Groups, Rings, and Fields

DHW-GRF Expository Notes

Michael Middlezong

1 October 2024

§1 Groups

Groups are a fundamental structure in abstract algebra, and they can be thought of as representing the structure of the symmetries of an object.

Example 1.1

For example, the rotational and reflectional symmetries of a square form the group called D_4.

Groups have certain properties that make them so fundamental, leading us to the definition of a group.

Definition 1.2. A **group** is a set G with a binary operation $\star\colon G \times G \to G$, satisfying the following properties:

1. **Closure:** For all $a, b \in G$, $a \star b \in G$. This is implied by the term "binary operation."
2. **Associativity:** For all $a, b, c \in G$,
$$(a \star b) \star c = a \star (b \star c).$$
This is another property of the operation itself.
3. **Existence of an identity:** There exists an element $e \in G$ such that for all $g \in G$:
$$e \star g = g \star e = g.$$
4. **Existence of inverses:** Every element must have an inverse. Precisely, for every element $g \in G$, there exists an element $h \in G$, which we call the inverse of g, satisfying
$$h \star g = g \star h = e,$$
where e is an identity element.

Sometimes, a group is referred to with the operation attached to it, like $(\mathbb{Z}, +)$, but when the operation is obvious, we just refer to the group by the set, like $\mathbb{Z}$.

Here is an example:

Example 1.3 (Additive integers)

The set of all integers $\mathbb{Z}$ with the binary operation addition $(+)$ form a group. This is because adding two integers gives another integer, addition is associative, 0 is an identity element, and for any element x, the element $-x$ is its inverse.

Example 1.4 (Symmetries of a square)

Consider all the actions we can do on a square that preserve its position in space. These are:

1. Do nothing.
2. Rotate by 90° (counter-clockwise).
3. Rotate by 180°.
4. Rotate by 270°.
5. Reflect about the vertical axis.
6. Reflect about the horizontal axis.
7. Reflect about a diagonal axis (say, $y = x$).
8. Reflect about the other diagonal axis (say, $y = -x$).

We can check that these form a group under the operation of "doing one thing after another." Notice how different this is from a group of just numbers! Also, this group has a certain structure which we call D_4.

Problem 1.5 (Problem 1B from Napkin)**.** Prove Lagrange's theorem for orders in the special case that G is a finite abelian group.

Solution. Since the map from g to gx is a bijection, we have

$$\prod_{g\in G} gx = \prod_{g\in G} g.$$

Since this is an abelian group, we can cancel $\prod_{g\in G} g$ from both sides to obtain

$$x^{|G|} = 1.$$

□