(1)

Binary Operations

If G is a non-empty set, then a binary operation on G is a (partial) function from $G \times G$ to G.

If we have non-empty G and binary operation $*$, then we have groupoid $(G, *)$.

We write $a * b = c$ when $(a, b) \in G \times G$ is mapped to $c \in G$ under the binary operation. It is also common to drop the star, particularly in the context of multiplication: $ab = c$.

A magma is a groupoid where the binary operation is total.

N.B. The definition "groupoid" varies between authors, and many prefer the term "partial magma". This is to avoid confusion with a groupoid in category theory in which every morphism is invertable.

Semigroups

Multiplication in a groupoid is <u>associative</u> iff:

$$\forall a, b, c \in G, \quad a(bc) = (ab)c,$$

and is <u>commutative</u> iff:

$$\forall a, b \in G, \quad ab = ba.$$

A magma $(G, *)$ is called a <u>semigroup</u> iff binary operation $*$ is associative.

Monoids

Element $1 \in G$ is called a two-sided <u>identity</u> iff:

$$\forall a \in G, \quad a1 = a = 1a.$$

A <u>monoid</u> G is a semigroup with a two-sided identity.

Lemma (Uniqueness)

If G is a monoid, then 1 is unique.

Proof:

Suppose that $1'$ is also an identity.

Then, for some $a \in G$:

$$a = a \cdot 1 \quad \text{and} \quad a = 1' \cdot a.$$

Then:

$$1 = 1' \cdot 1 = 1'$$

and so:

$$1 = 1'.$$

$\therefore$ The identity 1 is unique. $\square$

Groups and Inverses

In monoid G, $a \in G$ has a two-sided inverse iff:

$$\exists a^{-1} \in G,\ aa^{-1} = 1 = a^{-1}a.$$

A group G is a monoid such that each $a \in G$ has an inverse.

Similarly, if they exist, inverses are unique, and we will see soon that we can generalize our group axioms to one-sided axioms.

Element $1 \in G$ is called a left-sided identity iff:

$$\forall a \in G,\ 1a = a,$$

and a right-sided identity iff:

$$\forall a \in G,\ a1 = a.$$

Element $a^{-1} \in G$ is a left-sided inverse iff:

$$a^{-1}a = 1$$

and similarly for right-sided.

Lemma (Uniqueness of $^{-1}$)

In a monoid, the inverse of a, a^{-1}, is unique if it exists.

Proof:

Suppose that b_1, b_2 are two distinct elements such that:

$$b_1 a = 1 = a b_1, \quad b_2 a = 1 = a b_2.$$

Then:

$$\begin{aligned} b_1 &= b_1 1 \\ &= b_1 (a b_2) \\ &= (b_1 a) b_2 \\ &= 1 b_2 \\ &= b_2 \end{aligned}$$

So $b_1 = b_2$. ✗ (b_1 and b_2 are distinct)

So, it must be the case that if such a "b" exists, it must be unique. $\square$

Example 1

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ form infinite commutative groups under addition.

Each of these form a commutative monoid under multiplication. Note that in $\mathbb{Z}$, only 1 and -1 have inverses, but in $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, every element other than zero has an inverse. This is because they are fields. $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ form commutative groups under multiplication.

$\triangle$

Example 2

The even numbers $2\mathbb{Z}$ form a commutative semigroup under multiplication. They form a group under addition.

The odd integers form a commutative monoid under multiplication.

$\triangle$

Example 3

Recall that the difference between a groupoid and a magma is the totality of the binary operation.

If $G = \{1, 2\}$ and $* : G \times G \to G$ is a (partial) function defined by:

$$(1,1) \mapsto 1$$
$$(1,2) \mapsto 2,$$

then $(G, *)$ is a groupoid but not a magma. However, we can fix this by adding in:

$$(2,1) \mapsto 2$$
$$(2,2) \mapsto 1$$

so that $*$ is total.

In fact, $(G, *)$ is the cyclic group of order 2:

$*$	1	2
1	1	2
2	2	1

$\triangle$

Example 4

What happens if our binary operation is not surjective (onto)?

Let $G = \{1, 2\}$ and $*: G \times G \to G$ be a function such that $(a,b) \mapsto 1$.

Then, $(G, *)$ is a magma and a semigroup, but can never be a monoid because monoids have a two-sided identity element so that:

$$\forall a \in G, \quad 1 \cdot a = a = a \cdot 1$$

so $*$ is onto.

We formalize this with a lemma:

> If $(G, *)$ is a monoid, then its binary operation $*$ is surjective.

$\triangle$

Types of Magma

$$
\begin{tikzcd}
 & \text{Groupoid} \arrow[d, "\text{Totality}"] & \\
 & \text{Magma} \arrow[dl, "\text{Divisibility}"'] \arrow[dr, "\text{Associativity}"] & \\
\text{Quasigroup} \arrow[d, "\text{Identity}"] & & \text{Semigroup} \arrow[d, "\text{Identity}"'] \\
\text{Loop} \arrow[dr, "\text{Associativity}"'] & & \text{Monoid} \arrow[dl, "\text{Invertability}"] \\
 & \text{Group} &
\end{tikzcd}
$$

Example 5

Fix a monoid G. Then, the set of all functions from X to G is also a monoid with identity, the constant function $a \mapsto a$, and operation defined pointwise (i.e. $(f \cdot g)(x) = f(x) \cdot g(x)$).

Similarly, the set of all functions from X to X forms a monoid under functional composition, with identity $a \mapsto a$. We call this the transposition monoid.

Moreover, if X is finite, and we take the set of all bijections from X to X, then we have a group. Δ

Example 6

Fix monoid $(G, \cdot)$ and consider the power set 2^G. This is actually a monoid with operation:

$$(S, T) \mapsto \{ s \cdot t \mid s \in S, t \in T \}$$

and identity $\{1\}$.

Δ

Lemma (One-Sided)

The following axioms are equivalent to define a group:

(0) Closure : $\forall a, b \in G,\ ab \in G$
(1) Associativity: $\forall a, b, c \in G,\ a(bc) = (ab)c$
(2) Left Identity: $\exists 1 \in G,\ \forall a \in G,\ 1a = a$
(3) Left Inverse: $\forall a \in G,\ \exists b \in G,\ ba = 1.$

Proof:

Axioms (0) and (1) are clearly the same.

Given that $ba = 1$, let $c := ab$. Then:

$$
\begin{aligned}
1c &= (c^{-1}c)c \\
&= c^{-1}((ab)(ab)) \\
&= c^{-1}(a(ba)b) \\
&= c^{-1}(a1b) \\
&= c^{-1}c = 1
\end{aligned}
$$

So $c = 1$ and b behaves as a right inverse.

With this in mind, we also have:

$$a1 = a(ba) = (ab)a = 1a = a.$$

So 1 behaves as a right identity.

So, our one-sided axioms are equivalent.

$\square$

Lemma (Idempotent)

$\boxed{\text{If } G \text{ is a group, and } a^2 = a \text{ for some } a \in G, \text{ then } a = 1.}$

Proof:

Because we are in a group, there is an a^{-1} s.t. $a^{-1}a = 1$.

So, if we take $a^2 = a$ and multiply on the left by a^{-1}, we have:

$$a^{-1} \cdot a^2 = a^{-1} \cdot a$$

$$(a^{-1} \cdot a) \cdot a = a^{-1} \cdot a$$

$$1 \cdot a = 1$$

$$a = 1.$$

Thus $a^2 = a \Rightarrow a = 1$. $\square$

Example 7

$(M_2(\mathbb{R}), +)$ is a commutative group and $(M_2(\mathbb{R}), \cdot)$ is a non-commutative monoid.

In high school, we are used to being able to "cancel":

$$\forall a, b, c \neq 0, \quad ab = cb \Rightarrow a = c.$$

We are unable to cancel in our monoid. For example:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

but:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

Our observation that $a^2 = a \Rightarrow a = 1$ no longer holds either:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

$\triangle$

Homomorphisms

Let G and H be semigroups. Then a function $f: G \to H$ is a homomorphism iff:

$$\forall a,b \in G,\ f(ab) = f(a)f(b).$$

A surjective homomorphism is called an epimorphism, and an injective homomorphism is called a monomorphism.

A bijective homomorphism $f: G \to H$ is called an isomorphism, and we say G and H are isomorphic iff there exists an isomorphism $G \to H$, and we write $G \cong H$.

A homomorphism $f: G \to G$ is called an endomorphism, and an isomorphism $f: G \to G$ is called an automorphism.

N.B. Semigroup homomorphisms on monoids G and H don't necessarily imply that $f(1_G) = 1_H$ unlike in group axioms, so we sometimes add this extra axiom when defining monoid morphisms.

Example 8

Let $G = \mathbb{Z}$ and $H = \mathbb{Z}_m$.

Define $f : \mathbb{Z} \to \mathbb{Z}_m$ as $x \mapsto \bar{x}$.

Then f is an onto homomorphism called the canonical epimorphism of $\mathbb{Z}$ onto $\mathbb{Z}_m$.

$\triangle$

Example 9

If A is an Abelian group, then $f : A \to A$ defined as $f(a) = a^{-1}$ is an automorphism of A, and $g : A \to A$ defined as $g(a) = a^2$ is an endomorphism of A.

$\triangle$

Example 10

Let $m, k \in \mathbb{N}$, $m \neq 1 \neq k$.

Then $f : \mathbb{Z}_m \to \mathbb{Z}_{mk}$ defined as $f(\bar{x}) = \overline{kx}$ is a monomorphism.

$\triangle$

Example 11

The determinant function is a monoid epimorphism where:

$$\det : M_n(\mathbb{K}) \longrightarrow \{0, 1\}.$$

This only works for $(M_n(\mathbb{K}), \cdot)$ and not $(M_n(\mathbb{K}), +)$, however the trace function is a group epimorphism:

$$\operatorname{tr} : M_n(\mathbb{K}) \longrightarrow \mathbb{K}.$$

$\triangle$

Example 12

Let $G = \mathbb{Z} \times \mathbb{Z}$ be a monoid with coordinate-wise multiplication and $1_G = (1,1)$, and $H = \mathbb{Z} \times \{0\}$ with coordinate-wise multiplication and $1_H = (1,0)$.

Consider the embedding:

$$\iota : \mathbb{Z} \times \{0\} \hookrightarrow \mathbb{Z} \times \mathbb{Z}.$$

This is clearly a monomorphism of semigroups, but the identity is not preserved since:

$$(1, 0) \longmapsto (1, 0) \neq (1, 1).$$

$\triangle$

Kernel and Image

Let $f: G \to H$ be a group homomorphism.
The kernel of f is:

$$\text{Ker}(f) = \{ g \in G \mid f(g) = 1_H \},$$

and the set $f(G)$ is called the image:

$$\text{Im}(f) = f(G) = \{ f(g) \mid g \in G \}.$$

$$\boxed{f \text{ is a monomorphism iff } \text{Ker}(f) = \{1_G\}}$$

Proof:

If $a \neq 1$ is in $\text{Ker}(f)$, $f(a) = f(1) = 1$ and by injectivity $a = 1$. ※ Thus $\text{Ker}(f) = \{1\}$.

If $\text{Ker}(f) = \{1\}$, then for $a, b \in G$:

$$\begin{aligned}
&f(a) = f(b) \\
&f(a)(f(b))^{-1} = f(b)(f(b))^{-1} \\
&f(a)f(b^{-1}) = 1 \\
&f(ab^{-1}) = 1 \\
&ab^{-1} \in \text{Ker}(f) \\
&ab^{-1} = 1 \\
&a = 1b = b,
\end{aligned}$$

so $f(a) = f(b) \Rightarrow a = b$. $\square$

Algebraic Structures

So, we've seen groupoids, and how to build "group-like" structures.

We can abstract this concept to give "algebraic structures", which are non-empty sets, with zero or more binary operations.

For example, a set is a degenerate algebraic structure, with no binary operations.

Ring-like structures are sets with the two binary operations of multiplication and addition, with multiplication distributing over addition. A semiring is when the set is a monoid under both operations, and a ring is when the set is an Abelian group under addition. A field is a ring where each non-zero element has a multiplicative inverse.

Lattice structures two (or more) operations including meet and join, connected by the absorption law. Think $a \vee b$, $a \wedge b$.

Module-like structures involve two sets and two or more operations, such as vector spaces. Bialgebras have four or more operations.