.$

partitions of 5 $\begin{pmatrix} \vdots \\ 2+3 \\ 1+4 \\ 5 \end{pmatrix}$ $= 840.$

Sylow's Theorems

- If $p \mid |G|$, write $|G| = p^k m$, $p \nmid m$,

  a Sylow p-subgroup of G is a subgroup of size p^k.

- Sylow I: Sylow p-subgroups exist
- Sylow II: All Sylow p-subgroups are conjugate (gPg^{-1})
- Sylow III: # of Sylow p-subgroups is $\equiv 1 \pmod p$ and divides $|G|$ (actually divides m).

Exactly Sylow p-subgroup

$\Leftrightarrow$ It is normal

$$N_G(P) = \{ g \in G : gPg^{-1} = P \} = \mathrm{Stab}_G(P)$$

Orbit-Stabilizer says $\underbrace{\#\text{ Sylow subgroups}}_{n_p} = [G : N_G(P)]$

Ex: Show a group of order 30 has a cyclic subgroup of order 15

(Such a subgroup has index 2, which is necessarily normal, so $G \cong C_{15} \rtimes C_2$)

(Every group of order 15 is cyclic

If $|G| = 15$, then G has subgroups $|P_3| = 3$, $|P_5| = 5$ by Sylow's theorems. $n_3 \equiv 1 \pmod 3$, and $n_3 \mid 5$.

$n_5 \equiv 1 \pmod 5$, and $n_5 \mid 3$

so $n_3 = 1$ and $n_5 = 1$

so P_3, P_5 both normal.

Recognition theorem for direct products

(if H, K normal, $H \cap K = 1$, $HK = G$, then $G \cong H \times K$)

so $G \cong P_3 \times P_5 \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \underset{\text{CRT}}{\cong} \mathbb{Z}/15\mathbb{Z}$)

so $G \cong P_3 \times P_5 \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \underset{\text{CRT}}{\cong} \mathbb{Z}/15\mathbb{Z}$)

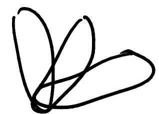
$|G| = 30$

$n_2 \equiv 1 \pmod 2$, $n_2 \mid 15$, $n_2 = 1, 3, 5, 15$

$n_3 \equiv 1 \pmod 3$, $n_3 \mid 10$, $n_3 = 1, 10$

$n_5 \equiv 1 \pmod 5$, $n_5 \mid 6$, $n_5 = 1, 6$

Cannot have both $n_3 = 10$ and $n_5 = 6$



20 elements of order 3 + 24 elements of order 5) = too many elements

So $n_3 = 1$ or $n_5 = 1$

So $\underbrace{P_3 \text{ is normal}}$, or $\underbrace{P_5 \text{ is normal.}}$

$|G/P_3| = 10$

G/P_3 has a subgroup of order 5, H/P_3 where $|H| = 15$.

(or argue that preimage has size 15)

$|G/P_5| = 6$

G/P_5 has a subgroup of order 3, preimage has size 15.

If G acts on X, then you get a homomorphism $G \to \mathrm{Perm}(X)$

If $H \leq G$ has index n, then G has a normal subgroup $N \leq H$ of index $\leq n!$

$[G:N] \leq n!$.

Let G act by left multiplication on cosets gH.

This gives a homomorphism $G \to S_n$.

It kernel N has $|N| = |\ker| = \dfrac{|G|}{|\text{image}|} \geq \dfrac{|G|}{n!}$

$$[G:N] = \frac{|G|}{|N|} \leq n!$$

$$[G:N] = \frac{\quad}{|N|} \leq n!$$

If $g \in N$, then $g(g'H) = g'H$ for all $g'H$

so $gH = H$

so $g \in H$.

(N is actually $\bigcap_g gHg^{-1}$)