Basic properties of groups

Identities and inverses

In mathematics defining a new concept entails pointing out the more immediate, even obvious, results – with proof. These are known as **propositions**.

Proposition 1

The identity element of a group $(G, \star)$ is unique.

Proof.

Suppose $e, e' \in G$ are both identity elements. Then we have

$$e = e \star e' = e' \star e = e'$$

so $e = e'$ are the same element. $\square$

Often, when multiplicative notation is used 1 denotes the identity element. Likewise, we use 0 to denote the identity under additive notation.

Question

The set $\mathbb{Z}$ has both 0 and 1. Are they equal? If not, then which is the true identity element? *Hint: Under which operation is $\mathbb{Z}$ a group?*

We shall see in Section **??**, that 1 **generates** the group $\mathbb{Z}$. Meanwhile, 0 generates the **trivial** subgroup of $\mathbb{Z}$.

Proposition 2 (The Cancellation Law)

Let $(G, \star)$ *denote a group. For every* $a, b, c \in G$,

$$a \star b = c \star b \implies a = c \qquad \text{and} \qquad b \star a = b \star c \implies a = c.$$

The $\implies$ symbol means "implies".

Exercise 1

Prove the Cancellation Law.

To ease readability, in the following we shall use multiplicative notation, i.e, if g, h are elements in the group $G = (G, \star)$, then we write $gh = g \star h$.

Proposition 3 (Properties of Inverses)

Let G denote a group.

(a) *For every $g \in G$, the inverse g^{-1} is unique.*

(b) *For every $g \in G$, $(g^{-1})^{-1} = g$.*

(c) *(**Shoes-Socks Theorem**) For every $g, h \in G$, $(gh)^{-1} = h^{-1}g^{-1}$.*

Exercise 2 (cf. Problem 45)

Prove Proposition 3.

Exercise 3 (cf. Problem 46)

Suppose G is a group with the property that every element is its own inverse. Prove G must be abelian.

Question

What is an example where the **converse** in Exercise 3 fails? In other words, name an abelian group with an element that is not its own identity.

Integer exponents

Recall: In $\mathbb{R}$ we have the property that multiplying exponents with the same base is the same as adding the exponents. In other words, for $a \in \mathbb{R}$, and integers n, m, we have

$$a^n a^m = a^{n+m}. \tag{1.1}$$

Consequently, we also have the property that

$$(a^n)^m = \underbrace{a^n \cdots a^n}_{m \text{ times}} = a^{\overbrace{n+\cdots+n}^{m \text{ times}}} = a^{m \cdot n}. \tag{1.2}$$

Suppose g is in the group $G = (G, \star)$ and $n \in \mathbb{N}$. We define $g^1 := g$, then recursively, $g^n := g^{n-1} \star g^1 = g^{n-1}g$. By associativity of groups, $g^n = \underbrace{g \cdot \dots \cdot g}_{n \text{ times}}$.

Question

What are the analogous notions when we use **additive notation**, i.e., for g, h in the group $G = (G, \star)$ write $g + h = g \star h$?

Exercise 4

Prove Equations (1.1) and (1.2) hold for groups.

Similarly, define $g^0 := e$ and for fixed $n \in \mathbb{N}$, define $a^{-n} := (a^{-1})^n$.

Question

What are the analogous notions under additive notation?

Exercise 5

What are the negative exponents for each element in D_4, the dihedral group of order 4? (See Example **??** and Exercise **??**.)