MAT 311 Abstract Algebra

Peter Schaefer

Spring 2024

Contents

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:

$$B = \{\text{John}, \text{Paul}, \text{Ringo}, \text{George}\}$$
$$\mathbb{N} = \{1, 2, 3, \ldots\}$$

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 $f : \mathbb{R} \to \mathbb{R}$ is a function, then is 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 $f : X \to Y$ 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 $f : X \to Y$ 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

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

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 $1 \ngeq 5$, 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, $* : S \times S \to S$. 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,

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

2.0.2 Def. Commutative

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

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

2.0.3 Def. Associative

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

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

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**,

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

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 **idenmptents** 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

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

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

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 $s \in S$:

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

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,

$$\begin{aligned} e_1 * e_2 &= e_1 && \text{since } e_1 \text{ is } \textbf{id} \\ e_1 * e_2 &= e_2 && \text{since } e_2 \text{ is } \textbf{id} \end{aligned}$$

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

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 $\langle S', *' \rangle$. □

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

$$(a * b) * c = a * (b * c). \qquad \textbf{associativity of *}$$

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

$$e * x = x * e = x. \qquad \textbf{identity element } e \textbf{ for *}$$

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

$$a * a' = a' * a = e. \qquad \textbf{inverse } a' \textbf{ of } a$$

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 $a * b = a * c$:

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

□

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 $a, b \in G$.

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

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 th 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.

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

□

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.

$*$	e
e	e

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

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

$*$	e	a
e	e	a
a	a	e

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 $G = \{e, a, b\}$

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

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:

$$\begin{array}{c|cccccc} * & e & a & \cdots & x & \cdots & y \\ \hline e & e & a & \cdots & x & \cdots & y \\ a & a & \_ & \cdots & a*x & \cdots & a*y \end{array}$$

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. □

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:

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

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 $\{e\}$.

5.1.4 Thm. Proving that a Subset of a Group is a Subgroup

Let H be a subset of a group G. If:

1. H is closed with respect to the operation of G and,

2. H is closed with respect to inverses,

then H is a subgroup of G.

Proof. Let $H \subseteq G$ and assume (1) and (2).

1. By (1), H is closed under the operation of G.

2. Associativity: Let $a, b, c \in H$. Note that $a, b, c \in G$, since $H \subseteq G$. Since G is a group, $a(bc) = (ab)c$. Thus associativity is "*inherited*" from G.

3. Identity: Let $a \in H$. By (2), $a^{-1} \in H$. By (1), $aa^{-1} = e \in H$.

4. Inverse: Let $a \in H$. By (2), $a^{-1} \in H$.

Thus H is a group, and thus also a subgroup of G. $\square$

Example

Prove that $\langle E, +\rangle \leq \langle \mathbb{Z}, +\rangle$.

Proof. Check: Is $E \subseteq \mathbb{Z}$? ✓

1. Is E closed w.r.t. $+$? Let $a, b \in E$. By definition, $\exists\ k, j \in \mathbb{Z}$ such that $a = 2k$ and $b = 2j$. So, $a + b = 2k + 2j = 2(k + j) \in E$. Thus, E is closed w.r.t. E.

2. is E closed w.r.t. inverses? Let $a \in E$. By definition, $\exists\ k \in \mathbb{Z}$ such that $a = 2k$. Multiplying both sides by -1 gives $-a = -2k = 2(-k) \in E$.

$\therefore E \leq \mathbb{Z}$ under $+$. □

5.1.5 Thm. Cyclic Subgroups

Let G be a group and let $a \in G$. Then $H = \{a^n : n \in \mathbb{Z}\}$ is a subgroup of G. This subgroup H is called the **cyclic subgroup** of G generated by a and is denoted $\langle a \rangle$.