# Lecture 2 Groups §4 Fraleigh.

Recall: A binary structure $(S, *)$ is a set $S$ with binary operation $*: S \times S \to S$ $\quad *(a,b) =: a * b$.

Def 4.1 A group $(G, *)$ is a binary structure such that.

$\boxed{G1}$: $*$ is associative

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

$\boxed{G2}$: Identity element

$$\exists\, e \in G \text{ s.t. } \forall\, a \in G \quad e*a = a*e = a.$$

$\boxed{G3}$: Inverse elements Say "$a'$ is the inverse of $a$ in $G$".

$$\forall\, a \in G \quad \exists\, a' \in G \text{ s.t. } a*a' = a'*a = e.$$

## Examples

1) $G = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are groups under $* = +$

G1 $+$ is associative

G2 $e = 0$

G3 $a \in G$ $a' = -a$
$a + (-a) = (-a) + a = 0$

2) $\bullet$ $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ with $* = \cdot$

G1 $\cdot$ is associative

G2 $e = 1$ is identity

G3 but $0 \in \mathbb{Q}, \mathbb{R}, \mathbb{C}$ has no inverse $\times$

NOT A GROUP.

$\bullet$ $\mathbb{Q}^\times, \mathbb{R}^\times, \mathbb{C}^\times$ with $* = \cdot$ is a group.

$\mathbb{Q}^\times = \mathbb{Q} \setminus 0$, $\mathbb{R}^\times = \mathbb{R} \setminus 0$, $\mathbb{C}^\times = \mathbb{C} \setminus 0$.

$\bullet$ $\mathbb{Q}^+, \mathbb{R}^+$ with $* = \cdot$ is a group. (foreshadow: this is a subgroup of $(\mathbb{Q}^\times, \cdot)$)

$\mathbb{Q}^+ = \{x \in \mathbb{Q} \mid x > 0\}$

3) $U = \{z \in \mathbb{C} \mid |z| = 1\} \subseteq \mathbb{C}$ $* = \cdot$ is a (sub) group of $\mathbb{C}$.

**Ques** Does $\mathrm{Mat}_n(\mathbb{R})$ ($n \times n$ matrices) with $* = \cdot$ form a group?

Answer $(Mat_n(\mathbb{R}), \cdot)$ is a binary structure ✓

G1 $\cdot$ is associative (recall from lin alg). ✓

G2 $e = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$ nxn identity matrix satisfies $e \cdot A = A \cdot e = A$ $\forall A \in Mat_n(\mathbb{R})$ ✓

G3 if $A \in Mat_n(\mathbb{R})$ has $\det(A) = 0$ then $A$ has no multiplicative inverse! Hence $(Mat_n(\mathbb{R}), \cdot)$ is not a group. ✗

Example The general linear group of size $n$, with entries in $\mathbb{R}$.

$GL_n(\mathbb{R}) = \{ A \in Mat_n(\mathbb{R}) \mid \det A \neq 0 \}$ with $* = \cdot$ is a group.

# Elementary Properties of Groups §4

**Def 4.3** A group $(G, *)$ is <u>abelian</u> if its binary operation is commutative.

pg 39 for a historical note on Abel.

$$\forall\, a, b \in G \qquad a * b = b * a$$

**Example** 1) $(G, +)$ with $G = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, or $\mathbb{C}$ is abelian.

2) $(G, \cdot)$ with $G = \mathbb{Q}^\times, \mathbb{R}^\times$ or $\mathbb{C}^\times$ is abelian.

3) $GL_n(\mathbb{R})$ is <u>not</u> <u>abelian</u>

$n = 2$. If $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ $B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ $AB \neq BA$.

Proofs from the axioms

**Thm 4.15** Left and right cancellation laws hold in a group:

$\forall\ a, b, c \in G$

$$a * b = a * c \Rightarrow b = c$$ left can.

$$b * a = c * a \Rightarrow b = c$$ right can.

⚠ If gp is not abelian left + right really matter!

**Proof** By G3 $\exists\ a' \in G$ s.t. $a' * a = e$.

Suppose $$a * b = a * c$$

then $$a' * (a * b) = a' * (a * c)$$

by G1 $$(a' * a) * b = (a' * a) * c$$

by G3 $$e * b = e * c$$

by G2 $$b = c \qquad \square$$

**Thm 4.16** (Solving equations in groups)

Let $(G, *)$ be a group and $a, b \in G$. Then

$a * x = b$ and $y * a = b$ have unique

solutions for $x$ and $y$, respectively. ("linear equations")

**Proof** Consider $a * x = b$, let $a' \in G$ be inverse of a $\boxed{G3}$

Then $a' * (a * x) = a' * b$

$\underline{G1} \Rightarrow (a' * a) * x = a' * b$

$\underline{G3} \Rightarrow e * x = a' * b.$

$\underline{G2} \Rightarrow x = a' * b \in G.$

See text for a slightly different proof.

Therefore, $x = a' * b$ is the unique solution $\square$

**Thm 4.17** Let $(G, *)$ be a group

1) The identity element of $G$ is unique

2) Every $a \in G$ has a unique inverse element.

**Proof** 1) Suppose $\exists$ $e, e' \in G$ both satisfying G2.

Then $e * e' = e$ and $e * e = e$

$$e * (e * e') = e * e \overset{G1, G2}{\Longrightarrow} e' = e.$$

2) Suppose $\exists$ $a', a'' \in G$ satisfy G3 for $a$. Then

$\cancel{a} * a' = e = \cancel{a} * a''$ apply cancellation from

Thm 4.15 $\Rightarrow$ $a' = a''$ Hence inverses are unique $\square$

**Corollary 4.18** ⊛ Let $(G, *)$ be a group. $\forall a, b \in G$.

$$(a * b)' = b' * a'$$

inverse of $(a*b)$

Recall for invertible matrices: $(AB)^{-1} = B^{-1}A^{-1}$

**Proof** Exercise remember to check two sides of the inverse (however this is not nessary see p. 43).

## Chapter 3

Exercises

## Chapter 4

Exercises