Algebra 1 Lecture 4:

Pf of 4th iso. Thm:

Tell them I didn't mean to send the message about pfs to them. ch. 3

$H \trianglelefteq A$

$\pi_H : G \to G/H$.

$A \to \pi(A)\ AH = \bar{A}$

$\pi^{-1}(\bar{A}) \leftarrow \bar{A}$

image of subgp. is a subgp. ✓ (KH -- proved already!)

preimage of a subgp. is a subgp. too: so if $S \le G/H$, $eH \in S$ ⇒ $\pi^{-1}(H)$ so $\ni$ $= H$. exercise

also if $\pi(a) = \pi(b) = S$, then $\pi(ab^{-1}) = ab^{-1}H = aH\, b^{-1}H = S.S = S$. as S is a subgp.

($a \to \bar{k}, b \to \bar{k}, ab^{-1} \to$ ... $\pi^{-1}e \ni e$ ⇒ $\pi^{-1}K \ne \emptyset$, so gen. ...)

Book also skips details! prob. don't do or maybe do

$H = \ker(\pi) \Rightarrow \pi^{-1}(\bar{A}) \supseteq H$.

Bijective corr.:

1). $\pi(\pi^{-1}(\bar{A})) = \bar{A}$ true for any surj. f^{e}. (like our proj.) (just $\subseteq$ true in general)

2). $\pi^{-1}(\pi A) = A$. $\supseteq$ true for any f =

just have to check: $\subseteq$.

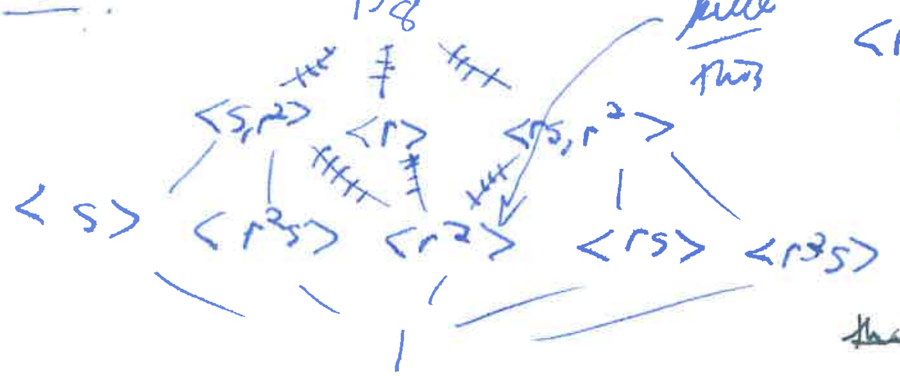
If $x \in \pi^{-1}(\pi A) \Rightarrow \pi(x) \in \pi(A) = \bar{A} \doteq AH$. Cut

$\Rightarrow x = ah,\ a \in A,\ h \in H$.

But $H \le A \Rightarrow ah \in A \Rightarrow x \in A$. ✓

The rest is just checking... left as an exercise.

Ex:



$\langle r^2\rangle \trianglelefteq D_8$.

(just have to check w/ s, as powers of r commute with r^2

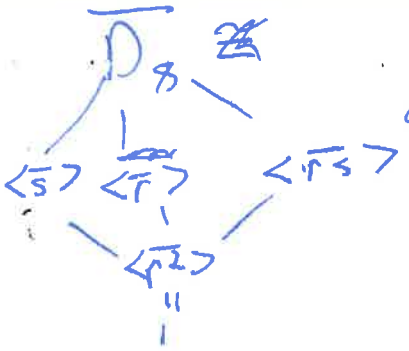
$s r^2 s^{-1} = s r^2 s = r^{-2} = r^2$

in fact $\langle r^2\rangle = Z(D_8)$?

(~~By Lagrange~~, if bigger, contains r or s, not possible)

$\bar{D}_8 = D_8/\langle r^2\rangle \cong \{\bar{1}, \bar{s}, \bar{r}, \bar{rs}\}$

$\bar{\ }$ means mod $\langle r^2\rangle$!



See that $\mathbb{Z}$ V_4 by picture.

	1	$\bar{s}$	$\bar{r}$	$\bar{r}\bar{s}$
1	1	$\bar{s}$	$\bar{r}$	$\bar{r}\bar{s}$
$\bar{s}$	$\bar{s}$	1	$\bar{r}\bar{s}$	$\bar{r}$
$\bar{r}$	$\bar{r}$	$\bar{r}\bar{s}$	1	$\bar{s}$
$\bar{r}\bar{s}$	$\bar{r}\bar{s}$	$\bar{r}$	$\bar{s}$	1

V_4 again

Size 4 $\Rightarrow$ abelian.

$\bar{r}\bar{s}\bar{r}\bar{s} = \bar{s}\bar{r}^{-1}\bar{r}\bar{s} = 1$.

$\bar{r}\bar{s} = \bar{s}\bar{r}^{-1} = \bar{s}\bar{r}$

$\bar{r}\bar{s}\bar{r} = \bar{s} = \bar{r}^{-1}\bar{r}\bar{s}$

Now, we go home.

Composition Series.

General idea in gp. theory:

Build up knowledge of G from N and G/N.

In particular, if $N \neq 1, G$, $|N|, |G/N|$ are both strictly smaller than $|G|$, so this ~~may help~~ is handy for induction pfs on $|G|$.

Picture from 4th Iso Th $\simeq$: G/N has "same" structure as G "above" N.

New proof of special case Cauchy: Th $\simeq$ (~~Cauchy~~): If G is a finite abelian gp, $p \mid |G|$ is prime, then $\exists g \leq G$, $|g| = p$.

pf: Induct on $|G|$. Use strong induction. (note: $n-1$ will never divide n, so the Lagrange ordinary induction will never help).

The base case, $G = \{e\}$ is clear, so is $|G| = 2, 3$, as then $G \cong \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/3\mathbb{Z}$.

Pf. For the induction step, ~~as~~ we have

$|G| > 1$, so $\exists g \in G, |g| \neq 1$.

If $|G| = p$, then $|g| = p$ by Lagrange $\Rightarrow$ done.

So, suppose $|G| > p$, and let $x \in G \setminus \{1\}$.

If $p \mid |x|$, say $|x| = pn$, then $|x^n| = \frac{np}{(np,n)} = \frac{np}{n} = p$.

So G has an elt. of order p. and we are done.

Thus, assume $p \nmid |x|$.

Let $N = \langle x \rangle$. As G is abelian, $N \trianglelefteq G$.

Now $|G/N| = \frac{|G|}{|N|} < |G|$ as $|N| > 1$.

Since $p \nmid |N| = |x|$, and $p \mid |G|$, we have $p \mid |G/N|$.

• GH changes
• go slower now

By induction, $|G/N|$ has an elt. of order p, say $yN = \bar{y}$.

(for a choice of rep. y) Now $y \notin N$ as

$|\bar{y}| \neq 1$, but $y^p \in N$ as $(\bar{y})^p = \bar{1}$. Thus,

$\langle y^p \rangle \neq \langle y \rangle$, or $|y^p| < |y|$. (can't be bigger.) But $|y^p| = \frac{|y|}{(n,p)}$

But if $n = |y|$, then $|y^p| = \frac{n}{(n,p)} < n \Rightarrow (n,p) > 1$

$\Rightarrow p \mid n$ (as p is prime).

But we already covered this case, so we are done. ∎

This isn't always enough, as

the isomorphism types of G/N, N do not determine G.

What are the obstructions to this technique?

Can we classify them?

Sometimes, there are no (nontrivial) normal subgps.!

Def: A gp. G is simple if $N \trianglelefteq G \Rightarrow N = 1$ or G.

These are the basic building blocks of gp theory, like the atoms or primes.

In fact, if $|G| = p$, then $G \cong \mathbb{Z}/p\mathbb{Z}$.

So by Lagrange, $H \leq G \Rightarrow H = 1$ or G.

So there are no other subgps at all!

Moreover, every abelian simple gp. is $\mathbb{Z}/p\mathbb{Z}$, which is surprisingly useful.

Non-ab. gps are more interesting. First non-ab. simple gp. is $|A_5| = 60$, we will see some

There is a classification of finite simple gps, one of the biggest pfs in math, stuff like

the "Monster" exists. Pf. ($\sim 8 \cdot 10^{53}$ elts) $\simeq 10{,}000$ pgs! (though people are working to cut that down)

SPORADIC... MOONSHINE

If you think of simple gps as "primes," want to come up w/ unique factorization theorem

Def: G a gp. A sequence

$$1 = N_0 \leq N_1 \leq \cdots \leq N_k = G$$

is a composition series if each $N_i \trianglelefteq N_{i+1}$, N_{i+1}/N_i is simple

("composition factors")

$1 \trianglelefteq \langle s \rangle \trianglelefteq \langle s, r^2 \rangle \trianglelefteq D_8$, $\mathbb{Z}$ one (recall: we did see $\langle s \rangle \trianglelefteq D_8$?).

Ex: $\mathbb{Z}_{12} \trianglelefteq \mathbb{Z}_2 \trianglelefteq \mathbb{Z}_2 \trianglelefteq \mathbb{Z}_3$, $1 \trianglelefteq \mathbb{Z}_2 \trianglelefteq \mathbb{Z}_2 \times \mathbb{Z}_2 \trianglelefteq \mathbb{Z}_6 \trianglelefteq \mathbb{Z}_{12}$ ← cyclic gps. corr. to prime factorization

Th (Jordan–Hölder): $G \neq 1$, $|G| < \infty$.

1). G has a comp. series

2). The comp. factors are unique (up to permutation) (extension problem)

Hölder Program:

1). Classify finite simple gps. ✓ done!

2). Find all ways of putting simple gps together (extension problem)

Hard Th (Feit Thompson): G simple of odd order $\Rightarrow G \cong \mathbb{Z}/p\mathbb{Z}$. ($p$ prime.) (whole journal dedicated)

Def: G is solvable if $\exists$

$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n$

G_{i+1}/G_i is abelian.

we will see in Galois theory

Fact: N, G/N solvable $\Rightarrow$ G solvable.

basically the 3rd iso Th, 4th iso Th. (see book E).

If we get $\overline{G_{i+1}/G_i} \cong G_{i+1}/G_i$ ~

To get a non-trivial family of simple gps.

Look in S_n.

Transposition = 2-cycle.

Ex: Transpositions generate S_n.

Eg: $(a_1 \cdots a_n) = (a_1 a_n)(a_2 a_{n-1}) \cdots (a_1 a_2)$ check!

trick: (one way)

Then true by existence of cycle decomp.

Define $\mathrm{sgn}(\sigma) = \begin{cases} +1 & \sigma \text{ product even \# of trans. (even perm)} \\ -1 & \sigma \text{ product of odd \# of trans. (odd perm).} \end{cases}$
sign

Thm: $\mathrm{sgn}(\sigma)$ is a well-defined hom $\mathrm{sgn}: S_n \to \{\pm 1\}$.

Pf: Suffices to show $\mathrm{sgn}(\sigma)$ is well-defined.
For this, it suffices to show
$\mathrm{sgn}(\sigma\tau) = -\mathrm{sgn}(\sigma)$ τ a trans.

see sheet

Poly in $x_1, \ldots, x_n$: $\Delta := \prod_{1 \le i < j \le n} (x_i - x_j)$ $\prod_{i<j}(x_i - x_j)$.

$\sigma \in S_n$ acts on indices: $\sigma\Delta = \prod_{1 \le i < j \le n}(x_{\sigma(i)} - x_{\sigma(j)})$ $\sigma(i) \ne \sigma(j)$ as σ injective.

Clearly, $\sigma_1\sigma_2\Delta = \sigma_1(\sigma_2\Delta)$.

Claim: $\sigma(\Delta) = \mathrm{sgn}(\sigma)\cdot\Delta$. maps each $x_k - x_l$ to itself or $x_l - x_k$ ($\sigma^{-1}: k, l \to i, j$ some i, j)

Ex: $\sigma = (123) \in S_3$ $\Delta = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$
$= (13)(12)$ $\sigma\Delta = (x_2 - x_3)(x_2 - x_1)(x_3 - x_1)$
$= (-1)^2 (x_1 - x_2)(x_1 - x_3)(x_2 - x_3) = \Delta$.

Pf: Suffices to show, for $\sigma(\Delta) = \varepsilon(\sigma)\Delta$.
1). $\varepsilon(\sigma_1\sigma_2) = \varepsilon(\sigma_1)\varepsilon(\sigma_2)$
2). $\varepsilon(\tau) = -1$, τ any trans. See next. —

1). If $\sigma_2(\Delta)$ has k factors $x_j - x_i$, $j > i$,
then $\sigma_1\sigma_2(\Delta)$ has k factors
$x_{\sigma_1(j)} - x_{\sigma_1(i)}$ with $j > i$ and rest of form
$x_{\sigma_1(j)} - x_{\sigma_1(i)}$ @ $j < i$

$\Rightarrow \sigma_1\sigma_2(\Delta) = (-1)^k \prod_{j<i}(x_{\sigma(j)} - x_{\sigma(i)}) = \varepsilon(\sigma_2)\varepsilon(\sigma_1)\Delta$.

2). $\tau = (12)$: $(12)\Delta = (x_2 - x_1)\prod_{\substack{i<j \\ \{i,j\} \ne \{1,2\}}}(x_i - x_j) = -\Delta$.

$\tau = (a\,b) \ne (12)$:
$\tau = \sigma(12)\sigma^{-1}$, $\sigma = (1a)(2b) \Rightarrow \varepsilon(\tau) = \varepsilon(12) = -1$.

over

Def: A_n = kernel of this map = {even perm} Index 2 subgp of S_n: See text in a still way before

Fact: A_n is simple, $n \geq 5$.
(insolvability of the quintic!)

(we will be able to prove such things later).

Extra time?

Go over HW?

Use below to see this.

Alt pf. $P(x_1, \dots, x_n) := \prod_{i<j} (x_i - x_j)$

$(\sigma(i) \neq \sigma(j)$ as perms. are injective)

S_n Given $\sigma \in S_n$, send (action notes)

$$P \mapsto P_\sigma := \prod_{i<j} (x_{\sigma(i)} - x_{\sigma(j)}).$$

Now if $k<\ell$, $x_k - x_\ell$ appears in P_σ as either $x_k - x_\ell$ or $x_\ell - x_k$

So $P_\sigma = \pm P$, say $P_\sigma =: \operatorname{sgn}(\sigma) P$.

$\operatorname{sgn}((k\ell)) = -1$. (just flips $x_k - x_\ell$ to $x_\ell - x_k$ or vice versa).

Not true

(appears since $\sigma^{-1}: k, \ell \mapsto i, j$ some i, j, so $i, j \to k, \ell$, but depends on if $i<j$ or $i>j$.

Start here. Finish this.

siam Conferences
www.siam.org/meetings/
A place to network and exchange ideas.

Date

Proof that sgn is a hom. $S_n \to \{\pm 1\}$.
~~enough to show:~~ well-defined.

Let $P = \prod_{i<j} (x_i - x_j)$, e.g. $n=4$

$P = (x_1-x_2)(x_1-x_3)(x_1-x_4)(x_2-x_3)(x_2-x_4)(x_3-x_4)$

Fix $\sigma \in S_n$ acts on P by permuting indices.

$$\sigma(P) = \prod_{i<j} (x_{\sigma(i)} - x_{\sigma(j)})$$

σ injective $\Rightarrow x_{\sigma(i)} \neq x_{\sigma(j)}$, $i \neq j$

each $x_k - x_\ell$ now appears as $\pm(x_k - x_\ell)$, as σ bijective

$k \neq \ell \to i, j$ s.t. $i<j$ or $i>j$

$\Rightarrow \sigma(P) = \pm P$

Say $\sigma(P) = \varepsilon(\sigma) P$

Enough to show:

1). ε is a hom.

2). $\varepsilon(\text{trans}) = -1$.

1): $\tau\sigma(P) = \prod_{i<j} (x_{\tau\sigma(i)} - x_{\tau\sigma(j)})$ but $\sigma(P)$ has k factors $x_j - x_i$, $j>i$. ($\varepsilon = (-1)^k$)

$\Rightarrow \tau\sigma(P)$ has k factors $x_{\tau(j)} - x_{\tau(i)}$, $j>i$.

Flipping these back gives a $(-1)^k = \varepsilon(\sigma)$ change, and then all factors of $\tau\sigma(\Delta)$ are $x_{\tau(p)} - x_{\tau(q)}$, $p<q$.

$$\Rightarrow \tau\sigma(P) = \varepsilon(\sigma) \prod_{p<q} x_{\tau(q)} - x_{\tau(p)} = \varepsilon(\sigma)\varepsilon(\tau) P \Rightarrow \varepsilon(\tau\sigma) = \varepsilon(\sigma)\varepsilon(\tau)$$ ★

encourage: try in an exa. $1/2$ with small n!

$\sigma = (13)$

$\sigma(P) = (x_3 - x_2)(x_3 - x_1)(x_3 - x_4)(x_2 - x_4)(x_2 - x_1)(x_4 - x_1)$

$= (-1)^3 P = -P$.

★ 1/1

2) Compute: $\varepsilon(i,j)$.

apply: $(1,2)$. only flips $(x_1 - x_2)$ to $(x_2 - x_1)$ (other factors still have $\sigma(i) < \sigma(j)$)

$\Rightarrow \varepsilon(1,2) = -1$.

For $(i,j) \neq (1,2)$

$\tau := (1\,i)(2\,j)$

$(i,j) = \tau(1,2)\tau$

(1) $\Rightarrow \varepsilon((i,j)) = \varepsilon(\tau)^2 \varepsilon(1,2) = -1$. ✓

$(x_1 - x_3)$ ↓ stays the same