11 BINARY OPERATIONS

In this section we abstract concepts such as addition, multiplication, intersection, etc. which give you a means of taking two objects and producing a third. This gives rise to sophisticated mathematical constructions such as groups and fields.

11.1 Binary operations

A *binary operation* $*$ on a set S is a function

$$* : S \times S \to S.$$

For convenience we write $a * b$ instead of $*(a, b)$.

Examples:

(i) Let $S = \mathbb{R}$ and $*$ be $+$. For $a, b \in \mathbb{R}$, $a * b = a + b$, addition (note that $a + b \in \mathbb{R}$). This is a binary operation.

(ii) Let $S = \mathbb{Z}$ and $*$ be $\times$. For $a, b \in \mathbb{Z}$, $a * b = ab$, multiplication (note that $ab \in \mathbb{Z}$). This is a binary operation.

(iii) Let $S = \mathbb{Z}$ and $a * b = \max\{a, b\}$, the largest of a and b. This is a binary operation.

(iv) Let $S = \mathbb{Q}$ and define $*$ by $a * b = a$. This is a binary operation.

(v) Let $S = \mathbb{Z}$ and $a * b = \frac{a}{b}$. This is **not** a binary operation, as it's not defined when $b = 0$, and also $\frac{a}{b}$ need not be in $\mathbb{Z}$.

(vi) Let $S = \{f : \mathbb{Z} \to \mathbb{Z}\}$, with $*$ composition of functions. This is a binary operation.

(vii) Let $S = \mathbb{N}$, with $*$ defined by $a * b = a^b$ (e.g., $2 * 3 = 2^3 = 8$). This is a binary operation.

11.2 Multiplication tables

For small sets, we may record a binary operation using a table, called the *multiplication table* (whether or not the binary operation is multiplication).

For example, let $S = \{\alpha, \beta, \gamma\}$. We may define a binary operation $*$ as follows:

$*$	α	β	γ
α	α	γ	β
β	α	β	β
γ	β	α	γ

where we take the row first and then the column. So, for example, $\alpha * \beta = \gamma$, $\beta * \alpha = \alpha$, etc.

In general, if $S = \{a_1, \ldots, a_n\}$, then the entry in the row labeled by a_j and column labeled by a_i is $a_j * a_i$.

Example:
Take $S = \mathbb{Z}_4$ and $* = \oplus$. This has multiplication table

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

11.3 Commutative and associative binary operations

Let $*$ be a binary operation on a set S. There are a number of interesting properties that a binary operation may or may not have. Specifying a list of properties that a binary operation must satisfy will allow us to define deep mathematical objects such as groups.

$*$ is *commutative* if

$$\forall\ a, b \in S, a * b = b * a.$$

$*$ is *associative* if

$$\forall\ a, b, c \in S, a * (b * c) = (a * b) * c.$$

Examples:

(i) Let $S = \mathbb{R}$, $a * b = a + b$. Let $a, b, c \in S$. Then $a * b = a + b = b + a = b * a$, so $*$ is commutative. Also $a * (b * c) = a + (b + c) = (a + b) + c = (a * b) * c$, so $*$ is associative.

(ii) Let $S = \mathbb{R}$, $a * b = a$. Then $2 * 1 = 2 \neq 1 = 1 * 2$, so $*$ is not commutative. However, if $a, b, c \in S$, then $a * (b * c) = a = a * b = (a * b) * c$, so $*$ is associative.

(iii) $S = \mathbb{Q} \setminus \{0\}$, $a * b = \frac{a}{b}$. Then $1 * 2 = \frac{1}{2} \neq 2 = 2 * 1$, so $*$ is not commutative. Also

$$1 * (2 * 3) = 1 * \left(\frac{2}{3}\right) = \frac{3}{2} \neq \frac{1}{6} = \left(\frac{1}{2}\right) * 3 = (1 * 2) * 3,$$

so $*$ is not associative.

Proposition 11.1 *Let A be a set and let $S = \{f : A \to A\}$ be the set of functions $A \to A$. Let $*$ be composition of functions.*
Then $*$ is associative.

Remark:

If $*$ is associative, then we can write $a * b * c$, meaning $(a * b) * c$ and $a * (b * c)$. More generally, we may define longer expressions $a_1 * \cdots * a_n$. Hence for $n \in \mathbb{N}$ and $a \in S$, we may define

$$a^n = \underbrace{a * \cdots * a}_{n}.$$

Examples:

(i) $S = \mathbb{Z}_8$, $* = \odot$.

$$1^3 = 1 \odot 1 \odot 1 = 1$$
$$3^2 = 3 \odot 3 = 1$$
$$3^3 = 3 \odot 3 \odot 3 = 1 \odot 3 = 3$$
$$2^3 = 2 \odot 2 \odot 2 = 4 \odot 2 = 0.$$

(ii) $S = \mathbb{Z}_8$, $* = \oplus$.

$$1^3 = 1 \oplus 1 \oplus 1 = 3$$
$$1^8 = \underbrace{1 \oplus \cdots \oplus 1}_{8} = 0$$
$$4^2 = 4 \oplus 4 = 0$$
$$4^3 = 0 \oplus 4 = 4.$$

(iii) $S = \{\text{permutationsof } \mathbb{N}_5\}$, $* = \circ$. Note that composition of functions is associative.

$$(12345)^3 = (12345)^2(12345) = (13524)(12345) = (14253)$$
$$(1234)^4 = i_{\mathbb{N}_5}.$$

11.4 Identity elements

Consider $\mathbb{Z}$. Note that $0+a = a+0 = a$ for all $a \in \mathbb{Z}$. Also note that $1 \times a = a \times 1 = a$ for all $a \in \mathbb{Z}$.

These two binary operations are said to have an identity element. We want to generalise this idea.

Definition 11.2 *Let $*$ be a binary operation on a set S. We say that $e \in S$ is an* identity element *for S (with respect to $*$) if*

$$\forall\ a \in S,\ e * a = a * e = a.$$

If there is an identity element, then it's unique:

Proposition 11.3 *Let $*$ be a binary operation on a set S. Let $e, f \in S$ be identity elements for S with respect to $*$. Then $e = f$.*

PROOF. Since e is an identity element and $f \in S$, we have $e * f = f$.
Since f is an identity element and $e \in S$, we have $e * f = e$.
Hence $e = e * f = f$. □

Examples:

(i) 0 is the identity element for $S = \mathbb{R}$ when $* = +$.

(ii) 1 is the identity element for $S = \mathbb{R}$ when $* = \times$.

(iii) Let $S = \mathbb{Q} \setminus \{0\}$ and $a * b = \frac{a}{b}$. Then there is no identity element.
Suppose that $e \in \mathbb{Q} \setminus \{0\}$ is an identity element. Then $e * 1 = 1 * e = 1$. Now $e * 1 = \frac{e}{1} = e$, so $e = 1$. But $1 * 2 = \frac{1}{2} \neq 2$, so 1 cannot be an identity element.

(iv) $S = \{a, b, c, d\}$, and define a binary operation $*$ on S by the multiplication table

	a	b	c	d
a	c	a	a	d
b	d	c	b	a
c	a	b	c	d
d	d	b	d	a

In this case c is an (the) identity element.

11.5 Groups

Let G be a non-empty set and $*$ a binary operation on G. We call $(G, *)$ a *group* if the following hold:

(G1) $*$ is associative

(G2) G has an identity element e with respect to $*$

(G3) $\forall\ g \in G$, $\exists\ h \in G$ such that $g * h = h * g = e$.

[We sometimes say G forms a group under $*$.]

Remark:

In **(G3)**, the element h is called an *inverse* to g. It is unique, since suppose $h_1, h_2 \in G$ with

$$g * h_1 = h_1 * g = e,$$

$$g * h_2 = h_2 * g = e.$$

Then

$$h_1 * (g * h_2) = h_1 * e = h_1$$

and

$$h_1 * (g * h_2) = (h_1 * g) * h_2 = e * h_2 = h_2$$

since $*$ is associative.
Hence $h_1 = h_2$.

Hence we may refer to *the* (unique) inverse to g, and write g^{-1}.

Examples:

(i) $G = \mathbb{Z}$, $* = +$. We have already seen that the identity element is 0, and that $*$ is associative. Let $a \in \mathbb{Z}$. Then $(-a) + a = a + (-a) = 0$, so $-a$ is the inverse of a (i.e., $a^{-1} = -a$). Hence $(\mathbb{Z}, +)$ forms a group.

(ii) Let $G = \mathbb{R} \setminus \{0\}$, with $* = \times$.
1 is the identity element, since $\forall\ a \in \mathbb{R}, a \times 1 = 1 \times a = a$.
Multiplication is associative.
Let $a \in \mathbb{R} \setminus \{0\}$. Then $(\frac{1}{a})a = a(\frac{1}{a}) = 1$. So $a^{-1} = \frac{1}{a}$.
Hence $(\mathbb{R} \setminus \{0\}, \times)$ forms a group.

(iii) Let $G = \{-1, 1, -i, i\} \subseteq \mathbb{C}$, with $*$ multiplication of complex numbers.
Then $-1 * 1 = -1$, $-1 * i = -i$, $i * i = -1$, etc.
$*$ forms a binary operation, with the following multiplication table:

$*$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

The identity element is 1. Also $1^{-1} = 1$, $(-1)^{-1} = -1$, $i^{-1} = -i$ and $(-i)^{-1} = i$, so each element has an inverse. Since multiplication is associative, it follows that $*$ is associative. Hence $(G, *)$ forms a group.

11.6 Cancellation in groups

Let $(G, *)$ be a group. Let $g, h_1, h_2 \in G$.
Suppose that $g * h_1 = g * h_2$. Then

$$g^{-1} * (g * h_1) = g^{-1} * (g * h_2).$$

Since $*$ is associative, this means

$$(g^{-1} * g) * h_1 = (g^{-1} * g) * h_2.$$

$g^{-1} * g = e$, so $h_1 = e * h_1 = e * h_2 = h_2$.
We have shown that $g * h_1 = g * h_2 \Rightarrow h_1 = h_2$. Hence in any given row of the multiplication table for $(G, *)$ we cannot have any repetitions. Further, each row much contain every element, since in the row labeled by g the element h occurs as $g*(g^{-1}*h)$.

Similarly $h_1 * g = h_2 * g \Rightarrow h_1 = h_2$, and each column of the multiplication table must contain every element of G, with no repetition.

11.7 Commutative groups

Definition 11.4 *A group* $(G, *)$ *is called* commutative *if* $*$ *is commutative, i.e.,* $\forall\ g, h \in G, g * h = h * g$.

All the groups in the above set of examples are commutative.

A group is commutative iff its multiplication table is symmetrical about the leading diagonal.

11.8 Integers modulo n under addition

Let $n \in \mathbb{N}$, and write $G = \mathbb{Z}_n = \{0, \ldots, n-1\}$. Let $* = \oplus$ (addition modulo n).

Note that $|G| = n$.

The identity element is 0.

Let $a \in \mathbb{Z}_n$. If $a \neq 0$, then $a^{-1} = n - a$, since $(n-a)+a = a+(n-a) = n \equiv 0 \mod n$.

We also have $0^{-1} = 0$. Hence every element has an inverse.

Addition is associative and commutative, so $(\mathbb{Z}_n, \oplus)$ forms a commutative group.

Example:

$G = (\mathbb{Z}_5, \oplus)$.

$\oplus$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	1	2
3	3	4	0	1	2
4	4	0	1	2	3

11.9 Integers modulo a prime under multiplication

Let p be a prime.

Define $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\} = \{1, 2, \ldots, p-1\}$.

Consider $\odot$, multiplication modulo p.

The identity element is 1.

$\odot$ is associative since multiplication is associative.

$\odot$ is commutative since multiplication is commutative.

Let $a \in \mathbb{Z}_p^*$. Then $\gcd(a, p) = 1$. So by Lemma 8.3, there is $b \in \mathbb{Z}$ such that $ab \equiv 1 \mod p$ (and $ba \equiv 1 \mod p$).

Now $b \equiv r \mod p$ for some $r \in \mathbb{Z}_p^*$. Hence a has inverse r, i.e., $a^{-1} = r$.

Hence $(\mathbb{Z}_p^*, \odot)$ is a commutative group.

Example:

$(\mathbb{Z}_5^*, \odot)$.

$\odot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Remark: Compare this to

$*$	1	i	$-i$	-1
1	1	i	$-i$	-1
i	i	-1	1	$-i$
$-i$	$-i$	1	-1	i
-1	-1	$-i$	i	1

.

Identifying $2 \leftrightarrow i$, $3 \leftrightarrow -i$, $4 \leftrightarrow -1$ gives the same multiplication table (these two groups are said to be *isomorphic* - this will be defined precisely in Algebraic Structures I).

In greater generality, if $n \in \mathbb{N}$, then we define $\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n : \gcd(n, x) = 1\}$ (the group of *units* in $\mathbb{Z}_n$).

Then $(\mathbb{Z}_n^*, \odot)$ forms a group. Note that if $n = p$, then this coincides with our previous definition of $\mathbb{Z}_p^*$.

Example:

$(\mathbb{Z}_8^*, \odot)$.

$\odot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

11.10 The symmetric group

Recall Section 5.7. Fix $n \in \mathbb{N}$. Write $\mathbb{N}_n = \{1, \ldots, n\}$.

Write S_n for the set of permutations $f : \mathbb{N}_n \to \mathbb{N}_n$. Recall that by Theorem 6.9 we have $|S_n| = n!$.

Consider the binary operation $\circ$ given by composition of permutations.

The identity map $i_{\mathbb{N}_n} : \mathbb{N}_n \to \mathbb{N}_n$ given by $i_{\mathbb{N}_n}(a) = a$ for all a is the identity element. Write $e = i_{\mathbb{N}_n}$.

Composition of functions is associative, so the binary operation is associative.

We saw in 5.5 that every permutation has an inverse.

Hence S_n forms a group under $\circ$. This is called the *symmetric group*.

When $f, g \in S_n$, we often write fg instead of $f \circ g$.

Example:

Let $(G, *) = (S_6, \circ)$. The elements (132645) and (143)(26) both have order six.

The element (13645) has order five. The elements (13), (24)(56) and (12)(34)(56) all have order two.

11.11 More on inverses in groups

Let $(G, *)$ be a group. Let $g, h \in G$.

What is $(g * h)^{-1}$?

Notice that

$$(g * h) * (h^{-1} * g^{-1}) = g * (h * h^{-1}) * g^{-1} = g * e * g^{-1} = g * g^{-1} = e$$

and

$$(h^{-1} * g^{-1}) * (g * h) = h^{-1} * (g^{-1} * g) * h = h^{-1} * e * h = h^{-1} * h = e,$$

so $h^{-1} * g^{-1} = (g * h)^{-1}$.

Example:

Let $(G, *) = (S_6, \circ)$. We have

$$((1234)(2346))^{-1} = (12463)^{-1} = (13642)$$

and

$$(2346)^{-1}(1234)^{-1} = (2643)(1432) = (13642).$$

By induction, if $g_1, g_2, \ldots, g_n \in G$, then

$$(g_1 * g_2 * \ldots * g_n)^{-1} = g_n^{-1} * \cdots * g_1^{-1}.$$

11.12 Another example

Let $G = \{e, (12)(34), (13)(24), (14)(23)\} \subseteq S_4$, with composition as the binary operation.

$((12)(34))^{-1} = (12)(34)$, $((13)(24)^{-1} = (13)(24)$ and $((14)(23))^{-1} = (14)(23)$. We check that G forms a group.

Write $a = (12)(34)$, $b = (13)(24)$ and $c = (14)(23)$. Then the multiplication table is

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Hence $\circ$ is a binary operation, and G forms a group.

Note that G is commutative.

11.13 Groups of a given size

Let $(G, *)$ be a group with identity element e.

If $G = \{e, a\}$, then there is only one possible multiplication table:

	e	a
e	e	a
a	a	e

.

If $G = \{e, a, b\}$, then there is only one possible multiplication table:

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

.

Note that $b = a * a = a^2$.

Now suppose $|G| = 4$. Then either $\forall x \in G, x^2 = e$ or $\exists x \in G, x^2 \neq e$. Suppose that the latter occurs. Then we may write $G = \{e, a, a^2, b\}$ for some b. In this case there is only one choice for the multiplication table for G:

	e	a	a^2	b
e	e	a	a^2	b
a	a	a^2	b	e
a^2	a^2	b	e	a
b	b	e	a	a^2

.

Note that $b = a^3$.

If $\forall x \in G, x^2 = e$, then there is only one possible type of group (up to renaming the elements).

So there are only two types of groups with four elements.

11.14 Cyclic groups

Let $(G, *)$ be a group with identity element e. Note that $\forall\ g \in G$ we have $g^0 = e$.

G is *cyclic* if there is $a \in G$ such that $G = \{a^k : k \in \mathbb{Z}\}$.

Examples:

(i) $(\mathbb{Z}, +)$, since $\mathbb{Z} = \{1^k : k \in \mathbb{Z}\}$.

$(\mathbb{Z}_n, \oplus)$, where $n \in \mathbb{N}$, since $\mathbb{Z}_n = \{1^k : k \in \mathbb{Z}\}$.

$(\mathbb{Z}_p^*, \odot)$, where p is prime. Here $\mathbb{Z}_p^* = \{2^k : k \in \mathbb{Z}\}$ if $p \neq 2$ and $\mathbb{Z}_2^* = \{1\}$.

11.15 Fields

Consider the real numbers $\mathbb{R}$.

There is more than one natural binary operation on $\mathbb{R}$: we have $+$ and $\times$.

We are interested in sets with two compatible binary operations.

Definition 11.5 *Let F be a non-empty set and let $+, *$ be binary operations on F (they need not be addition and multiplication).*

We say $(F, +, *)$ is a field *if the following are satisfied:*

(F1) *$(F, +)$ is a commutative group. Write 0 for the identity.*

(F2) *$(F \setminus \{0\}, *)$ is a commutative group. Write 1 for the identity.*

(F3) *$\forall a, b, c \in F,\ a * (b + c) = (a * b) + (a * c)$. ($*$ is* distributive *over $+$).*

Note that F will have an identity element with respect to $+$ (the additive identity) and a (usually different) identity element with respect to $*$ (the multiplicative identity).

Each element $a \in F$ has an inverse with respect to $+$, written $-a$.
Each element $a \in F \setminus \{0\}$ has an inverse with respect to $*$, written a^{-1}.

$\mathbb{R}$ and $\mathbb{Q}$ are both fields when $+$ is addition and $*$ is multiplication.

11.16 Some finite fields

Let $p \in \mathbb{N}$ be a prime. Let $F = \mathbb{Z}_p$. Write $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$.

Consider $\oplus$ and $\odot$ as the binary operations on F.

We saw that $(\mathbb{Z}_p, \oplus)$ forms a commutative group (with identity element 0). Hence (F1) is satisfied.

We also saw that $(\mathbb{Z}_p^*, \odot)$ is a commutative group (with identity element 1). Hence (F2) is satisfied.

It is clear that $\forall a, b, c \in \mathbb{Z}_p$, $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$ (since multiplication is distributive over addition in the integers).

Hence $(F, \oplus, \odot)$ is a field. Note that F is finite.

$\mathbb{Q}$ and $\mathbb{Z}_p$ are the fundamental examples of fields - in a sense every field 'contains' a copy of one of these.