# 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 <u>second</u> 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 $*$. $\square$

# 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 $\phi$ 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 $\phi$ 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 $\phi$ is operation preserving.

Since $\phi$ is one-to-one, onto, and operation preserving, thus $\phi$ 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 $s \in S$:

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

### 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. $\square$

### 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

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

$\mathfrak{G}_2$: 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:

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

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:

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

### 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 $G$. □

**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 $\langle a\rangle$.

#### 5.1.6 Def. Cyclic Group and Generator of a Cylic Group

Let $G$ be a group and let $a \in G$. Then $G$ is **cyclic** if

$$G = \{a^n : n \in \mathbb{Z}\} = \langle a\rangle.$$

'$a$' is called the **generator** of the cyclic group.

# 6 Cyclic Groups

**Recall**

- If $G$ is a group, $a \in G$, and $G = \{a^n : n \in \mathbb{Z}\}$ then $G = \langle a \rangle$ is a *cyclic group* generated by $a$.
- Every cyclic group is Abelian.
- The *Division Algorithm*: if $m \in \mathbb{Z}^+$ and $n \in \mathbb{Z}$, then there exists unique $q, r \in \mathbb{Z}$ such that
$$n = mq + r \text{ and } 0 \leq r < m.$$

### 6.0.1 Thm. Cyclic Subgroups are Cyclic

A subgroup of a cyclic group is cyclic.

*Proof.* Let $G$ be a cyclic group, say $G = \langle a \rangle$, where $a \in G$. Let $H$ be a subgroup of $G$. Since $H \subseteq G$, every element of $H$ must be a power of $a$. Consider the *smallest* positive power of $a$, $a^m \in H$, for $m \in \mathbb{Z}^+$. Let $a^n \in H$ for $n \in \mathbb{Z}$.

By the division algorithm, there exists unique, $\exists! q, r \in \mathbb{Z}$ such that $n = mq + r$ where $0 \leq r < m$. Then,
$$a^n = a^{mq+r} = a^{mq}a^r$$
$$a^r = a^{-mq}a^n = (a^m)^{-q}a^n$$
Since we know that $a^m \in H$, we know that $(a^m)^{-q} \in H$. We also asserted that $a^n \in H$. Thus, we can conclude that $a^r \in H$. But $0 \leq r < m$, and $m$ is the *smallest* positive integer such that $a^m \in H$. Thus $r = 0$. So,
$$n = mq + 0 = mq$$
$$a^n = a^{mq}$$
Thus every element of $H$ takes the form $(a^m)^q$, and $H$ is cyclic, with generator $\langle a^m \rangle$. □

### 6.0.2 Def. Cyclic Group of Order n

If $G$ is a cyclic group of *order* $n$, then
$$G = \langle a \rangle = \underbrace{\{e = a^0, a^1, a^2, \ldots, a^{n-1}\}}_{n \text{ elements}} \text{ and } a^n = e.$$
We say the *order of $a$ is $n$*, meaning $a^n = e$. Otherwise, the order of $a$ is infinite, and hence the order of $G$ is infinite.

### 6.0.3 Thm. Cyclic Groups and the Integer

Let $G = \langle a \rangle$.

1. Every cyclic group of order $n$ is isomorphic to $\langle \mathbb{Z}_n, +_n \rangle$.
2. Every cyclic group of order infinity is isomorphic to $\langle \mathbb{Z}, + \rangle$.

*Proof.*

1. Let $G = \langle a \rangle$ be a cyclic group of order $n$. Then
$$G = \{e = a^0, a^1, a^2, \ldots, a^{n-1}\}$$
Consider $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$. Define $\phi : \mathbb{Z}_n \to G$ by $\phi(x) = a^x$.
   (a) One-to-one: assume $a^x = a^y$. Then $x = y$. Thus $\phi$ is one-to-one.
   (b) Onto: let $a^x \in G$. Then choose $x \in \mathbb{Z}_n$, and $\phi(x) = a^x$. Thus, $\phi$ is onto.
   (c) Operation Preserving: $\phi(x + y) = a^{x+y} = a^x a^y = \phi(x)\phi(y)$. Thus $\phi$ is operation preserving.

   Thus $\phi$ is an isomorphism and $\langle \mathbb{Z}_n, +_n \rangle \simeq G$.
2. Follows nearly identical as above.

□

**Note**

The above theorem implies that all cyclic groups of order $n$ are isomorphic to each other, and all cyclic groups of order infinity are isomorphic to each other. This is because isomorphism is an equivalence relation.

## 6.1 Subgroups of Cyclic Groups

### 6.1.1 Thm. Order of Subgroups of Cyclic Groups

Let $G = \langle a \rangle$ by a cyclic group of order $n$. Let $b \in G$ and let $b = a^s$ for $s \in \mathbb{Z}$. Then $\langle b \rangle$ is a cyclic subgroup of $G$ containing $\frac{n}{d}$ elements, where $d = \gcd(n, s)$.

### 6.1.2 Cor. Order of Subgroups of Cyclic Groups

If $G = \langle a \rangle$ is a cyclic group of order $n$, then the other generators of $G$ are the elements of the form $a^r$ where $\gcd(n, r) = 1$.

**Cyclic Subgroup Diagrams**

Example cyclic diagram for $\mathbb{Z}_{12} = \langle Z \rangle$.

$$
\begin{array}{ccccccc}
 & & & & \langle Z \rangle & & \\
 & & & / & & \backslash & \\
 & & \langle 2 \rangle & & & & \langle 3 \rangle \\
 & / & & \backslash & & / & \\
\langle 4 \rangle & & & & \langle 6 \rangle & & \\
 & \backslash & & / & & & \\
 & & \langle 0 \rangle & & & &
\end{array}
$$

## 6.2 Infinite Cyclic Groups

The subgroups of $\langle \mathbb{Z}, + \rangle$ are of the form $\langle n\mathbb{Z}, + \rangle$ for $n \in \mathbb{Z}$. For example,

$$
\begin{aligned}
2\mathbb{Z} &= \{\ldots, -4, -2, 0, 2, 4, \ldots\} \\
5\mathbb{Z} &= \{\ldots, -10, -5, 0, 5, 10, \ldots\}
\end{aligned}
$$

# 7 Generating Sets and Cayley Digraphs

This section is not covered in this course.

# 8 Groups of Permutations

**IDEA**: A *permutation* of a set can be thought of as a rearrangement of the elements of the set.

### 8.0.1 Def. Permutation

A permutation of a set $A$ is a function $\phi : A \to A$ that is both one-to-one and onto. This means $\phi$ is a bijection from $A$ to itself.

Note: We will use "tabular notation" for $\phi$.

#### Example

Let $A = \{1, 2, 3, 4, 5, 6\}$ and consider two permutations of $A$:
$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 3 & 5 & 4 & 2 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 6 & 5 & 4 \end{pmatrix}$. Note that the operation of *permutation multiplication* is function composition. That is, $fg = f \circ g$.

1. $fg = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 6 & 2 & 4 & 5 \end{pmatrix}$
2. $g^2 f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 2 & 5 & 4 & 1 \end{pmatrix}$
3. $f^{-1} g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 2 & 1 & 4 & 5 \end{pmatrix}$

### 8.0.2 Thm. Permutations Multiplication and Groups

Let $A$ be a nonempty set and let $S_A$ be the collection of all permutations of $A$. Then $S_A$ is a group under permutation multiplication.

*Proof.* Note Permutation Multiplication is a binary operation on $S_A$.

- $\mathfrak{G}_1$ Let $f, g, h \in S_A$. Let $a \in A$

$$\begin{aligned}[f(gh)](a) &= [f \circ (g \circ h)](a) \\ &= f((g \circ h)(a)) \\ &= f(g(h(a))) = (f \circ g)h(a) = [(fg)h](a)\end{aligned}$$

  $\therefore \langle S_A, + \rangle$ is associative.

- $\mathfrak{G}_2$ Let $i(a) = a$ for all $a \in A$. Then $i$ is the identity permutation.
- $\mathfrak{G}_3$ Every permutation in $S_A$ is bijective, so every permutation has an inverse.

$\therefore S_A$ is a group. □

### 8.0.3 Def. Symmetric Group

Let $A$ be the finite set $A = \{1, 2, 3, \ldots, n\}$. The group of all permutations of $A$ is called the **symmetric group**, denoted $S_n$.

Note: $|S_n| = n!$

**Example**

Consider $S_3$, which would be the group of all permutations of the set $A = \{1, 2, 3\}$. This set is also known as $D_3$, the group of symmetries of an equilateral triangle, where a symmetry is a movement of a shape to make it coincide with its former position. The letter $D$ is used because this type of group is called a *dihedral group*, which are the groups of symmetries of regular polygons that include rotations and reflections.

Labeling the vertices of the triangle $1, 2,$ and $3$, we get the following, where $\rho$ are rotations and $\mu$ are reflections.

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad \mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$
$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$
$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \qquad \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

However, when we consider $D_4$, the dihedral group consisting of symmetries of a square, we notice that $S_4 \neq D_4$.

### 8.0.4 Thm. Cayley's Theorem

Every group is isomorphic to a group of permutations.

*Proof.* Let $G$ be a group, and let $a \in G$ be fixed. Define $\pi_a : G \to G$ by

$$\pi_a(x) = ax, \qquad \forall\, x \in G$$

First, we prove that $\pi_a$ is a permutation of $G$.

*Proof.* A permutation is one-to-one and onto.

1. One-to-one: Assume $\pi_a(x_1) = \pi_a(x_1)$ for $x_1, x_2 \in G$.

$$\begin{aligned} \pi_a(x_1) &= \pi_a(x_1) \\ ax_1 &= ax_2 \\ x_1 &= x_2 && \text{by left cancellation} \end{aligned}$$

   Thus $\pi_a$ is one-to-one.

2. Onto: Let $y \in G$. Show $\exists\, x \in G$ such that $y = \pi_a(x)$.

$$\begin{aligned} y = \pi_a(x) &= ax \\ a^{-1}y &= x \end{aligned}$$

   Choose $x = a^{-1}y$. Thus $\pi_a$ is onto.

Thus $\pi_a$ is a permutation of $G$. □

Let $G^* = \{\pi_a : a \in G\}$. We must show that $G^*$ is a group (consisting of permutations). It suffices to show that $G^*$ is a subgroup of $S_G$, the group of all permutations of $G$. Note: $G^* \subseteq S_G$.

*Proof.* A subgroup is closed under the operation and inverses.

1. Closed under operation of $S_G$: Consider $\pi_a, \pi_b \in G^*$ for $a, b \in G$. For $x \in G$,

$$(\pi_a \circ \pi_b)(x) = \pi_a(bx) = abx = \pi_{ab}(x)$$

   Since $ab \in G$, we know that $\pi_{ab} \in G^*$, so $G^*$ is closed under the operation.

2. Closed under inverses: Let $\pi_a \in G^*$. Since $\pi_a$ is a bijection, we know $\pi_a$ has an inverse $(\pi_a)^{-1}$. Note: $\pi_e$ is the identity of $S_G$. Consider $(\pi_a)^{-1} = \pi_{a^{-1}}$. For $x \in G$,

$$(\pi_{a^{-1}} \circ \pi_a)(x) = a^{-1}ax = ex = \pi_e(x)$$
$$(\pi_a \circ \pi_{a^{-1}})(x) = aa^{-1}x = ex = \pi_e(x)$$

   Thus $(\pi_a)^{-1} = \pi_{a^{-1}} \in G^*$, and $G^*$ is closed under inverses.

Thus $G^* \leq S_G$. □

It remains to be proven that $G \simeq G^*$. Consider $\phi : G \to G6*$, by

$$\pi(a) = \pi_a.$$

*Proof.* An isomorphism is onto-to-one, onto, and operation preserving.

1. One-to-one: Let $\phi(a) = \phi(b)$ for $a, b \in G$.

$$\phi(a) = \phi(b)$$
$$\pi_a = \pi_b$$

   Using $x \in G$,

$$\begin{aligned} \pi_a(x) &= \pi_b(x) \\ ax &= bx \\ a &= b && \text{by right cancellation} \end{aligned}$$

   Thus $\phi$ is one-to-one.

2. Onto: Given any $\pi_a \in G^*$, $\exists\ a \in G$, such that $\phi(a) = \pi_a$. Thus $\phi$ is onto.

3. Operation Preserving: Show $\phi(ab) = \phi(a) \circ \phi(b)$, $\forall\ a, b \in G$.

$$\begin{aligned} \phi(ab) &= \pi_{ab} \\ &= \pi_a \circ \pi_b \\ &= \phi(a) \circ phi(b) \end{aligned}$$

   Thus $\phi$ is operation preserving.

Thus $\phi$ is an isomorphism, and $G \simeq G^*$. □

Thus group $G$ is isomorphic to a group of permutations $G^*$. □

# 9 Orbits, Cycles, and the Alternating Groups

Consider the set $A = \{1, 2, 3, \ldots, 8\}$ and let $\sigma \in S_8$ be defined by $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 6 & 4 & 7 & 1 & 2 & 8 \end{pmatrix}$. How does $\sigma$ "move" elements in $A$?

$$\begin{aligned} &1 \mapsto 3 \mapsto 6 \mapsto 1 \\ &2 \mapsto 5 \mapsto 7 \mapsto 2 \\ &8 \mapsto 8 \end{aligned}$$

### 9.0.1 Def. Orbits

The **orbits** of a permutation $\sigma$ are the equivalence class of $A$ determined by $a \sim b$ if and only if $b = \sigma^n(a)$ for some $n \in \mathbb{Z}$.

### 9.0.2 Def. Cycle

A permutation is a cycle if it has *at most* **one** orbit containing more than one element.

#### Example

Writing $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix}$ as a cycle.

$$(1, 3, 5, 4)$$

Note: elements that are not moved by the permutation do **not** appear in the cycle.

#### Example

In $S_8$, perform $(1, 3, 6)(2, 8)(4, 7, 5)$ and express the answer as a permutation.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 7 & 4 & 1 & 5 & 2 \end{pmatrix}$$

In $S_6$, write $(1, 4, 5, 6)(2, 1, 5)$ as a permutation. Does $(2, 1, 5)(1, 4, 5, 6)$ result in the same permutation? No, they do not.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 3 & 5 & 2 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 3 & 2 & 6 & 5 \end{pmatrix}$$

#### Notes

Disjoint cycles commute. Every permutation $\sigma$ of a finite set can be expressed asa product of disjoint cycles.

### 9.0.3 Def. Transposition

A cycle of length two (2) is called a **transposition**.

#### Note

Every cycle can be expressed as a product of one or more transpositions, although it is *not* unique.

In $S_5$,

$$\begin{aligned} (1, 2, 3, 4, 5) &= (1, 5)(1, 4)(1, 3)(1, 2) \\ &= (5, 4)(5, 3)(5, 2)(5, 1) \\ &= (5, 4)(5, 2)(5, 1)(1, 4)(3, 2)(4, 1) \end{aligned}$$

### 9.0.4 Def. Even and Odd Permutations

A permutation is **even** if it can be expressed as a product of an even number of transpositions. A permutation is **odd** if it can be expressed as a product of an odd number of transpositions.

#### Note

If $i$ is the identity permutation, then $i$ is even.

### 9.0.5 Thm. Permutations are either Even or Odd

If $\sigma \in S_n$, then $\sigma$ cannot be both even and odd.

*Proof.* Let $\sigma \in S_n$ and assume $\sigma$ can be both even and odd. Note that $\sigma^{-1}$ is also both even and odd. But, $i = \sigma\sigma^{-1}$ is even, while $\sigma$ is odd and $\sigma^{-1}$ is even, or $\sigma$ is even and $\sigma^{-1}$ is odd. This would imply that $i$ could be odd, which is a contradiction. $\square$

#### Recall

$S_n$ is the group of all permutations on $\{1, 2, 3, \ldots, n\}$. Each of these permutations can be expressed as a product of *transpositions*. Even though this breakdown is not unique, the above theorem shows that every breakdown of a particular permutation must either be even or odd. All of the even permutations are given a special designation.

### 9.0.6 Def. The Alternating Group

The set of all even permutations in $S_n$ is called the **alternating group** on $\{1, 2, \ldots, n\}$, denoted as $A_n$.

#### Notes

The alternating group $A_n$ is a subgroup of $S_n$. Additionally, recall that $|S_n| = n!$. Thus $|A_n| = \frac{n!}{2}$.

# 10 Cosets and the Theorem of Lagrange

### 10.0.1 Thm. Relation for Cosets

Let $H \leq G$. Let the relation $\sim_L$ be defined on $G$ by $a \sim_L b$ if and only if $a^{-1}b \in H$ for all $a, b \in G$. Similarly, let the relation $\sim_R$ be defined on $G$ by $a \sim_R b$ if and only if $ab^{-1} \in H$ for all $a, b \in G$. Then $\sim_L$ and $\sim_R$ are both equivalence relations on $G$.

*Proof of $\sim_L$.* Let $G$ be a group and $H \leq G$. Define $a\ sim_L b$ by $a^{-1}b \in H$.

1. Reflexive on $G$:
$$a^{-1}a = e \in H$$
Thus $\sim_L$ is reflexive.

2. Symmetric on $G$: Assume $a \sim_L b$. Since $a^{-1}b \in H$,
$$\begin{aligned}(a^{-1}b)^{-1} &\in H\\ b^{-1}(a^{-1})^{-1} &\in H\\ b^{-1}a &\in H\end{aligned}$$
Thus $\sim_L$ is symmetric.

3. Transitive on $G$ Assume $a \sim_L b$ and $b \sim_L c$. Since $a^{-1}b \in H$ and $b^{-1}c \in H$,
$$\begin{aligned}(a^{-1}b)(b^{-1}c) &\in H\\ a^{-1}bb^{-1}c &\in H\\ a^{-1}c \in H\end{aligned}$$
Thus $\sim_L$ is transitive.

Therefore, $\sim_L$ is an equivalence relation. $\square$

(The proof for $\sim -R$ is essentially the same.)

#### Note

Recall that equivalence relations define a partition on a set. Let $a \in G$ be fixed. The partition cell containing $a$ consists of all arbitrary $x \in G$ such that $a \sim_L x$. This implies $a^{-1}x \in H$, so there exists $h \in H$ such that $a^{-1}x = h$. That is, there exists $h \in H$ such that $x = ah$. Therefore, the partition cell containing $a$ is $\{ah : h \in H\}$.

### 10.0.2 Def. Coset

Let $G$ be a group and $H \leq G$. For any element $a \in G$, the symbol $aH$ denotes the set of all products $ah$ as $a$ remains fixed and $h$ ranges over $H$. The set $aH$ is called the **left coset** of $H$ in $G$. Similarly, $Ha = \{ha : h \in H\}$ is the **right coset** of $H$ in $G$.

#### Notes

Cosets of $G$ are subsets of $G$. If $G$ is Abelian, then the left and right cosets are the same. That is, $aH = Ha$ for all $a \in G$.

If $a \in Hb$, then $Ha = Hb$.

*Proof.* Assume $a \in Hb$. We must show that $Ha \subseteq Hb$ and $Ha \supseteq Hb$.

$Ha \subseteq Hb$. Let $x \in Ha$. We know $\exists\ h_1 \in H$ such that $x = h_1a$.
Since $a \in Hb$, we know $\exists\ h_2 \in H$ such that $a = h_2b$.
So $x = h_1a = h_1(h_2b) = (h_1h_2)b$. $h_1h_2 \in H$, so $x \in Hb$. $\square$

$Ha \supseteq Hb$. Let $y \in Hb$. We know $\exists\ h_3 \in H$ such that $y = h_3 b$.
Since $a \in Hb$, we know $\exists\ h_2 \in H$ such that $a = h_2 b \implies b = h_2^{-1} a$.
So $y = h_3 b = h_3(h_2^{-1} a) = (h_3 h_2^{-1})a$. $h_3 h_2^{-1} \in H$, so $y = Ha$. ☐

Thus $Ha \subseteq Hb$ and $Ha \supseteq Hb$ and therefore $Ha = Hb$. ☐

**Note**

A consequence of above is that a given coset can be written in more than one way. if a coset of $H$ has $n$ elements, say $a_1, a_2, \ldots, a_n$, then it can be written $n$ different ways: $Ha_1, Ha_2, \ldots, Ha_n$.

**Example**

Consider $D_4$, the symmetries of a square. Let $H = \{\rho_0, \mu_2\}$. List the right cosets of $H$ in $D_4$ and the elements of each coset. See table 8.12 (not shown).

$$\begin{aligned} H\rho_0 &= \{\rho_0, \mu_2\} = H\mu_2 \\ H\rho_1 &= \{\rho_1, \delta_1\} = H\delta_1 \\ H\rho_2 &= \{\rho_2, \mu_1\} = H\mu_1 \\ H\rho_3 &= \{\rho_3, \delta_2\} = H\delta_2 \end{aligned}$$

### 10.0.3 Thm. One-to-one Correspondence of Cosets

If $Ha$ is any coset of $H$ in $G$, then there is a one-to-one correspondence from $H$ to $Ha$.

*Proof.* Define $f : H \to Ha$ by $f(h) = ha$.

1. One-to-one: Let $f(h_1) = f(h_2)$.

$$\begin{aligned} h_1 a &= h_2 a \\ h_1 &= h_2 \end{aligned}$$

   Thus $f$ is one-to-one.

2. Onto: Let $ha \in Ha$. Choose $h$, and $f(h) = ha$. So $f$ is onto.

Thus $f$ is a one-to-one correspondence from $H$ to $Ha$. ☐

**Consequence**: Any coset $Ha$ of $H$ has the same number of elements as $H$ and thus all cosets of $H$ in $G$ have the same cardinality.

### 10.0.4 Thm. Lagrange's Theorem

Let $G$ be a finite group and let $H$ be a subgroup of $G$. The order of $G$ is a multiple of the order of $H$. Or, the order of $H$ is a divisor of the order of $G$.

$$|G| = |H| \cdot |G : H|$$

### 10.0.5 Def. Index of H in G

The **index of** $H$ **in** $G$, denoted as $(G : H)$ or $|G : H|$, is the number of cosets of $H$ in $G$.

### 10.0.6 Cor. Groups of Prime Order

If $G$ is a group with a prime number $p$ elements, then $G$ is a cyclic group. Furthermore, any element $a \neq \mathbf{id}$ in $G$ is a generator in $G$.

*Proof.* Let $G$ be a group having $p$ elements, where $p$ is prime. If $a \in G$ but $a \neq \mathbf{id}$, then the order of $a$ is some integer $m \neq 1$.

Then $\langle a \rangle = \{a, a^2, \ldots, a^m = \mathbf{id}\}$ has $m$ elements, $|\langle a \rangle| = m$.

By Lagrange's Theorem, the order of $G$ is a multiple of $|\langle a \rangle|$. But $|G|$ is prime $p$, and $m \neq 1$, so $p = m$. So $|\langle a \rangle| = |G|$, and thus $\langle a \rangle = G$. $\square$

# 11 Direct Products and Finitely Generated Abelian Groups

## 11.1 Summary of Groups

**Finite Groups**

| Order | Symbol | Name & Notes |
|---|---|---|
| $n$ | $\mathbb{Z} = \{0, 1, \dots, n-1\}$ | All order $n$ cyclic groups are isomorphic to $\langle \mathbb{Z}_n, +_n \rangle$ |
| $n!$ | $S_n$ = all permutations of $\{1, 2, \dots, n\}$ | "Symmetric group" |
| $\frac{n!}{2}$ | $A_n$ = all even permutations of $S_n$ | "Alternating group" |
| $2n$ | $D_n$ all symmetries of a regular $n$-gon | "Dihedral group" |

**Infinite Groups**

| Symbol | Notes |
|---|---|
| $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ | All infinite cyclic groups are isomorphic to $\langle \mathbb{Z}, + \rangle$ |
| $\mathbb{Q},\ \mathbb{R},\ \mathbb{C}$ | only under $+$ |
| $\mathbb{Q}^*,\ \mathbb{R}^*, \mathbb{C}^*$ | only under $\cdot$ |
| $S_A$ | only when $A$ is an infinite set |

**IDEA**

Use known groups as building blocks to form new groups.

#### 11.1.1 Def. Generalized Cartesian Product

The Cartesian product of sets $S_1, S_2, \dots, S_n$ is the set of all ordered $n$-tuples $(a_1, a_2 \dots, a_n)$ where $a_i \in S_i$ for $i \in \{1, 2, \dots, n\}$

Notation: $S_1 \times S_2 \times \cdots \times S_n$ or $\prod_{i=1}^n S_i$

#### 11.1.2 Thm. Group of Direct Products

Let $G_1, G_2, \dots, G_n$ be groups. For $(a_1, a_2, \dots, a_n), (b_1, b_2, \dots, b_n) \in \prod_{i=1}^n G_i$, define the binary operation *multiplication by components by*

$$(a_1, a_2, \dots, a_n)(b_1, b_2, \dots, b_n) = (a_1 b_1, a_2 b_2, \dots, a_n b_n).$$

Then $\prod_{i=1}^n G_i$ is a group called the **direct product of the groups** $G_i$.

*Proof.* A group must be associative, have an identity, and have inverses for every element

1. $\mathfrak{G}_1$: Associative. Consider

$$(a_1, a_2, \dots, a_n)(b_1, b_2, \dots, b_n)(c_1, c_2, \dots, c_n) \in \prod_{i=1}^n G_i.$$

Then,

$$\begin{aligned}(a_1, a_2, \dots, a_n)[(b_1, b_2, \dots, b_n)(c_1, c_2, \dots, c_n)] &= (a_1, a_2, \dots, a_n)(b_1 c_1, b_2 c_2, \dots, b_n c_n) \\ &= (a_1 b_1 c_1, a_2 b_2 c_2, \dots, a_n b_n c_n) \\ [(a_1, a_2, \dots, a_n)(b_1, b_2, \dots, b_n)](c_1, c_2, \dots, c_n) &= (a_1 b_1, a_2 b_2, \dots, a_n b_n)(c_1, c_2, \dots, c_n) \\ &= (a_1 b_1 c_1, a_2 b_2 c_2, \dots, a_n b_n c_n)\end{aligned}$$

Thus multiplication by components is associative.

2. $\mathfrak{G}_2$: Identity Exists.

Note that each $G_i$ for $i \in \{1, 2, \dots, n\}$ is a group, so each has an identity $e_i$. It is clear that $(e_1, e_2, \dots, e_n)$ is the identity of $\prod_{i=1}^n G_i$.

3. $\mathfrak{G}_3$: Inverses Exist.

   Note that each $G_i$ for $i \in \{1, 2, \ldots, n\}$ is a group, so each $a_i$ has inverse $a_i^{-1}$. It is clear that

$$(a_1, a_2, \ldots, a_n)^{-1} = (a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1}).$$

Thus $\prod_{i=1}^{n} G_i$ is a group. $\square$