# 1 Binary operations (09/20)

This course is about the theory of groups. Groups are sets equipped with extra structure, a binary operation, which satisfies certain conditions, namely associativity, the existence of an identity, and the existence of inverses.

**Definition 1.1** (Products)**.** Let $S$ be a set. The **product** of $S$ with itself, written $S \times S$, is the set of ordered pairs $(a, b)$ where $a$ and $b$ are in $S$. Elements of $S \times S$ are often called **ordered tuples**.

**Definition 1.2** (Binary operations)**.** A binary operation on a set $S$ is a function $m\colon S \times S \to S$. For $a, b \in S$ we will often write $a \cdot b$ or even $ab$ for $m(a, b)$. This is multiplicative notation. We will also have occasion to use additive notation and write $a + b$ for $m(a, b)$.

**Definition 1.3** (Properties of binary operations)**.** Let $m\colon S \times S \to S$ be a binary operation on a set $S$, written $m(a, b) = a \cdot b$.

(a) We say $m$ is **commutative** if $a \cdot b = b \cdot a$ for all $a, b \in S$.

(b) We say $m$ is **associative** if $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in S$.

(c) We say $m$ is **unitary** if there exists a (two-sided) **identity element**, which is an element $e \in S$ such that $e \cdot a = a = a \cdot e$ for all $a \in S$. If $m$ is unitary, then the identity element $e$ is unique; see Lemma 1.5.

(d) We say $m$ has the **Latin square property** if for each $a, b \in S$ there exist unique $x, y \in S$ such that $a \cdot x = b$ and $y \cdot a = b$.

(e) We say that a *unitary* binary operation $m$ has **inverses** if for each $a \in S$ there exists $b \in S$ such that $a \cdot b = b \cdot a = e$ for an identity element $e$ (which is unique by Lemma 1.5). Such an element $b$ is called a (two-sided) **inverse** of $a$ and is written as $a^{-1}$. Inverses are unique if $m$ is additionally associative by Exercise 1.3.

**Example 1.4.** Binary operations can be very simple, too simple to be of interest. For example, let $\mathbf{Z}$ be the **set of integers**. Define $m\colon \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}$ by setting $m(a, b) = 17$ for all integers $a, b$. In the notation above, we let $a \cdot b = 17$ for all $a, b \in \mathbf{Z}$. This is a binary operation, which is commutative and associative, but not terribly useful.

**Lemma 1.5** (Identities are unique)**.** *Suppose that $m$ is a unitary binary operation on a set $S$. If $e$ and $e'$ are identity elements, then $e = e'$.*

*Proof.* We have $e = e \cdot e' = e'$, where the first equality uses the identity property of $e'$ and the second equality uses the identity property of $e$. □

**Notation 1.6.** We will sometimes write 1 for the identities with respect to binary operations when writing multiplicatively; and we will sometimes write 0 for the identities with respect to binary operation written additively. Similarly, we might write $-a$ for the inverse of $a$ when writing additively.

**Remark 1.7** (Commutative diagrams)**.** Associativity can be expressed as follows. Let $m \times \mathrm{id}_S\colon S \times S \times S \to S \times S$ be defined by $(m \times \mathrm{id}_S)(a, b, c) = (m(a, b), c)$ and let $\mathrm{id}_S \times m\colon S \times S \times S \to S \times S$ be defined by $(\mathrm{id} \times m)(a, b, c) = (a, m(b, c))$. The functions $m \circ (m \times \mathrm{id}_S)$ and $m \circ (\mathrm{id} \times m)$ define two functions on the set $S \times S \times S$ of ordered triples of elements of $S$. (These might be called ternary operations.) The binary

operation $m$ is associative if these two functions are equal. In contemporary mathematics, it is common to express this via a **commutative diagram**. In this case, the diagram would be as follows:

$$\begin{array}{ccc} S \times S \times S & \xrightarrow{m \times \mathrm{id}_S} & S \times S \\ {\scriptstyle \mathrm{id}_S \times m}\downarrow & & \downarrow{\scriptstyle m} \\ S \times S & \xrightarrow[m]{} & S. \end{array}$$

Saying that the diagram is commutative amounts to asserting that the two ways of traversing the diagram from the upper left to the bottom right by composing functions result in the same function $S \times S \times S \to S$. Commutative diagrams need not be square. For example, let $t\colon S \times S \to S \times S$ be defined by $t(a, b) = (b, a)$. Commutativity is the statement that the following triangular diagram commutes:

$$\begin{array}{ccc} S \times S & \xrightarrow{t} & S \times S \\ & {\scriptstyle m}\searrow \quad \swarrow{\scriptstyle m} & \\ & S, & \end{array}$$

which means that $m \circ t = m$.

**Remark 1.8.** If $m$ is a binary operation on $S$ satisfying the Latin square property, then the multiplication table of $m$ is a Latin square: each element of $S$ appears exactly once in each row and column. In the context of binary operations, these are called Cayley tables. For example, the Latin square of Figure 1 can be viewed

| $+$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

Table 1: A Cayley table, which in this case represents a Latin square (the bottom right $3 \times 3$ part of the table).

as the "addition table" of a binary operation $m$ on the set $S = \{0, 1, 2\}$.

**Example 1.9.** Let $\mathbf{N} = \{0, 1, 2, 3, 4, 5, \ldots\}$ be the set of **natural numbers**, which we take to be the non-negative integers. On $\mathbf{N}$ we have the binary operation of addition, given by $m(a, b) = a + b$. This binary operation is commutative, associative, and unital; it has neither the Latin square property nor inverses.

**Example 1.10.** Let $\mathbf{Z}$ be the set of integers. On $\mathbf{Z}$ the binary operation of addition has all of the properties (a)-(e) of Definition 1.3. We can also multiply integers: the binary operation of multiplication satisfies properties (a)-(c) but not (d) or (e).

**Example 1.11.** We can construct Cayley tables for the outcomes of simple games. For example, consider the two-player game of rock, paper, scissors. The plays are denoted by $r$, $p$, and $s$. The outcomes of possible plays are listed in Figure 2. For example, if $p \cdot s = s = s \cdot p$ represents the fact that scissor beats paper, no matter who plays it. Now, consider

$$(r \cdot p) \cdot s = p \cdot s = s \quad \text{and} \quad r \cdot (p \cdot s) = r \cdot s = r,$$

which shows that this commutative binary operation is not associative.

| $\cdot$ | $r$ | $p$ | $s$ |
|---|---|---|---|
| $r$ | $r$ | $p$ | $r$ |
| $p$ | $p$ | $p$ | $s$ |
| $s$ | $r$ | $s$ | $s$ |

Table 2: A Cayley table for rock, paper, scissors. The associated binary operation is commutative, but not associative.

## 1.1 Exercises

**Exercise 1.1.** If $S$ and $I$ are sets, let $S^I$ be the set of functions $f\colon I \to S$. Let $I = \{0, 1\}$. Prove that for any set $S$ there is a bijection $p\colon S^I \to S \times S$.

**Exercise 1.2.** Let $S = \{1, \dots, n\}$ for some positive integer $n$. Compute the number of binary operations on $S$.

**Exercise 1.3.** Show that if $m$ is a unital, associative binary operation on a set $S$, then inverses are unique when they exist: if $a \in S$ and $x, y \in S$ are inverses of $a$, then $x = y$.

**Exercise 1.4** (The Eckmann–Hilton argument)**.** Let $S$ be a set with two binary operations $\bullet$ and $\circ$ satisfying the following two axioms:

(i) $\bullet$ and $\circ$ each has a two-sided identity element, $\mathbf{1}_\bullet$ and $\mathbf{1}_\circ$, respectively;

(ii) for each $a, b, c, d \in S$, there is the identity $(a \circ b) \bullet (c \circ d) = (a \bullet c) \circ (b \bullet d)$.

Prove that (a) $\mathbf{1}_\bullet = \mathbf{1}_\circ$, (b) $\bullet = \circ$, (c) $\bullet$ is associative, and (d) $\bullet$ is commutative.

**Exercise 1.5.** Find a binary operation which is not commutative and not associative.