

MAT 311 Abstract Algebra

Peter Schaefer

Spring 2024

Contents

| | | |
|----------|--|-----------|
| 1 | Sets and Relations | 3 |
| 1.0.1 | Def. What <i>is</i> Abstract Algebra | 3 |
| 1.1 | Sets | 3 |
| 1.1.1 | Def. Set | 3 |
| 1.1.2 | Def. Subset | 3 |
| 1.1.3 | Def. Proper Subset | 3 |
| 1.1.4 | Def. Cartesian Product | 3 |
| 1.2 | Relations | 4 |
| 1.2.1 | Def. Relation | 4 |
| 1.2.2 | Def. Function | 4 |
| 1.2.3 | Def. One-to-One | 4 |
| 1.2.4 | Def. Onto | 4 |
| 1.2.5 | Def. One-to-One Correspondence | 4 |
| 1.3 | Partitions and Equivalence Relations | 4 |
| 1.3.1 | Def. Partition | 4 |
| 1.3.2 | Def. Equivalence Relation | 4 |
| 1.3.3 | Def. Equivalence Class | 4 |
| 2 | Binary Operations | 6 |
| 2.0.1 | Def. Binary Operation | 6 |
| 2.0.2 | Def. Commutative | 6 |
| 2.0.3 | Def. Associative | 6 |
| 2.1 | Finite Sets | 6 |
| 3 | Isomorphic Binary Structures | 8 |
| 3.0.1 | Def. Binary Algebraic Structure | 8 |
| 3.0.2 | Def. Isomorphism | 8 |
| 3.0.3 | Def. Identity Element | 8 |
| 3.0.4 | Thm. Identity Uniqueness | 9 |
| 3.0.5 | Thm. Isomorphism and Identity | 9 |
| 4 | Groups | 10 |
| 4.0.1 | Def. Group | 10 |
| 4.0.2 | Def. Abelian Group | 10 |
| 4.0.3 | Thm. Cancellation Laws | 10 |
| 4.0.4 | Thm. Unique Solutions | 10 |
| 4.0.5 | Thm. Unique Identity and Inverse | 11 |
| 4.0.6 | Thm. Inverse of Two Elements | 11 |
| 4.1 | Finite Groups and Group Tables | 11 |

| | | |
|----------|--|-----------|
| 5 | Subgroups | 13 |
| 5.1 | Notation | 13 |
| 5.1.1 | Def. Order | 13 |
| 5.1.2 | Def. Subgroup | 13 |
| 5.1.3 | Def. Improper and Proper Subgroups | 13 |

1 Sets and Relations

1.0.1 Def. 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

1.1.1 Def. 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 $x \notin S$.

1.1.2 Def. 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

1.1.3 Def. 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.

1.1.4 Def. 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

1.2.1 Def. 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".

1.2.2 Def. 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.

1.2.3 Def. 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 $x_1 = x_2$.

1.2.4 Def. 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 $f(x) = y$.

1.2.5 Def. 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

1.3.1 Def. 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.

1.3.2 Def. 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 $x\mathcal{R}z$.

1.3.3 Def. 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

2.0.1 Def. 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,

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

2.0.2 Def. Commutative

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

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

2.0.3 Def. 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

3.0.1 Def. Binary Algebraic Structure

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

3.0.2 Def. 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 $x_1, x_2 \in \mathbb{R}$.

$$\phi(x_1) = \phi(x_2)$$

$$e^{x_1} = e^{x_2}$$

$$\ln e^{x_1} = \ln e^{x_2}$$

$$x_1 = x_2$$

Thus ϕ is one-to-one.

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

$$y = \phi(x) = e^x$$

$$\ln y = \ln e^x = x$$

Choose $x = \ln y$. Thus ϕ is onto.

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

$$\phi(x + y) = e^{x+y}$$

$$= e^x \cdot e^y$$

$$= \phi(x) \cdot \phi(y)$$

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

3.0.3 Def. Identity Element

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

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

3.0.4 Thm. 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,

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

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

3.0.5 Thm. 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

4.0.1 Def. 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.

4.0.2 Def. Abelian Group

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

4.0.3 Thm. Cancellation Laws

If $\langle G, * \rangle$ is a group, then the left and right cancellation laws hold in G .

• **Left:**

$$\text{if } a * b = a * c \text{ then } b = c$$

• **Right:**

$$\text{if } b * a = c * a \text{ then } b = c$$

Proof for Left. Assume $\langle G, * \rangle$ is a group and $a * b = a * c$:

$$\begin{aligned} a * b &= a * c \\ \bar{a} * a * b &= \bar{a} * a * c & \mathfrak{G}_3 \\ e * b &= e * c & \mathfrak{G}_3 \\ b &= c & \mathfrak{G}_2 \end{aligned}$$

□

The proof for right cancellation follows the same structure.

4.0.4 Thm. Unique Solutions

If $\langle G, * \rangle$ is a group and if $a, b \in G$, then $a * x = b$ and $y * a = b$ have unique solutions x and y in G .

Proof. Assume $\langle G, * \rangle$ is a group and consider $a * x = b$ for $a, b \in G$.

$$\begin{aligned} a * x &= b \\ \bar{a} * (a * x) &= \bar{a} * b & \mathfrak{G}_3 \\ (\bar{a} * a) * x &= \bar{a} * b & \mathfrak{G}_1 \\ e * x &= \bar{a} * b & \mathfrak{G}_3 \\ x &= \bar{a} * b & \mathfrak{G}_2 \end{aligned}$$

Assume x_1 and x_2 are both solutions to the above equation.

$$a * x_1 = b \text{ and } a * x_2 = b$$

Thus $a * x_1 = a * x_2$. By left cancellation,

$$x_1 = x_2$$

Thus the solution is unique. □

The $y * a = b$ proof follows the same structure.

4.0.5 Thm. Unique Identity and Inverse

If $\langle G, * \rangle$ is a group, then the identity element and the inverse of each element are unique.

4.0.6 Thm. Inverse of Two Elements

Let $\langle G, * \rangle$ be a group. Then for all $a, b \in G$, we have $(a * b)' = a' * b'$.

Proof.

$$\begin{array}{ll}
 (a * b) * (a * b)' = e & \text{by definition of } \mathfrak{G}_3 \\
 a * b * (a * b)' = e & \mathfrak{G}_1, \text{ associativity} \\
 (a' * a) * b * (a * b)' = a' * e & \mathfrak{G}_1 \\
 b * (a * b)' = a' * e & \mathfrak{G}_3 \\
 b' * b * (a * b)' = b' * a' * e & \\
 (a * b)' = b' * a' & \mathfrak{G}_1, \mathfrak{G}_3
 \end{array}$$

□

4.1 Finite Groups and Group Tables

Cayley Tables

Let $\langle G, * \rangle$ be a finite group.

1. If $\|G\| = 1$, then $G = \{e\}$, where e is the identity.

$$\begin{array}{c|c}
 * & e \\
 \hline
 e & e
 \end{array}$$

This is known as the **trivial group**.

2. If $\|G\| = 2$, then $G = \{e, a\}$.

$$\begin{array}{c|cc}
 * & e & a \\
 \hline
 e & e & a \\
 a & a & e
 \end{array}$$

Note: by \mathfrak{G}_3 , e must appear in every row and column of a group table, and exactly once.

3. If $\|G\| = 3$, then $G = \{e, a, b\}$

$$\begin{array}{c|ccc}
 * & e & a & b \\
 \hline
 e & e & a & b \\
 a & a & b & e \\
 b & b & e & a
 \end{array}$$

Claim: No row or column of a Cayley Table may contain the same element twice.

Proof. Let $a, x, y \in G$ for $\langle G, * \rangle$, where $x \neq y$. Consider the Cayley Table:

| $*$ | e | a | \cdots | x | \cdots | y |
|-----|-----|-----|----------|---------|----------|---------|
| e | e | a | \cdots | x | \cdots | y |
| a | a | $-$ | \cdots | $a * x$ | \cdots | $a * y$ |

Suppose a row can have the same element twice, say $a * x = a * y$. By left cancellation $x = y$, a contradiction. Thus no row or column can have the same element twice. \square

By the pigeon-hole principle, each element of a group must be represented in each row and column exactly once.

5 Subgroups

5.1 Notation

1. Usually we will not use $*$ to denote a binary operation and instead will use *juxtaposition*. That is, we write ab instead of $a * b$. If the binary operation is commutative, $a + b$ is often used.
2. 0 is often used to represent the identity for the operation $+$ and 1 to represent the identity for \cdot . We will also continue to use e , and personally I will often use **id**.
3. Instead of a' to represent a 's inverse, we will use the more common a^{-1} when the operation is \cdot and $-a$ when the operation is $+$.
4. Exponentiation:

$$\begin{aligned} a^n &= aaa \cdots a && (n \text{ copies}) \\ a^{-n} &= a^{-1}a^{-1} \cdots a^{-1} && (n \text{ copies}) \\ a^0 &= e \end{aligned}$$

5.1.1 Def. Order

If G is a group, then the **order** of G , denoted as $|G|$, is the number of elements in G .

5.1.2 Def. Subgroup

Let H be a subset of a group G . H is a **subgroup** of G if H itself is a group under the operation of G .
Notation: $H \leq G$.

5.1.3 Def. Improper and Proper Subgroups

G is an **improper** subgroup of itself. All other subgroups of G are **proper** subgroups, denoted as $H < G$.

Fact: All groups have a trivial subgroup $\{e\}$.