Group Theory

Lecture Notes by Lorenz Halbeisen

http://user.math.uzh.ch/halbeisen/4students/gt.html

0. Introduction

A theory of groups first began to take form at the end of the eighteenth century. It developed slowly and attracted very little notice during the first decades of the nineteenth century. Then, in a few years around 1830, the theory of groups took a giant leap forward and made a major contribution to the general development of mathematics in the work of Galois and Abel on the solvability of algebraic equations.

Since then, the concepts underlying the theory of groups have been elaborated and extended into many branches of mathematics. There have been applications to such diverse fields as number theory, crystallography, and the theory of knots.

This module is mainly concerned with finite groups, especially the groups of rigid motions of the five Platonic solids, which are tetrahedron, cube, octahedron, dodecahedron, and icosahedron. But our first task is to clarify what is meant by a group.

Let us consider two different sets, each with a binary operation: The first set is $\mathbb{Z} := \{\ldots, -2, -1, 0, 1, 2, \ldots\}$, the set of integers, and the binary operation on $\mathbb{Z}$ is addition.

The second set is the set of non-zero rational numbers $\mathbb{Q}^* := \mathbb{Q} \setminus \{0\}$, where $\mathbb{Q} := \big\{n/m : n \in \mathbb{Z} \wedge m \in \mathbb{Z} \setminus \{0\}\big\}$, and the binary operation on $\mathbb{Q}^*$ is multiplication.

Thus, we have two so-called *structures*, which we denote by $(\mathbb{Z}, +)$ and $(\mathbb{Q}^*, \cdot\,)$ respectively.

In $\mathbb{Z}$, there is an element x such that for each $y \in \mathbb{Z}$ we have $x + y = y + x = y$, namely $x = 0$. Such an element we call a **neutral element**. Hence, we get:

Observation 1. $(\mathbb{Z}, +)$ has a neutral element.

Similarly, in $\mathbb{Q}^*$, there is an element x such that for each $y \in \mathbb{Q}^*$ we have $x \cdot y = y \cdot x = y$, namely $x = 1$. Hence, we get:

Observation 2. $(\mathbb{Q}^*, \cdot\,)$ has a neutral element.

Are there some neutral elements in $(\mathbb{Z}, +)$ other than 0, or are there some neutral elements in $(\mathbb{Q}^*, \cdot\,)$ other than 1 ?

No, of course, you would say, but why not? Let us prove it for the structure $(\mathbb{Z}, +)$: Assume that $z \in \mathbb{Z}$ is a neutral element. So, for any $y \in \mathbb{Z}$ we have $z+y = y+z = y$. In particular we get $z+0 = 0+z = 0$, but since 0 is neutral, we also have $z+0 = 0+z = z$, hence, $z = 0$. This proves the following:

Observation 3. $(\mathbb{Z}, +)$ has exactly one neutral element, namely 0.

Similarly, one can prove the following (see Hw1.Q1a):

Observation 4. $(\mathbb{Q}^*, \cdot\,)$ has exactly one neutral element, namely 1.

For every $x \in \mathbb{Z}$ there is a $y \in \mathbb{Z}$ such that $x + y = y + x = 0$, in fact, $y = -x$. Such a y is called an **inverse** of x.

Observation 5. In $(\mathbb{Z}, +)$, each element has an inverse.

Notice that this is not true in $(\mathbb{N}, +)$, where $\mathbb{N} = \{0, 1, 2, \ldots\}$. Why ?

Similarly, for every $q \in \mathbb{Q}^*$ there is a $p \in \mathbb{Q}^*$ such that $q \cdot p = p \cdot q = 1$, in fact, $q = 1/p$. Hence, we get:

Observation 6. In $(\mathbb{Q}^*, \cdot\,)$, each element has an inverse.

Notice that this is not true in $(\mathbb{Q}, \cdot\,)$. Why?

Is there more than one inverse element to some $x \in \mathbb{Z}$, or is there more than one inverse element to some $q \in \mathbb{Q}^*$?

No, of course, you would say again, but why not? Let us prove it for the structure $(\mathbb{Z}, +)$: Assume that there are $y_1, y_2 \in \mathbb{Z}$ such that $x + y_1 = y_1 + x = 0$ and $x + y_2 = y_2 + x = 0$. Therefore we have

$$\begin{aligned} y_2 + x &= 0 && \text{add } y_1 \text{ on both sides from the right} \\ y_2 + \underbrace{x + y_1}_{=0} &= \underbrace{0 + y_1}_{=y_1} \\ \underbrace{y_2 + 0}_{=y_2} &= y_1 && \text{and we finally get} \\ y_2 &= y_1 \end{aligned}$$

This proves the following:

Observation 7. In $(\mathbb{Z}, +)$, each element has exactly one inverse.

In a similar way, one can prove the following (see Hw1.Q1b):

Observation 8. In $(\mathbb{Q}^*, \cdot\,)$, each element has exactly one inverse.

As we have seen so far, $(\mathbb{Z}, +)$ and $(\mathbb{Q}^*, \cdot\,)$ are very similar: Both structures have a unique neutral element and in both structures there are inverse elements. In fact, such structures, *i.e.*, sets with a binary operation satisfying certain axioms, are called *groups*.

In this module we will investigate different types of (mainly finite) groups. In other words, we will set up the axioms for groups and look what we get out of them. It will be seen that the input (just three axioms) is small, but the output (dozens of theorems and propositions) is quite extensive.