

MAT 311 Abstract Algebra

Peter Schaefer

Spring 2024

Contents

1	Sets and Relations	2
1.1	Sets	2
1.2	Relations	3
1.3	Partitions and Equivalence Relations	3
2	Binary Operations	5
2.1	Finite Sets	5
3	Isomorphic Binary Structures	7
4	Groups	9

1 Sets and Relations

Definition: What *is* Abstract Algebra

- Algebra: procedures for performing operations, i.e. $+$, $-$, \times , \div , and methods for solving equations. It uses bldspecific operations on **specific** objects.
- Abstract Algebra: discuss **general** structures and the relationships between the elements of these structures.

1.1 Sets

Definition: Set

A set is a collection of objects. These objects are called "elements". A set is typically uppercase, and elements are typically lowercase.

Set Notation

1. List Notation:

$$B = \{\text{John, Paul, Ringo, George}\}$$

$$\mathbb{N} = \{1, 2, 3, \dots\}$$

2. Set-builder Notation:

$$B = \{b : b \text{ is a Beatle}\}$$

Well-Defined Sets

Sets must be **well-defined**. That is, given set S and any element x , either $x \in S$ or $x \notin S$.

Definition: Subset

A set A is a subset of set B , written as $A \subseteq B$, if every element of A is also in B .

Note: every non-empty set has at least two subsets:

- The set itself
- \emptyset

Definition: Proper Subset

If $A \subseteq B$ but $A \neq B$, then A is a **proper subset** of B , written $A \subset B$ or $A \subsetneq B$.

Note: A set B is an *improper subset* of itself.

Definition: Cartesian Product

Let A and B be sets. The set $A \times B = \{(a, b) : a \in A \text{ and } b \in B\}$ is the cartesian product of A and B .

Note: $A \times B = B \times A \iff A = B$, or $A \times B = \emptyset$.

Example

Let $A = \{c : c \text{ is a primary color}\}$ and let $B = \{\epsilon, \delta\}$. Find:

1. $B \times B = \{(\epsilon, \epsilon), (\epsilon, \delta), (\delta, \epsilon), (\delta, \delta)\}$
2. $A \times \emptyset = \emptyset$

1.2 Relations

Definition: Relation

A **relation** between sets A and B is a subset \mathcal{R} of $A \times B$. It is a collection of ordered pairs. Note: $(a, b) \in \mathcal{R} \equiv a\mathcal{R}b$ means "a is related to b".

Definition: Function

A **function** is a relation in which no two of the ordered pairs have the same first term. Note: if $f : \mathbb{R} \rightarrow \mathbb{R}$ is a function, then it passes the vertical-line test.

Definition: One-to-One

A function is **one-to-one**, or **injective**, if no two ordered pairs have the same second term.

To prove f is one-to-one, first assume that $f(x_1) = f(x_2)$, then show that $x_1 = x_2$.

Definition: Onto

A function $f : X \rightarrow Y$ is **onto**, or **surjective**, if the codomain is equal to the range, meaning every element $y \in Y$ has some $x \in X$ such that $f(x) = y$.

Definition: One-to-One Correspondence

A function $f : X \rightarrow Y$ is a **one-to-one correspondence**, or a **bijection**, if it is both one-to-one and onto.

1.3 Partitions and Equivalence Relations

Definition: Partition

A **partition** of a set S is a collection of non-empty subsets of S such that:

1. The union of these subsets is S .
2. These subsets are pairwise disjoint.

Note: these subsets are called **cells** of the partition.

Definition: Equivalence Relation

An **equivalence relation** \mathcal{R} on a set S must be:

1. Reflexive, meaning $x\mathcal{R}x \quad \forall x \in S$.
2. Symmetric, meaning if $x\mathcal{R}y$, then $y\mathcal{R}x$.
3. Transitive, meaning if $x\mathcal{R}y$ and $y\mathcal{R}z$, then $x\mathcal{R}z$.

Definition: Equivalence Class

$\bar{x} = \{y \in S : x\mathcal{R}y\}$ is the equivalence class of x

Example

Let $S = \mathbb{R}$. Define $x\mathcal{R}y$ iff $x \geq y$. Is \mathcal{R} an equivalence relation on S ?

1. Is \mathcal{R} reflexive? $\forall x \in S, x\mathcal{R}x$, so YES.
2. Is \mathcal{R} symmetric? Consider 5 and 1: $5 \geq 1$ but $1 \not\geq 5$, so NO.
3. Is \mathcal{R} transitive? If $x \geq y$ and $y \geq z$ then $x \geq z$, so YES.

Since \mathcal{R} is not symmetric, it is not an equivalence relation on S .

Note on Partition Cells and Equivalence Classes

Partitions give rise to equivalence relations and vice versa. The *cells* of the partition are analogous to the *equivalence classes* of the equivalence relation.

2 Binary Operations

Definition: Binary Operation

A **binary operation** $*$ on a set S is a function from $S \times S$ into S , $*$: $S \times S \rightarrow S$. That is, $*$ is a rule which assigns to each ordered pair $(a, b) \in S \times S$ exactly one element $a * b \in S$.

Condition 1: Uniquely Defined

For all $a, b \in S \times S$, $a * b$ must be **uniquely defined**. This means that $*$ cannot be undefined for any $a * b$, and each $a * b$ must have exactly one result, not two or more.

Condition 2: Closed under $*$

S must be **closed** under $*$. That is,

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

Definition: Commutative

A binary operation $*$ on a set S is commutative if

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

Definition: Associative

A binary operation $*$ on a set S is associative if

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

2.1 Finite Sets

Example

Let $S = \{a, b, c, d\}$. Define a binary operation $*$ on S using the following table. Complete the table so that $*$ is commutative.

$*$	a	b	c	d
a	b	d	a	a
b	d	a	c	b
c	a	c	b	b
d	a	b	b	c

Note: $*$ is commutative iff the table is symmetric along the main diagonal.
Is $*$ associative? Why or why not? **No**,

$$\begin{aligned} a * (b * c) &= a * c = a \\ (a * b) * c &= d * c = b \end{aligned}$$

Example

Suppose that $*$ is associative and commutative operation on a set S . Show that $H = \{a \in S : a * a = a\}$ is closed under $*$. Note that the elements of H are called **idempotents** of the binary operation $*$.

Proof. Let $a, b \in H$. Show $a * b \in H$.

We know $a * a = a$ and $b * b = b$. Show $(a * b) * (a * b) = a * b$.

$$\begin{aligned} LHS &= (a * b) * (a * b) \\ &= a * (b * a) * b && \text{since } * \text{ is associative} \\ &= a * (a * b) * b && \text{since } * \text{ is commutative} \\ &= (a * a) * (b * b) && \text{since } * \text{ is associative} \\ &= a * b \\ &= RHS \end{aligned}$$

Thus, H is closed under $*$.

□

3 Isomorphic Binary Structures

Definition: Binary Algebraic Structure

A **binary algebraic structure** $\langle S, * \rangle$ is a set S together with a binary operation $*$.

Definition: Isomorphism

Let $\langle S, * \rangle$ and $\langle S', *' \rangle$ be binary structures. An **isomorphism** of S with S' is a *one-to-one* function $\phi : S \mapsto S'$ such that

$$\forall x, y \in S, \quad \phi(x * y) = \phi(x) *' \phi(y).$$

Notation: $\langle S, * \rangle \simeq \langle S', *' \rangle$

Example 1

Prove that $\langle \mathbb{R}, + \rangle \simeq \langle \mathbb{R}^+, \cdot \rangle$.

Proof. Consider $\phi : \mathbb{R} \mapsto \mathbb{R}^+$, where $\phi(x) = e^x$.

1. One-to-one: Assume $\phi(x_1) = \phi(x_2)$ for some $x_1, x_2 \in \mathbb{R}$.

$$\begin{aligned} \phi(x_1) &= \phi(x_2) \\ e^{x_1} &= e^{x_2} \\ \ln e^{x_1} &= \ln e^{x_2} \\ x_1 &= x_2 \end{aligned}$$

Thus ϕ is one-to-one.

2. Onto: Let $y \in \mathbb{R}^+$. Let us find $x \in \mathbb{R}$ such that $y = \phi(x)$.

$$\begin{aligned} y &= \phi(x) = e^x \\ \ln y &= \ln e^x = x \end{aligned}$$

Choose $x = \ln y$. Thus ϕ is onto.

3. Operation Preserving: Need to show that $\phi(x + y) = \phi(x) \cdot \phi(y)$.

$$\begin{aligned} \phi(x + y) &= e^{x+y} \\ &= e^x \cdot e^y \\ &= \phi(x) \cdot \phi(y) \end{aligned}$$

Thus ϕ is operation preserving.

Since ϕ is one-to-one, onto, and operation preserving, thus ϕ is an isomorphism of $\langle \mathbb{R}, + \rangle$ and $\langle \mathbb{R}^+, \cdot \rangle$, and $\langle \mathbb{R}, + \rangle \simeq \langle \mathbb{R}^+, \cdot \rangle$. \square

Definition: Identity Element

Let $\langle S, * \rangle$ be an algebraic structure. An element $e \in S$ is the identity element **id** for $*$ if for all $s \in S$:

$$\underbrace{\overbrace{e * s}^{\text{left id}} = \overbrace{s * e}^{\text{right id}}}_{\text{two-sided id}} = s$$

Theorem: Identity Uniqueness

A binary structure $\langle S, * \rangle$ has at most one identity element.

Proof. Assume e_1 and e_2 are both identity elements for $\langle S, * \rangle$. Thus,

$$\begin{array}{ll} e_1 * e_2 = e_1 & \text{since } e_1 \text{ is id} \\ e_1 * e_2 = e_2 & \text{since } e_2 \text{ is id} \end{array}$$

Since binary operations are uniquely defined, $e_1 = e_2$ must be true. $\therefore \langle S, * \rangle$ has at most one identity element. \square

Theorem: Isomorphism and Identity

Suppose $\langle S, * \rangle$ has identity element e . If $\phi : S \mapsto S'$ is an isomorphism of $\langle S, * \rangle$ with $\langle S', *' \rangle$, then $\phi(e)$ is the identity element for $\langle S', *' \rangle$.

Proof. Assume $\langle S, * \rangle$ has identity e and $\phi : S \mapsto S'$ is an isomorphism. Let $s' \in S'$.

$$\begin{aligned} \phi(e) *' s' &= \phi(e) *' \phi(s) \\ &= \phi(e * s) && \text{since } \phi \text{ is operation preserving} \\ &= \phi(s) = s' \end{aligned}$$

Thus $\phi(e) *' s' = s'$.

$$\begin{aligned} s' *' \phi(e) &= \phi(s) *' \phi(e) \\ &= \phi(s * e) && \text{since } \phi \text{ is operation preserving} \\ &= \phi(s) = s' \end{aligned}$$

Thus $s' *' \phi(e) = s'$. So $\phi(e) *' s' = s' *' \phi(e) = s'$. Thus $\phi(e)$ is the identity of $\langle S', *' \rangle$. \square

Showing Two Binary Structure are *not* Isomorphic

To show that two binary structures are *not* isomorphic, you need to show that one binary structure has some property that other does not, meaning they are structurally distinct.

Example

Is $\langle \mathbb{Z}, + \rangle \simeq \langle \mathbb{R}, \cdot \rangle$? **No**, because \mathbb{Z} is countably infinite, whereas \mathbb{R} are uncountably infinite. These two sets have different cardinalities.

4 Groups

Definition: Group

A **group** $\langle G, * \rangle$ is a set G *closed* under the binary operation $*$, such that the following axioms are satisfied:

\mathfrak{G}_1 : For all $a, c, b \in G$, we have

$$(a * b) * c = a * (b * c). \quad \text{associativity of } *$$

\mathfrak{G}_2 : There is an element e in G such that for all $x \in G$,

$$e * x = x * e = x. \quad \text{identity element } e \text{ for } *$$

\mathfrak{G}_3 : Corresponding to each $a \in G$, there is an element a' in G such that

$$a * a' = a' * a = e. \quad \text{inverse } a' \text{ of } a$$

Note: G does not *need* to be commutative.

Definition: Abelian Group

A group G is **Abelian** if its binary operation is **commutative**.