Part I

Abstract Algebra

Definition (Binary Operations)

- A binary operation on a set A is an everywhere defined function
  - $f : A \times A \to A$.

Note: A binary operation must satisfy

- f assigns an element $f(a, b)$ of A to each ordered pair (a, b) in $A \times A$.
- Since a binary operation is a function, only one element of A is assigned to each ordered pair.

Definition (Binary Operations)

- A binary operation on a set A is an everywhere defined function
  - $f : A \times A \to A$.

Note: A binary operation must satisfy

- f assigns an element $f(a, b)$ of A to each ordered pair (a, b) in $A \times A$.
- Since a binary operation is a function, only one element of A is assigned to each ordered pair.

Notation

- It's customary to denote binary operations by a symbol such as $*$
  - $a * b$, instead of $*(a, b)$
  - $*$: multiplication
  - $a * b$: the product of a and b
- A is closed under the operation $*$, if a and b are elements in A, $a * b \in A$.

Notation

- It's customary to denote binary operations by a symbol such as $*$
  - $a * b$, instead of $*(a, b)$
  - $*$: multiplication
  - $a * b$: the product of a and b
- A is closed under the operation $*$, if a and b are elements in A, $a * b \in A$.

Notation

- It's customary to denote binary operations by a symbol such as $*$
  - $a * b$, instead of $*(a, b)$
  - $*$: multiplication
  - $a * b$: the product of a and b
- A is closed under the operation $*$, if a and b are elements in A, $a * b \in A$.

Example

- Let $A = \mathbb{Z}$. Define $a * b$ as $a + b$.
  - $*$ is a binary operation on $\mathbb{Z}$.

Example

- Let $A = \mathbb{R}$. Define $a * b$ as a/b.
  - $*$ is not a binary operation, since it is not defined for every ordered pair of elements of $\mathbb{R}$.
  - For example, $3 * 0$ is not defined, since we can not divide by zero.

Example

- Let $A = \mathbb{Z}$. Define $a * b$ as $a + b$.
  - $*$ is a binary operation on $\mathbb{Z}$.

Example

- Let $A = \mathbb{R}$. Define $a * b$ as a/b.
  - $*$ is not a binary operation, since it is not defined for every ordered pair of elements of $\mathbb{R}$.
  - For example, $3 * 0$ is not defined, since we can not divide by zero.

Definition

- If $A = \{a_1, a_2, \ldots, a_n\}$ is a finite set, a binary operation on A can be defined by means of a multiplication table.

$$
\begin{array}{c|cccccc}
* & a_1 & a_2 & \ldots & a_j & \ldots & a_n \\
\hline
a_1 & & & & & & \\
a_2 & & & & & & \\
\vdots & & & & & & \\
a_i & & & & a_i * a_j & & \\
\vdots & & & & & & \\
a_n & & & & & &
\end{array}
$$

Example ($\vee$ and $\wedge$)

- Let
  - $A = \{0, 1\}$
- Define binary operations $\vee$ and $\wedge$ by the following tables:

$\vee$	0	1
0	0	1
1	1	1

$\wedge$	0	1
0	0	0
1	0	1

Example (How Many Operations Can Be Defined on A?)

- Let
  - $A = \{a, b\}$
- How many binary operations can be defined on A.
  - Every binary operation $*$ on A can be described by a table

$*$	a	b
a		
b		

  - Then what?

Example (How Many Operations Can Be Defined on A?)

- Let
  - $A = \{a, b\}$
- How many binary operations can be defined on A.
  - Every binary operation $*$ on A can be described by a table

$*$	a	b
a		
b		

  - Then what?

Example (How Many Operations Can Be Defined on A?)

- Let
  - $A = \{a, b\}$
- How many binary operations can be defined on A.
  - Every binary operation $*$ on A can be described by a table

$*$	a	b
a		
b		

  - Then what?

Definition (Properties of Binary Operations)

- For all elements a, b, and c in A
  - Commutative $a * b = b * a$
  - Associative $a * (b * c) = (a * b) * c$
  - Idempotent $a * a = a$

Definition (Properties of Binary Operations)

- For all elements a, b, and c in A
  - Commutative $a * b = b * a$
  - Associative $a * (b * c) = (a * b) * c$
  - Idempotent $a * a = a$

Definition (Properties of Binary Operations)

- For all elements a, b, and c in A
  - Commutative $a * b = b * a$
  - Associative $a * (b * c) = (a * b) * c$
  - Idempotent $a * a = a$

Definition (Identity)

- An element e in A is called an identity element if $\forall a \in A$
  - $e * a = a * e = a$

Note:

- An identity element must be unique.

Definition (Inverse)

- An element $a' \in A$ is called an inverse of a and written as a^{-1} if
  - $a * a' = a' * a = e$, or
  - $a * a^{-1} = a^{-1} * a = e$

Definition (Identity)

- An element e in A is called an identity element if $\forall a \in A$
  - $e * a = a * e = a$

Note:

- An identity element must be unique.

Definition (Inverse)

- An element $a' \in A$ is called an inverse of a and written as a^{-1} if
  - $a * a' = a' * a = e$, or
  - $a * a^{-1} = a^{-1} * a = e$

Definition (Identity)

- An element e in A is called an identity element if $\forall a \in A$
  - $e * a = a * e = a$

Note:

- An identity element must be unique.

Definition (Inverse)

- An element $a' \in A$ is called an inverse of a and written as a^{-1} if
  - $a * a' = a' * a = e$, or
  - $a * a^{-1} = a^{-1} * a = e$

Theorem

- *Let* $*$ *be a binary operation on a set* A*, and suppose that* $*$ *satisfies the following properties for any* a, b*, and* c *in* A*:*
  - $a * a = a$
  - $a * b = b * a$
  - $a * (b * c) = (a * b) * c$
- *Define a relation* $\leqslant$ *on* A *by*
  - $a \leqslant b$ *if and only if* $a = a * b$
- *Then* $(A, \ \leqslant)$ *is a poset, and* $\forall a, b \in A$*,* $GLB(a, b) = a * b$*.*

Proof.

- We must show that
  - $\leqslant$ is reflexive, antisymmetric and transitive.
  - $a * b = a \wedge b$ for all a and b in A.

Proof: $\leqslant$ is reflexive

Proof. Def $a \leqslant b$ if and only if $a = a * b$.

- Since $a = a * a$
  - $a \leqslant a$ for all a in A
  - $\leqslant$ is reflexive.

Proof: $\leqslant$ is reflexive

Proof. Def $a \leqslant b$ if and only if $a = a * b$.

- Since $a = a * a$
  - $a \leqslant a$ for all a in A
  - $\leqslant$ is reflexive.

❀

Proof: $\leqslant$ is antisymmetric

Proof. Def $a \leqslant b$ if and only if $a = a * b$.

- Now suppose that
  - $a \leqslant b$ and $b \leqslant a$
  - $a = a * b = b * a = b$, by definition and property 2
  - so $a = b$
  - Thus $\leqslant$ is antisymmetric.

Proof: $\leqslant$ is antisymmetric

Proof. Def $a \leqslant b$ if and only if $a = a * b$.

- Now suppose that
  - $a \leqslant b$ and $b \leqslant a$
  - $a = a * b = b * a = b$, by definition and property 2
  - so $a = b$
  - Thus $\leqslant$ is antisymmetric.

Proof: $\leqslant$ is antisymmetric

Proof. Def $a \leqslant b$ if and only if $a = a * b$.

- Now suppose that
  - $a \leqslant b$ and $b \leqslant a$
  - $a = a * b = b * a = b$, by definition and property 2
  - so $a = b$
  - Thus $\leqslant$ is antisymmetric.

Proof: $\leqslant$ is antisymmetric

Proof. Def $a \leqslant b$ if and only if $a = a * b$.

- Now suppose that
  - $a \leqslant b$ and $b \leqslant a$
  - $a = a * b = b * a = b$, by definition and property 2
  - so $a = b$
  - Thus $\leqslant$ is antisymmetric.

Proof: $\leqslant$ is transitive

Proof. Def $a \leqslant b$ if and only if $a = a * b$.

- If $a \leqslant b$ and $b \leqslant c$
  - then $a = a * b = a * (b * c) = (a * b) * c = a * c$,
  - so $a \leqslant c$
  - $\leqslant$ is transitive.

Proof: $\leqslant$ is transitive

Proof. Def $a \leqslant b$ if and only if $a = a * b$.

- If $a \leqslant b$ and $b \leqslant c$
  - then $a = a * b = a * (b * c) = (a * b) * c = a * c$,
  - so $a \leqslant c$
  - $\leqslant$ is transitive.

❀

Proof: $\leqslant$ is transitive

Proof. Def $a \leqslant b$ if and only if $a = a * b$.

- If $a \leqslant b$ and $b \leqslant c$
  - then $a = a * b = a * (b * c) = (a * b) * c = a * c$,
  - so $a \leqslant c$
  - $\leqslant$ is transitive.

Proof: $a * b = a \wedge b$ for all a and b in A

Proof. Def $a \leqslant b$ if and only if $a = a * b$.

1. $a * b$ is a lower bound for a and b
   - $a * b = a * (b * b) = (a * b) * b$
   - so $a * b \leqslant b$
   - similarly, $a * b \leqslant a$
   - $a * b$ is a lower bound for a and b
2. If $c \leqslant a$ and $c \leqslant b$, then $c \leqslant a * b$
   - $c = c * a$ and $c = c * b$ by definition
   - $c = (c * a) * b = c * (a * b)$
   - So, $c \leqslant a * b$

- Therefore, $a * b$ is the greatest lower bound of a and b.

Proof: $a * b = a \wedge b$ for all a and b in A

Proof. Def $a \leqslant b$ if and only if $a = a * b$.

1. $a * b$ is a lower bound for a and b
   - $a * b = a * (b * b) = (a * b) * b$
   - so $a * b \leqslant b$
   - similarly, $a * b \leqslant a$
   - $a * b$ is a lower bound for a and b
2. If $c \leqslant a$ and $c \leqslant b$, then $c \leqslant a * b$
   - $c = c * a$ and $c = c * b$ by definition
   - $c = (c * a) * b = c * (a * b)$
   - So, $c \leqslant a * b$

- Therefore, $a * b$ is the greatest lower bound of a and b.

Proof: $a * b = a \wedge b$ for all a and b in A

Proof. Def $a \leqslant b$ if and only if $a = a * b$.

1. $a * b$ is a lower bound for a and b
   - $a * b = a * (b * b) = (a * b) * b$
   - so $a * b \leqslant b$
   - similarly, $a * b \leqslant a$
   - $a * b$ is a lower bound for a and b
2. If $c \leqslant a$ and $c \leqslant b$, then $c \leqslant a * b$
   - $c = c * a$ and $c = c * b$ by definition
   - $c = (c * a) * b = c * (a * b)$
   - So, $c \leqslant a * b$

- Therefore, $a * b$ is the greatest lower bound of a and b.

Proof: $a * b = a \wedge b$ for all a and b in A

Proof. Def $a \leqslant b$ if and only if $a = a * b$.

1. $a * b$ is a lower bound for a and b
   - $a * b = a * (b * b) = (a * b) * b$
   - so $a * b \leqslant b$
   - similarly, $a * b \leqslant a$
   - $a * b$ is a lower bound for a and b
2. If $c \leqslant a$ and $c \leqslant b$, then $c \leqslant a * b$
   - $c = c * a$ and $c = c * b$ by definition
   - $c = (c * a) * b = c * (a * b)$
   - So, $c \leqslant a * b$

Therefore, $a * b$ is the greatest lower bound of a and b.

Proof: $a * b = a \wedge b$ for all a and b in A

Proof. Def $a \leqslant b$ if and only if $a = a * b$.

1. $a * b$ is a lower bound for a and b
   - $a * b = a * (b * b) = (a * b) * b$
   - so $a * b \leqslant b$
   - similarly, $a * b \leqslant a$
   - $a * b$ is a lower bound for a and b
2. If $c \leqslant a$ and $c \leqslant b$, then $c \leqslant a * b$
   - $c = c * a$ and $c = c * b$ by definition
   - $c = (c * a) * b = c * (a * b)$
   - So, $c \leqslant a * b$

- Therefore, $a * b$ is the greatest lower bound of a and b.

Proof: $a * b = a \wedge b$ for all a and b in A

Proof. Def $a \leqslant b$ if and only if $a = a * b$.

1. $a * b$ is a lower bound for a and b
   - $a * b = a * (b * b) = (a * b) * b$
   - so $a * b \leqslant b$
   - similarly, $a * b \leqslant a$
   - $a * b$ is a lower bound for a and b
2. If $c \leqslant a$ and $c \leqslant b$, then $c \leqslant a * b$
   - $c = c * a$ and $c = c * b$ by definition
   - $c = (c * a) * b = c * (a * b)$
   - So, $c \leqslant a * b$

Therefore, $a * b$ is the greatest lower bound of a and b.

Proof: $a * b = a \wedge b$ for all a and b in A

Proof. Def $a \leqslant b$ if and only if $a = a * b$.

1. $a * b$ is a lower bound for a and b
   - $a * b = a * (b * b) = (a * b) * b$
   - so $a * b \leqslant b$
   - similarly, $a * b \leqslant a$
   - $a * b$ is a lower bound for a and b
2. If $c \leqslant a$ and $c \leqslant b$, then $c \leqslant a * b$
   - $c = c * a$ and $c = c * b$ by definition
   - $c = (c * a) * b = c * (a * b)$
   - So, $c \leqslant a * b$

Therefore, $a * b$ is the greatest lower bound of a and b.