Chapter 10. Abstract algebra

C.O.S. Sorzano

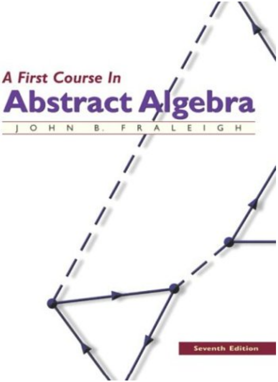
Biomedical Engineering

December 17, 2013

Outline

10 Abstract algebra
- Sets
- Relations and functions
- Partitions and equivalence relationships
- Binary operations
- Groups and subgroups
- Homomorphisms and isomorphisms
- Algebraic structures

References



J.B. Fraleigh. A first course in Abstract Algebra. Pearson, 7th Ed. (2002)

Outline

10 Abstract algebra

- Sets
- Relations and functions
- Partitions and equivalence relationships
- Binary operations
- Groups and subgroups
- Homomorphisms and isomorphisms
- Algebraic structures

Sets

Definition 1.1 (Set)

*A **set** is a well-defined collection of **elements**. We denote the different elements as $a \in S$.*

Definition 1.2 (Empty set)

*The only set without any element is the **empty set** ($\emptyset$).*

Describing sets

We may provide the elements of a set:

- Intensional definition: by giving a property they all meet (*e.g., even numbers from 1 to 10*)
- Extensional definition: by listing all the elements in the set (*e.g.,*$\{2, 4, 6, 8, 10\}$). The order in which the different elements are written has no meaning.

Sets

Definition 1.3 (Subset and proper subset)

*B is **subset** of A (denoted $B \subseteq A$ or $A \supseteq B$) if all the elements of B are also elements of A. B is a **proper subset** of A if B is a subset of A and B is different from A ($B \subset A$ or $A \supset B$).*

Properties

- A is an improper subset of A.
- $\emptyset$ is a proper subset of A.

Definition 1.4 (Power set (Partes de un conjunto))

*The set of all subsets of a set A is called the **power set** of A.*

Example

Let $A = \{1, 2, 3\}$ the power set of A is

$$P(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

Sets

Definition 1.5 (Cartesian product)

The cartesian product of the sets A and B is the set of all ordered pairs in which the first element comes from A and the second element comes from B.

$$A \times B = \{(a, b) | a \in A, b \in B\}$$

Note that because of the ordered nature of the pair $A \times B \neq B \times A$.

Example

Let $A = \{1, 2, 3\}$ and $B = \{4, 5\}$.

$$A \times B = \{(1, 4), (1, 5), (2, 4), (2, 5), (3, 4), (3, 5)\}$$

Definition 1.6 (Cardinality)

The cardinality of a set is the number of elements it has.

Sets

Definition 1.7 (Disjoint sets)

Two sets are disjoint if they do not have any element in common.

Some useful sets

- Integer numbers: $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$, $|\mathbb{Z}| = \aleph_0$
- Natural numbers, positive integers: $\mathbb{N} = \mathbb{Z}^+ = \{1, 2, 3, ...\}$, $|\mathbb{N}| = \aleph_0$
- Negative integers: $\mathbb{Z}^- = \{..., -3, -2, -1\}$, $|\mathbb{Z}^-| = \aleph_0$
- Non-null integers: $\mathbb{Z}^* = \mathbb{Z} - \{0\} = \{..., -2, -1, 1, 2, ...\}$, $|\mathbb{Z}^*| = \aleph_0$
- Rational numbers: $\mathbb{Q}$, $|\mathbb{Q}| = \aleph_0$
- Real numbers: $\mathbb{R}$, $|\mathbb{R}| = \aleph_1$
- Interval: $[0, 1]$, $|[0, 1]| = \aleph_1$
- Complex numbers: $\mathbb{C} = \{a + bi | a, b \in \mathbb{R}\}$, $|\mathbb{C}| = \aleph_1$

Outline

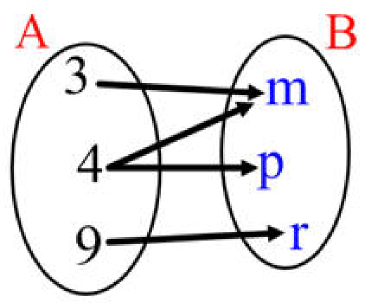
10. Abstract algebra
    - Sets
    - Relations and functions
    - Partitions and equivalence relationships
    - Binary operations
    - Groups and subgroups
    - Homomorphisms and isomorphisms
    - Algebraic structures

Relations

Definition 2.1 (Relation)

*A **relation** aRb is a subset of the cartesian product $A \times B$.*

Example



Functions

Definition 2.2 (Function)

A ***function*** $f : X \to Y$ *is a relation between* X *and* Y *in which each* $x \in X$ *appears at most in one of the pairs* (x, y)*. We may write*

$$(x, y) \in f \text{ or } f(x) = y$$

The ***domain*** *of* f *is* X*, the* ***codomain*** *of* f *is* Y*. The* ***support*** *of* f *is the set of all those values in* X *for which there exists a pair* (x, y)*. The* ***range*** *of* f *are all values in* Y *for which there exists at least one pair* (x, y)*.*

Example

$$\begin{array}{rcl} f : \mathbb{R} & \to & \mathbb{R} \\ f(x) & = & x^3 \end{array}$$

$$(2, 8) \in f \Leftrightarrow f(2) = 8$$

$$+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$$

$$((2, 3), 5) \in + \Leftrightarrow +((2, 3)) = 5 \Leftrightarrow 2 + 3 = 5$$

Classification of functions

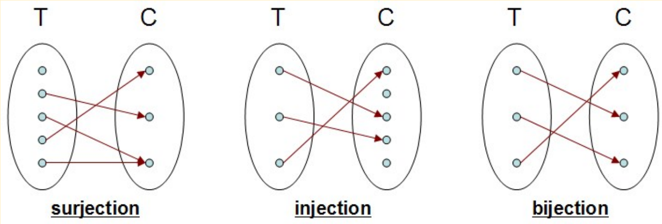
Definition 2.3

Functions can be classified as ***surjective, injective or bijective****:*

Surjective: *A function is surjective if every point of the codomain has* ***at least one*** *point of the domain that maps onto it. They are also called* ***onto*** *functions.*

Injective: *A function is injective if every point of the codomain has* ***at most one*** *point in the domain that maps onto it. They are also called* ***one-to-one*** *functions.*

Bijective: *A function is bijective if it is injective and surjective.*



Inverse function

Definition 2.4 (Inverse function)

*Consider an injective function $f : X \to Y$. $f^{-1} : Y \to X$ is the **inverse** of f iff*

$$(x, y) \in f \Rightarrow (y, x) \in f^{-1}$$

Example

- $f(x) = x + 3 \Rightarrow f^{-1}(y) = y - 3$
- $f(x) = x^3 \Rightarrow f^{-1}(y) = y^{\frac{1}{3}}$
- $f(x) = x^2$ is not invertible because it is not injective ($f(-2) = f(2) = 4$)

Inverse function

Theorem 2.1

- *If f is invertible, its inverse is unique.*
- *If f is bijective, so is f^{-1}.*
- *X and Y have the same cardinality if there exists a bijective function between the two.*

Example

Consider the following function $f : \mathbb{Z} \to \mathbb{N}$

$$\begin{array}{cccccccc} 0 & -1 & 1 & -2 & 2 & -3 & 3 & \dots \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & \dots \end{array}$$

$$f = \{(0,0),(-1,1),(1,2),(-2,3),(2,4),(-3,5),(3,6),\dots\}$$

f is bijective. Consequently, $\mathbb{Z}$ has the same cardinality as $\mathbb{N}$.

Outline

10 Abstract algebra

- Sets
- Relations and functions
- Partitions and equivalence relationships
- Binary operations
- Groups and subgroups
- Homomorphisms and isomorphisms
- Algebraic structures

Partition

Definition 3.1 (Partition)

A partition of a set S is a collection of non-empty subsets such that each element of S belongs to one and only one subset (cell) of the partition. We denote as $\bar{x}$ the subset that contains the element x. All cells in a partition are disjoint to any other cell.

Examples

- We may partition the set of natural numbers into the subset of even numbers ($\{2, 4, 6, ...\}$) and the subset of odd numbers ($\{1, 3, 5, ...\}$).
- We may partition the set of integer numbers into the subset of all multiples of 3 ($\{..., -6, -3, 0, 3, 6, ...\}$), the subset of all numbers whose remainder after dividing by 3 is 1 ($\{..., -5, -2, 1, 4, 7, ...\}$), and the subset of all numbers whose remainder after dividing by 3 is 2 ($\{..., -4, -1, 2, 5, 8, ...\}$).

Equivalence relation

Definition 3.2 (Equivalence relation)

*R is an **equivalence relation** in S if it verifies:*

1. *R is **reflexive**: xRx*
2. *R is **symmetric**: $xRy \Rightarrow yRx$*
3. *R is **transitive**: $xRy, yRz \Rightarrow xRz$*

Examples

1. $=$ is an equivalence relation.
2. Congruence modulo n is an equivalence relation (two numbers are related if they have the same remainder after dividing by n)
   Example: 1 and 4 have remainder 1 after dividing by 3. We write
   $$1 \equiv 4(mod 3)$$
3. $\forall n, m \in \mathbb{Z} \quad nRm \Leftrightarrow nm \geq 0$ is not an equivalence relationship because it is not transitive (e.g., $-3R0$, $0R5$ but $-3\not R5$).

Partition and equivalence relation

Theorem 3.1

Let S be a non-empty set, and R an equivalence relation defined on S. Then R partitions S with the cells

$$\bar{a} = \{x \in S | xRa\}$$

Additionally, we may define another equivalence relation $\sim$

$$a \sim b \Leftrightarrow \bar{a} = \bar{b}$$

Partition and equivalence relation

Example

Congruence modulo 3 is an equivalence relation in $\mathbb{Z}$ (two numbers are related if they have the same remainder after dividing by 3)

$$\bar{0} = \{..., -6, -3, 0, 3, 6, ...\}$$
$$\bar{1} = \{..., -5, -2, 1, 4, 7, ...\}$$
$$\bar{2} = \{..., -4, -1, 2, 5, 8, ...\}$$

Additionally

$$... = \bar{0} = \bar{3} = \bar{6} = ... \Rightarrow 0 \sim 3 \sim 6 \sim ...$$
$$... = \bar{1} = \bar{4} = \bar{7} = ... \Rightarrow 1 \sim 4 \sim 7 \sim ...$$
$$... = \bar{2} = \bar{5} = \bar{8} = ... \Rightarrow 2 \sim 5 \sim 8 \sim ...$$

and

$$\mathbb{Z} = \bar{0} \cup \bar{1} \cup \bar{2}$$

Partition and equivalence relation

Example

Consider the cartesian product $\mathbb{Z} \times (\mathbb{Z} - \{0\})$. Let (m_1, n_1) and (m_2, n_2) be two ordered sets of this cartesian product. Consider now the equivalence relation

$$(m_1, n_1) \sim (m_2, n_2) \Leftrightarrow m_1 n_2 - m_2 n_1 = 0$$

The set of rational numbers is formally defined $\mathbb{Q}$ as the set of equivalence classes of $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ under the relation $\sim$.

Outline

10 Abstract algebra

- Sets
- Relations and functions
- Partitions and equivalence relationships
- Binary operations
- Groups and subgroups
- Homomorphisms and isomorphisms
- Algebraic structures

Binary operations

Introduction

What is addition?

Let us assume that we arrive to a classroom in Mars, and that martians are learning to add. The teacher says

Gloop, poyt

and the students reply:

Bimt.

Then, the teacher says:

Ompt, gaft

and the students reply:

Poyt.

We don't know what they do but it seems that when the teacher gives two elements, students respond with another element.

Introduction (continued)

What is addition?
This is what we do when we say "three plus four", "seven". And we may not use any two elements ("three plus apples" is not defined). We can only use elements on a given set. This is what we formally call a binary operation.

Definition 4.1 (Binary operation)

A binary operation on a set S is a function:

$$\begin{aligned} * : S \times S &\rightarrow S \\ *(a, b) &= a * b \end{aligned}$$

Binary operations

Examples

The following binary operations are all different:

$$+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$$
$$+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$$
$$+ : \mathcal{M}_{m\times n}(\mathbb{R}) \times \mathcal{M}_{m\times n}(\mathbb{R}) \to \mathcal{M}_{m\times n}(\mathbb{R})$$

The following is not a binary operation because it is not well defined

$$+ : \mathcal{M}(\mathbb{R}) \times \mathcal{M}(\mathbb{R}) \to \mathcal{M}(\mathbb{R})$$

we don't know how to add a 2×2 matrix with a 3×3 one.

Closed set

Definition 4.2

Let S be a set and H a subset of S. H is said to be ***closed with respect to the operation*** $*$ *defined in S iff*

$$\forall a, b \in H \quad a * b \in H$$

Then we may define the binary operation in H:

$$\begin{aligned} * : H \times H &\rightarrow H \\ *(a, b) &= a * b \end{aligned}$$

which is called the ***binary operation induced*** *in H.*

Closed set

Example

Let $S = \mathbb{Z}$ and $H = \{n^2 | n \in \mathbb{Z}^+\} = \{1, 4, 9, 16, 25, 36, ...\}$. H is not closed with respect to addition. For example:

$$\begin{matrix} 1 \in H \\ 4 \in H \end{matrix} \quad \text{but } 1 + 4 \notin H$$

Example

Let $S = \mathbb{Z}$ and $H = \{n^2 | n \in \mathbb{Z}^+\} = \{1, 4, 9, 16, 25, 36, ...\}$. H is closed with respect to multiplication. For example:

$$\begin{matrix} n^2 \in H \\ m^2 \in H \end{matrix} \quad \text{and } n^2 \cdot m^2 = (nm)^2 \in H$$

Closed set

Example

Let S be the set of **real-valued functions with a single real argument** $S = \{\mathbb{R} \to \mathbb{R}\}$. Let us define the **addition** of functions as

$$\begin{aligned} + : (\mathbb{R} \to \mathbb{R}) \times (\mathbb{R} \to \mathbb{R}) &\to \mathbb{R} \to \mathbb{R} \\ (f+g)(x) &= f(x) + g(x) \end{aligned}$$

Similarly for the **multiplication** and **subtraction** of functions. Let us define the **composition** of functions as

$$\begin{aligned} \circ : (\mathbb{R} \to \mathbb{R}) \times (\mathbb{R} \to \mathbb{R}) &\to \mathbb{R} \to \mathbb{R} \\ (f \circ g)(x) &= f(g(x)) \end{aligned}$$

S is closed with respect to addition, subtraction, multiplication and composition.

Definition of a binary operation

Example

To define a binary operation either we give the full table (**intensional definition**) as in

$a * b$	$b = 0$	$b = 1$	$b = 2$
$a = 0$	0	1	2
$a = 1$	1	2	0
$a = 2$	2	0	1

or

$a \triangle b$	$b = 0$	$b = 1$	$b = 2$
$a = 0$	1	2	0
$a = 1$	1	1	2
$a = 2$	0	0	2

or we give a rule to compute it (**extensional definition**) as in

$$a * b = (a + b) \mod 3$$

Properties of a binary operation

Definition 4.3 (Commutativity)

*A binary operation is **commutative** iff*

$$a * b = b * a$$

Example

$*$ is commutative because its definition table is symmetric with respect to the main diagonal, but $\triangle$ is not commutative.

Properties of a binary operation

Definition 4.4 (Associativity)

A binary operation is ***associative*** *iff*

$$(a * b) * c = a * (b * c)$$

Example

$\triangle$ is not associative because

$$(0 \triangle 0) \triangle 0 = 1 \triangle 0 = 1$$
$$0 \triangle (0 \triangle 0) = 0 \triangle 1 = 2$$

But $*$ is associative

$$(0 * 0) * 0 = 0 * 0 = 0$$
$$0 * (0 * 0) = 0 * 0 = 0$$

We would have to test all possible triples, but after a a little bit of work we could show that $*$ is associative.

Properties of a binary operation

Example

Function composition is associative although not commutative.

Proof

Function composition is not commutative

$$(f \circ g)(x) = f(g(x)) \neq g(f(x)) = (g \circ f)(x)$$

Function composition is associative

$$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x))) = f((g \circ h)(x)) = (f \circ (g \circ h))(x)$$

Properties of a binary operation

Example

A function may not be well defined. For instance,

$$\begin{array}{rcl} / : \mathbb{Q} \times \mathbb{Q} & \rightarrow & \mathbb{Q} \\ a/b & = & \frac{a}{b} \end{array}$$

is not well defined for $b = 0 \in \mathbb{Q}$

Example

A function may not be closed in S. For instance,

$$\begin{array}{rcl} / : \mathbb{Z} \times \mathbb{Z} & \rightarrow & \mathbb{Z} \\ a/b & = & \frac{a}{b} \end{array}$$

is not closed because $a = 1 \in \mathbb{Z}, b = 3 \in \mathbb{Z}$ but $\frac{1}{3} \notin \mathbb{Z}$.

Properties of a binary operation

Definition 4.5 (Existence of a neutral element)

A binary operation has a ***neutral element****, e, iff*

$$\forall a \in S \quad a * e = e * a = a$$

Example

0 is the neutral element of addition in $\mathbb{R}$ because

$$\forall r \in \mathbb{R} \quad r + 0 = 0 + r = r$$

1 is the neutral element of multiplication in $\mathbb{R}$ because

$$\forall r \in \mathbb{R} \quad r \cdot 1 = 1 \cdot r = r$$

Addition in $\mathbb{N}$ has no neutral element since $0 \notin \mathbb{N}$.

Properties of a binary operation

Definition 4.6 (Existence of an inverse element)

A binary operation has an ***inverse element*** *iff*

$$\forall a \in S \quad \exists b \in S | a * b = b * a = e$$

being e the neutral element of $*$.

Example

The inverse element of 2 with respect to addition in $\mathbb{R}$ is -2 because

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

The inverse element of 2 with respect to multiplication in $\mathbb{R}$ is $\frac{1}{2}$ because

$$2 \cdot \frac{1}{2} = \frac{1}{2} \cdot 2 = 1$$

Multiplication in $\mathbb{N}$ has no inverse element since $\forall n \in \mathbb{N} \quad \frac{1}{n} \notin \mathbb{N}$.

Outline

10 Abstract algebra
- Sets
- Relations and functions
- Partitions and equivalence relationships
- Binary operations
- Groups and subgroups
- Homomorphisms and isomorphisms
- Algebraic structures

Groups and subgroups

Introduction

Groups and subgroups are algebraic structures. They are the ones that allow solving equations like

$$x + x = a \Rightarrow x = \frac{a}{2}$$

and that the equation

$$x \cdot x = a$$

does not have a solution in $\mathbb{R}$ if $a < 0$.
We'll see that defining a group amounts to define the elements belonging to the group as well as the operations that can be used with them.

Groups

Definition 5.1 (Group)

*Given a set S and a binary operation $*$ defined on S, the pair $(S, *)$ is a **group** if G is closed under $*$ and*

G1. *$*$ is associative in S*

G2. *$*$ has a neutral element in S*

G3. *$*$ has an inverse element in S*

Definition 5.2 (Abelian group)

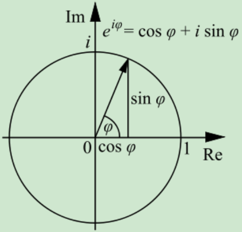
*$(S, *)$ is an **abelian group** if $(S, *)$ is a group and $*$ is commutative.*

Definition 5.3 (Subgroup)

Let $(S, *)$ be a group. Let H be a subset of S, $H \subseteq S$, and $*_H$ be the $*$ induced operation in H. The pair $(H, *_H)$ is a subgroup of $(S, *)$ if it verifies the conditions to be a group.

Example

Consider $S = \{z \in \mathbb{C} | z = e^{i\varphi} \quad \forall \varphi \in \mathbb{R}\}$. $(U, \cdot)$ is a group.



Proof

G1. $\cdot$ is associative in S

$$z_1(z_2z_3) = e^{i\varphi_1}(e^{i\varphi_2}e^{i\varphi_3}) = e^{i\varphi_1}(e^{i(\varphi_2+\varphi_3)}) = e^{i(\varphi_1+\varphi_2+\varphi_3)}$$
$$(z_1z_2)z_3 = (e^{i\varphi_1}e^{i\varphi_2})e^{i\varphi_3} = (e^{i\varphi_1+\varphi_2})e^{i\varphi_3} = e^{i(\varphi_1+\varphi_2+\varphi_3)}$$

Example (continued)

Proof

G2. $\cdot$ has a neutral element in S
$1 = e^{i0} \in S$

$$z \cdot 1 = e^{i\varphi} e^{i0} = e^{i(\varphi+0)} = e^{i\varphi} = z$$
$$1 \cdot z = e^{i0} e^{i\varphi} = e^{i(0+\varphi)} = e^{i\varphi} = z$$

G3. $\cdot$ has an inverse element in S
For each $z = e^{i\varphi}$, its inverse element with respect to $\cdot$ is $z^{-1} = e^{-i\varphi}$

$$zz^{-1} = e^{i\varphi} e^{-i\varphi} = e^{i(\varphi-\varphi)} = e^{i0} = 1$$
$$z^{-1}z = e^{-i\varphi} e^{i\varphi} = e^{i(-\varphi+\varphi)} = e^{i0} = 1$$

Groups

Example

- $(\mathbb{N}, +)$ is not a group because it has no neutral element.
- $(\mathbb{N} \cup \{0\}, +)$ is not a group because it has no inverse element.
- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ and $(\mathbb{R}^n, +)$ are abelian groups.
- $(\mathcal{M}_{m\times n}, +)$ is an abelian group.
- $(\mathbb{R}, \cdot)$ is not a group because 0 has no inverse.
- $(\mathcal{M}_{n\times n}(\mathbb{R})), \cdot)$ is not a group because $\begin{pmatrix} 0 & 0 & ... & 0 \\ 0 & 0 & ... & 0 \\ ... & ... & ... & ... \\ 0 & 0 & ... & 0 \end{pmatrix}$ has no inverse.
- Let $S \in \mathcal{M}_{n\times n}(\mathbb{R})$ be the set of invertible matrices of size $n \times n$. $(S, \cdot)$ is a group (although not abelian). It is called the General Linear Group of degree n ($GL(n, \mathbb{R})$).

Groups

Example

The existence of groups is what allows us to solve equations. For instance, consider the equation

$$5 + x = 2$$

and its solution in the group $(\mathbb{Z}, +)$

$$\begin{array}{rcll} 5 + x & = & 2 & \text{[Addition of the inverse of 5 with respect to + in both} \\ -5 + (5 + x) & = & -5 + 2 & \text{[Addition is associative]} \\ (-5 + 5) + x & = & -3 & \text{[Definition of inverse]} \\ 0 + x & = & -3 & \text{[Definition of neutral element]} \\ x & = & -3 & \end{array}$$

Example

Consider the equation

$$2x = 3$$

and its solution in the group $(\mathbb{Q}, \cdot)$

$$\begin{array}{rcll}
2x & = & 3 & \text{[Multiplication by the inverse of 2 in both sides]} \\
\frac{1}{2}(2x) & = & \frac{1}{2}3 & \text{[Multiplication is associative]} \\
(\frac{1}{2}2)x & = & \frac{2}{3} & \text{[Definition of inverse]} \\
1x & = & \frac{2}{3} & \text{[Definition of neutral element]} \\
x & = & \frac{2}{3} &
\end{array}$$

Groups

Theorem 5.1 (Cancellation laws)

Given any group $(S, *)$, $\forall a, b, c \in S$ it is verified

- *Left cancellation:* $a * b = a * c \Rightarrow b = c$
- *Right cancellation:* $b * a = c * a \Rightarrow b = c$

Theorem 5.2 (Existance of a unique solution of linear equations)

Given any group $(S, *)$, $\forall a, b \in S$ the linear equations

$$a * x = b \text{ and } y * a = b$$

always have a unique solution in S.

Theorem 5.3 (Properties of the inverse)

Given any group $(S, *)$, $\forall a \in S$ its inverse is unique and $\forall a, b \in S$

$$(a * b)^{-1} = (b^{-1}) * (a^{-1})$$

Outline

10 Abstract algebra
- Sets
- Relations and functions
- Partitions and equivalence relationships
- Binary operations
- Groups and subgroups
- Homomorphisms and isomorphisms
- Algebraic structures

Homomorphisms

Example

Consider the sets $S = \{a, b, c\}$ and $S' = \{A, B, C\}$ with the operations $* : S \times S \to S$ and $*' : S' \times S' \to S'$

$x * y$	$y = a$	$y = b$	$y = c$
$x = a$	a	b	c
$x = b$	b	c	a
$x = c$	c	a	b

and

$x *' y$	$y = A$	$y = B$	$y = C$
$x = A$	A	B	C
$x = B$	B	C	A
$x = C$	C	A	B

We may construct a function that "translates" elements in S into elements in S' with the "same properties".

$$\begin{array}{rcl} \phi : S & \to & S' \\ \phi(a) & = & A \\ \phi(b) & = & B \\ \phi(c) & = & C \end{array}$$

We note that

$$b * c = a \Rightarrow \phi(b) *' \phi(c) = \phi(a) \Rightarrow B *' C = A$$

Homomorphisms

Definition 6.1 (Group homomorphism)

Given two groups $(S, *)$ *and* $(S', *')$*, the function* $\phi : S \to S'$ *is a* ***group homomorphism*** *iff* $\forall a, b \in S$

$$\phi(a * b) = \phi(a) *' \phi(b)$$

Definition 6.2 (Group isomorphism)

Given two groups $(S, *)$ *and* $(S', *')$*, the function* $\phi : S \to S'$ *is a group isomorphism iff it is a group homomorphism and it is bijective.*

Homomorphisms

Example

Consider the two groups $(\mathbb{R}^n, +)$ and $(\mathbb{R}^m, +)$ and a matrix $A \in \mathcal{M}_{m\times n}(\mathbb{R})$. The application

$$\begin{array}{rcl} \phi : \mathbb{R}^n & \to & \mathbb{R}^m \\ \phi(\mathbf{x}) & = & A\mathbf{x} \end{array}$$

is a group homomorphism because

$$\phi(\mathbf{u}+\mathbf{v}) = A(\mathbf{u}+\mathbf{v}) = A\mathbf{u} + A\mathbf{v} = \phi(\mathbf{u}) + \phi(\mathbf{v})$$

Example

Consider the two groups $(GL(n,\mathbb{R}), \cdot)$ and $(\mathbb{R}, \cdot)$. The application

$$\begin{array}{rcl} \phi : GL(n,\mathbb{R}) & \to & \mathbb{R} \\ \phi(A) & = & \det\{A\} \end{array}$$

is a group homomorphism because

$$\phi(AB) = \det\{AB\} = \det\{A\}\det\{B\} = \phi(A)\cdot\phi(B)$$

Homomorphisms

Theorem 6.1

Let $\phi : S \to S'$ be a group homomogrphism between two groups. Then,

- $\phi(e) = e'$
- $\phi(a^{-1}) = (\phi(a))^{-1}$

Definition 6.3 (Kernel of a group homomorphism)

Let $\phi : S \to S'$ be a group homomogrphism between two groups. Then, the kernel of ϕ is the set

$$\mathrm{Ker}\{\phi\} = \{x \in S | \phi(x) = e'\}$$

Example

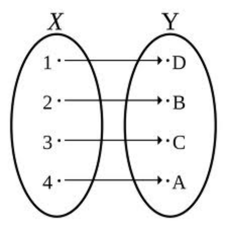
Let $\phi(\mathbf{x}) = A\mathbf{x}$. Then,

$$\mathrm{Ker}\{\phi\} = \{x \in \mathbb{R}^n | A\mathbf{x} = \mathbf{0}\} = \mathrm{Nul}\{A\}$$

Isomorphisms

Theorem 6.2 (Isomorphisms and cardinality)

If two groups $(S, *)$ and $(S', *')$ are isomorph (i.e., there exists an isomorphism between the two groups), then S and S' have the same cardinality.



Isomorphisms

Example

- $\mathbb{Q}$ and $\mathbb{R}$ cannot be isomorph because the cardinality of $\mathbb{Q}$ is $\aleph_0$ and the cardinality of $\mathbb{R}$ is $\aleph_1$.
- There are as many natural numbers as natural even numbers. In other words, the cardinality of $\mathbb{N}$ and $2\mathbb{N}$ are the same. The reason is that the function $\phi(n) = 2n$ is an isomorphism between $\mathbb{N}$ and $2\mathbb{N}$.

Example

Consider the set $\mathbb{R}_c = [0, c) \in \mathbb{R}$ and the operation $x +_c y = (x + y) \mod c$. The pair $(\mathbb{R}_c, +_c)$ is a group. Consider now the two particular cases $(\mathbb{R}_{2\pi}, +_{2\pi})$ and $(\mathbb{R}_1, +_1)$ and the mapping

$$\begin{array}{rcl} \phi : \mathbb{R}_{2\pi} & \rightarrow & \mathbb{R}_1 \\ \phi(x) & = & \frac{x}{2\pi} \end{array}$$

ϕ is an isomorphism between $(\mathbb{R}_{2\pi}, +_{2\pi})$ and $(\mathbb{R}_1, +_1)$. In fact, all $(\mathbb{R}_c, +_c)$ groups are isomorph to any other $(\mathbb{R}_{c'}, +_{c'})$ group.

Isomorphisms

Cardinality is a *group property*. The nice things about isomorphisms is that they preserve group properties.

Theorem 6.3

If two groups $(S, *)$ and $(S', *')$ are isomorph, then

- *If $*$ is commutative, so is $*'$.*
- *If there is an order relation in S, it can be "translated" into an order relation in S'.*
- *If $\forall s \in S$ there exists a solution in S of the equation $x * x = s$, then $\forall s' \in S'$ there exists a solution in S' of the equation $x' *' x' = s'$.*
- *If $\forall a, b \in S$ there exists a solution in S of the equation $a * x = b$, then $\forall a', b' \in S'$ there exists a solution in S' of the equation $a' *' x' = b'$.*
- *The kernel of any isomorphism ϕ between $(S, *)$ and $(S', *')$ is $\mathrm{Ker}\{\phi\} = \{e\}$ being e the neutral element of $*$ in S.*

Isomorphisms

Example

$((Z), +)$ is not isomorph to $((Q), +)$ because the equation

$$x + x = s$$

has a solution in $\mathbb{Q}$ for any $s \in \mathbb{Q}$ (that is $x = \frac{s}{2}$), but it does not have a solution in $\mathbb{Z}$ for any $s \in \mathbb{Z}$ (it only has a solution in $\mathbb{Z}$ if s is an even number).

Example

$((R), \cdot)$ is not isomorph to $((C), \cdot)$ because the equation

$$x \cdot x = z$$

has two solution in $\mathbb{C}$ for any $z \in \mathbb{C}$ (if $z = re^{i\theta}$, then $x = \pm re^{i\frac{\theta}{2}}$ are the two solutions) , but it does not have a solution in $\mathbb{R}$ for any $z \in \mathbb{R}$ (it only has a solution in $\mathbb{R}$ if z is a non-negative number).

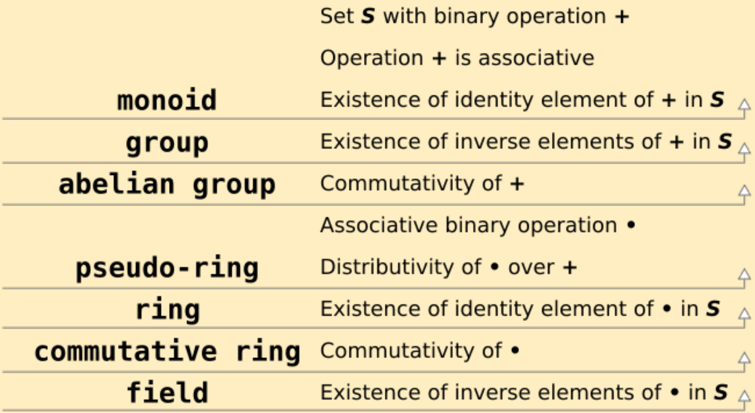
Outline

10 Abstract algebra

- Sets
- Relations and functions
- Partitions and equivalence relationships
- Binary operations
- Groups and subgroups
- Homomorphisms and isomorphisms
- Algebraic structures

Algebraic structures

Algebraic structures are tools that help us to define operate on numbers and elements within a set, solve equations, etc.



Algebraic structures

Definition 7.1 (Ring)

The tuple $(S, *, \circ)$ *is a* ***ring*** *iff*

R1. $(S, *)$ *is an abelian group.*

R2. $\circ$ *is associative.*

R3. $\circ$ *is distributive with respect to* $*$*, i.e.,* $\forall a, b, c \in S$

- *Left-distributive:* $a \circ (b * c) = (a \circ b) * (a \circ c)$
- *Right-distributive:* $(a * b) \circ c = (a \circ c) * (b \circ c)$

Example

- $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ are rings.
- $(\mathcal{M}_{m\times n}(\mathbb{R}), +, \cdot)$ is a ring.
- $(\mathbb{R} \to \mathbb{R}, +, \cdot)$ is a ring.

Theorem 7.1 (Properties of rings)

Let $(S, *, \circ)$ be a ring and let e be the neutral element of $*$ in S. For any $a \in S$, let a' be the inverse of a with respect to the operation $*$. Then $\forall a, b \in S$

- $a \circ e = e \circ a = e$.
- $a \circ b' = a' \circ b = (a \circ b)'$
- $a' \circ b' = a \circ b$

Example

Consider the ring $(\mathbb{R}, +, \cdot)$. We are used to the properties $\forall a, b \in \mathbb{R}$

- $a \cdot 0 = 0 \cdot a = 0$.
- $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$
- $(-a) \cdot (-b) = a \cdot b$

But, as stated by the previous theorem, these are properties of all rings.

Definition 7.2 (Kinds of rings)

A ring $(S, *, \circ)$ is

- ***commutative*** *iff $\circ$ is commutative.*
- ***unitary*** *iff $\circ$ has a neutral element (referred as 1).*
- ***divisive*** *if it is unitary and*

$$\forall a \in S - \{e\} \quad \exists! a^{-1} \in S, | a \circ a^{-1} = a^{-1} \circ a = 1$$

  That is each element has a multiplicative inverse.

Example

- $(\mathbb{P}, +, \cdot)$ the set of polynomials with coefficients from a ring is a ring.

Algebraic structures

Definition 7.3 (Field (*cuerpo*))

A divisive, commutative ring is called a ***field****.*

Example

- $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, and $(\mathbb{C}, +, \cdot)$ are fields.
- $(\mathbb{Z}, +, \cdot)$ is not a field because multiplication has not an inverse in $\mathbb{Z}$.

Definition 7.4 (Vector space over a field)

Consider a field $(\mathbb{K}, *, \circ)$. *A* ***vector space*** *over this field is a tuple* $(V, +, \cdot)$ *so that* V *is a set whose elements are called vectors, and* $+ : V \times V \to V$ *is a binary operation under which* V *is closed,* $\cdot : \mathbb{K} \times V \to V$ *is an operation between scalars in the field* $(\mathbb{K})$ *and vectors in the vector space* (V) *such that* $\forall a, b \in \mathbb{K}, \forall \mathbf{u}, \mathbf{v} \in V$

V1. $(V, +)$ *is an abelian group.*

V2. $(a \cdot \mathbf{u}) \in V$

V3. $a \cdot (b \cdot \mathbf{u}) = (a \circ b) \cdot \mathbf{u}$

V4. $(a * b) \cdot \mathbf{u} = a \cdot \mathbf{u} + b \cdot \mathbf{u}$

V5. $a \cdot (\mathbf{u} + \mathbf{v}) = a \cdot \mathbf{u} + a \cdot \mathbf{v}$

V6. $1 \cdot \mathbf{u} = \mathbf{u}$

Algebraic structures

Examples

- $(\mathbb{R}^n, +, \cdot)$ and $(\mathbb{C}^n, +, \cdot)$.
- $(\mathcal{M}_{m\times n}(\mathbb{R}), +, \cdot)$: the set of matrices of a given size with coefficients in a field.
- $(\mathbb{P}, +, \cdot)$: the set of polynomials with coefficients in a field.
- $(\{X \to V\}, +, \cdot)$: the set of all functions from an arbitrary set X onto an arbitrary vector space V.
- The set of all continuous functions is a vector space.
- The set of all linear maps between two vector spaces is also a vector space.
- The set of all infinite sequences of values from a field is also a vector space.

Algebraic structures

Definition 7.5 (Algebra)

Consider a vector space $(V, +, \cdot)$ *over a field* $(\mathbb{K}, *, \circ)$ *and a binary operation* $\bullet : V \times V \to V$. $(V, +, \cdot, \bullet)$ *is an* ***algebra*** *iff* $\forall a, b \in \mathbb{K}, \forall \mathbf{u}, \mathbf{v}, \mathbf{w} \in V$

A1. Left distributivity: $(\mathbf{u} + \mathbf{v}) \bullet \mathbf{w} = \mathbf{u} \bullet \mathbf{w} + \mathbf{v} \bullet \mathbf{w}$

A2. Right distributivity: $\mathbf{u} \bullet (\mathbf{v} + \mathbf{w}) = \mathbf{u} \bullet \mathbf{v} + \mathbf{u} \bullet \mathbf{w}$

A3. Compatibility with scalars: $(a \cdot \mathbf{u}) \bullet (b \cdot \mathbf{v}) = (a \circ b) \cdot (\mathbf{u} \bullet \mathbf{v})$

Examples

- Real numbers ($\mathbb{R}$) are an algebra ("1D").
- Complex numbers ($\mathbb{C}$) are an algebra ("2D").
- Quaternions are an algebra ("4D").

Outline

10 Abstract algebra
- Sets
- Relations and functions
- Partitions and equivalence relationships
- Binary operations
- Groups and subgroups
- Homomorphisms and isomorphisms
- Algebraic structures