Algebra I Lecture 1: Review of basic gp. theory (Comprehensive, but fast)

* Have students read Ch. 0! And read along in book; I won't cover all!

Def (where to start?) A group. Is a pair $(G, *)$, $*: G \times G \to G$ (binary op), G a set, s.t.

1). $*$ is assoc. $(a*(b*c) = (a*b)*c$, i.e., order doesn't matter)

2). $\exists$ identity $e \in G$ s.t. $a*e = e*a = a \ \forall a \in G$ (two-sided) (even though $*$ not required) exercise: why?

3). $\forall a \in G$, $\exists$ inverse a^{-1} s.t. $a*a^{-1} = a^{-1}*a = e$.

Abelian gp: $a*b = b*a$ (commutative) [Set w structure, general mantra]

Examples:
- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ under $+$, $e = 0$, $a^{-1} = -a$.
- $(\mathbb{Z}/n\mathbb{Z}, +)$ $(\mathbb{Z}/n\mathbb{Z})^\times, \times)$. (Ch. 0!) e.g.: $2 \in \mathbb{Z}/7\mathbb{Z}$: $2 \cdot 4 \equiv 1 \pmod 7$
- Vector spaces! (forget structure).
- More soon.

New from old: $A \times B = \{(a, b) \mid a \in A, b \in B\}$

$(a_1, b_1)(a_2, b_2) := (a_1 a_2, b_1 b_2)$ Note abuses of notation!

Properties:
- Inverses, identities unique.
  - Ex: If $ab = ca = e$, $c = cab = c(ab) = ce = c$ (Last time I do this!)
  - $(ca)b$, $eb = b$
- $(a^{-1})^{-1} = a$ (apply i t!)
- $(ab)^{-1} = b^{-1}a^{-1}$ (Socks-shoes!)
- $ab = ac \Rightarrow b = c$ (apply a^{-1}!).

Subgps: $H \leq G \iff H \subseteq G$. is also a gp. with the same op.

Ex: Cyclic subgp $g \in G$.

$\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\} < G$.

Size $|\langle g \rangle| =$ order of $g = |g|$

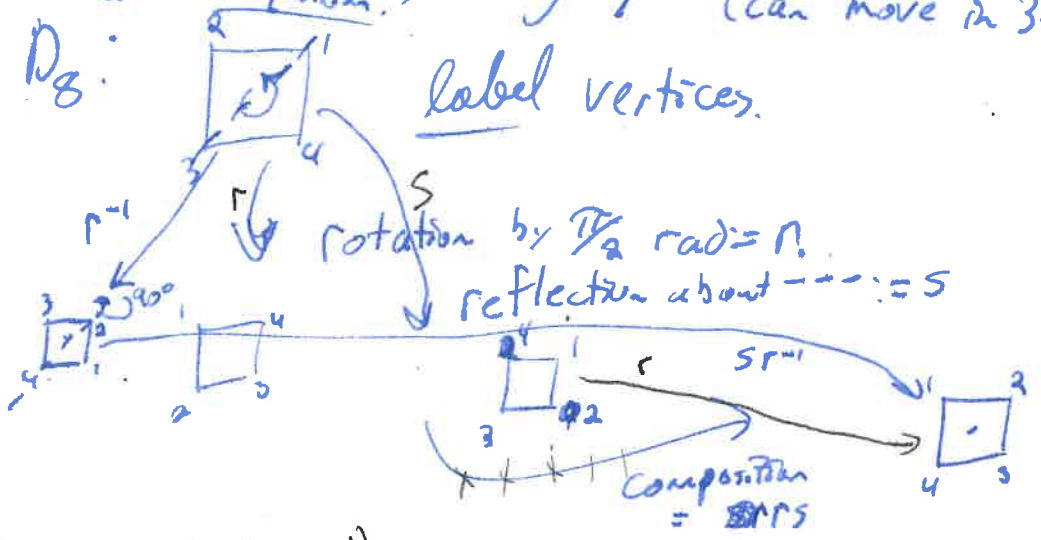
(1)

If $d \mid |g|$ (d divides), then $\langle g^{|g|/d} \rangle < \langle g \rangle < G$. (subgp is transitive!)

Dihedral Groups: Groups of symmetry of regular polygons.

$D_{2n} = \{$symmetries of reg. n-gon$\}$ under composition. (note: sometimes notation differs here!)

Ex: D_8: (can move in 3-D, have to get shape back)



Structure of D_{2n}: "s then r"

r = rotation by $2\pi/n$ rad. (counterclockwise).

s = reflection through line b/w vertex 1 & origin. (poly centered at origin)

Thm) $|D_{2n}| = 2n$:

If $1 \le i \le n$, $\exists\, \sigma \in D_{2n} \mid \sigma : 1 \to i$.

vertex 2 must go to $i+1$ or $i-1$.

by reflecting across line through i, origin can move if free.

$\Rightarrow$ $2n$ positions of vertices 1, 2. ($|D_{2n}| \le 2n$).

But these determine the rest, so $|D_{2n}| = 2n$. ($|D_{2n}| \ge 2n$: $\exists$ $2n$ of them: n rotations, n reflections)

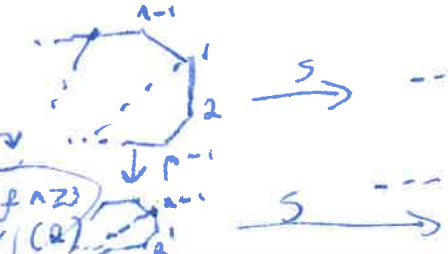
Then: 1) $|r| = n$ ($\forall r$, $\langle r \rangle = \{1, r, r^2, \dots, r^{n-1}\}$)

2) $|s| = 2$ (clear).

3) $D_{2n} = \{1, r, \dots, r^{n-1}, s, sr, sr^2, \dots, sr^{n-1}\}$. (obj exercise).

but just cancellation law + $s \notin \langle r \rangle$ + $|D_{2n}| \le 2n$

4) $rs = sr^{-1}$ (track 1, 2:



(induction)

$\Rightarrow$ $r^i s = sr^{-i}$.

Note: $rs = sr \Rightarrow sr = sr^{-1} \Rightarrow r^2 = 1$, $\forall n \in \mathbb{Z}$ (D_{2n} not abelian)

We say r, s generate G, $G = \langle r, s \rangle$, which means "all of G = (finite) prod. of elts in r, s & their inverses".

relns: equations of the generators.

Presentation: $G = \langle S \mid R_1, \dots, R_m \rangle$ (i.e., largest gp. sat. rel^{ns} which imply all rel^{ns} of elts of S.) (will specify later @ free gps)

$D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$.

Not unique! Not transparent! Could be lots of surprising cancellation, we have a "reasonable" gp since we started from the (geometric) means.

Ex from hwk: $\langle x, y \mid x^2 = y^2 = (xy)^2 = 1 \rangle$: order 4
$\langle x, y \mid x^2 = y^3 = (xy)^3 = 1 \rangle$: order 12!

Symmetric gps. $\Omega \neq \emptyset$: a set.

$S_\Omega = (\{$ bijections $\Omega \to \Omega\}, \circ)$. (a gp. by basic properties of $fcns$)

$S_{\{1, \dots, n\}} = S_n$. Of course, $|S_n| = n!$

two line notation

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 2 & 5 & 6 \end{pmatrix} \longrightarrow$ cycle notation $(13)(24)$ (Don't write one cycles). $\in S_{10}$ too! have to know context!

(Do more examples!)

Ex'. $(12)(13) = (132) \neq (123) = (13)(12) \Rightarrow S_{3n}$ is nonabelian if $n \geq 3$.

This cycle decomposition is unique up to order of cycles & cyclic perms. of them (make unique by writing smallest # first and using increasing #s). (Not obvious!)

Arithmetic in S_n: Right to left

$(132) \cdot (15) = (1532)$. (already seen)

Inverses: write cycles in reverse order.

$[(1532)(46)]^{-1} = (2351)(64) = (1235)(46)$. (Check it yourself!)

E-Z: Disjoint cycles commute. (affect disjoint sets)

Exercise: Order of perm. = lcm of cycle lengths.

- There is an isomorphism $S_3 \cong D_6$.

Geometry: Rigid motions of $\Delta \leftrightarrow$ perms of vertices

Call perms corr. to a symmetry

Formally.

Def^n: A homomorphism $\varphi: G \to H$ from $(G, *)$ to (H, Δ) is a map s.t. $\varphi(a * b) = \varphi(a) \Delta \varphi(b)$ $\forall a, b \in G$.

Preserves gp. structure.

(Philosophy) Understand hard things by mapping to E-Z ones!!

An isomorphism is a bijective hom. (Rep^n thm)

"If we paint the elts green, that doesn't matter"

Matrix gps:

Ex: $G = (GL_n(\mathbb{R}), \cdot)$ (invertible ($\det \neq 0$) matrices with entries in $\mathbb{R}$).

Can replace $\mathbb{R}$ by any field.

A field is a set F w/ 2 binary ops $+, \cdot$ w.

$(F, +)$ an abel. gp., $F \setminus \{0\}$ is also an ab. gp. s.t.

we have the distributive law

$$a(b+c) = ab + bc \quad \forall a, b, c \in F.$$

$\det$ is a homomorphism $\det : GL_n(F) \to F^* := F \setminus \{0\}$.

kernel of a hom $\varphi : G \to H$: $\ker \varphi := \{ g \in G \mid \varphi(g) = e_H \}$.

The kernel is a subgp of G:

Test: $S \subseteq G$ is a subgp if
1). $S \neq \emptyset$ (know of trivial)
2). $a, b \in S \Rightarrow ab^{-1} \in S$.

$\ker(\varphi) \leq G$ as: $\varphi(e_G) = e_H$
(as $\varphi(e_G \cdot g) = \varphi(e_G) \cdot \varphi(g) = \varphi(g) \forall g$
& identities in gps are unique)

and so $\ker(\varphi) \neq \emptyset$,
and
$a, b \in \ker(\varphi) \Rightarrow \varphi(ab^{-1}) = \varphi(a)\varphi(b^{-1})$
$= \varphi(b^{-1}) = \varphi(b)^{-1} = e_H^{-1} = e_H \Rightarrow ab^{-1} \in \ker(\varphi)$
(as $\varphi(b)\varphi(b^{-1}) = \varphi(bb^{-1}) = \varphi(e_G) = e_H$).

In the case of $\det$,
the kernel is the special linear gp $SL_n(F)$
$= \{ M \in GL_n(F) \mid \det M = 1 \}$.

Fact: $SL_2(\mathbb{Z}) = \langle S, T \rangle$, where $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.