Feb25

Thursday, February 25, 2021 1:00 PM

Theorem (Cayley's Theorem)

· Every finite group is isomorphic to a subgroup of S_n

Rmk Can take $n = |G|$

Observe

It suffices to produce an injective homomorphism $\phi: G \longrightarrow S_n$.

$$G \simeq \operatorname{im}\phi \leq S_n$$

Recall:

Homomorphisms to S_n closely related to group actions.

Main Tool: Group Actions.

Setup: G a group. A a set.

$$\left\{\begin{array}{l}\text{Actions of}\\ G \text{ on } A\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{Homomorphisms}\\ \phi: G\longrightarrow S_A\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{Homoms}\\ G\longrightarrow S_n\end{array}\right\}$$

$$G \circlearrowright A \longmapsto \left(\begin{array}{l}\phi(g): A \longrightarrow A\\ \qquad a\longmapsto g\cdot a\end{array}\right)$$

$$g\cdot a=\phi(g)(a) \longleftarrow\!\shortmid\ \phi$$

If $|A| = n$. Then $A \longleftrightarrow \{1, \dots, n\}$

Hw 3 #7 $\Longrightarrow S_A \simeq S_n$

Want $G \longrightarrow S_n$. Need action G on a set of size n.

inj

faithful

How do we detect injectivity?

An action is faithful if only elt of G acting trivially is 1

$\underset{\text{HW3 \#4(b)}}{\Longleftrightarrow}$ $\phi : G \longrightarrow S_A$ injective.

So... to prove Cayley's theorem we most produces a faithful action of G on a finite set.

TOOL: G act on itself by left multiplication!

$$G \circlearrowleft G \qquad g \cdot a = ga.$$

Unwind this very explicitly $|G| = n$.

$$G = \{g_1, g_2, \dots, g_n\} \longleftrightarrow \Omega_n = \{1, 2, \dots, n\}$$

$$g_i \longleftrightarrow i$$

$$g\cdot g_i = g_j \underset{\leftsquigarrow}{\longleftrightarrow} \underline{g\cdot i = j}$$

$$\begin{array}{l} \phi : G \longrightarrow S_G \\ \quad g \longmapsto (g_i \mapsto g g_i) \end{array} \longleftrightarrow \begin{array}{l} \underset{=}{\psi} : G \longrightarrow S_n \\ \quad\quad g \longmapsto \sigma_g \end{array}$$

Proof of Cayley's Theorem

Goal show ψ is injective.

$g \in \ker \psi$. Then $\sigma_g(i) = i$

$$\Updownarrow$$

$$g g_i = g_i \Longleftrightarrow g\cdot i = i$$

$\rightsquigarrow g = 1$ $\quad\varnothing$

Rmk ① $G \circlearrowright G$ left mult is faithful.

② Labelling on G is arbitrary & affects ψ. "Better" to observe

$G \hookrightarrow S_G$ (canonical... doesn't involve arbitrary choices)

Example (Klein 4-group)

$V_4 = \{1, a, b, c\}$ s.t. $a^2 = b^2 = c^2 = 1$

$ab = ba = c$

Choose a labelling

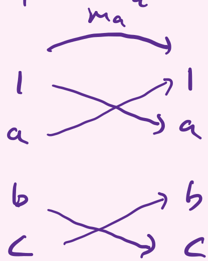
$1 \longleftrightarrow 1$
$a \longleftrightarrow 2$
$b \longleftrightarrow 3$
$c \longleftrightarrow 4$

(isomorphic to
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

$(1,0) \leftrightarrow a$
$(0,1) \leftrightarrow b$
$(1,1) \leftrightarrow c$)

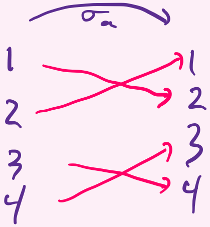
Compute $\sigma_a \in S_4$

1) Compute m_a = mult by a on V_4



1) $a \cdot 1 = a$ $\quad \sigma_a(1) = 2$
2) $a \cdot a = 1$ $\quad \sigma_a(2) = 1$
3) $a \cdot b = c$ $\quad \sigma_a(3) = 4$
4) $a \cdot c = a \cdot ab$ $\quad \sigma_a(4) = 3$
$= a^2 b$
$= b$

2) Apply Labelling



$\rightsquigarrow \sigma_a = (1\,2)(3\,4) \in S_4$

Exercise

$\sigma_b \doteq (1\,3)(2\,4)$
$\sigma_c = (1\,4)(2\,3)$
$\sigma_1 = (1)$

So $\phi : V_4 \longrightarrow S_4$ inj

& $V_4 \simeq \operatorname{im}\phi = \{(1), (12)(34), (13)(24), (14)(23)\}$

$\le S_4$

Observation

The action of G on G by left mult has only 1 orbit.

$$g \xrightarrow[\times hg^{-1}]{} h$$

Def$^{\underline{n}}$ An action $G \circlearrowright A$ is *transitive* if $\forall\, a, b \in A$, $\exists\, g \in G$ w/ $g \cdot a = b$ (only one orbit).

Slight Generalization of Cayley's Theorem

Let $H \le G$. Let $A = G/H$. Then G acts on G/H by left multiplication

$$g \cdot (xH) = gxH$$

Exercise: This is an action.

Observe

1) $H = \{1\}$ recover $G \circlearrowright G$ by left mult.

2) If $|G:H| = n < \infty$, then

$$A = \{x_1 H, x_2 H, \dots, x_n H\}$$

Get $G \longrightarrow S_A \simeq S_n$

$$g \cdot x_i H = x_j H \leftrightsquigarrow g \cdot i = j$$

Ex $G = D_8$ $H = \{1, s\}$

$$A = \{H, rH, r^2H, r^3H\} \longleftrightarrow \{1, 2, 3, 4\}$$

$$r \cdot r^i H = r^{i+1} H \longleftrightarrow (1\ 2\ 3\ 4)$$

$$= \sigma_r$$

What about σ_s?

$$\left.\begin{array}{lll} 1)\ s \cdot H = H & \longleftrightarrow & \sigma_s(1) = 1 \\ 2)\ s \cdot rH = r^3H & \longleftrightarrow & \sigma_s(2) = 4 \\ 3)\ s \cdot r^2H = r^2H & \longleftrightarrow & \sigma_s(3) = 3 \\ 4)\ s \cdot r^3H = rH & \longleftrightarrow & \sigma_s(4) = 2 \end{array}\right| \quad \sigma_s = (2\,4).$$

Fully defines $\phi : D_8 \longrightarrow S_4$

e.g. $\phi(r^2 s) = \phi(r)\phi(r)\phi(s)$

$= (1\,2\,3\,4)(1\,2\,3\,4)(2\,4) = \cdots$

$$\operatorname{im}\phi = \langle (1\ 2\ 3\ 4), (2\ 4) \rangle \leq S_4.$$

Theorem (Generalized Cayley's Theorem)

$H \leq G$. $A = G/H$. $G \circlearrowright A$ by left multiplication.

1) G acts transitively on A. (one orbit)

2) $G_H = H$

↑ Stabilizer of H.

3) Let $\pi_H : G \longrightarrow S_A$ be perm rep.

Then

$$\ker \pi_H = \bigcap_{x \in G} xHx^{-1} \quad \checkmark$$

Furthermore, this is the largest normal subgroup of G contained in H.

(in part, H normal $\iff \ker \pi_H = H$)

Proof

① $xH, yH \in A$. $g = yx^{-1}$

Then $g \cdot xH = yx^{-1}xH = yH$ ✓

②

$$G_H = \{ g \in G \mid g \cdot H = H \} \overset{\text{HW 4 8a}}{=} H$$

③ $\ker \pi_H = \{ g \in G \mid g\, xH = xH \quad \forall x \}$

$$= \{ g \in G \mid x^{-1} g x H = H \quad \forall x \}$$

$$= \{ g \in G \mid x^{-1} g x \in H \quad \forall x \}$$

$$= \{ g \in G \mid g \in x H x^{-1} \quad \forall x \}$$

$$= \bigcap_{x \in G} x H x^{-1}$$

✓

Show largest normal sub contained in H

✓ a kernel

$\ker \pi_H \le 1 H 1^{-1} = H$ ✓

Let $N \le H$ normal in G.

For $\forall x$ $\quad \underset{\underset{N}{\|}}{xNx^{-1}} \le xHx^{-1}$

So $N \le \bigcap xHx^{-1} = \ker \pi_H$

Observe This generalizes Cayley.

Let $H = \{1\}$. So $A = G/\{1\} = G$.

Get $\pi_1 : G \longrightarrow S_G$

& $\ker \pi_1 = \bigcap x\{1\}x^{-1} = \{1\}$

$x \in G$

So π_1 is injective.

Consequence:

Theorem:

Let $|G| = n$. Let p prime, smallest prime factor of n.

If $H \leq G$ & $|G:H| = p$, then $H \trianglelefteq G$.

Rmk

① n even, $p = 2$. We already know subgps of index 2 are normal.

② ERROR in Feb 16 Lecture. (Thanks Felix)

$g \notin H$, 2 cosets H, gH. (first pt of (#)).

$gHg^{-1} \in \{H \text{ or } gH\}$ False

What's true, If $gHg^{-1} \neq H$ then

$\exists\ \underline{gh} \in H \cap gH$

$\uparrow$ only needed this.

Rest of proof ok.

Proof Let $H \leq G$ of index p.

$$A = G/H = \{x_1H, x_2H, \dots, x_pH\}$$

Action $G \circlearrowright A$ by left mult gives

$$\pi_H : G \longrightarrow S_p$$

Let $K = \mathrm{Ker}(\pi_H) \leq H$.

Goal show $K = H$.

Let $k = |H:K|$. Show $k = 1$.

Know $|G:K| = |G:H| \cdot |H:K| = p \cdot k$

↑ $K, H \trianglelefteq G$ 3rd iso thm.

General case exercise.

$$\begin{tikzcd}
G \arrow[rr, "\pi_H"] \arrow[d] & & S_p \\
G/K \arrow[urr] & &
\end{tikzcd}$$

↑ injective by F.I.T.

$LG \implies |G/K| \mid |S_p|$

$$pk \mid p! = p(p-1)(p-2)\cdots$$

$$k \mid (p-1)!$$

⇝ All prime factors of $k < p$.

All prime factors of k are prime

factors of G, hence $\geq p$.

So $k = 1$

$$\Longrightarrow |H:K| = 1$$

$$\Longrightarrow H = K = \ker \pi_H \trianglelefteq G \quad \varnothing$$

Summary of left mult actions

Upshot: Cayley's Thm & nice structural results in full generality.

Got faithful & transitive

↑ No interesting kernel.

↑ No interesting partition by the orbits.

(e.g. $A_n = \ker(S_n \circlearrowright \{\pm\Delta\})$)

Next Introduce a more interesting & complex action.

Groups Acting on Themselves by Conjugation

Def$^{\underline{n}}$

The action of G on G by conjugation is

$$g * a = gag^{-1}$$

Lemma This is an action.

Proof

1) $1 * a = 1 a 1^{-1} = a$

2) $g, h \in G$

$$(gh) * a = gha(gh)^{-1}$$
$$= ghah^{-1}g^{-1}$$
$$= g * (\underline{hah^{-1}})$$
$$= g * (h * a)$$

Def^n

$a, b \in G$ are called conjugate if $\exists\, g \in G$ s.t.

$b = g * a = gag^{-1}$ (i.e, a, b same orbit)

The orbits of this action are called conjugacy classes.

Examples

① Never interesting for abelian groups

G abelian

$$g * a = gag^{-1} = gg^{-1}a = a$$

Trivial action.

② Action is never transitive unless $G = \{1\}$

$G * 1 = \{x 1 x^{-1} \mid x \in G\} = \{1\}$

Might get more interesting partitions.

③ $S_3 \circlearrowright S_3$ by conj.

$\{(1)\}$ by ② ← 1 cycle (1)

$S_3 * (1\,2) = \{(1\,2), (1\,3), (2\,3)\}$ ← 2 cycles (3)

$$\left.\begin{aligned}
(1\,3)(1\,2)(1\,3)^{-1} &= (2\,3)\\
(2\,3)(1\,2)(2\,3) &= (1\,3)\\
(1\,2\,3)(1\,2)(1\,3\,2) &= (2\,3)\\
(1\,3\,2)(1\,2)(1\,2\,3) &= (1\,3)
\end{aligned}\right\}\text{ Check.}$$

$S_3 * (1\,2\,3) = \{(1\,2\,3), (1\,3\,2)\}$.

↑ 3 cycles (2)

Line up by shape....

All different sizes

One can generalize this slightly

Def^n

Let $S \subseteq G$ be any subset. $g \in G$.

$gSg^{-1} = \{gxg^{-1} \mid x \in S\} \subseteq G$ called a conjugate of S. This defines an action.

Defn The power set of G is

$$\mathcal{P}(G) = \{\text{subsets } S \subseteq G\} \quad (= 2^G)$$

Then $G \circlearrowright \mathcal{P}(G)$

$g * S = gSg^{-1}$!

Check this an action.

Prop Let $G \circlearrowright \mathcal{P}(G)$ by conjugation

① $S \subseteq G$.

G_S = stabilizer of S = $N_G(S)$

② For $a \in A$

$$G_{\{a\}} = C_G(\{a\}) = C_G(a)$$

Proof

① $G_S = \{g \in G \mid gSg^{-1} = S\} = N_G(S)$

② $C_G(a) = \{g \in G \mid ga = ag\}$

$= \{g \in G \mid gag^{-1} = a\}$

$= N_G(\{a\})$

$\overset{①}{=} G_{\{a\}}$.

Recall from last time

Theorem (Orbit Stabilizer Theorem)

Let $G \curvearrowright A$. Then for $a \in A$

$$|G \cdot a| = |G : G_a|$$

Corollary

① $\#\{\text{conjugates of } S \subseteq G\} = |G : N_G(S)|$

② $\#\{\text{conjugates of } a \in G\} = |G : C_G(a)|$

Proof

① $\#\{\text{conjugates of } S\} = |G * S|$

$$= |G : G_S|$$

$$= |G : N_G(S)|.$$

② identical

This will give us rich numerical data!

Recall

$G \curvearrowright A$. The orbits $\mathcal{O}_1, \dots, \mathcal{O}_r$ partition A TH 1

So $|A| = |O_1| + |O_2| + \cdots + |O_r|$

$\rightsquigarrow$ $G @ G$ by conjugation partitions G into conjugacy classes, whose size we know by corollary.

Lemma $a \in G$. $a \in Z(G) \iff$ its conjugacy class is $\{a\}$.

Pf/ $a \in Z(a) \iff \underset{\forall g}{ga = ag} \iff \underset{\forall g}{gag^{-1} = a} \iff G * a = \{a\}$

$\emptyset$

Theorem (The Class Equation)

Let G be a finite. Let $g_1, \dots, g_r \in G$ be representatives of the distinct conjugacy classes of G not in $Z(G)$.

$$\left(G @ G \quad \underbrace{O_1, O_2, \dots, O_s}_{\text{singletons}}, \underset{\substack{\ni \\ g_1}}{O_{s+1}}, \underset{\substack{\ni \\ g_2}}{O_{s+2}}, \dots, \underset{\substack{\ni \\ g_r}}{O_{s+r}} \leftarrow \right)$$

Then
$$\boxed{|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|}$$

Proof

Conjugacy Classes

$$\{z_1\}, \{z_2\}, \ldots, \{z_s\} \qquad \forall\ z_i \in Z(G)$$

$$\{G * g_1\}, \ldots, \{G * g_r\}$$

$$\rightsquigarrow |G| = |O_1| + |O_2| + \cdots + |O_{s+r}|$$

$$= \underbrace{|\{z_1\}| + \cdots + |\{z_s\}|}_{} + \underbrace{|G * g_1| + \cdots + |G * g_s|}_{}$$

$$= |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|$$