Lecture 2 : Basics on Groups II

Recall: $(G, *, e)$ group
- $a * b \in G \quad \forall a, b \in G$
- e neutral element

(i) Assoc: $(a*b)*c = a*(b*c) \quad \forall a,b,c \in G$

(ii) Neutral: $a*e = e*a = a \quad \forall a \in G$ (unique!)

(iii) Inverse: $\forall a \in G \ \exists b \in G : a*b = b*a = e$ (unique!)

G, G' gps $\quad \varphi : G \longrightarrow G'$ gp homomorphism

means $\varphi(a*b) = \varphi(a) * \varphi(b)$ ($\rightsquigarrow \varphi(e) = e'$, $\varphi(x^{-1}) = \varphi(x)^{-1}$)

$\boxed{\text{TODAY:}}$

① Subgroups, Normal subgps $\rightsquigarrow$ quotients of gps by subgroups

② Hom spaces

② cyclic groups $\rightsquigarrow$ presentations of groups

• **Nice groups**: those given as "symmetries of a structure"

Advantage: Associativity is automatic!

"**Structure**": a finite set $X = \{1, 2, \dots, n\}$ for $n = |X|$

"**Symmetries**" = bijections $\sigma : X \longrightarrow X$

Group operation = composition of two maps

$$\begin{tikzcd} X \arrow[r, "\sigma"] \arrow[rr, bend right] & X \arrow[r, "\tau"] & X \end{tikzcd}$$

$\tau * \sigma := \tau \circ \sigma = \tau\sigma$ (usually we omit $\circ$)

Ex: ① S_n = permutations on n letters

② D_n = symmetries of n-gon

• <u>More examples</u>: $\mathbb{F}_n$ = free group on n letters

$$\boxed{\mathbb{F}_n = \text{"words" in the alphabet } \{a_1, \dots, a_n\}}$$

<u>Group structure</u>: $*$ = concatenation (+ cancellations)

e = empty word

<u>Eg</u>: $w_1 = a_2^{-2} a_1 a_2 a_1 \rightsquigarrow w_1^{-1} = a_1^{-1} a_2^{-1} a_1^{-1} a_2^{2}$

$w_2 = a_1^{-1} a_2 \rightsquigarrow w_2^{-1} = a_2^{-1} a_1$

$$w_1 w_2 = (a_2^{-2} a_1 a_2 a_1)(a_1^{-1} a_2) = a_2^{-2} a_1 a_2 \underbrace{(a_1 a_1^{-1})}_{e} a_2 = a_2^{-2} a_1 \overbrace{a_2 a_2}^{= a_2^2} = a_2^{-2} a_1 a_2^2$$

$$w_2 w_1 = (a_1^{-1} a_2)(a_2^{-2} a_1 a_2 a_1) = a_1^{-1} a_2^{-1} a_1 a_2 a_1$$

<u>Why</u>? Use $\mathbb{F}_n$ to define <u>presentations</u> of fin. gen gps G

[Word problem $\rightsquigarrow$ decide when two words give the same element in G]

$\boxed{\text{Subgroups}}$

Def A subset $H \subset G$ is a subgroup of G if:

(write: $H < G$)

(i) $e \in H$

(ii) $x, y \in H \Rightarrow xy \in H$

(iii) $x \in H \Rightarrow x^{-1} \in H$

(H inherits gp structure from G)

Lemma: $\emptyset \neq H \subset G$ subgroup iff $\boxed{x, y \in H \Rightarrow xy^{-1} \in H}$

Pf/ (i) $x \in H \quad y = x \rightsquigarrow xy^{-1} = xx^{-1} = e \in H$ ✓

(iii) $x = e,\ y \in H \rightsquigarrow xy^{-1} = ey^{-1} = y^{-1} \in H$ ✓

(ii) $x, y \in H \rightsquigarrow x, y^{-1} \in H \rightsquigarrow x(y^{-1})^{-1} = xy \in H$ ✓

Key players = normal subgroups

Def: A subgroup $H < G$ is called <u>normal</u> if $\forall a \in G$, $b \in H$ we have $aba^{-1} \in H$

Notation: $H \triangleleft G$ (\triangleleft in LaTeX)

Examples: $\{e\}$, G

Obs: If G is abelian, every subgroup H of G is normal

(Ex: $G = \mathbb{Z}$)

Q: Is the converse true? **A**: NO (last slide today)

Q: Subgroups from gp homomorphisms?

A: Yes (just as in Linear Algebra)

Def: Given $\varphi : G \longrightarrow G'$ gp homomorphism

$$\operatorname{Ker}(\varphi) := \{ x \in G : \varphi(x) = e' \} = \text{Kernel of } \varphi$$

$$\operatorname{Im}(\varphi) := \{ \varphi(x) : x \in G \} = \text{Image of } \varphi$$

Lemma: (1) $\operatorname{Ker}(\varphi) \lhd G$ & (2) $\operatorname{Im}(\varphi) < G'$

⚠ $\operatorname{Im}\varphi$ need not be normal

Ex: $G = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} : \begin{array}{l} a, b, c \in \mathbb{C} \\ a, c \neq 0 \end{array} \right\} \xhookrightarrow{\ \varphi\ } GL_2(\mathbb{C})$

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{-1} \underset{\varphi(G)}{\underset{\cap}{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}}} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \underbrace{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}}_{\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \notin \varphi(G)$$

Pf/ (1) <u>Claim 1</u> $\mathrm{Ker}(\varphi) < G$

Need to check 3 properties:

(i) $a, b \in \mathrm{Ker}(\varphi)$: $\varphi(ab) = \varphi(a)\,\varphi(b) = e' \cdot e' = e'$

$\Longrightarrow a.b \in \mathrm{Ker}(\varphi)$

(ii) $\varphi(e) = e'$ (Lecture 1) $\Longrightarrow e \in \mathrm{Ker}(\varphi)$

(iii) $a \in \mathrm{Ker}(\varphi)$ $\varphi(a^{-1}) \underset{\text{Lecture 1}}{=} \varphi(a)^{-1} = (e')^{-1} = e' \Rightarrow a^{-1} \in \mathrm{Ker}\,\varphi$

<u>Claim 2</u> : $b \in \mathrm{Ker}(\varphi)$, $a \in G \Longrightarrow a^{-1} b a \in \mathrm{Ker}\,\varphi$.

Indeed: $\varphi(a^{-1} b a) = \varphi(a)^{-1} \underbrace{\varphi(b)}_{=e'} \varphi(a) = e'$ ✓

(2) $\mathrm{Im}(\varphi) < G'$ $\rightsquigarrow$ exercise

More notation & definitions

- $\mathrm{Hom}_{Gps}(G, G')$ = set of group homomorphisms $G \to G'$
- $\varphi \in \mathrm{Hom}(G, G')$ is an <u>isomorphism</u> if $\exists\, \varphi' \in \mathrm{Hom}(G', G)$ st $\varphi \circ \varphi' = id_{G'}$ & $\varphi' \circ \varphi = id_G$

<u>Def</u>: G & G' are <u>isomorphic</u> groups (write $G \simeq G'$) if $\exists\, \varphi \in \mathrm{Hom}(G, G')$ isomorphism.

- $\mathrm{End}(G) = \mathrm{Hom}(G, G)$ is a monoid under compositions
- $\mathrm{Aut}(G)$ = isomorphisms in $\mathrm{Hom}(G, G)$ is a group

$$\boxed{\text{Quotient groups}}$$

GOAL: Given $H < G$ want to build G/H

Consider the relation $\sim$ on G given by $x \sim y$ if $x^{-1}y \in H$

(equiv: $xH = yH$ as sets)

Lemma: $\sim$ is an equivalence relation.

Pf/ • Symmetry: Say $x \sim y \Rightarrow x^{-1}y \in H \underset{H \text{ subgp}}{\Longrightarrow} (x^{-1}y)^{-1} = y^{-1}x \in H$

$\Rightarrow y \sim x$

• Reflexive: $x \sim x \iff x^{-1}x = e \in H$ ✓

• Transitive $x \sim y$ & $y \sim z \overset{?}{\Longrightarrow} x \sim z$

$$\Rightarrow \quad x^{-1}z = (x^{-1}y)(y^{-1}z) \in H \cdot H \underset{H \text{ subgp.}}{\subseteq} H$$

$\square$

Def : $\boxed{G/H}$ = set of equivalence classes in G with respect to $\sim$.

= left cosets (modulo H) $= \{ xH \quad x \in G \}$

Similarly : $\boxed{H \backslash G}$ = right cosets (modulo H) (equiv $Hy = Hx^{-1}$)

= set of equiv classes in G under $x \sim' y \iff yx^{-1} \in H$

Q: Do G/H and/or $H \backslash G$ have any algebraic structure ?

A: Only when $H \lhd G$

Proposition 1: Assume $H \lhd G$. Then, G/H has a group induced from G.

The natural projection $\pi : G \twoheadrightarrow G/H$ is a gp homomorphism

$g \longmapsto gH$

& $\mathrm{Ker}(\pi) = H$

Explicitly : $g_1 H \cdot g_2 H := g_1 g_2 H$

$e_{G/H} = 1 \cdot H$ & $(gH)^{-1} = g^{-1} H$

Pf/ • **Claim 1**: Law of composition is well-defined, ie

$$\boxed{g_1 \sim g_1' \ \& \ g_2 \sim g_2' \overset{?}{\Longrightarrow} g_1 g_2 \sim g_1' g_2'}$$

Indeed, $g_\ell \sim g_\ell' \Rightarrow g_1^{-1} g_1' \in H$
$(\ell = 1, 2)$ $\qquad g_2^{-1} g_2 \in H$

Want to show: $(g_1 g_2)^{-1} g_1' g_2' \in H$

$$(g_1 g_2)^{-1} g_1' g_2' = g_2^{-1} \underbrace{(g_1^{-1} g_1')}_{\in H} g_2' = \underbrace{g_2^{-1} \underbrace{(g_1^{-1} g_1')}_{\in H} g_2}_{\in H \text{ because } H \triangleleft G} \underbrace{g_2^{-1} g_2'}_{\in H} \in H$$

• **Claim 2**: Law of composition in G/H is associative
(This is inherited from G)

• The assertions: $eH = e_{G/H}$ & $(gH)^{-1} = g^{-1}H$ are clear □

$\boxed{\text{Cyclic groups}}$

Motivating example: $(\mathbb{Z}, +)$ is abelian, so every $N < \mathbb{Z}$ is normal

Q: What does $\mathbb{Z}/N$ look like?

Lemma: Fix $N < \mathbb{Z}$. Then, $\exists\, n \in \mathbb{Z}_{\geq 0}$ s.t

$$N = n \cdot \mathbb{Z} = \{0, \pm n, \pm 2n, \dots\}$$

Pf/ • If $N = \{0\}$, then $n = 0$ ✓

• Assume $N \neq \{0\}$ & let $\boxed{n = \min N \cap \mathbb{Z}_{>0}}$

Claim: $N = n\mathbb{Z}$

$N \supseteq n\mathbb{Z}$ ✓ If $N \not\subseteq n\mathbb{Z}$ & $\exists\ 0 < m \in N \setminus n\mathbb{Z}$

Pick $k \in \mathbb{Z}_{\geq 0}$ s.t $k < \frac{m}{n} < k+1 \Rightarrow kn < m < (k+1)n$

$\Rightarrow 0 < m - nk < n$ in N Contr!

$\square$

A: $\mathbb{Z}/N = \boxed{\mathbb{Z}/n\mathbb{Z}}$ with law of composition "addition modulo n"

- The earlier example is a cyclic group

Def A group G is cyclic if $\exists\, g \in G$ s.t every element of G is of the form g^m for some $m \in \mathbb{Z}$, that is:

also not unique

$$g^m = \begin{cases} \underbrace{g \cdots\cdots g}_{m \text{ times}} & \text{if } m > 0 \\ \underbrace{g^{-1} \cdots\cdots g^{-1}}_{(-m) \text{ times}} & \text{if } m < 0 \end{cases}$$

Name: g = a generator for G (not unique!)

Eg for $\mathbb{Z}$: $\{\pm 1\}$ = set of generators of $\mathbb{Z}$.

Exercise: Number of generators of $\mathbb{Z}/n\mathbb{Z} = \Phi(n) := \{ \ell \in \{1, \dots, n-1\} : \gcd(\ell, n) = 1 \}$

(Normal) Subgroups generated by a set

Lemma: Fix H_1, H_2 subgroups of G. Then

(1) $H_1 \cap H_2$ is a subgroup of G

(2) If $H_1 \lhd G$ & $H_2 \lhd G$, then $H_1 \cap H_2 \lhd G$.

Proof: Easy & works for arbitrary intersections.

⇝ **Def:** Given a set $X \subseteq G$, we define $\langle X \rangle \subset G$ as the smallest subgroup of G containing the set X.

Name: $\langle X \rangle$ <u>subgroup generated by X</u>.

Obs: $\langle \emptyset \rangle = \{e\}$. (trivial subgp)

Similarly: $N\langle X \rangle$ = <u>normal subgroup generated by</u> X
= smallest normal subgp containing X.

Def. G is *finitely generated* if $\exists$ finite $A \subset G$ with $\langle A \rangle = G$.

For cyclic groups: $G = \langle \{g\} \rangle$ for some $g \in G$

$$= \{e, g, g^2, g^3, \dots, g^{-1}, g^{-2}, g^{-3}, \dots\}$$

$\rightsquigarrow$ 2 options: $\{e, g, g^2, \dots\}$ is infinite (A)

$\{ \qquad \}$ is finite (B)

Option (A): G is isomorphic to $\mathbb{Z}$ $\qquad \mathbb{Z} \xrightarrow{\sim} G$, $n \longmapsto g^n$

Option (B) Pick n = smallest positive integer s.t.

$g^n \in \{e, g, g^2, \dots, g^{n-1}\}$ $\qquad (n > 1$ if $G \neq \{e\})$

Claim: $g^n = e$ $\quad$ [If not, $g^n = g^\ell$ for $0 < \ell < n$ $\Rightarrow g^{n-\ell} = e \in \{e, g, \dots, g^{n-\ell-1}\}$ Contra!]

$$\Rightarrow \begin{cases} g^{-1} = g^{n-1} \quad \& \\ G = \{e, g, g^2, \dots, g^n\} \simeq \mathbb{Z}/n\mathbb{Z} \quad \text{via } g^m \longleftarrow \overline{m} \end{cases}$$

Classification Thm: All cyclic groups are isomorphic to

$\mathbb{Z}$ or $\mathbb{Z}/n\mathbb{Z}$ for some $n \in \mathbb{Z}_{\geq 1}$

(infinite) (finite cyclic)

These are examples of group presentations: (generators & relns)

$\mathbb{Z} = \langle g \rangle = \langle g \mid \text{only obvious rules } (g^0 = e,\ g^k g^l = g^{k+l}) \rangle$

usually omitted

$\mathbb{Z}/n\mathbb{Z} = \{ 0, \bar{1}, \bar{2}, \ldots, \bar{n} \} = \langle g \mid g^n = e \rangle$

$= \langle g \mid g^n \rangle$

(More next time)

$\boxed{\text{EXAMPLE: Quaternions}}$

Def: Quaternion group $\boxed{Q_8}$ has group presentation

$$\boxed{Q_8 = \langle \bar{e}, i, j, k \mid \bar{e}^2 = e,\ i^2 = j^2 = k^2 = ijk = \bar{e} \rangle}$$

Explicitly: Write $e = 1$ & $\bar{e} = -1$

Then $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$

Q: How to read this from the presentation?

- $-i := \bar{e}\, i = i\bar{e}$ ($\bar{e}$ & i commute since $i^2 = \bar{e}$)
- $(i)^{-1} = -i$ because $i^2 = -1$.
- $ij = k$ since $ijk = k^2 \implies ijkk^{-1} = k^2k^{-1}$

⇝ Cayley Table (multiplication Table) for Q_8 is:

Each entry $(\ )_{xy} = xy$

$x \backslash y$	1	i	j	k	-1	$-i$	$-j$	$-k$
1	1	i	j	k	-1	$-i$	$-j$	$-k$
i	i	-1	k	$-j$	$-i$	1	$-k$	j
j	j	$-k$	-1	i	$-j$	k	1	$-i$
k	k	j	$-i$	-1	$-k$	$-j$	i	1
-1	-1	$-i$	$-j$	$-k$	1	i	j	k
$-i$	$-i$	1	$-k$	j	i	-1	k	$-j$
$-j$	$-j$	k	1	$-i$	j	$-k$	-1	i
$-k$	$-k$	$-j$	i	1	k	j	$-i$	-1

HARD: Check assoc from table

Obs: Q_8 is non-abelian

Why? $ij = k$, $ji = -k$ & $k \neq -k$

Obs 2: Proper Subgroups of Q_8 are $\{\pm 1\}$, $\langle i \rangle$, $\langle j \rangle$, $\langle k \rangle$

(Idea: Any 2 symbols, say i, j, generate all Q_8)

$\langle i \rangle = \{\pm 1, \pm i\}$, etc.

Obs 3: These subgroups are normal subgps of Q_8

Pf/ ± 1 commute with all elements

$$g\langle i\rangle g^{-1} = \langle g i g^{-1}\rangle$$

- $g = j \rightsquigarrow j i j^{-1} = j i(-j) = (-k)(-j) = -i \in \langle i\rangle$
- $g = k \rightsquigarrow k i k^{-1} = k i(-k) = j(-k) = i \in \langle i\rangle$

Others follow from this because -1 is central (commutes with all other elements)

and $-g\langle i\rangle(-g)^{-1} = g\langle i\rangle g^{-1}$.

Conclusion: Q_8 is NOT abelian & all its subgroups are normal.

($\rightsquigarrow$ example of a Hamiltonian gp)