Lecture # 14 - October 31^{st}, 2023

Axioms of Groups

Defn: A group G is a set along w/ a map $\bullet : G \times G \longrightarrow G$ st

1. (unital) $\exists\ e \in G$ st $\bullet(g,e) = g = \bullet(e,g)\ \forall g \in G$
2. (associative) $\bullet(a, \bullet(b,c)) = \bullet(a \bullet (b,c))$
3. (inverses) $\forall g \in G,\ \exists\ g^{-1}$ st $\bullet(g, g^{-1}) = e = \bullet(g^{-1}, g)$.

$\hookrightarrow$ Typically write $\bullet(g,h) = g \bullet h$ or gh

Denote G w/ $\bullet$ by $(G, \bullet)$

Ex:

1. $(\mathbb{R}^n, +)$
2. $(\mathbb{R}, \times)$ Not a group!
3. $(\mathbb{R} \setminus 0, \times)$
4. $(\mathbb{Z}, +)$
5. $(\mathbb{Z} \setminus 0, \times)$ Not a group!
6. $(M_{n,n}(\mathbb{R}), +)$
7. $(M_{n,n}(\mathbb{R}),$ matrix multiplication$)$ Not a group!
8. $(GL_n(\mathbb{R}),$ matrix multiplication$)$
9. $(S^1, \cdot)$ w/ $S^1 = \{ z \in \mathbb{C} \mid |z| = 1 \}$

Ex: Symmetric groups

S = set, $G = \{ f : S \to S \mid f = \text{bij} \}$ w/ $\bullet$ = fcn composition

$\hookrightarrow S = \{1, \dots, n\}$, $G = \Sigma_n$ = symmetric group on n-letters.

Ex: $\mathbb{Z}/n\mathbb{Z}$ w/ $\bullet = (a+b) \bmod n$

① $e = 0$

② Claim: $(a \bmod n) + b \bmod n = (a+b) \bmod n$

Pf: Write $a = i \cdot n + r$ w/ $0 \le r < n$

$b = j \cdot n + s$ w/ $0 \le s < n$

$r + s = k \cdot n + t$ w/ $0 \le t < n$

$(a \bmod n) + b \bmod n$

$= r + (j \cdot n + s) \bmod n$

$= (k+j) \cdot n + t \bmod n$

$= t$

$(a+b) \bmod n = ((i+j+k) \cdot n + t) \bmod n = t$ $\square$

So $((a+b) \bmod n + c) \bmod n$

$= (a+b+c) \bmod n$

$= (a + (b + c \bmod n) \bmod n)$

$\Rightarrow$ associative

③ $k \in \mathbb{Z}/n\mathbb{Z}$, $k^{-1} = -k + n \bmod n$

↳ Called cyclic group of order n.

Defn: A group G is abelian if $g \cdot h = h \cdot g$ $\forall g, h \in G$.

Question: Which of the above groups are abelian?

Lemma: $G = $ grp

① $hg = kg$ or $gh = gk \Rightarrow h = k$ (cancellation law)

② $g \cdot h = h$ or $h \cdot g = h \Rightarrow g = e$ (units are unique!)

Proof: ① $hg = kg \iff hgg^{-1} = k \cdot gg^{-1} \iff h \cdot e = k \cdot e \iff h = k$

② $gh = h \iff gh = eh \iff g = e$ $\square$

Product Groups

Defn: $G, H =$ grps, $G \times H$ becomes a grp w/ group law:

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 \cdot g_2, h_1 \cdot h_2)$$

↳ Check of axioms left to reader.

Subgroups

Defn: A subgroup of a grp G is a subset $H \subseteq G$ st

① $e \in H$

② $g \in H \Rightarrow g^{-1} \in H$

③ $g, h \in H \Rightarrow gh \in H$.

Lemma: A subgroup $H \subseteq G$ is a grp.

Proof: ③ $\Rightarrow$ $\cdot : G \times G \to G$ gives a map $H \times H \to H$.

The check of the axioms of H to be a group are left to reader. $\square$

Ex: ① Upper triangular matrices in $GL_n(\mathbb{R})$

② $SL_n(\mathbb{R}) \subseteq GL_n(\mathbb{R})$

③ $\{\exp(2\pi i/n)\} \subseteq S^1 \subseteq \mathbb{C}$ w/ multiplication

④ $\mathbb{Q} \subseteq \mathbb{R}$ w/ add. or $\mathbb{Q} - 0 \subseteq \mathbb{R}$ w/ mult.

⑤ $\left. \left\{ \begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix} \in GL_2(\mathbb{R}) \;\middle|\; a \in \mathbb{R} \right\} \subseteq GL_2(\mathbb{R}) \right\}$ Not subgroup!

Lemma: Every subgroup of $(\mathbb{Z}, +)$ is of the form

$$n \cdot \mathbb{Z} = \{ k \in \mathbb{Z} \mid k = i \cdot n \text{ for some } i \in \mathbb{Z} \}$$

Proof: Let $H \subseteq \mathbb{Z}$ be a subgroup.

$|H| = 1 \Rightarrow H = \{0\}$

$|H| \neq 1 \Rightarrow \exists$ minimal element $n \in \mathbb{Z}_{>0}$ st $n \in H$.

Spse $g \in H$ w/ $g > n$. Write $g = i \cdot n + r$ w/ $0 \leq r < n$.

$r = g - i \cdot n \in H \Rightarrow r = 0 \Rightarrow g = i \cdot n \in n \cdot \mathbb{Z}$.

If $g \in H$ w/ $g < 0 \Rightarrow -g \in H$ w/ $-g > 0 \Rightarrow -g = i \cdot n$ for some i

$\Rightarrow g = -i \cdot n \Rightarrow g \in n \cdot \mathbb{Z}$. $\square$

Defn: Given a subset $S \subseteq G$, the <u>subgroup generated</u> by S is the smallest subgroup of G that contains S, denote it $\langle S \rangle$.

↳ $\langle S \rangle$ = take all possible products of elements in S and take all those products's inverses.

Ex:

① $\langle n \rangle \subseteq (\mathbb{Z}, +)$, then $\langle n \rangle = n \cdot \mathbb{Z}$

② $\langle H \rangle \subseteq G$ w/ $H \subseteq G$ a subgroup, then $H = \langle H \rangle$.

③ $g \in G$, $\langle g \rangle = \{ g^n, g^{-n} \text{ for } n \in \mathbb{Z} \}$.

Ex: $a, b \in \mathbb{Z}$, $\langle a, b \rangle = \gcd(a,b) \cdot \mathbb{Z}$

↳ Set $d = \gcd(a,b)$.

$\exists\, r, s$ st $d \cdot r = a$, $d \cdot s = b \Rightarrow \langle a, b \rangle \subseteq d \cdot \mathbb{Z}$.

Euclid's algorithm $\Rightarrow d = r \cdot a + s \cdot b$ for some $r, s \in \mathbb{Z}$.

$\Rightarrow d \cdot \mathbb{Z} \subseteq \langle a, b \rangle$ $\square$

Group homomorphisms

Defn: G, G' = grps. A map $\varphi : G \to G'$ is a grp <u>homomorphism</u> if
$$\varphi(g \cdot h) = \varphi(g) \cdot \varphi(h)$$

Ex:

① $\det : GL_n(\mathbb{R}) \longrightarrow (\mathbb{R} \setminus 0, \times)$

② $\exp : (\mathbb{R}, +) \longrightarrow (\mathbb{R}, \times)$

③ $\varphi : (\mathbb{Z}, +) \to G$ w/ $\varphi(n) = g^n$ for some $g \in G$.

④ Inclusion of a subgrp $i : H \hookrightarrow G$.

⑤ $A \in M_{n,m}(\mathbb{R})$, $A : \mathbb{R}^m \longrightarrow \mathbb{R}^n$

⑥ $\mathbb{Z}/n \longrightarrow S^1$ by $j \mapsto \exp(2\pi i \cdot j/n)$

Lemma: $\varphi : G \to G'$ grp hom

① $\varphi(e) = e'$

② $\varphi(g^{-1}) = \varphi(g)^{-1}$

Proof:

① $\varphi(g) = \varphi(g \cdot e) = \varphi(g) \cdot \varphi(e) \Rightarrow \varphi(e) = e'$

② $e' = \varphi(e) = \varphi(g \cdot g^{-1}) = \varphi(g) \cdot \varphi(g^{-1}) \Rightarrow \varphi(g^{-1}) = \varphi(g)^{-1}$ $\square$

Defn: $\varphi : G \to G'$ grp hom

① $\mathrm{Im}(\varphi) = \{ g' \in G' \mid \exists\, g \in G \text{ w/ } \varphi(g) = g' \}$

② $\mathrm{Ker}(\varphi) = \{ g \in G \mid \varphi(g) = e' \}$

Lemma:

① $\mathrm{Im}(\varphi) \subseteq G'$ is a subgroup

② $\mathrm{Ker}(\varphi) \subseteq G$ is a subgroup

Proof: ① (i) $e' = \varphi(e) \in Im(\varphi)$

(ii) $\varphi(g) \cdot \varphi(h) = \varphi(gh) \in Im(\varphi)$

(iii) $\varphi(g)^{-1} = \varphi(g^{-1}) \in Im(\varphi)$

② (i) $\varphi(e) = e' \Rightarrow e \in Ker(\varphi)$

(ii) $g, h \in Ker(\varphi) \Rightarrow \varphi(gh) = \varphi(g) \cdot \varphi(h) = e' \Rightarrow gh \in Ker(\varphi)$

(iii) $g \in Ker(\varphi) \Rightarrow \varphi(g^{-1}) = \varphi(g)^{-1} = e' \Rightarrow g^{-1} \in Ker(\varphi)$. $\square$

Lemma: $\varphi: G \to G'$ is injective iff $Ker(\varphi) = \langle e \rangle$

Proof: $(\Rightarrow)$: $a \in Ker(\varphi) \Rightarrow \varphi(a) = e' = \varphi(e) \Rightarrow a = e$.

$(\Leftarrow)$: $\varphi(a) = \varphi(b) \Rightarrow e' = \varphi(a) \cdot \varphi(b)^{-1} = \varphi(a) \cdot \varphi(b^{-1}) = \varphi(a \cdot b^{-1})$

$\Rightarrow a \cdot b^{-1} \in Ker(\varphi)$

$\Rightarrow a \cdot b^{-1} = e$

$\Rightarrow a = b$ $\square$