Group Theory

Alec Zabel-Mena

Text

Herstein (1965). Topics in Algebra. Blaisdel Publishing Co.

February 24, 2021

Chapter 1

Classical Algebra.

1.1 Definitions and Examples

Definition. We call a nonempty set G a **group** under a binary operation $\cdot$ if the following hold:

(1) $a, b \in G$ implies $a \cdot b \in G$.

(2) For all $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(3) There is an element $e \in G$, called the **identity element** such that $a \cdot e = e \cdot a = a$, for all $a \in G$.

(4) For all $a \in G$, there is a corresponding element a^{-1}, called the **inverse element** of a, such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

We call G **abelian** (or **commutative**) if $a \cdot b = b \cdot a$, for all $a, b \in G$. We call $|G|$ the **order** of G and denote it $\operatorname{ord} G$.

Example 1.1. (1) Let S be an n element set, and let S_n be the set of all $1-1$ mappings of S onto itself (i.e all permutations of elements of S). Then S_n forms a group over function composition $\circ$.

Indeed, whenever $f, g \in S_n$, $f \circ g \in S_n$, likewise, $f \circ (g \circ h) = (f \circ g) \circ h$. The identity map $i : S \to S$ defined by the rule $i : s \to s$ serves as the identity element; $f \circ i = i \circ f = f$. Finally since whenever $f \in G$, f is $1-1$ andd onto, f^{-1} exists and is also $1-1$ and onto; moreover $f \circ f^{-1} = f^{-1} \circ f = i$, so f^{-1} is the inverse of f. It is also easy to see that $\operatorname{ord} S_n = n!$. It is worth noting that S_n is not ingeneral commutative, as $f \circ g \neq g \circ f$.

(2) The integers $\mathbb{Z}$ form a group over $+$ (the usual addition), but not over $\cdot$ (the usual multiplication). The rationals $\mathbb{Q}$ do form a group under $\cdot$. The reals $\mathbb{R}$ and the complex numbers $\mathbb{C}$ form abelian groups under both $+$ and $\cdot$.

(3) Let $G = \{-1, 1\}$m then $(G, \cdot)$ forms a group of order 2, where $\cdot$ is the usual multiplication.

(4) By example 1, we have that S_3 forms a group of order $3! = 6$. Now consider the maps $\phi : 1 \to 2, 2 \to 3, 3 \to 3$ and $\psi : 1 \to 3, 2 \to 3, 3 \to 1$. We can check that $\phi^2 = \psi^3 = i$, also notice that $\phi\psi : 1 \to 2, 2 \to 2, 3 \to 1$ and $\psi\phi : 1 \to 1, 2 \to 3, 3 \to 2$, so $\phi\psi \neq \psi\phi$. Likewise we also have $\psi^2 = \psi\psi : 1 \to 2, 2 \to 1, 3 \to 2$ and $\psi^{-1}\phi : 1 \to 3, 2 \to 2, 3 \to 1$. Indeed, in S_3, $\phi\psi = \psi^{-1}\phi$; it turns out that S_3 is a special case of a more general group.

(5) $\mathbb{Z}/n\mathbb{Z}$ forms an abelian group under $+$ (addition $\mod n$), and that $U(\mathbb{Z}/n\mathbb{Z})$ forms a group under $\cdot$ (multiplication $\mod n$).

(6) If we take $(G, \cdot)$ and $(H, *)$ to be groups, and consider their product $G \times H$, define the binary operation $\times$ by taking $(a, b) \times (c, d) = (a \cdot c, b * d)$, where $a, c \in G$ and $b, d \in H$, then $(g \times H, \times)$ forms a group.

Definition. We say a group G is **cyclic** if for some $g \in G$, $G = \{g^i : i \in \mathbb{Z}\}$. We call g the **generator** of G and write $G = (g)$.