Lecture 8: Groups, more examples.

Last time, we defined groups.

Def: A group is a pair $(G, *)$ where S is a set and $* : G \times G \to G$ is a binary operation such that:

(1) $*$ is associative, i.e
$\forall x, y, z \in G, \quad x * (y * z) = (x * y) * z$

(2) there is an (identity) element $e \in G$ s.t.
$\forall x \in G, \quad x * e = e * x = x$

(3) For every $x \in G$, there is an inverse $x^{-1} \in G$, i.e.
$\forall x \in G, \exists\, x^{-1} \in G$ s.t $\quad x * x^{-1} = x^{-1} * x = e$.

Examples:

(1) from last time: $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, ... but not $(\mathbb{N}, +)$
$(\mathbb{R} \setminus 0, \cdot)$, $(\mathbb{C} \setminus 0, \cdot)$, $(\mathbb{Q} \setminus 0, \cdot)$ but not $(\mathbb{Z} \setminus 0, \cdot)$

(2) $\left(\mathbb{Z}/_{n\mathbb{Z}}, +\right) = \left(\{\bar{0}, \bar{1}, \dots, \overline{n-1}\}, +\right)$ is a group.

(3) Let $\zeta = e^{i\frac{2\pi}{n}}$, $U_n = \{1, \zeta, \zeta^2, \dots, \zeta^{n-1}\}$.
with multiplication operation is a group.

(4) $U = \{e^{i\theta} \mid \theta \in \mathbb{R}\} \subset \mathbb{C}$
$(U, \cdot)$ is a group.

↑ all these examples are abelian.

Def: $(G, *)$ is called Abelian if $*$ is commutative
i.e. $\forall x, y \in G, \quad x * y = y * x$

more examples:

(5) $(\mathbb{R}^n, +)$, $(\mathbb{C}^n, +)$, $(\{f : \mathbb{R} \to \mathbb{R}\}, +)$ ← all functions $\mathbb{R} \to \mathbb{R}$; + ← function addition.

(any vector space with vector addition is a group.

(6) $M_n(\mathbb{R}) =$ $n \times n$ matrices.

$(M_n(\mathbb{R}), +)$ is group. $\quad e = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ \vdots & & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$

(7) $(M_n(\mathbb{R}), \cdot)$ is <u>not</u> a group because the zero-matrix doesn't have an inverse.

$\cdot$ ← matrix multiplication

(When does a matrix have an inverse? To have an inverse, it must have no kernel. $\dim \operatorname{Ker} A = 0$.

rank-nullity theorem says: $\dim \operatorname{Ker} A + \dim \operatorname{Range} A = n$

so it must have full range and no kernel.

<u>Theorem</u>: The following are equivalent for $A \in M_n(\mathbb{R})$ $n \times n$

FROM LINEAR ALGEBRA

(1) A is invertible (non-singular)

(2) $\operatorname{Ker} A = \{0\}$ $\quad (\dim \operatorname{Ker} A =: \operatorname{null} A = 0)$

(3) $\operatorname{Range}(A) = \mathbb{R}^n$ $\quad (\operatorname{rank} A = \dim \operatorname{Range} A = n)$

(4) $\det A \neq 0$.)

(8) $(GL_n(\mathbb{R}), \cdot)$ is a group.

$$GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid A \text{ is invertible } (\det A \neq 0)\}$$

Let's check that in detail.

We need to check:

(1) $\cdot$ is a binary operation on $GL_n(\mathbb{R})$.

ie $\cdot : GL_n(\mathbb{R}) \times GL_n(\mathbb{R}) \longrightarrow GL_n(\mathbb{R})$

ie. if we multiply two invertible matrices, the product is invertible.

Indeed: $\det(AB) = \det A \det B$

so if $\det A \neq 0$, $\det B \neq 0$, $\det(AB) \neq 0$.

So AB is invertible. {in other words, $\cdot$ is "closed" on $GL_n(\mathbb{R})$}

(2) matrix multiplication is associative.
(we already know this from a few lectures ago)

(3) there is an identity element. $e = I_n$, $\forall A \in GL_n(\mathbb{R})$

$$I_n A = A I_n = A.$$

(4) Inverses: $AA^{-1} = A^{-1}A = I$

A^{-1} is the matrix inverse.

$GL_n(\mathbb{R})$ is not abelian.