

Lecture 2 : Basics in 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 $\varphi: G \longrightarrow G'$ gp homomorphism
means $\varphi(a * b) = \varphi(a) * \varphi(b)$ ($\Rightarrow \varphi(e) = e'$
 $\varphi(x^{-1}) = \varphi(x)^{-1}$)

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 $\sigma: X \rightarrow X$

Group operation = composition of two maps

$$X \xrightarrow{\sigma} X \xrightarrow{\tau} X$$

$$\tau * \sigma := \tau \circ \sigma = \tau\sigma \quad (\text{usually we omit } \circ)$$

Ex.: ① S_n = permutations on n letters

② D_n = symmetries of n -gon

- More examples: $\mathbb{F}_n$ = free group on n letters

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

Group structure: $*$ = concatenation (+ cancellations)

e = empty word

Eg. $w_1 = a_2^{-2} a_1 a_2 a_1$

$w_2 = a_1^{-1} a_2$

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

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

Subgroups

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

(i) $e \in H$

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

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

(write: $H < G$)

(H inherits gp structure from G)

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

Key players = normal subgroups

Def: A subgroup $H < G$ is called normal 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?

Q: Subgroups from gp homomorphisms?

A: Yes (just as in Linear Algebra)

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

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

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

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

! $\text{Im } \varphi$ need not be normal

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

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

Pf/ (1) Claim 1 $\text{Ker}(\varphi) < G$

Need To check 3 properties:

$$(i) \quad a, b \in \text{Ker}(\varphi) : \varphi(ab) = \varphi(a) \varphi(b) = e' \cdot e' = e' \\ \Rightarrow a.b \in \text{Ker}(\varphi)$$

$$(ii) \quad \varphi(e) = e' \quad (\text{Lecture 1}) \Rightarrow e \in \text{Ker}(\varphi)$$

$$(iii) \quad a \in \text{Ker}(\varphi) \quad \varphi(a^{-1}) = \varphi(a)^{-1} = (e')^{-1} = e' \Rightarrow a^{-1} \in \text{Ker} \varphi$$

Lecture 1

$$\text{Claim 2} : b \in \text{Ker}(\varphi), \quad a \in G \Rightarrow a^{-1}ba \in \text{Ker} \varphi.$$

$$\text{Indeed: } \varphi(a^{-1}ba) = \varphi(a)^{-1} \underbrace{\varphi(b)}_{=e'} \varphi(a) = e' \quad \checkmark$$

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

More notation & definitions

- $\text{Hom}_{\text{Gps}}(G, G') = \text{Set of group homomorphisms } G \rightarrow G'$
- $\varphi \in \text{Hom}(G, G')$ is an isomorphism if $\exists \varphi' \in \text{Hom}(G', G)$
st $\varphi \circ \varphi' = \text{id}_{G'}$ & $\varphi' \circ \varphi = \text{id}_G$

Def: G & G' are isomorphic groups (write $G \cong G'$)
if $\exists \varphi \in \text{Hom}(G, G')$ isomorphism.

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

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 $x \sim y \Rightarrow x^{-1}y \in H \Rightarrow (x^{-1}y)^{-1} = y^{-1}x \in H \Rightarrow y \sim x$
 $\downarrow$
 $H \text{ subgp}$

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

• Transitive $x \sim y$ & $y \sim z \stackrel{?}{\Rightarrow} x \sim z$
 $\Rightarrow x^{-1}z = (x^{-1}y)(y^{-1}z) \in H \cdot H \subseteq H$
 $\downarrow$
 $H \text{ subgp.}$

□

Def : $\boxed{G/H}$ = set of equivalence classes in G with respect to $\sim$.
= left cosets (modulo H) = $\{xH \mid x \in G\}$

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

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

The natural projection $\pi: G \twoheadrightarrow G/H$ is a gp homomorphism
 $g \mapsto gH$
& $\text{Ker}(\pi) = H$

Explicitly : $g_1H \cdot g_2H := g_1g_2H$
 $e_{G/H} = 1 \cdot H$ & $(gH)^{-1} = g^{-1}H$

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

$$\boxed{g_1 \sim g'_1 \ \& \ g_2 \sim g'_2 \stackrel{?}{\Rightarrow} g_1 g_2 \sim g'_1 g'_2}$$

Indeed, $g_l \sim g'_l \Rightarrow g_l^{-1} g'_l \in H$
($l=1,2$) $g_2^{-1} g_2 \in H$ Want to show: $(g_1 g_2)^{-1} g'_1 g'_2 \in H$

$$(g_1 g_2)^{-1} g'_1 g'_2 = g_2^{-1} \underbrace{(g_1^{-1} g'_1)}_{\in H} g'_2 = g_2^{-1} \underbrace{(g_1^{-1} g'_1) g'_2}_{\in H} \underbrace{g_2^{-1} g_2}_{\in H} \in H$$

$\in H$ because $H \triangleleft G$

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

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

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, $\exists n \in \mathbb{Z}_{>0}$ st
 $N = n \cdot \mathbb{Z} = \{0, \pm n, \pm 2n, \dots\}$

Bf/. If $N = \{0\}$, then $n = 0 \checkmark$

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

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

$N \supseteq n\mathbb{Z} \checkmark$

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

Pick $k \in \mathbb{Z}_{>0}$ s.t. $k < \frac{m}{n} < k+1 \Rightarrow kn < m < (k+1)n$
 $\Rightarrow 0 < m - nk < n$ in N Contr!

□

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:

$$g^m = \begin{cases} \underbrace{g \cdots g}_{m \text{ times}} & \text{if } m > 0 \\ \underbrace{g^{-1} \cdots g^{-1}}_{(-m) \text{ times}} & \text{if } m < 0 \end{cases} \quad \rightarrow \text{also not unique}$$

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

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

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

(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 $H_1 \triangleleft G$ & $H_2 \triangleleft G$, then $H_1 \cap H_2 \triangleleft G$.

Proof: Easy & works for arbitrary intersections

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

Name: $\langle X \rangle$ subgroup generated by X .

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

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

Def: G is finitely-generated $\iff \exists$ finite $A \subset G$ with $\langle A \rangle = G$.

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

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

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

$\{ \text{---} \}$ is finite (B)

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

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

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

Claim: $g^n = e$ $\left[\begin{array}{l} \text{If not, } g^n = g^l \text{ for } 0 \leq l < n \\ \Rightarrow g^{n-l} = e \in \{e, g, \dots, g^{n-l-1}\} \text{ (contr.)} \end{array} \right]$

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

Classification Thm: All cyclic groups are isomorphic to

$$\begin{array}{ccc} \mathbb{Z} & \cong & \mathbb{Z}/n\mathbb{Z} \text{ for some } n \in \mathbb{Z}_{>0} \\ \text{(infinite)} & & \text{(finite cyclic)} \end{array}$$

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

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

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} = \{0, \bar{1}, \bar{2}, \dots, \bar{n}\} &= \langle g \mid g^n = \underline{e} \rangle \\ &= \langle g \mid g^n \rangle \end{aligned}$$

usually omitted

(More next time)

EXAMPLE: Quaternions

Def: Quaternion group Q_8 has group presentation

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

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

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

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 $ijk = k^2 \Rightarrow ijkk^{-1} = k^2k^{-1}$

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

Obs2: 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

± 1 commutes with all elements

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

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

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

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

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

Conclusion: Q_8 is nonabelian & all its subgroups are normal

($\Rightarrow$ example of a Hamiltonian gp)