Chapter 2

Groups

Beginning of Jan. 29, 2021

2.1 What is a Group?

Definition 2.1.1

A **group** $(G, \cdot)$ is a non-empty set G with a binary operation $\cdot : (a, b) \mapsto a \cdot b$ from $G \times G$ to G satisfying

(1) associative law: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in G$,

(2) identity: $\exists\, e \in G$ such that $a \cdot e = e \cdot a = a$ for all $a \in G$, and

(3) given $a \in G$, there exists $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

If in addition $a \cdot b = b \cdot a$ then G is **commutative** or **Abelian**. The fact that $a, b \in G \implies a \cdot b \in G$ is callused **closure**. Sometimes we omit the $\cdot$ and simply write ab.

Some examples and nonexamples of groups:

(1) $(\mathbb{Z}, +)$ is a group with identity 0 and $x^{-1} := -x$.

(2) $(\mathbb{Z} \setminus \{0\}, +)$ is *not* a group since there's no additive identity.

(3) $(\mathbb{Z}, \times)$ is *not* a group since some elements don't have inverse.

(4) $(\mathbb{Q} \setminus \{0\}, \times)$ is a group with identity 1 and inverse $x^{-1} := 1/x$.

(5) $(\mathrm{GL}_2(\mathbb{R}), \cdot)$ is a group, where $\mathrm{GL}_2(\mathbb{R})$ (General Linear group) denotes the set of all *invertible* 2-by-2 real matrices and $\cdot$ is the normal matrix multiplication.

Proof.

(1) Closure: $\det(A)\det(B) = \det(AB)$ and so AB is invertible. It's trivial that the entries are also real, so $AB \in \mathrm{GL}_2(\mathbb{R})$.

(2) Associativity: matrix multiplications are already associative.

(3) Existence of identity: $I_{2\times 2}$.

(4) Existence of inverse: $(AB)^{-1} = B^{-1}A^{-1} \in \mathrm{GL}_2(\mathbb{R})$.

□

(6) $(\mathrm{GL}_n(\mathbb{R}), \cdot)$ is a group.

(7) $(\mathrm{SL}_n(\mathbb{R}), \cdot)$ is a group where $\mathrm{SL}_2(\mathbb{R})$ is the set of n-by-n matrices with determinants 1.

(8) $(O_n(\mathbb{R}), \cdot)$ is a group where $O_n(\mathbb{R}) \subset \mathrm{GL}_n(\mathbb{R})$ denotes all n-by-n symmetric, invertible matrices.

Definition 2.1.2

For $n \in \mathbb{Z}^+$, the **symmetric group** S_n is the group of **permutations** of n objects, i.e., the set of bijective functions from $\{1, 2, \ldots, n\}$ to $\{1, 2, \ldots, n\}$.

Proof that S_n is a group.

(1) Closure: pick $\sigma, \tau \in S_n$. Since the composition of bijections is bijective, we see that $\sigma \circ \tau$ is by definition another permutation of n elements.

(2) Associativity: this follows from the fact that composition of functions functions are associative.

(3) Existence of identity: the identity map $\begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$.

(4) Existence of inverse: the inverse σ^{-1} of bijective σ exists.

□