Feb23

Tuesday, February 23, 2021 2:57 PM

Philosophy to establish isomorphisms

1) Build surjection $\phi : G \longrightarrow H$ (homomorphism)
2) Identify $K = \ker \phi$
3) Know (F.I.T) $G/K \simeq H$.

Exercise $M, N \trianglelefteq G$. Suppose $MN = G$

① $\dfrac{G}{M \cap N} \simeq \dfrac{G}{M} \times \dfrac{G}{N}$ (First iso thm)

② $M \cap N = \{1\}$ then

$G \simeq N \times M$ (① + 2nd iso thm)

Technique: Passing to the quotient.

Suppose $N \trianglelefteq G$ & $\phi : G \longrightarrow H$

$$\begin{tikzcd} G \arrow[r, "\phi"] \arrow[d, "\pi"] & H \\ G/N \arrow[ur, dashed, "\bar{\phi}"] & \end{tikzcd}$$

← when does this exist?

$\bar{\phi} \circ \pi = \phi$

Notation

If $\overline{\Phi}$ exists, we say ϕ "passes to the quotient"

Prop ϕ passes to G/N

$$\iff N \leq \ker\phi$$

Proof

$* \quad \overline{\Phi}(\underset{\uparrow}{gN}) = \overline{\phi}\circ\pi(g) = \underset{\uparrow}{\phi(g)}$ if $\overline{\Phi}$ exists

$\overline{\Phi}$ exists $\iff \forall\, gN = g'N,\ \phi(g)=\phi(g')$

$\iff \forall\, gN = g'N \quad \underline{gg'^{-1}} \in \ker\phi$

$\iff N \leq \ker\phi$

$$\boxed{gg'^{-1}N = N}$$

Consequence

Suppose $N, K \trianglelefteq G$ & $N \leq K$

$$\begin{tikzcd}
G \arrow[r, two heads, "\pi"] \arrow[d, "\tau"] & G/K \\
G/N \arrow[ur, "\overline{\pi}"'] &
\end{tikzcd}$$

exists, surjective.

Example

$10\mathbb{Z} \leq 5\mathbb{Z} \leq \mathbb{Z}$

$$\begin{tikzcd}
\mathbb{Z} \arrow[r] \arrow[d] & \mathbb{Z}/5\mathbb{Z} \\
\mathbb{Z}/10\mathbb{Z} \arrow[ur] & \bar{2} \\
\bar{2}, \bar{7} \arrow[ur, <->] &
\end{tikzcd}$$

The 4th isomorphism theorem

$N \trianglelefteq G$

$$\left\{ \begin{matrix} H \text{ s.t} \\ N \leq H \leq G \end{matrix} \right\} \xleftrightarrow{\text{nice!}} \left\{ H \leq G/N \right\}$$

Philosophically

G/N knows about stuff in G "above N"

N knows about stuff in G "below N"

Idea

Know stuff about N & G/N, deduce stuff about G.

If $|G| < \infty$, & $N \neq 1, G$. Then

$|N|$ & $|G/N|$ smaller than $|G|$

⇝ INDUCTION!!!! (on order of group)

Put into action

Theorem (Cauchy's Theorem Abelian Case)

G be a finite abelian group. p a prime number. $p \mid |G|$.
Then $\exists\, x \in G$ w/ $|x| = p$.

Proof

Induction on $|G|$

Base Case $|G| = 1$. Vacuous.

Inductive Step Assume true for groups smaller than G. Fix $x \in G$ w/ $x \neq 1$.

Case 0 $|G| = p$. Then $|x| = p$ by Lagrange's thm.

(assume $|G| > p$)

Case 1 $|x| = np$. Then $|x^n| = p$ x^n works!

Case 2 $p \nmid |x|$. Let $N = \langle x \rangle \trianglelefteq G$ ← G abelian.

Lagrange $|G| = |N| \cdot |G/N|$ divisible by p.

$\rightsquigarrow p \mid |G/N|$. But $|G/N| < |G|$ so

induction $\Longrightarrow \exists\ \bar{g} = gN \in G/N$

w/ $|\bar{g}| = p$.

$\rightsquigarrow g^p \in N$ & $g \notin N$.

$\langle g^p \rangle \subsetneq \langle g \rangle \implies \gcd(p, |g|) \neq 1$

so $= p$.

$\rightsquigarrow p \mid |g| \implies$ Back in case 1

w/ $x = y$.

Remarks

① **Lagrange's Thm**

$$H \leq G \implies |H| = n \mid |G|$$

A potential converse would be

If $n \mid |G| \implies \exists\, H \leq G$ of order n.

(We proved true if G abelian & n prime)

FALSE IN GENERAL

Coming up

Sylow: True for $n = p^k$. p prime.

$(p^k \mid |G| \implies \exists\, H \leq G$ w/ $|H| = p^k)$

Remark 2

This techique sort of factors G into

$N \trianglelefteq G$ & G/N.

Group Classification & Factorization

There is a notion of primality w/ regards to the "factorization" in Rmk 2.

Def$^{\underline{n}}$

A group G is simple if it has no nontrivial proper normal subgroups.

(i.e. $H \trianglelefteq G$ then $H=G$ or $H=\{1\}$)

Example: $\mathbb{Z}_p$ p prime.

"Reduces Group Theory into 2 peices

"Factorization Step" (Jordan Hölder Program)

A way to take

$$\begin{tikzcd} & N \arrow[r, shift left] \arrow[r, shift right] & \cdots \\ G \arrow[ur] \arrow[dr] & & \\ & G/N \arrow[r, shift left] \arrow[r, shift right] & \cdots \end{tikzcd}$$

until everything is simple.

Classification of Finite Simple Groups

Come in 18 infinite families

- $\mathbb{Z}_p$ p primes
- → A_n $n \geq 5$ (Alternating groups)
- $SL_n(\mathbb{F}_q)/Z(SL_n(\mathbb{F}_q))$ (Hw 5)

  (except $n=2$ & $q=2$ or 3)

+ 26 extra "sporadic simple groups"

↑Biggest one is called the MONSTER

$\approx 10^{53}$ elements.

Prof. Borcherds @ Berkeley.

Transpositions & Alternating Groups

Recall

$\sigma \in S_n$ can be written as a product of disjoint cycles (in a unique way)

(Prove this today!!)

Also useful to think about σ as a product of swaps (or 2-cycles).

(We lose uniqueness).

↑ even in # of swaps.

Ex

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

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

... No coincidence that each case had even # of swaps.

Def^{n} A 2-cycle is often called a transposition.

Lemma

Any permutation is a product of transpositions

Proof

I suffices to show true for an m-cycle.

$$(a_1\ a_2 \cdots a_m) = (a_1\ a_m)(a_1\ a_{m-1}) \cdots (a_1\ a_3)(a_1\ a_2)$$

$\uparrow \qquad \uparrow$

n-1 2-cycles

Theorem

Let $\sigma = \tau_1 \tau_2 \cdots \tau_r$ for τ_i, π_i

$= \pi_1 \pi_2 \cdots \pi_s$ transpositions.

Then $r \equiv s \mod 2$.

Def^n If r even call σ even

" r odd " odd

Proof (use group actions).

Define $\Delta = \prod_{1 \le i < j \le n} (x_j - x_i)$

(e.g. $n=4$

$$\Delta = (x_2 - x_1)(x_3 - x_1)(x_4 - x_1)(x_3 - x_2)(x_4 - x_2)(x_4 - x_3))$$

For $\sigma \in S_n$. let

$$\sigma \cdot \Delta = \prod_{1 \le i < j \le n} (x_{\sigma(j)} - x_{\sigma(i)})$$

Observe 1) $\sigma \bullet \Delta = \pm \Delta$

(each $x_j - x_i$ appears as a factor, potentially as $x_i - x_j$)

Define $\sigma \bullet (-\Delta) = -\sigma(\Delta)$

2) $\sigma, \gamma \in S_n$

$$\gamma\sigma \bullet (\Delta) = \gamma \bullet (\sigma \bullet \Delta)$$

3) $\mathrm{id} \bullet \Delta = \Delta$

Get a group action $S_n \circlearrowright \{\Delta, -\Delta\}$

Let $\tau = (a\ b)$ a swap. $(b > a)$

what is $\tau \bullet \Delta$

$$\Delta = \Big(\prod_{\substack{i,j \neq \\ a \text{ or } b}} (x_j - x_i)\Big)\Big(\prod_{i \neq a,b} \pm (x_i - x_a)(x_i - x_b)\Big)(x_b - x_a)$$

$$\tau \bullet \Delta = \Big(\prod_{\substack{i,j \\ \neq a \text{ or } b}} (x_j - x_i)\Big)\Big(\prod_{i \neq a,b} \pm (x_i - x_b)(x_i - x_a)\Big)(x_a - x_b)$$

$$= -\Delta.$$

So...

$$\sigma \bullet \Delta = (\tau_1 \tau_2 \cdots \tau_r)\Delta = (-1)^r \Delta$$

$$= (\pi_1 \cdots \pi_s)\,\Delta = (-1)^s \Delta$$

So $(-1)^r = (-1)^s \implies r \equiv s \mod 2$

Observe

This defines a permutation representation

$$S_n \xrightarrow{\overset{\text{sgn}}{\varepsilon}} \{\pm 1\} = S_{\{\Delta, -\Delta\}}$$

$$\sigma \longmapsto \begin{cases} 1 & \text{if } \sigma(\Delta) = \Delta \quad (\sigma \text{ even}) \\ -1 & \text{if } \sigma \cdot \Delta = -\Delta \quad (\sigma \text{ odd}) \end{cases}$$

Note

$$\varepsilon((a_1 \cdots a_n)) = (-1)^{n-1}$$

⚠ A n cycle is even $\Longleftrightarrow$ n is odd | yikes!

Def$^{\underline{n}}$ The alternating group is

$$A_n := \ker(\varepsilon) \trianglelefteq S_n.$$

It is the set of even permutation.

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

Pf/ $$\frac{\overset{n!}{|S_n|}}{|A_n|} \underset{\substack{\uparrow \\ \text{L.G.}}}{\cong} |S_n/A_n| \underset{\substack{\uparrow \\ \text{FIT}}}{\cong} |\{\pm 1\}| = 2$$

---

we will show

Theorem If $n \geq 5$, A_5 is simple.

Consequence

No subgroup of A_5 whose order is $30 = |A_5|/2$. In particular, converse to Lagrange fails!

Pf/ If $H \leq A_5$ w/ $|H| = 30$

$\Rightarrow |A_5 : H| = 2$

$\Rightarrow H \trianglelefteq A_5$ but A_5 simple ↯

In fact

A_4 ordr 12. No sub ordr 6.

$$A_4 = \left\{ \begin{array}{llll} (12)(34) = \sigma_1 & \tau_i & t_i^2 & \\ (13)(24) = \sigma_2 & (123) & (132) & \\ (14)(23) = \sigma_3 & (124) & (142) & id \\ & (134) & (143) & \\ & (234) & (243) & \end{array} \right\}$$

Exercise

1) $\langle \tau_i, \tau_j \rangle = A_4$ $i \neq j$ (LG, show 7 elts)

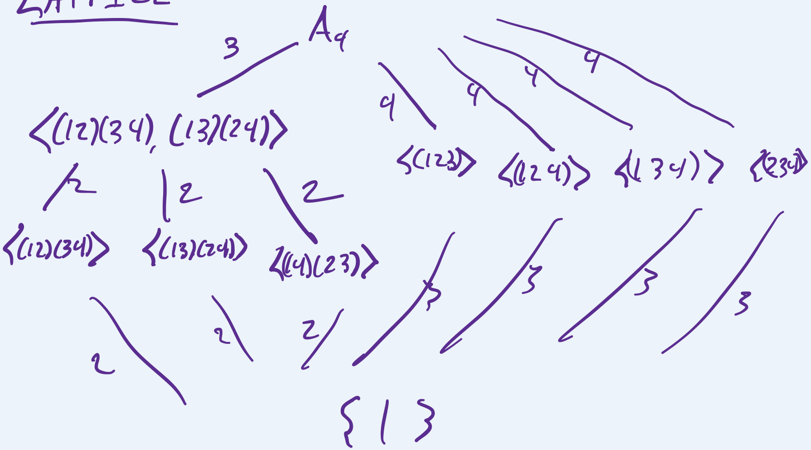
2) $\langle \tau_i, \sigma_j \rangle = A_4$

3) $|\langle \sigma_1, \sigma_2, \sigma_3 \rangle| = 4$ (V_4)

$\Longrightarrow$ To have 6, either 1 or 2

But then you have 12.

LATTICE



Group Actions

Recall G a group

A a set

An action

$$\begin{aligned} G\times A &\longrightarrow A \\ (g,a) &\longmapsto g\cdot a \end{aligned} \quad \text{s.t.}$$

1) $g\cdot(h\cdot a) = (gh)\cdot a$

2) $1\cdot a = a$

$\Updownarrow$ equivalent

Induces a permutation rep:

$$\begin{aligned} \phi : G &\longrightarrow S_A \\ g &\longmapsto \phi(g)(a) = g\cdot a \end{aligned}$$

---

1) Kernel $= \{g\in G \mid g\cdot a = a \quad \forall\, a\in A\}$

$= \ker\phi$

2) Action faithful if kernel $=\{1\}$

3) For $a\in A$, the stabilizer of a is

$$G_a := \{g\in G \mid g\cdot a = a\}$$

4) Orbit $G\cdot a = \{ b \mid g\cdot a = b \text{ some } g\in G\}$

TAKEHOME #1

$$\left(\begin{array}{ll} a\sim b & \text{if} \\ g\cdot a = b & \text{some } g\end{array}\right) \longleftarrow$$ equiv relation whose equivalence classes are $G\cdot a$.

⤳ Orbits partition A.

Theorem (Orbit Stabilizer Theorem)

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

Proof

$$\begin{tikzcd} G\cdot a \arrow[r, "\phi", "\simeq"'] & G/G_a \\ \begin{matrix} b \\ \shortparallel \\ g\cdot a \end{matrix} \arrow[r, mapsto] & gG_a \end{tikzcd}$$

not a group set of left cosets of G_a.

1) Well defined

If $\underline{g\cdot a = h\cdot a} \iff h^{-1}\cdot(g\cdot a) = h^{-1}\cdot(h\cdot a)$

$\iff (h^{-1}g)\cdot a = a$

$\iff h^{-1}g \in G_a$

$\iff \underline{gG_a = hG_a}$ $\downarrow$

2) Also proved injectivity.

3) $gG_a = \phi(g\cdot a)$ & $g\cdot a \in G\cdot a$

proves surjectivity.

Rmk $G = S_n$. $G \circlearrowright \{1,\ldots,n\}$.

$G\cdot i = \{1,\ldots,n\}$

$$n = |G\cdot i| \underset{\uparrow \text{ O.S.}}{=} |G:G_i| \overset{\text{L.G.}}{=} |G|/|G_i| = n!/|G_i|$$

$\rightsquigarrow |G_i| = (n-1)!$ confirms HW4 #6.

Cycle Decompositions in S_n

Theorem

$\sigma \in S_n$ has a decomposition into disjoint cycles unique up to reordering & cyclic permutations

Pf/ $A = \{1,\ldots,n\}$

$G = \underline{\underline{\langle \sigma \rangle}} \le S_n$. $\quad G \circlearrowright A$. $\leftarrow$ orbits are the cycles

TH $\rightsquigarrow$ Partitions A into disjoint orbits

$\{O_1, O_2, \ldots, O_r\} \leftarrow$

Let $\mathcal{O}=\mathcal{O}_1$ $\quad G \circlearrowright \mathcal{O} \ni x$

$$G/G_x \longleftrightarrow \mathcal{O}$$

$$\sigma^i G_x \longleftrightarrow \sigma^i x$$

G/G_x cyclic order d.

⇝ $|\mathcal{O}| = d$.

$$G/G_x = \{G_x, \sigma G_x, \sigma^2 G_x, \dots, \sigma^{d-1} G_x\}$$

$$\mathcal{O} = \{x, \sigma x, \sigma^2 x, \dots, \sigma^{d-1} x\}$$

⇝ Get a d-cycle

$(x_1\ \sigma x\ \cdots\ \sigma^{d-1}x)$ in σ.

Do this for each orbit...

$$\underset{\mathcal{O}_1}{\underset{\shortparallel}{(x_1\ \sigma x_1 \cdots \sigma^{d_1-1}x_1)}} \cdots \underset{\mathcal{O}_r}{\underset{\shortparallel}{(x_r, \sigma x_r \cdots \sigma^{d_r-1}x_r)}}$$

Proves existence

Uniqueness

disjoint

$$\sigma = (a_1 \cdots a_t)(- - - -)$$

$$G \cdot a_1 = \{a_1, \sigma(a_1), \sigma^2(a_1), \ldots, \}$$

$$(G \cdot a_2) = \{a_1, a_2, \ldots, a_n\} \neq a_t$$

Uniqueness up to ordering O_i &

Cyclicly permuting cycles