1. Introduction to Group Theory

Definition 1.1. A **group** is a pair $(G, \cdot)$ where G is a set and $\cdot$ is a binary operation on G such that

(i) for all $a, b, c \in G$, it holds $(a \cdot b) \cdot c = a \cdot (b \cdot c)$,

(ii) there is $e \in G$ for all $a \in G$ such that $e \cdot a = a \cdot e = a$, and

(iii) for all $a \in G$, there is $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Instead of saying $(G, \cdot)$ is a group, we say *G is a group under $\cdot$*. If the operation is understood from the context, we simply say G is a group.

We will study various types of groups. Let's begin with one of the most basic. An **Abelian group** is a group $(G, \cdot)$ with the aditional property that

$$a \cdot b = b \cdot a$$

for all $a, b \in G$. In this case, we use $+$ insted of $\cdot$ for the binary operation of the group, and denote its identity by 0. A finite group is a a group where the underlying set is finite.

Example 1. (i) Some Abelian groups: $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Z}/n\mathbb{Z}, +)$

(ii) More Abelian groups: $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$. Why do we choose to use $\cdot$ instead of $+$ in this case?

(iii) $((\mathbb{Z}/n\mathbb{Z})^\times, +)$ is not a group.

(iv) Let $(A, \bullet)$ and $(B, \circ)$ be groups. Then the set

$$A \times B = \{(a, b) \mid a \in a, b \in B\}$$

is a group under the operation defined by the rule

$$(a, b) \cdot (c, d) = (a \bullet c, b \circ d).$$

What is the identity of this group? How are inverses defined?

Proposition 1.2. *Suppose $(G, \cdot)$ is a group. Then*

(i) the identity of G is unique

(ii) For any $a \in G$, its inverse a^{-1} is unique.

(iii) For any $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$

(iv) Finite products are well-defined.

Proof. (i) If both e and f are identities of G, then $e = ef = f$. The first equality is due to the fact because f is identity, the second because e is also an identity.

(ii) Let $a \in G$. If both b and c are inverses of a, then

$$b = be = b(ac) = (ba)c = ec = c.$$

(iii) Classwork.

(iv) Classwork.

□

Notation. Let x be any element of a group. The product of x with itself n times is denoted x^n. The product of x^{-1} with itself n times is denoted x^{-n}. We define $x^0 = e$. If the group is Abelian, we write nx instead of x^n and $-nx$ instead of x^{-n}. Also, $0x = 0$.

Remark 1.2.1. For an Abelian group we denote $e = 0$, and, for a nonAbelian group, $e = 1$. When not mentioned, we denote the identity of a group by 1.

Proposition 1.3. *Let G be a group and let $a, b \in G$. The left and right cancellation laws hold in G, that is, for any $u, v \in G$ it holds*

(i) if $au = av$, then $u = v$, and

(ii) if $ub = vb$, then $u = v$.

Proof. Exercise. □

Definition 1.4. Let G be a group and $x \in G$. The **order** of x is

$$\min\left\{n \in \mathbb{Z}^+ \mid x^n = 1\right\},$$

provided it exists. If no such integer exists, the order of x is defined to be infinity. We denote the order of x by $|x|$.

Remark 1.4.1. This notation must not be regarded as an absolute value. The use of the bars should cause no problem because it is used in a different context.

Exercise 1. Compute $|\overline{6}|$ in $\mathbb{Z}/9\mathbb{Z}$ and $|\overline{2}|$ in $(\mathbb{Z}/7\mathbb{Z})^\times$.