

## CONTENTS

|                             |   |
|-----------------------------|---|
| 1. Review .....             | 1 |
| 2. Examples .....           | 1 |
| 3. Subgroups.....           | 2 |
| 4. Permutation Groups ..... | 3 |

## 1. REVIEW

Recall that a group is a triple  $(G, \cdot, e)$  consisting of a set  $G$ , a composition law  $\cdot$ , and an identity element  $e$ . Depending on the context, the identity may also be denoted by  $1$ ,  $e_G$ , or  $1_G$ .

We also defined, for each  $x \in G$ , the cyclic subgroup  $\langle x \rangle$ , which consists of all powers (positive, negative, and zero) of  $x$ . The cardinality of  $\langle x \rangle$  is also called the order of  $x$  (and it can be infinite).

Let us now turn to examples.

## 2. EXAMPLES

**Example 2.1** (The integers under addition). The triple

$$(\mathbb{Z}, +, 0) \tag{2.1}$$

is a group. Its composition law is

$$\mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}, \quad (m, n) \longmapsto m + n. \tag{2.2}$$

The identity element is  $0$ , and the inverse of  $m$  is  $-m$ .

**Example 2.2** (The integers under multiplication: a non-example). The triple

$$(\mathbb{Z}, \times, 1) \tag{2.3}$$

is *not* a group, although it is a semigroup. Multiplication is associative and  $1$  is an identity, so axioms **(1)** and **(2)** hold. Axiom **(3)** fails because most integers do not have multiplicative inverses in  $\mathbb{Z}$ .

**Example 2.3** (Integers modulo  $n$ ). Let  $n$  be a positive integer. The set of residue classes modulo  $n$  is

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}. \tag{2.4}$$

For example,

$$\begin{aligned} \bar{0} &= \{0, \pm n, \pm 2n, \pm 3n, \dots\}, \\ \bar{1} &= \{1, 1 \pm n, 1 \pm 2n, 1 \pm 3n, \dots\}. \end{aligned}$$

Every integer can be written  $m = an + r$  with  $0 \leq r < n$ , and then  $\overline{m} = \overline{r}$ . Addition is defined by

$$\overline{m} + \overline{\ell} = \overline{m + \ell}. \quad (2.5)$$

Thus

$$(\mathbb{Z}/n\mathbb{Z}, +, \overline{0}) \quad (2.6)$$

is a group, called the *cyclic group of order  $n$* .

In the preceding examples that are groups, the group operation is both associative and commutative.

**Example 2.4** (The general linear group). The set

$$\mathrm{GL}_n(\mathbb{R}) = \{A : A \text{ is an invertible } n \times n \text{ matrix with entries in } \mathbb{R}\} \quad (2.7)$$

is a group under matrix multiplication. Its identity is the identity matrix

$$I_n = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}. \quad (2.8)$$

Thus the group is written  $(\mathrm{GL}_n(\mathbb{R}), \cdot, I_n)$ , and the composition law sends  $(A, B)$  to  $AB$ . Note that the group  $\mathrm{GL}_n(\mathbb{R})$  carries additional geometric structure: it is a topological space, a differentiable manifold, and a real algebraic group. In particular, it is a *Lie group*.

**Example 2.5** (The special linear group). Consider the following subset of the previous example:

$$\mathrm{SL}_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : \det(A) = 1\}. \quad (2.9)$$

It is a group under matrix multiplication. Indeed,  $I_n \in \mathrm{SL}_n(\mathbb{R})$ , and if  $A, B \in \mathrm{SL}_n(\mathbb{R})$ , then

$$\det(AB) = \det(A)\det(B) = 1, \quad (2.10)$$

so  $AB \in \mathrm{SL}_n(\mathbb{R})$ . Moreover,

$$\det(A^{-1}) = \det(A)^{-1} = 1, \quad (2.11)$$

so  $A^{-1} \in \mathrm{SL}_n(\mathbb{R})$ . Associativity is inherited from matrix multiplication. Thus  $(\mathrm{SL}_n(\mathbb{R}), \cdot, I_n)$  is a group.

### 3. SUBGROUPS

**Definition 3.1** (Subgroup). Let  $(G, \cdot, e)$  be a group. A subset  $H \subseteq G$  is called a *subgroup* of  $G$  if  $H$ , under the restriction of the operation on  $G$ , is itself a group.

Not all subsets are groups. For example, the subset  $\{0, 3\} \subset \mathbb{Z}$  is not a group under addition, since it is not closed under addition.

**Proposition 3.1.** Let  $(G, \cdot, e)$  be a group, and let  $H \subseteq G$  be a subset satisfying the following conditions:

(1)  $e \in H$ .

(2)  $H$  is closed under the group operation: if  $h_1, h_2 \in H$ , then

$$h_1 \cdot h_2 \in H. \quad (3.1)$$

(3)  $H$  is closed under inverses: if  $h \in H$ , then

$$h^{-1} \in H. \quad (3.2)$$

Then  $H$  is a subgroup of  $G$ .

*Proof.* The operation on  $H$  is the restriction of the operation on  $G$ . Associativity is therefore inherited from  $G$ , so it does not need to be checked separately. By condition (2)  $H$  is closed under this operation, and since  $e$  is an identity in  $G$ , it also satisfies the identity property of  $H$ . Finally, condition (3) ensures that the inverse in  $G$  of every element of  $H$  also belongs to  $H$ .  $\square$

*Remark.* Suppose  $H \subseteq G$  is finite. If  $e \in H$  and  $H$  is closed under the group operation, then  $H$  is automatically closed under inverses. To see this, fix  $h \in H$  and consider the map

$$L_h: H \longrightarrow H, \quad x \longmapsto hx. \quad (3.3)$$

This map is well-defined because  $H$  is closed under the group operation. It is injective: if  $hx = hy$ , then multiplying on the left by  $h^{-1}$  in  $G$  gives  $x = y$ . Since  $H$  is finite,  $L_h$  is therefore surjective. Because  $e \in H$ , there exists  $y \in H$  such that  $hy = e$ . By uniqueness of inverses in  $G$ , we have  $y = h^{-1}$ . Hence  $h^{-1} \in H$ .

*Exercise 3.1.* This shows that for every  $h \in H$  there exists  $g$  such that  $hg = e$ , so  $g$  is a right inverse. Why is  $g$  also a left inverse?

#### 4. PERMUTATION GROUPS

Next we turn to a very important class of finite groups, the so-called permutation groups. You have probably seen these before, but I want to reintroduce the notation. Let

$$[n] := \{1, 2, \dots, n\}. \quad (4.1)$$

A permutation of  $[n]$  is a bijection  $p: [n] \rightarrow [n]$ . It may be displayed in two-line notation as

$$p = \begin{pmatrix} 1 & 2 & \cdots & n \\ p(1) & p(2) & \cdots & p(n) \end{pmatrix}. \quad (4.2)$$

If  $p$  and  $q$  are permutations, we use the convention

$$qp = q \circ p; \quad (4.3)$$

thus the rightmost permutation is applied first. Let us also note that if  $p$  is a permutation, we write  $p^{-1}$  for the inverse permutation; that is, if  $p(i) = k$ , then  $p^{-1}(k) = i$ . One can check that

$$pp^{-1} = p^{-1}p = \text{id}, \quad (4.4)$$

where  $\text{id}$  is the identity permutation.

Let  $S_n$  denote the set of all permutations of  $[n]$ .

**Proposition 4.1.** *The triple  $(S_n, \circ, \text{id})$  is a group.*

*Proof.* The composite of two bijections is again a bijection, so  $S_n$  is closed under composition. Composition of functions is associative, the identity map  $\text{id}$  is the identity element, and the inverse of a bijection is again a bijection. Hence all the group axioms hold.  $\square$