Abstract Algebra A

soupless

January 31, 2024

Contents

Lecture 1: Sets and relations

Definition 1.1 (Cartesian product)

Let A and B be sets. The *Cartesian product* of A and B, denoted by $A \times B$, is defined as

$$A \times B \ := \ \{(a, b) \mid a \in A,\, b \in B\}.$$

Definition 1.2 (Relation)

A relation R between sets A and B is a subset of $A \times B$. That is, $R \subseteq A \times B$.

We let $aRb \equiv (a, b) \in \mathbb{R}$ for each $a \in A$ and $b \in B$ where R is a relation. It is an implicit assumption that A and B have to be nonempty, otherwise, the relation is trivial.

Theorem 1.1

If A and B are finite sets, then there are $2^{|A|\cdot|B|} - 1$ relations.

Proof: Let A and B be finite sets. Then, the question is equivalent to finding the number of subsets of $A \times B$, which is $|\mathcal{P}(A \times B)| - 1 = 2^{|A\times B|} - 1 = 2^{|A|\cdot|B|} - 1$. ■

Definition 1.3 (Function)

A function ϕ mapping X into Y is a relation between X and Y with the property that each $x \in X$ appears as the first member of exactly one ordered pair $(x, y) \in \phi$ for all $y \in Y$.

Definition 1.4 (Domain, codomain, range)

Let $\phi : X \to Y$ be a function mapping X to Y. Then,

- X is the domain of ϕ,
- Y is the codomain of ϕ,
- $\phi[X]$ is the range of ϕ such that $\phi[X] = \{\phi(x) \mid x \in X\}$.

Another notation would be $X \xrightarrow{\phi} Y$ to denote the type signature, and $x \xmapsto{\phi} y$ to denote the function definition.

Definition 1.5 (Injective function)

A function $\phi : X \to Y$ is *injective* or one-to-one (1-1) if, for all elements x_1 and x_2 of X, $\phi(x_1) = \phi(x_2)$ implies $x_1 = x_2$.

Example: Let $f : \mathbb{R} \to \mathbb{R}$ such that $f(x) = 2x + 3$ for all $x \in \mathbb{R}$. Is f injective?

Let x_1 and x_2 be arbitrary elements of $\mathbb{R}$, and suppose that $f(x_1) = f(x_2)$. Then,

$$\begin{aligned} f(x_1) &= f(x_2) \\ 2x_1 + 3 &= 2x_2 + 3 \\ 2x_1 &= 2x_2 \\ x_1 &= x_2 \end{aligned}$$

Hence, f is injective.

Example: Let $g : \mathbb{R} \to \mathbb{R}$ such that $g(x) = x^2$ for all $x \in \mathbb{R}$. Is g injective?

No, because $g(-1) = 1$, and $g(1) = 1$, but $-1 \neq 1$.

Definition 1.6 (Surjective function)

A function $\phi : X \to Y$ is surjective or onto if $\phi[X] = Y$. Equivalently, $\forall y \in Y\ \exists x \in X (\phi(x) = y)$.

Example: Let $F : \mathbb{R} \to \mathbb{R}$ defined by $F(x) = x^2$ for each $x \in \mathbb{R}$. Is F surjective?

Since $F(x) \geq 0$ for all $x \in \mathbb{R}$, then $F(x) = -1$ has no solution. Hence, F is not surjective.

Example: Let $G : \mathbb{N} \to \mathbb{N}$ such that $G(x) = x + 1$ for each $x \in \mathbb{N}$. We define $\mathbb{N} = \{1, 2, 3, \ldots\}$. Is G surjective?

No, because $G(x) = 1$ has no solution in $\mathbb{N}$. Hence, G is not surjective.

Example: Let $\phi : \mathbb{N} \to \mathbb{N}$ such that $\phi(n)$ is the nth prime number for each $n \in \mathbb{N}$. Then, ϕ is injective. However, it is not surjective, because $\phi(x) = 4$ has no solution.

Example: Let $g : \mathbb{R} \to \mathbb{R}$ such that $g(x) = x + 1$ for each $x \in \mathbb{R}$. Prove that g is surjective.

Let $y \in \mathbb{R}$ be arbitrary. Then, $g(x) = y \implies x + y = 1 \implies x = y - 1$. Since $g(y - 1) = y - 1 + 1 = y$, this means g is surjective.

Definition 1.7 (Bijective function)

If $\phi : X \to Y$ is both injective and surjective, then ϕ is bijective.

Definition 1.8 (Inverse)

Let $\phi : X \to Y$ be a bijective function. The inverse of ϕ, denoted by ϕ^{-1}, is the function $\phi^{-1} : Y \to X$ such that $\phi^{-1}(y) = x \Leftrightarrow \phi(x) = y$ for all $x \in X$ and $y \in Y$.

A representation for finite domain maps would be through a matrix representation like

$$\phi : \begin{bmatrix} x_1 & x_2 & \cdots & x_n \\ \phi(x_1) & \phi(x_2) & \cdots & \phi(x_n) \end{bmatrix}$$

Definition 1.9 (Function composition)

Let $\phi : A \to B$ and $\theta : B \to C$ be functions. The composition $\theta\phi$ is the function $\theta\phi : A \to C$ defined by $\theta\phi(a) = \theta\left(\phi(a)\right)$ for each $a \in A$.

Definition 1.10 (Function equality)

Let $f : X \to Y$ and $g : X \to Y$. Then, $f = g$ if $\forall x \in X\, (f(x) = g(x))$.

Theorem 1.2

Given functions $\alpha : A \to B$, $\beta : B \to C$, and $\gamma : C \to D$, then:

1. $(\gamma\beta)\alpha = \gamma(\beta\alpha)$. That is, function composition is associative.
2. If α and β are both injective, then $\beta\alpha$ is injective.
3. If α and β are both surjective, then $\beta\alpha$ is also surjective.

Proof: We prove each property listed in the theorem:

- Suppose we have the functions $\alpha : A \to B$, $\beta : B \to C$, and $\gamma : C \to D$. Let $a \in A$ be arbitrary. Then,

$$(\gamma\beta)\alpha(a) = \gamma\beta\left(\alpha(a)\right)$$

$$(\gamma\beta)\alpha(a) = \gamma\left(\beta\left(\alpha(a)\right)\right)$$

$$\gamma(\beta\alpha)(a) = \gamma\left(\beta\alpha(a)\right)$$
$$\gamma(\beta\alpha)(a) = \gamma\left(\beta\left(\alpha(a)\right)\right)$$

Hence, $(\gamma\beta)\alpha(a) = \gamma(\beta\alpha)(a)$. Therefore, $(\gamma\beta)\alpha = \gamma(\beta\alpha)$.

- Let $\alpha : A \to B$ and $\beta : B \to C$ be injective functions. Then, $\beta\alpha : A \to C$. Suppose that for all $a_1, a_2 \in A$, $\beta\alpha(a_1) = \beta\alpha(a_2)$. We get the following derivation:

$$\beta\alpha(a_1) = \beta\alpha(a_2)$$
$$\beta\left(\alpha(a_1)\right) = \beta\left(\alpha(a_2)\right)$$
$$\alpha(a_1) = \alpha(a_2)$$
$$a_1 = a_2$$

  Therefore, $\beta\alpha$ is injective.

- Let $\alpha : A \to B$ and $\beta : B \to C$ be surjective functions. Let $c \in C$ be arbitrary. Then, there exists $b \in B$ such that $\beta(b) = c$. Since α is surjective, there exists $a \in A$ such that $\alpha(a) = b$. Then, $\beta(b) = \beta(\alpha(a)) = \beta\alpha(a) = c$. Hence, there exists $a \in A$ such that $\beta\alpha(a) = c$, and so for all $c \in C$, there exists $a \in A$ such that $\beta\alpha(a) = c$. Therefore, $\beta\alpha$ is surjective. ■

Lecture 2: Sets and relations, continued

Theorem 2.1

Let $\alpha : A \to B$ be a bijective function. Then there exists a function $\theta : B \to A$ such that $\forall a \in A\,(\theta\alpha(a) = a)$ and $\forall b \in B\,(\alpha\theta(b) = b)$. The function θ is called the inverse of α and is denoted by $\theta = \alpha^{-1}$.

Proof: Suppose $\alpha : A \to B$ is a bijective function. Construct a function $\theta : B \to A$ satisfying the properties $\forall a \in A\,(\theta\alpha(a) = a)$ and $\forall b \in B\,(\alpha\theta(b) = b)$. We define $\theta : B \to A$ by $\theta(b) = a$ iff $\alpha(a) = b$.

Let $a \in A$ be arbitrary. Consider $\theta\alpha(a)$. Suppose $\alpha(a) = b$. Then, $\theta\alpha(a) = \theta(\alpha(a)) = \theta(b) = a$.

Let $b \in B$ be arbitrary. Consider $\alpha\theta(b)$. Suppose $\theta(b) = a$. Then, $\alpha\theta(b) = \alpha(\theta(b)) = \alpha(a) = b$. ■

Definition 2.1 (Identity function)

The identity function is a function having the same domain and codomain such that $x \mapsto x$ for all x in the domain.

Theorem 2.2

Let $\alpha : A \to B$ be a bijective function. Then, $\alpha^{-1} : B \to A$ is bijective.

Proof: We first prove that α^{-1} is injective. Let b_1, b_2 be arbitrary elements from B, and suppose that $\alpha^{-1}(b_1) = \alpha^{-1}(b_2)$. Then,

$$\alpha^{-1}(b_1) = \alpha^{-1}(b_2)$$
$$\alpha\alpha^{-1}(b_1) = \alpha\alpha^{-1}(b_2)$$
$$b_1 = b_2$$

Hence, α^{-1} is injective.

We now prove that α^{-1} is surjective. Let $a \in A$. We know that $\alpha^{-1}\alpha(a) = a$. Since $\alpha(a) \in B$, this means that there is an element $b \in B$ such that $\alpha^{-1}(b) = a$. Hence, for all $a \in A$, there exists an element $b \in B$ such that $\alpha^{-1}(b) = a$, and so α^{-1} is surjective.

Therefore, α^{-1} is surjective. ■

Definition 2.2 (Equivalence relation)

R is called an equivalence relation on a set S if R is a relation from S to S and it satisfies the following:

1. $\forall a \in S(aRa)$.
2. $\forall a, b \in S(aRb \implies bRa)$.
3. $\forall a, b, c \in S(aRb \wedge bRc \implies aRc)$.

Example: Define R on $\mathbb{R}^*$ such that $aRb \Leftrightarrow ab > 0$ for all $a, b \in \mathbb{R}^*$. Let $a, b, c \in \mathbb{R}^*$ be arbitrary. Since $a \in \mathbb{R}^*$, we have $a \neq 0$, and since $x^2 > 0$ for all nonzero real numbers, we get $aa > 0$ which is equivalent to aRa. Thus, R is reflexive. Now, suppose aRb. Then, $ab > 0$. Multiplication under real numbers is commutative, hence, $ba > 0$, and so bRa. This means R is symmetric. Lastly, suppose aRb and bRc. Then, $ab > 0$ and $bc > 0$. We get $ab^2c > 0$, and dividing both sides by b^2, we get $ac > 0$. Hence, aRc, and so R is transitive.

Therefore, R is an equivalence relation.

Example: Define $\sim$ on $\mathbb{Z}$ by $a \sim b \Leftrightarrow a \equiv b \pmod 4$. We verify if $\sim$ is an equivalence relation on $\mathbb{Z}$.

We have $4 \mid 0 \implies 4 \mid a - a$, and so $a \equiv a \pmod 4$. Hence, $\sim$ is reflexive. Now, suppose $a \sim b$. Then, $4 \mid a - b \implies 4 \mid (-1)(a-b) \implies 4 \mid b - a$. Hence, $b \sim a$, and $\sim$ is symmetric. Lastly, suppose $a \sim b$ and $b \sim c$. Then, $4 \mid a - b$ and $4 \mid b - c$. We have $4 \mid a - b + b - c \implies 4 \mid a - c$. Hence, aRc, and so R is transitive.

Therefore, $\sim$ is an equivalence relation on $\mathbb{Z}$.

Definition 2.3 (Equivalence class)

Let $\sim$ be an equivalence relation on S. Let $a \in S$, The equivalence containing a, denoted by $[a]$, is the set defined by

$$[a] := \{x \in S \mid a \sim x\}.$$

Example: We have shown that R is an equivalence relation on $\mathbb{R}^*$. Finding the equivalence class containing 2,

$$\begin{aligned}
[2] &= \{x \in \mathbb{R}^* \mid 2Rx\} \\
[2] &= \{x \in \mathbb{R}^* \mid 2x > 0\} \\
[2] &= \{x \in \mathbb{R}^* \mid x > 0\} \\
[2] &= \mathbb{R}^+
\end{aligned}$$

Finding the equivalence class containing $\sqrt{2}$,

$$\begin{aligned}
[\sqrt{2}] &= \{x \in \mathbb{R}^* \mid \sqrt{2}Rx\} \\
[\sqrt{2}] &= \{x \in \mathbb{R}^* \mid \sqrt{2}x > 0\} \\
[\sqrt{2}] &= \{x \in \mathbb{R}^* \mid x > 0\} \\
[\sqrt{2}] &= \mathbb{R}^+
\end{aligned}$$

Finding the equivalence class containing $-e$,

$$\begin{aligned}
[-e] &= \{x \in \mathbb{R}^* \mid -eRx\} \\
[-e] &= \{x \in \mathbb{R}^* \mid -ex > 0\} \\
[-e] &= \{x \in \mathbb{R}^* \mid x < 0\} \\
[-e] &= \mathbb{R}^-
\end{aligned}$$

Example: We have shown that $\sim$ is an equivalence relation on $\mathbb{Z}$ where $a \sim b \Leftrightarrow a \equiv b \pmod 4$.

Finding the equivalence class containing a,

$$\begin{aligned}
[a] &= \{x \in \mathbb{Z} \mid x \sim a\} \\
[a] &= \{x \in \mathbb{Z} \mid x \equiv a \pmod 4\} \\
[a] &= \{x \in \mathbb{Z} \mid 4 \mid x - a\} \\
[a] &= \{x \in \mathbb{Z} \mid 4 \mid x - a\} \\
[a] &= \{x \in \mathbb{Z} \mid 4k = x - a, k \in \mathbb{Z}\} \\
[a] &= \{x \in \mathbb{Z} \mid 4k + a = x, k \in \mathbb{Z}\} \\
[a] &= \{4k + a \mid k \in \mathbb{Z}\}
\end{aligned}$$

Hence, the equivalence class containing 0 is just $\{4k \mid k \in \mathbb{Z}\}$. The equivalence class containing 1 is $\{4k+1 \mid k \in \mathbb{Z}\}$, $\{4k+2 \mid k \in \mathbb{Z}\}$ for the equivalence class containing 2, and $\{4k+3 \mid k \in \mathbb{Z}\}$ for the equivalence class containing 3. The equivalence class containing 5 is just $[1]$ since $5 \in [1]$. Finally, $\mathbb{Z} = [0] \cup [1] \cup [2] \cup [3]$.

Definition 2.4 (Partition, cells)

A partition P of a set S is a collection of nonempty disjoint subsets of S whose union is S. Each element of P is called a *cell*.

Example: In $\mathbb{Z}$, one such partition is $\{\mathbb{Z}^-, \mathbb{Z}^+, \{0\}\}$

Example: Let $S = \{1, 2, 3, 4, 5\}$. One partition would be $P_1 = \{\{1\}, \{2\}, \{3\}, \{4\}, \{5\}\}$. Another partition would be $P_2 = \{\{1, 2\}, \{3\}, \{4\}, \{5\}\}$. The number of 2-cell partitions of S would be $\binom{5}{2}$.

Theorem 2.3

The equivalence classes of an equivalence relation on a set S constitute a partition of S.

Proof: Let $\sim$ be an equivalence relation on S. For any $a \in S$, we have $a \in [a]$. Let $a, b \in S$ such that $[a] \neq [b]$. There will be two cases:

- The intersection of $[a]$ and $[b]$ is nonempty. This means that there exists an element x in both $[a]$ and $[b]$. Then, $x \sim a$ and $x \sim b$, so $a \sim b$. Let $y \in S$ be arbitrary. Suppose $y \in [a]$. Then, $y \sim a$. Since $a \sim b$, then $y \sim b$, so $y \in [b]$. Hence, $[a] \subseteq [b]$. Similarly, suppose $y \in [b]$. Then, $y \sim b$. Then, $a \sim b$ implies $b \sim a$, so $y \sim a$. Hence, $y \in [a]$, and so $[b] \subseteq [a]$. Hence, $[a] = [b]$. This contradicts our assumption that $[a] \neq [b]$. Hence, $[a] \cap [b] = \emptyset$.
- The intersection of $[a]$ and $[b]$ is empty. Hence, $[a] \cap [b] = \emptyset$.

In either case, we get $[a] \cap [b] = \emptyset$.

Since each equivalence class is disjoint to another, and every element belongs to an equivalence class containing it, this means that the collection of all equivalence classes of S is a partition of S. ■

Lecture 3: Introduction to groups

Definition 3.1 (Binary operation)

A binary operation $*$ on a set S is a function $* : S \times S \to S$.

We let $a * b \equiv *((a, b))$ for each $a, b \in S$.

Definition 3.2 (Closure)

If $*$ is a binary operation on S, then S is closed under $*$.

Example:

- $+$ is a binary operation on $\mathbb{R}$ because the signature of $+$ is $\mathbb{R} \times \mathbb{R} \to \mathbb{R}$.
- $-$ is a binary operation on $\mathbb{R}$ since $- : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$.
- $\div$ is not a binary operation on $\mathbb{R}$ since $a \div 0$ is not in $\mathbb{R}$. However, $\div$ is a binary operation on $\mathbb{R}\backslash\{0\}$.
- Define θ on $\mathbb{R}^+$ by $a\theta b = a^b$. Then, θ is a binary operation on $\mathbb{R}^+$.
- Define ϕ on $\mathbb{R}$ by $a\phi b = \sqrt{ab}$. Then, ϕ is not a binary operation on $\mathbb{R}$ since if $ab < 0$, then $\sqrt{ab} \notin \mathbb{R}$.

Note 3.1 (Ordinary addition, ordinary multiplication)

We call $+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ as ordinary addition, and $\cdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$.

Definition 3.3 (Commutative binary operation)

A binary operation $*$ on S is commutative iff $\forall a, b \in S\, (a * b = b * a)$.

Definition 3.4 (Set of $m \times n$ matrices)

We define $M_{mn}(\mathbb{R})$ as the set of all $m \times n$ matrices whose entries belong to $\mathbb{R}$.

Definition 3.5 (General linear matrix set)

We define $GL(n, \mathbb{R})$ as the set of $n \times n$ nonsingular matrices with real entries.

Example:

- In $M_{mn}(\mathbb{R})$, matrix addition is a binary operation. It is also commutative.
- In $GL(n, \mathbb{R})$, matrix multiplication is a binary operation but it is not commutative. Matrix addition is not a binary operation, i.e., $I_n + (-1)I_n$ is not in $GL(n, \mathbb{R})$.

Definition 3.6 (Associative binary operation)

A binary operation $*$ on S is an associative binary operation iff $\forall a, b, c \in S\, (a*(b*c) = (a*b)*c)$.

Example: Define the operation $*$ on $\mathbb{R}$ by $a * b = a + b + ab$. Is $*$ an associative binary operation?

It is trivial that $*$ is a binary operation. Checking if it is associative,

$$
\begin{aligned}
a * (b * c) &= a * (b + c + bc) \\
a * (b * c) &= a + (b + c + bc) + a(b + c + bc) \\
a * (b * c) &= a + b + c + bc + ab + ac + abc \\
(a * b) * c &= (a + b + ab) * c \\
(a * b) * c &= (a + b + ab) + c + (a + b + ab)c \\
(a * b) * c &= a + b + ab + c + ac + bc + abc
\end{aligned}
$$

We see that $a * (b * c) = (a * b) * c$. Hence, $*$ is an associative binary operation.

Example: Let $S = \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \middle| a, b \in \mathbb{R} \right\}$. Let $*$ be matrix multiplication. Verify if $*$ is a commutative or associative binary operation on S.

Let $A = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ where $a, b \in \mathbb{R}$, and $B = \begin{bmatrix} c & -d \\ d & c \end{bmatrix}$ where $c, d \in \mathbb{R}$. Then,

$$AB = \begin{bmatrix} a & -b \\ -b & a \end{bmatrix} * \begin{bmatrix} c & -d \\ d & c \end{bmatrix}$$
$$AB = \begin{bmatrix} ac - bd & -ad - bc \\ ad + bc & ac - bd \end{bmatrix}$$
$$AB = \begin{bmatrix} ac - bd & -(ad + bc) \\ ad + bc & ac - bd \end{bmatrix}$$

This means $AB \in S$. Solving for BA,

$$BA = \begin{bmatrix} c & -d \\ d & c \end{bmatrix} * \begin{bmatrix} a & -b \\ -b & a \end{bmatrix}$$
$$BA = \begin{bmatrix} ac - bd & -bc - ad \\ ad + bc & -bd + ac \end{bmatrix}$$
$$BA = \begin{bmatrix} ac - bd & -(ad + bc) \\ ad + bc & ac - bd \end{bmatrix}$$

This also means that $BA \in S$. Note that $AB = BA$. Hence, matrix multiplication is commutative. It is also associative, since the general matrix multiplication is associative.

Example: Let $S = \{a, b, c\}$. Define $*$ on S by

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

.

Is $*$ a binary operation? If it is, is it commutative and/or associative?

The operation $*$ is a binary operation since every output of $*$ is in S. It is not commutative, since $a * c \neq c * a$. Checking if it is associative is left for the reader.

Theorem 3.1

There are n^{n^2} binary operations on a set S such that $|S| = n$.

Proof: We have n choices for each cell in the table. There are n^2 cells in the matrix, so there will be n^{n^2} combinations for the matrix. Hence, there are n^{n^2} binary operations on a set S such that $|S| = n$. ■

Definition 3.7 (Group)

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

- $\mathcal{G}_1 : \forall a, b, c \in G (a * (b * c) = (a * b) * c)$.
- $\mathcal{G}_2 : \exists e \in G\ \forall a \in G (e * a = a * e = a)$.
- $\mathcal{G}_3 : \forall a \in G\ \exists a' \in G (a * a' = a' * a = e)$.

In the third axiom, a' is called the inverse of a. We let $a^{-1} \equiv a'$ for each $a \in G$.

Example :

- Is $\langle \mathbb{R}, +$ a group?

  Yes, $\langle \mathbb{R}, +$ is a group because:
  - $+$ is associative,
  - $+$ has an identity element which is 0,
  - An arbitrary element a from $\mathbb{R}$ has an inverse $-a$ such that $a + (-a) = 0$.
- Is $GL(2, \mathbb{R})$ a group? Yes, $GL(2, \mathbb{R})$ is a group because:
  - Matrix multiplication is associative,
  - $+$ has an identity element which is I_2,
  - A nonsingular 2×2 matrix has a nonsingular inverse, which is in $GL(2, \mathbb{R})$.

Lecture 4: Introduction to groups, continued

Definition 4.1 (Set of integers modulo n)

We define $\mathbb{Z}_n$ be the set of integers modulo n, such that

$$\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}.$$

Note that $a \pmod{n}$ is the remainder when a is divided by n.

Example: Let $*$ be the binary operation on $\mathbb{Z}_n$ defined by $a * b = (a + b) \pmod{n}$. The table for $*$ on $\mathbb{Z}_4$ is

$*$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Theorem 4.1

$\langle \mathbb{Z}_n, * \rangle$ is a group.

Proof: This is because it satisfies the group axioms:

- The operation $*$ is a binary operation in $\mathbb{Z}_n$.
- The binary operation $*$ is associative on $\mathbb{Z}_n$.
- The binary operation $*$ has an identity element which is 0.
- If $a \in \mathbb{Z}_n$, then $a^{-1} = n - a \pmod{n}$. ■

Definition 4.2 (Set of integers relatively prime to n)

We define U_n to be the set of integers relatively prime to n. That is,

$$U_n = \{x \mid 1 \leq x \leq n \wedge \gcd(n, x) = 1\}.$$

Theorem 4.2

$\langle U_n, * \rangle$ is a group.

Proof: $\langle U_n, * \rangle$ satisfies the group axioms:

- U_n is closed under $*$.

  Let $a, b \in U_n$. Then, $\gcd(a, n) = \gcd(b, n) = 1$. Suppose $\gcd(ab, n) \neq 1$. Then, there exists an integer p such that $p \mid n$ and $p \mid ab$. Let d be such a number. Then, by Euclid's lemma, if $p \mid ab$, then $p \mid a$ or $p \mid b$. Suppose $p \mid a$. Then, $\gcd(a, n) \geq p$ which contradicts our assumption that $\gcd(a, n) = 1$. Similarly, if $p \mid b$, then $\gcd(b, n) \geq p$ which also contradicts our assumption that $\gcd(b, n) = 1$. Regardless of the case, we have a contradiction.

  Hence, $\gcd(ab, n) = 1$.

- $*$ is associative.

  Multiplying integers in modular arithmetic is associative. Since U_n has a binary operation utilizing modular arithmetic, this means $*$ is associative.

- U_n has an identity element under $*$.

  Let $a, e \in U_n$. Then, we must have $ae = a$, or equivalently, $ae \equiv a \pmod{n}$. Then, $n \mid ae - a$ which is the same as $n \mid a(e-1)$. By Euclid's lemma, either $n \mid a$ or $n \mid e-1$, which is the same as $e \equiv 1 \pmod{n}$. Clearly, $\gcd(1, n) = 1$, so our identity element is 1.

- Every element in U_n has an inverse.

  We are to find $x \in U_n$ such that $ax \equiv 1 \pmod{n}$ for every $a \in U_n$. This is the same as finding x such that $nk = ax - 1 \Leftrightarrow ax - nk = 1$. By Bezout's lemma, there exists an x satisfying the equation. Hence, a has an inverse in U_n. ■

Example:

- The table for $\mathbb{Z}_6$ is

$*$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

- The table for U_9 is

$*$	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

- Let $G = \{e, a, b, c, d\}$ where e is the identity in G under $*$. Complete the table below:

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

Example: Define $*$ on $\mathbb{R}$ by $a * b = a + b + ab$. Verify if $\langle \mathbb{R}, * \rangle$ is a group.

We can see that $a+b+ab = (a+1)(b+1)-1$. Since $a, b \in \mathbb{R}$, then $a*b \in \mathbb{R}$. We also know that $*$ is associative. Consider $a * e = a$. Solving for the identity,

$$\begin{aligned} a + e + ae &= a \\ e + ae &= 0 \\ e(1+a) &= 0 \end{aligned}$$

This means $e = 0$. To check if every element in $\mathbb{R}$ has an inverse under $*$, suppose $b = a^{-1}$. Then, $a * b = 0$. Solving for b in terms of a,

$$\begin{aligned} a + b + ab &= 0 \\ b + ab &= -a \end{aligned}$$

$$b(1+a) = -a$$
$$b = \frac{-a}{1+a}$$

We can see that b exists only if $a \neq 1$. Hence, not all elements have an inverse, so $\langle \mathbb{R}, * \rangle$ is not a group.

Note 4.1

Let G be a group. For any $a, b \in G$, we define ab as $a * b$ where $*$ is the binary operation of G, if $*$ is not stated.

Theorem 4.3

The identity element in a group is unique.

Proof: Suppose e_1 and e_2 are both identities of a group. Then, $e_1e_2 = e_1$ since e_2 is an identity. Similarly, $e_1e_2 = e_2$ since e_1 is an identity. By transitivity, we have $e_1 = e_2$. ■

Theorem 4.4

Let $a, b, c \in G$ where G is a group. Then,

(i) $ac = bc \implies a = b$. This is called right cancellation.

(ii) $ca = cb \implies a = b$. This is called left cancellation.

Proof: Let $a, b, c \in G$ be arbitrary. We prove each item:

(i) Suppose that $ac = bc$. Then, $acc^{-1} = bcc^{-1}$. Since the binary operation in G is associative, we have $a(cc^{-1}) = b(cc^{-1})$, which simplifies to $a = b$.

(ii) Suppose that $ca = cb$. Then, $c^{-1}ca = c^{-1}cb$. Since the binary operation in G is associative, we have $(c^{-1}c)a = (c^{-1}c)b$, which simplifies to $a = b$. ■

Theorem 4.5

Let G be a group. The inverse of any element in G is unique.

Proof: Let $g \in G$ be arbitrary. Let $a, b \in G$ be inverses of g. Then, $ag = ga = e$, and $bg = gb = e$, where e is the identity in G. Consider agb. We have $a(gb) = b$, and $(ag)b = a$. Since G is associative, then $a = b$. ■

Theorem 4.6

Let G be a group and let $a \in G$. Then, $(a^{-1})^{-1} = a$.

Proof: Since the inverse of a is a^{-1} and by the uniqueness of inverses, the inverse of a^{-1}, $(a^{-1})^{-1}$, is a. ■

Theorem 4.7

Let G be a group. If $a, b \in G$, then $(ab)^{-1} = b^{-1}a^{-1}$.

Proof: Let G be a group, and let $a, b \in G$ be arbitrary. Then,

$$ab(ab)^{-1} = e$$
$$a^{-1}ab(ab)^{-1} = a^{-1}e$$
$$eb(ab)^{-1} = a^{-1}$$

$$b^{-1}eb(ab)^{-1} = b^{-1}a^{-1}$$
$$b^{-1}b(ab)^{-1} = b^{-1}a^{-1}$$
$$(ab)^{-1} = b^{-1}a^{-1}$$

■

Theorem 4.8

Let G be a group. Let $a_1, a_2, \ldots, a_n \in G$. Then, $(a_1a_2\cdots a_n)^{-1} = a_n^{-1}a_{n-1}^{-1}\cdots a_2^{-1}a_1^{-1}$.

Proof: Let $n \in \mathbb{N}$ be arbitrary, and suppose that for all $i \in \mathbb{N}$ less than n, $(a_1a_2\cdots a_i)^{-1} = a_i^{-1}a_{i-1}^{-1}\cdots a_2^{-1}a_1^{-1}$.

$$(a_1a_2\cdots a_n)^{-1} = a_n^{-1}(a_1a_2\cdots a_{n-1})^{-1}$$
$$(a_1a_2\cdots a_n)^{-1} = a_n^{-1}a_{n-1}^{-1}\cdots a_2^{-1}a_1^{-1}$$

Hence, $(a_1a_2\cdots a_n)^{-1} = a_n^{-1}a_{n-1}^{-1}\cdots a_2^{-1}a_1^{-1}$. ■