Group Theory

Meta goal: to classify finite symmetries/finite groups

This course: to understand the basic principles and develop enough theory to classify groups of certain orders (small)

Idea: divide and conquer (1) $G \rightsquigarrow N \triangleleft G$, G/N
(2) extensions: how do N and G/N fit together

I. Recall and examples

Def: A group G is a set with an associative product $G \times G \to G$, a unit e such that each element $g \in G$ has inverse g^{-1}.

$H < G$ is a subgroup if it is a group with the multiplication as defined in G.

$gH = \{gh \mid h \in H\}$ is a right coset

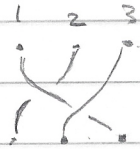
$G/H = \{gH \mid g \in G\}$ is the set of right cosets

$N \triangleleft G$ is a normal subgroup if for all $g \in G$: $gN = Ng$ (or $N = g^{-1}Ng$)

Lemma: If $N \triangleleft G$ is a normal subgroup then $G/N := \{gN \mid g \in G\}$ is a group, the quotient group, with multiplication $(gN)\cdot(\tilde{g}N) := g\tilde{g}N$.

Th (Lagrange) If G is finite and H a subgroup then $|G| = |H| \, |G/H|$

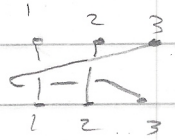
Examples: Cyclic groups C_n ($\simeq \mathbb{Z}/n\mathbb{Z}$)
Dihedral groups D_{2n} = Sym (regular n-gon)
Permutation groups S_n = Sym ($\{1,2,\dots,n\}$)
Matrix groups $GL_n\mathbb{R}$, $O(n)$, ...
⋮
Braid groups Br_n :



$n=3$

⋮

Examples of normal subgroups:
$C_n \triangleright C_k$ if $k \mid n$
$D_{2n} \triangleright C_n$
$S_n \triangleright A_n$ alternating group
$Br_n \triangleright PBr_n$ pure braid group



Def: A map $\phi: G_1 \to G_2$ is a group homomorphism if
$\phi(g\tilde{g}) = \phi(g)\,\phi(\tilde{g})$.

Th (First Isomorphism):
If $\phi: G_1 \to G_2$ is a group homomorphism then
$\operatorname{im}\phi = \{\phi(g) \mid g \in G_1\} \subset G_2$ is a subgroup
$\ker\phi = \{g \mid \phi(g) = e \in G_2\}$ is a normal subgroup
and $G_1/\ker\phi \cong \operatorname{im}\phi$ is an isomorphism
$g\cdot\ker\phi \longmapsto \phi(g)$ □

Ex: $\phi: S_n \to \{1,-1\} \subset \mathbb{Q}^\times$ group of non-zero rationals under multiplication
$\sigma \mapsto \operatorname{sgn}(\sigma)$
$\Rightarrow \ker\phi = A_n$ and $S_n/A_n \simeq \{1,-1\}$

$\phi: Br_n \to S_n$ $\beta \mapsto$ permutation induced
$\Rightarrow \ker\phi = PBr_n$ and $Br_n/PBr_n \simeq S_n$.

II. Generators and Relations

"spanning set"

Def: Let S be a subset of G. The subgroup generated by S is the smallest subgroup of G containing S

$$\langle S \rangle := \bigcap_{S \subseteq H \leq G} H \qquad (\langle \emptyset \rangle = \{e\})$$

Def: G is finitely generated if there exists a finite set $S \subseteq G$ with

$$\langle S \rangle = G.$$

S is a generating set.

Ex: $S_3 \simeq D_6$

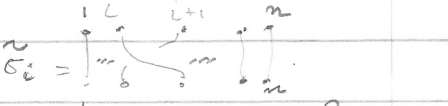
$\langle (123) \rangle = \{e, (123), (132)\} \simeq C_3 \leq S_3$

$\langle (123), (12) \rangle = S_3$

$\Rightarrow$ S_3 is finitely generated

Indeed, any finite group is finitely generated: $\langle G \rangle = G$

Ex: Br_n is generated by $\tilde{\sigma}_1, \dots, \tilde{\sigma}_{n-1}$

$\tilde{\sigma}_i =$ 

Note: $\langle S \rangle = \{ s_1 \cdots s_k \mid s_i \in S \text{ or } s_i^{-1} \in S \}$

Hence, if $\langle S \rangle = G$, then any homomorphism $\phi : G \to H$ is determined by its restriction to S.

We are now seeking a group $F(S) \supseteq S$ satisfying the Universal Property:

(Any $f : S \to H$ can be extended to a group homomorphism in a unique way.)

Given a group H,

$$\begin{array}{ccc} S & \xrightarrow{f} & H \\ {\scriptstyle i}\downarrow & \nearrow_{\phi} & \\ F(S) & & \end{array}$$

2.1 Free groups

S a set. Take a disjoint copy S^{-1} with elements x^{-1} for each $x \in S$.

A word w in S is a finite string $x_1 \dots x_m$ with $x_i \in S \cup S^{-1}$.
(Note, the empty word is a word.)
Words w_1 and w_2 can be concatenated to form a new word $w_1 . w_2$.
The deletion of a substring $x . x^{-1}$ or $x^{-1} . x$ from a word is an elementary contraction:

$$w = w_1 . x . x^{-1} . w_2 \longrightarrow w' = w_1 . w_2$$
$$w_1 . x^{-1} x . w_2 \longrightarrow w' = w_1 . w_2$$

If w does not allow for any elementary contraction then w is reduced.

Prop: (a) Every word can be transformed by elementary contractions to a reduced word.
(b) The reduced word so obtained is unique.

proof: Occurances of $x . x^{-1}$ or $y^{-1} . y$ are deleted.
Clearly if $x . x^{-1}$ and $y^{-1} . y$ are disjoint it does not matter in which order they are deleted.
If the string $x . x^{-1} . x$ (or $x^{-1} . x . x^{-1}$) both reductions lead to x (or x^{-1}). So it does not matter which is chosen – the end result is unique.

Notation: With $[w]$ for the reduced word obtained from w.

Def: The free group on S, denoted $F(S)$, consists of reduced words in S. The product for two reduced words w_1 and w_2 is $[w_1 . w_2]$, the empty word is the unit, and if $w = x_1 \dots x_m$ then $w^{-1} = x_m^{-1} \dots x_1^{-1}$.

$[w_1 . w_2 . w_3]$

Note: Associativity of the product follows from uniqueness of the reduced word.

2.2 Universal Property

Th: Given a set S and any group G and any map $f: S \to G$, then is a unique homomorphism $\phi: F(S) \to G$ s.th. $S \xrightarrow{f} G$ commutes.

$S \hookrightarrow F(S) \xrightarrow{\phi} G$

proof: For $x \in S$, define $\phi(x) = f(x)$ and $\phi(x^{-1}) = f(x)^{-1}$; for $w = x_1 \cdots x_m$, define $\phi(w) = \phi(x_1) \cdots \phi(x_m)$.
Then ϕ is a group homomorphism:
Note that $x \cdot x^{-1}$ and $x^{-1} \cdot x$ go to the identity in G and hence the value on $w_1 \cdot w_2$ is the same as on $[w_1 \cdot w_2]$. (S is independent)
Vice versa, ϕ is unique as it is completely determined by its values on S. (S is generating)

Cor: Every group G is the quotient of a free group.

proof: Take $S = G$ and $f: G \to G$ the identity.
Then $\phi: F(G) \to G$ is surjective.
Hence by the first isomorphism theorem

$$F(G)/\ker\phi \cong G.$$

□

2.3 Presentations

Def: Let B be a subset of G. The normal subgroup generated by B is the smallest normal subgroup containing B

$$\langle\langle B \rangle\rangle := \bigcap_{B \subseteq N \trianglelefteq G} N$$

Note: $\langle\langle B \rangle\rangle = \langle \{ g^{-1} r g \mid g \in G, r \in B \} \rangle$

proof: Clearly "$\geq$". But also "$\subseteq$" as $B \subseteq$ RHS and RHS is normal: for $h \in G$

$$h^{-1} (\Pi g_i^{-1} b_i g_i) h = \Pi (g_i h)^{-1} b_i (g_i h)$$

□

Ex: S_3, $\langle\langle (12) \rangle\rangle = \langle$ all 2-cycles $\rangle = S_3$

Def: Let X be a set and R a subset of $F(X)$. The group with generators X and relations R is defined as

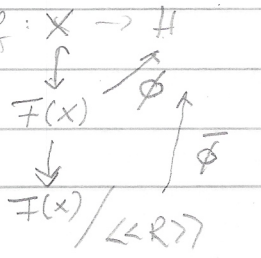
$$\langle X \mid R \rangle := F(X) / \langle\langle R \rangle\rangle .$$

If S is a subset of a group G and $R \subseteq F(S)$ is such that the map $S \hookrightarrow G$ induced an isomorphism

$$F(S)/\langle\langle R \rangle\rangle \xrightarrow{\cong} G$$

then $\langle S \mid R \rangle$ is a presentation of G.

Lemma: Let $\langle X \mid R \rangle$ and H be groups. Then a map $f: X \to H$ can be extended to a group homomorphism $\phi: \langle X \mid R \rangle \to H$ if and only if $\phi(w) = e \in H$ for all $w \in R$.

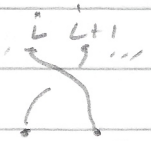


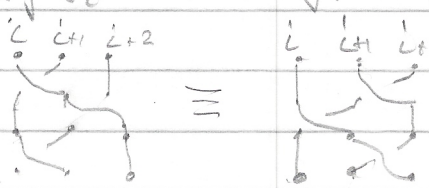
Examples : • $C_n = \langle g \mid g^n \rangle$

• $D_{2n} = \langle g, s \mid g^n, s^2, sgsg \rangle$

• $S_n = \langle \sigma_1, \dots, \sigma_{n-1} \mid \sigma_i^2 = 1, \quad \sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1} \rangle$
with $\sigma_i = (i, i+1)$ $\qquad \sigma_i \sigma_j = \sigma_j \sigma_i$ for $|i-j| \geq 2$

• $\mathcal{B}r_n = \langle \tilde{\sigma}_1, \dots, \tilde{\sigma}_{n-1} \mid \tilde{\sigma}_i \tilde{\sigma}_{i+1} \tilde{\sigma}_i = \tilde{\sigma}_{i+1} \tilde{\sigma}_i \tilde{\sigma}_{i+1}, \quad \tilde{\sigma}_i \tilde{\sigma}_j = \tilde{\sigma}_j \tilde{\sigma}_i \quad |i-j| \geq 2 \rangle$

with $\tilde{\sigma}_i =$ 



• $\mathcal{B}r_n \xrightarrow{\Phi} S_n$ defines a surjective homomorphism
$\tilde{\sigma}_i \longmapsto \sigma_i$ with kernel $P\mathcal{B}r_n$

3. Isomorphism Theorems

First isomorphism theorem:

Let $\phi: G_1 \to G_2$ be a homomorphism.

Then (1) $\operatorname{Im}\phi$ is a subgroup of G_2

(2) $\ker\phi$ is a normal subgroup of G_1

(3)

$$\overline{\phi}: G_1/\ker\phi \longrightarrow \operatorname{im}\phi \qquad \text{is an isomorphism}$$
$$g.\ker\phi \longmapsto \phi(g)$$

Ex: $Br_n = \langle \tilde{\sigma}_1, \dots, \tilde{\sigma}_{n-1} \mid \tilde{\sigma}_i\tilde{\sigma}_j = \tilde{\sigma}_j\tilde{\sigma}_i \text{ for } |i-j| \geq 2$
$\tilde{\sigma}_i\tilde{\sigma}_{i+1}\tilde{\sigma}_i = \tilde{\sigma}_{i+1}\tilde{\sigma}_i\tilde{\sigma}_{i+1} \rangle$.

We want to define $\phi: Br_n \to \mathbb{Z} = \langle 1 \rangle$
$\tilde{\sigma}_i \longmapsto 1$

Note: $\phi(\tilde{\sigma}_i\tilde{\sigma}_j) = \phi(\tilde{\sigma}_i)\phi(\tilde{\sigma}_j) = 2 = \phi(\tilde{\sigma}_j\tilde{\sigma}_i)$
$\phi(\tilde{\sigma}_i\tilde{\sigma}_{i+1}\tilde{\sigma}_i) = 3 = \phi(\tilde{\sigma}_{i+1}\tilde{\sigma}_i\tilde{\sigma}_{i+1})$

Hence, ϕ takes the relations to e and ϕ is a homomorphism.

$$Br_n/\ker\phi \simeq \operatorname{im}\phi \simeq \mathbb{Z}$$

BTW: this proves the order of each $\tilde{\sigma}_i$ is ∞: $\langle\tilde{\sigma}_i\rangle \to Br_n \xrightarrow{\simeq} \mathbb{Z}$

Ex: $Br_n \xrightarrow{\phi} S_n$ surjective homom. as relations are preserved
$\tilde{\sigma}_i \longmapsto \sigma_i$.
$PBr_n := \ker\phi \trianglelefteq Br_n$

will make this more formal later

Second isomorphism theorem:

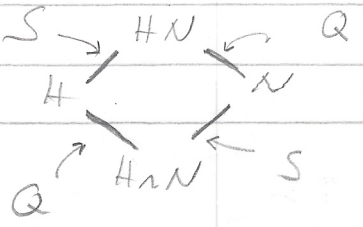
Let G be a group; $H \leq G$ a subgroup and $N \trianglelefteq G$ a normal subg.
Then (1) $HN \leq G$ is a subgroup of G
(2) $H \cap N \trianglelefteq H$ is a normal subgroup of H
(3) $H/H\cap N \longrightarrow HN/N$ is an isomorphism
$h.(H\cap N) \longmapsto h.N$

proof: (1) Let $h_1, h_2 \in H$, $n_1, n_2 \in N$.
Then $(h_1 n_1)(h_2 n_2) = h_1 h_2 \tilde{n} n_2$ for $\tilde{n} = h_2^{-1} n_1 h_2 \in N$
$\in HN$
$(h_1 n_1)^{-1} = n_1^{-1} h_1^{-1} = h_1^{-1} \hat{n}$ for $\hat{n} = h_1 n_1^{-1} h_1^{-1} \in N$
$e \in HN$
Hence, HN is a subgroup.
(2) Let $x \in H\cap N$ and $h \in H$
Then $h^{-1} x h \in H$ as $x \in H$, and
$h^{-1} x h \in N$ as $h \in G$ and N is normal.
Hence $h^{-1} x h \in H \cap N$,
(3) The map $\phi: H \longrightarrow HN \longrightarrow HN/N$ is a (surjective) homom.
$h \longmapsto h \longmapsto hN$

$h \in \ker\phi$ iff $h.N = N$ iff $h \in N$.
Hence $\ker\phi = H\cap N$.
By the First Iso Th, $H/H\cap N \simeq HN/N$.

Ex: $G = C_{12} = \langle \sigma \mid \sigma^{12} \rangle$
$H = C_6 = \langle \sigma^2 \rangle$
$N = C_4 = \langle \sigma^3 \rangle$
$H\cap N = \langle \sigma^6 \rangle \simeq C_2$
$HN/N = G/N \simeq C_3$
$H/H\cap N \simeq C_3$

Diamond Lemma: If H, N are both normal in G
then $HN/N \simeq Q \simeq H/H\cap N$ and $HN/H \simeq S \simeq N/H\cap N$:



Third isomorphism theorem

Let N, K be normal subgroups of G with $K \leq N$.
Then (1) $N/K \trianglelefteq G/K$
(2) $(G/K)/(N/K) \simeq G/N$

proof: (1) Let $gK \in G/K$, $nK \in N/K$.
Then
$$(gK)^{-1}(nK)(gK) = g^{-1}ng\,K \in N/K \text{ as } g^{-1}ng \in N$$

(2) Consider the homomorphism $G/K \xrightarrow{\phi} G/N$
$$gK \mapsto gN$$
Then $gK \in \ker\phi$ iff $gN = N$ iff $g \in N$.
So $\ker\phi = N/K$ and by the first iso. th. we are done. □

Ex: $V_4 \trianglelefteq A_4 \trianglelefteq S_4$
$$(S_4/V_4)/(A_4/V_4) \simeq S_4/A_4 \simeq C_2$$

Subgroup Correspondence:

$\pi : G \to G/N$

$$\{\text{subgroup of } G/N\} \xleftrightarrow{1:1} \{\text{subgroups of } G \text{ containing } N\}$$
$$\{\text{normal} \quad " \quad "\} \xleftrightarrow{1:1} \{\text{normal} \quad " \quad " \quad "\}$$
$$H/N \longleftarrow H \quad (H \supseteq N)$$
$$Q \leq G/N \longmapsto \pi^{-1}(Q) = \{g \in G \mid \underbrace{gN}_{\pi(g)} \in Q\}$$

3.3 Simple groups

Def: $G \neq \{e\}$ is *simple* if G and $\{e\}$ are the only normal subgroups.

Ex: C_n is simple iff $n = p$.

Ex: S_n, $n \geq 3$, is *not* simple as $S_n \trianglerighteq A_n \neq \{e\}$

Ex: $A_3 \cong C_3$ is simple.
$A_4 \trianglerighteq V_4 \neq \{e\}$ is *not* simple

Th: A_n is simple for $n \geq 5$

proof for $n = 5$:

Normal subgroups are unions of conjugacy classes!
(if $x \in N$ then $g^{-1}xg \in N$ for all $g \in G$)
The conjugacy classes of A_5 (and their sizes) are:

1 — $\{e\}$

20 — $\{(123)\}$ — $\exists \sigma \in S_5 : \sigma^{-1}(123)\sigma = (abc)$
σ even ✓, σ odd — replace by $(45)\sigma$

15 — $\{(12)(34)\}$ — $\exists \sigma \in S_5 : \sigma^{-1}(12)(34)\sigma = \tau = (ab)(cd)$
σ odd — replace by $(34)\sigma$

12 — $\{(12345)\}$ — if $\sigma^{-1}(12345)\sigma = (\sigma(1)\sigma(2)\sigma(3)\sigma(4)\sigma(5)) = (12345)$
$\Rightarrow$ σ is determined by $\sigma(1)$ and σ is a power of (12345)
$\Rightarrow |\text{orbit}_{A_5}(12345)| = |A_5|/|\text{Stab}| = 5!/2/5 = 12$

12 — $\{(21345)\}$

Also, if $N \leq A_4$ then $|N| \mid 60$ and $e \in N$.