Algebraic Structures

Slides week 1

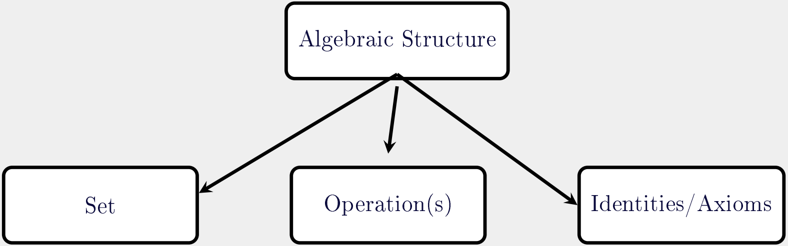
Paula Lins

University of Lincoln

2023/24

Algebraic structures

What are algebraic structures?



Why algebraic structures?

Algebraic Structures

- Algebra can help to reveal how things are built.
- Algebraic structures help us to understand what different mathematical objects have in common, and what the important differences are.
- Algebraic structures allow us to understand things more abstractly.
- Abstraction is a powerful tool because it allow us to understand all sorts of things in full generality.

Module structure

Module structure

- Chapter 1: Groups
- Chapter 2: Rings (including integral domains and fields)
- Chapter 3: Applications to polynomial rings
- Chapter 4: Field extensions

About Group Theory

- Groups are key to modern mathematics,
- Group Theory is the branch of mathematics that studies groups.
- Group Theory is a strong-point of algebraic research in Lincoln School of Mathematics and Physics.

Week 1

Week 1: Goals

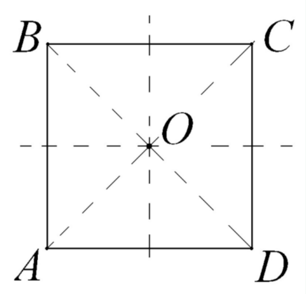
Today:

- Groups
- Direct products

Groups

In mathematics, **Groups** are precise mathematical objects (not just any group in common language).

Example: Transformations of a square (as a rigid figure)



There are four rotations around the centre O:

- 0°, 90°, 180°, and 270°.

There are four reflexions:

- vertical and horizontal,
- two diagonal reflexions.

These eight elements form the group of isometries D_8 of a square.

Example: The integers $\mathbb{Z}$

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}.$$

We know the following four things about $\mathbb{Z}$:

1. If we take two elements x and y of $\mathbb{Z}$, $x + y$ is also in $\mathbb{Z}$, ($\mathbb{Z}$ is **closed**)
2. if you add 3 integers together, whether you initially sum the first two or the last two doesn't matter, ($\mathbb{Z}$ is **associative**)
3. adding 0 to any integer doesn't change that integer, (0 is an **identity element**)
4. for each integer, there is another integer which when added to the first integer brings you back to 0.
   (Every elements has an **inverse**)

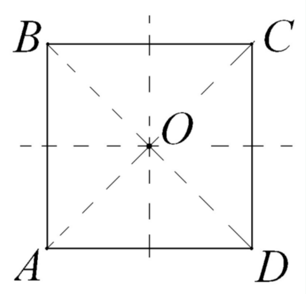
This means that $\mathbb{Z}$ with addition $+$ forms a **group**.

Definition.

A **group** is a set G together with an operation $*$ such that **all** of the following holds.

1. **Closure:** If $x, y \in G$, then $x * y$ is also in G.
2. **Associativity:** If $x, y, z \in G$, then
$$x * (y * z) = (x * y) * z.$$
3. **Existence of identity element**: We can find an element $e \in G$ satisfying
$$e * x = x * e = x, \text{ for all } x \in G.$$
4. **Existence of inverse elements:** If $x \in G$, we can find $y \in G$ such that
$$x * y = y * x = e.$$

Example: Transformations of a square (as a rigid figure)



There are four rotations around the centre O:

- 0°, 90°, 180°, and 270°.

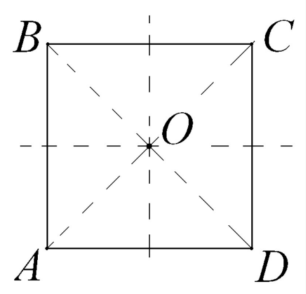
There are four reflexions:

- vertical and horizontal,
- two diagonal reflexions.

These eight elements form the group of isometries D_8 of a square.

This is called the **Dihedral group** of order 8.

Example: Transformations of a square (as a rigid figure)



What is the operation in D_8?

Given two transformations T_1 and T_2:

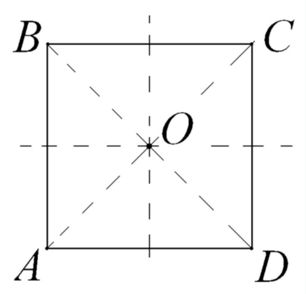
$$T_1 * T_2 = T_1T_2 = \text{apply } T_1, \text{ and then apply } T_2.$$

For instance, if $a =$ (anticlockwise) rotating 90°, then

$$a^2 = a * a = \text{ rotating } 180^\circ$$
$$a^4 = e,$$

where e denotes the initial position.

Example: Transformations of a square (as a rigid figure)



D_8 is **closed**: Let

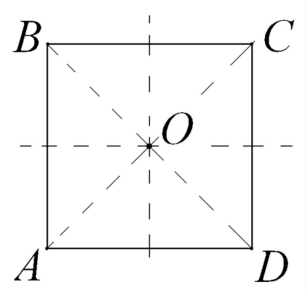
$$a = \text{(anticlockwise) rotating } 90^\circ$$
$$b = \text{vertical reflection .}$$

Where does $a * b$ send A? And B?

$$A \overset{a}{\mapsto} D \overset{b}{\mapsto} A, \quad \text{so} \quad A \overset{a*b}{\longmapsto} A.$$
$$B \overset{a}{\mapsto} A \overset{b}{\mapsto} D, \quad \text{so} \quad B \overset{a*b}{\longmapsto} D.$$

Thus, $a * b$ is the diagonal reflection in AC.

Example: Transformations of a square (as a rigid figure)



Another product: Again

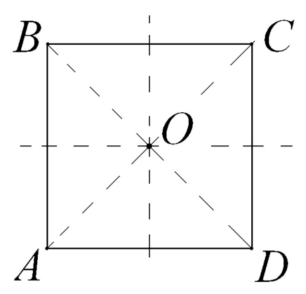
$$a = \text{(anticlockwise) rotating } 90^\circ$$
$$b = \text{vertical reflection} .$$

Where does $b * a$ send A? And B?

$$A \overset{b}{\mapsto} D \overset{a}{\mapsto} C, \qquad \text{so} \quad A \overset{b*a}{\longmapsto} C.$$
$$B \overset{b}{\mapsto} C \overset{a}{\mapsto} B, \qquad \text{so} \quad B \overset{b*a}{\longmapsto} B.$$

Thus, $a * b$ is the diagonal reflection in $BD \implies \mathbf{a * b \neq b * a}$!!

Example: Transformations of a square (as a rigid figure)



Associativity:
$\alpha * (\beta * \gamma) = (\alpha * \beta) * \gamma.$

This rule is satisfied by D_8.

Existence of identity element: Denote

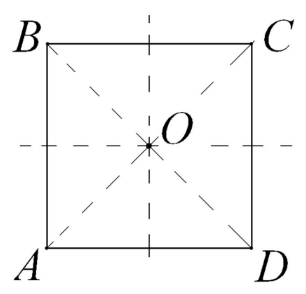
$$e = \text{ the rotation by } 0^{\circ}.$$

Then

$$T * e = T = e * T,$$

This means that e is the **identity element**.

Example: Transformations of a square (as a rigid figure)



Existence of inverse:

$$a = \text{(anticl.) rotating } 90^{\circ},$$
$$a^3 = \text{(anticl.) rotating } 270^{\circ}.$$

Thus,

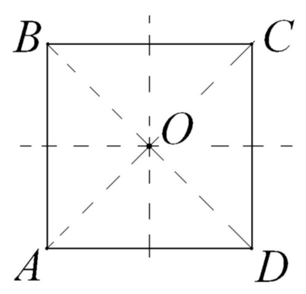
$$a * a^3 = \text{(anticl.) rotating } 360^{\circ}$$
$$= e.$$

Thus, a^3 is the **inverse** of a, and a is the **inverse** of a^3.

Similarly, for $b =$ vertical reflection , we have

$b * b = e,$ that is, b is its own **inverse**.

Example: Transformations of a square (as a rigid figure)



We conclude that D_8

- is **close under** $*$,
- is **associative**,
- has an **identity element** e, and
- has **inverse elements** for all its elements.

This means that D_8 is a **group**.

Notation

Warning! Multiplication: $a * b$, $a \cdot b$, ab, ...

We write group operations as follows.

- Often: $a * b$,
- Often: ab,
- Sometimes: $a \cdot b$, $a + b$, $a \odot b$, $a \otimes b$, ...

Inverse elements

Inverse of $a \in G$ is often denoted by:

- $-a$, (**additive notation**),
- a^{-1}. (**multiplicative notation**)

Notation

Identity element

- Most often: e,
- Often (in the literature): 1 or 1_G (to specify the group),
- Sometimes: 0 (in additive notation).

Recognizing groups/non-groups

Is the following a group?

$$\mathbb{N} = \{1, 2, 3, \ldots\} \text{ with } +$$

No! Because no element has an inverse!

Is the following a group?

$$G = \{\text{black}, \text{white}\} \quad \text{with} \quad * = \text{ mixing colours.}$$

No! Because

$$\text{black} * \text{white} = \text{gray}$$

is not an element of G.

That is, G is not **closed** under $*$.

Recognizing groups/non-groups – part 2

Is the following a group?

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\} \text{ with } + .$$

Yes! We checked it on slide 17.

Is the following a group?

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\} \text{ with multiplication.}$$

No! No element other than -1 and 1 has an inverse.

For instance, there is no $x \in \mathbb{Z}$ such that

$$2x = 1 = x2.$$

Is the following a group?

$$2\mathbb{Z} = \{2z \mid z \in \mathbb{Z}\} = \{ \text{ even numbers } \} \text{ with } + .$$

To show that $2\mathbb{Z}$ is a group: must show **all** group axioms.

Closed with $+$: Two elements of $2\mathbb{Z}$ are of the form $2z_1$ and $2z_2$ with $z_1, z_2 \in \mathbb{Z}$. Thus

$$2z_1 + 2z_2 = 2(z_1 + z_2) \in 2\mathbb{Z}$$

because $z_1 + z_2 \in \mathbb{Z}$.

Associativity: We know that $\mathbb{Z}$ is associative, that is

$$(a + b) + c = a + (b + c), \text{ for all } a, b, c \in \mathbb{Z},$$

thus $2\mathbb{Z} \subset \mathbb{Z}$ also is.

Is the following a group?

$$2\mathbb{Z} = \{2z \mid z \in \mathbb{Z}\} = \{ \text{ even numbers } \} \text{ with } + .$$

Identity element: Notice that

$$0 = 2 \cdot 0 \in 2\mathbb{Z}$$

because $0 \in \mathbb{Z}$. Moreover, for all $2z \in 2\mathbb{Z}$, it holds

$$2z + 0 = 2z = 0 + 2z.$$

Thus, 0 is the **identity element**.

Is the following a group?

$$2\mathbb{Z} = \{2z \mid z \in \mathbb{Z}\} = \{\text{ even numbers }\} \text{ with } + .$$

Inverse element: Given $2z \in 2\mathbb{Z}$ we know that

$$-2z = 2(-z) \in 2\mathbb{Z}$$

because $-z \in \mathbb{Z}$. Thus, $-2z$ is an element in $2\mathbb{Z}$ satisfying

$$2z + (-2z) = 0 = (-2z) + 2z.$$

Hence, $-2z$ is the **inverse** of $2z$.

Is the following a group?

$$\{2z+1 \mid z \in \mathbb{Z}\} = \{\text{ odd numbers }\} \text{ with } + .$$

To show that something is **not** a group: must only show that **one** group axiom fails.

In this case, 3 and 5 are odd number. However,

$$3+5=8 \text{ is not odd.}$$

Thus, the set of odd numbers is **not closed** under $+$, and hence it is **not** a group.

Direct product

Direct product

Definition/Proposition

Let G and H be groups (with opration given in multiplicative notation).
The **direct product** of G and H is a group $G \times H$, given by

$$G \times H = \{(g, h) \mid g \in G, h \in H\}$$

and operation

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2).$$

We must show that $G \times H$ is in fact a group!

But first, let us see examples of direct products.

Example of direct product: $\mathbb{Z} \times \mathbb{Z}$

Example

We know that $\mathbb{Z}$ is a group, thus we can take

$$\mathbb{Z} \times \mathbb{Z} = \{(a, b) \mid a, b \in \mathbb{Z}\}.$$

An example of two elements and their product is:

$$(1,\ 2) \cdot (0,\ 5) = (1 + 0,\ 2 + 5) = (1,\ 7).$$

Remark: We could also write

$$(1,\ 2) + (0,\ 5) = (1 + 0,\ 2 + 5) = (1,\ 7).$$

Example of direct product: $\mathbb{Z} \times D_8$

Example

We know that D_8 is the group of symmetries of a square. So, we can consider

$$\mathbb{Z} \times D_8 = \{(x, y) \mid x \in \mathbb{Z}, y \in D_8\}.$$

Two examples of pairs of elements and their products are:

$$(0,\, a) \cdot (7,\, a^2) = (0 + 7,\, a * a^2) = (7,\, a^3),$$
$$(-1,\, b) \cdot (5,\, b) = (-1 + 5,\, b * b) = (4,\, b^2) = (4, e).$$

Remark. Notice that, since the two groups have different operations, we need to use different operations in the first and the second entry.

Proof that $G \times H$ is a group

Let us now show that the direct product of two (arbitrary) groups is a group.

Closed:

Given (g_1, h_1) and (g_2, h_2) in $G \times H$, we must show that their product is also in $G \times H$.

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2) \in G \times H$$

because G and H are groups, thus $g_1 g_2 \in G$ and $h_1 h_2 \in H$.

Proof that $G \times H$ is a group

Associative:

Since G and H are associative, we have $g_1(g_2g_3) = (g_1g_2)g_3$ and $h_1(h_2h_3) = (h_1h_2)h_3$. Thus,

$$\begin{aligned}
(g_1, h_1)((g_2, h_2)(g_3, h_3)) &= (g_1, h_1)(g_2g_3, h_2h_3) \\
&= (g_1(g_2g_3), h_1(h_2h_3)) \\
&= ((g_1g_2)g_3, (h_1h_2)h_3) \\
&= (g_1g_2, h_1h_2)(g_3, h_3) \\
&((g_1, h_1)(g_2, h_2))(g_3, h_3).
\end{aligned}$$

Identity element:

Let e_G and e_H be the identity elements of G and H, respectively.

Then,

$$\begin{aligned}(g,h)(e_G,e_H) &= (ge_G, he_H) \\ &= (g,h)\end{aligned}$$

and

$$\begin{aligned}(e_G,e_H)(g,h) &= (e_G g, e_H h) \\ &= (g,h)\end{aligned}$$

Thus, (e_G, e_H) is the identity element of $G \times H$.

Proof that $G \times H$ is a group

Inverse elements:

Let $(g, h) \in G \times H$.

We must find $(g', h') \in G \times H$ such that

$$(g, h)(g', h') = (e_G, e_H) = (g', h')(g, h).$$

Since G is a group and $g \in G$, there exists $g^{-1} \in G$. That is,

$$gg^{-1} = e_G = g^{-1}g.$$

Similarly, we can find $h^{-1} \in H$, such that $hh^{-1} = e_H = h^{-1}h$.
Then,

$$\begin{aligned}(g, h)(g^{-1}, h^{-1}) &= (gg^{-1}, hh^{-1}) \\ &= (e_G, e_H) \\ &= (g^{-1}, h^{-1})(g, h)\end{aligned}$$

Proof that $G \times H$ is a group

Inverse elements (continuation):

Thus, (g^{-1}, h^{-1}) is the **iverse** of (g, h).

One can write

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

Proof that $G \times H$ is a group

Proof that $G \times H$ is a group

Since $G \times H$

- is **closed** under multiplication,
- is **associative**,
- has **identity element** (e_G, e_H), and
- has **inverse** for each of its elements,

we conclude, $G \times H$ is a **group**.

Next lecture

Exercises before next lecture

- Practical 1: Question 1.1 (items **(a)** to **(f)**).

Next time...

- Abelian groups,
- uniqueness of identity and inverse elements.