Abstract Algebra
Part I: Group Theory
Let $X$ be a set.

**Cartesian product**

$$X \times X = \{(x_1, x_2) \mid x_1, x_2 \in X\}$$

A **binary operation** on $X$ is a function

$$m : X \times X \to X$$
Let $X$ be a set. 

**Cartesian product**

$$ X \times X = \{(x_1, x_2) \mid x_1, x_2 \in X\} $$

A **binary operation** on $X$ is a function

$$ m : X \times X \to X $$

Often, we’re thinking of multiplication or additions, and so we denote the operation with $\star$, as in

$$ a \star b = m(a, b). $$
Properties of binary operations

1. **Commutativity**
2. **Associativity**
3. **Identity** (0 in addition, I in matrix multiplication)
4. **Inverses**

A Group is a pair \((G, \star)\) consisting of a set \(G\) and a binary operation \(\star\) on \(G\) such that:

1. \(\star\) is associative.
2. There is an identity element \(e \in G\). That is, \(e \star g = g = g \star e\) for any \(g \in G\).
3. Every element of \(G\) has an inverse. That is, for any \(g \in G\), there is an element \(g^{-1}\) such that \(gg^{-1} = e = g^{-1}g\).

If \((G, \star)\) is also commutative, then we say \((G, \star)\) is abelian.
Properties of binary operations

- Commutativity
- Associativity
- Identity (0 in addition, \( I \) in matrix multiplication)
- Inverses
Properties of binary operations

- Commutativity
- Associativity
- Identity (0 in addition, $I$ in matrix multiplication)
- Inverses

A **Group** is a pair $(G, \star)$ consisting of a set $G$ and a binary operation $\star$ on $G$ such that:

1. $\star$ is associative.
2. There is an identity element $e \in G$. That is,
   \[ e \star g = g = g \star e \quad \text{for any } g \in G. \]
3. Every element of $G$ has an inverse. That is, for any $g \in G$, there is an element $g^{-1}$ such that $gg^{-1} = e = g^{-1}g$. 
Properties of binary operations

- Commutativity
- Associativity
- Identity (0 in addition, $I$ in matrix multiplication)
- Inverses

A **Group** is a pair $(G, \star)$ consisting of a set $G$ and a binary operation $\star$ on $G$ such that:

1. $\star$ is associative.
2. There is an identity element $e \in G$. That is,
   
   $$e \star g = g = g \star e$$
   
   for any $g \in G$.
3. Every element of $G$ has an inverse. That is, for any $g \in G$, there is an element $g^{-1}$ such that $gg^{-1} = e = g^{-1}g$.

If $(G, \star)$ is also commutative, then we say $(G, \star)$ is **abelian**.
Modular arithmetic

Fix two positive integers $a, b \in \mathbb{Z}$. Then, $b$ can be written uniquely as

$$b = q \times a + r \quad \text{with} \quad 0 \leq r < a.$$ 

Then we say "$b$ is congruent to $r$ (mod $a$)," denoted

$$b \equiv r \pmod{a}.$$
Modular arithmetic

Fix two positive integers \( a, b \in \mathbb{Z} \). Then, \( b \) can be written uniquely as

\[
    b = q \times a + r \quad \text{with } 0 \leq r < a.
\]

Then we say “\( b \) is congruent to \( r \) (mod \( a \)),” denoted

\[
    b \equiv r \pmod{a}.
\]

An (equivalence) relation on a set \( X \) is a relationship between any two values \( a, b \in X \), written \( a \sim b \), satisfying

- reflexivity: \( a \sim a \) for all \( a \in X \),
- symmetry: if \( a \sim b \), then \( b \sim a \), and
- transitivity: if \( a \sim b \) and \( b \sim c \), then \( a \sim c \).
Modular arithmetic

Fix two positive integers \( a, b \in \mathbb{Z} \). Then, \( b \) can be written uniquely as

\[
b = q \ast a + r \quad \text{with} \quad 0 \leq r < a.
\]

Then we say “\( b \) is congruent to \( r \) (mod \( a \)),” denoted

\[
b \equiv r \pmod{a}.
\]

An (equivalence) relation on a set \( X \) is a relationship between any two values \( a, b \in X \), written \( a \sim b \), satisfying

- **reflexivity**: \( a \sim a \) for all \( a \in X \),
- **symmetry**: if \( a \sim b \), then \( b \sim a \), and
- **transitivity**: if \( a \sim b \) and \( b \sim c \), then \( a \sim c \).

Fix \( n \in \mathbb{Z}_{>1} \). One relation on \( \mathbb{Z} \) is

\[
a \sim b \text{ if and only if } a \equiv b \pmod{n}.
\]
Modular arithmetic

Fix two positive integers \(a, b \in \mathbb{Z}\). Then, \(b\) can be written uniquely as
\[
b = q \times a + r \quad \text{with} \quad 0 \leq r < a.
\]
Then we say “\(b\) is congruent to \(r\) (mod \(a\)),” denoted
\[
b \equiv r \pmod{a}.
\]

An (equivalence) relation on a set \(X\) is a relationship between any two values \(a, b \in X\), written \(a \sim b\), satisfying

- reflexivity: \(a \sim a\) for all \(a \in X\),
- symmetry: if \(a \sim b\), then \(b \sim a\), and
- transitivity: if \(a \sim b\) and \(b \sim c\), then \(a \sim c\).

Fix \(n \in \mathbb{Z}_{>1}\). One relation on \(\mathbb{Z}\) is
\[
a \sim b \text{ if and only if } a \equiv b \pmod{n}.
\]

The equivalence classes are
\[
\bar{a} = \{a + kn \mid k \in \mathbb{Z}\} = \{a, a + n, a - n, a + 2n, a - 2n, \ldots\}.
\]
Multiplication tables

\((\mathbb{Z}/3\mathbb{Z}, +)\):
**Multiplication tables**

\[(\mathbb{Z}/3\mathbb{Z}, +) :\]

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>
### Multiplication tables

$$(\mathbb{Z}/3\mathbb{Z}, +) :$$

<table>
<thead>
<tr>
<th></th>
<th>$\bar{0}$</th>
<th>$\bar{1}$</th>
<th>$\bar{2}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\bar{0}$</td>
<td>$\bar{0}$</td>
<td>$\bar{1}$</td>
<td>$\bar{2}$</td>
</tr>
<tr>
<td>$\bar{1}$</td>
<td>$\bar{1}$</td>
<td>$\bar{2}$</td>
<td>$\bar{0}$</td>
</tr>
<tr>
<td>$\bar{2}$</td>
<td>$\bar{2}$</td>
<td>$\bar{0}$</td>
<td>$\bar{1}$</td>
</tr>
</tbody>
</table>
### Multiplication tables

$$(\mathbb{Z}/3\mathbb{Z}, +) :$$

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>
## Multiplication tables

**$(\mathbb{Z}/3\mathbb{Z}, +)$:**

<table>
<thead>
<tr>
<th></th>
<th>$\bar{0}$</th>
<th>$\bar{1}$</th>
<th>$\bar{2}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\bar{0}$</td>
<td>$\bar{0}$</td>
<td>$\bar{1}$</td>
<td>$\bar{2}$</td>
</tr>
<tr>
<td>$\bar{1}$</td>
<td>$\bar{1}$</td>
<td>$\bar{2}$</td>
<td>$\bar{0}$</td>
</tr>
<tr>
<td>$\bar{2}$</td>
<td>$\bar{2}$</td>
<td>$\bar{0}$</td>
<td>$\bar{1}$</td>
</tr>
</tbody>
</table>

**$(\text{ThreeFruit}, \star)$:**

<table>
<thead>
<tr>
<th></th>
<th>fig</th>
<th>apple</th>
<th>grape</th>
</tr>
</thead>
<tbody>
<tr>
<td>fig</td>
<td>grape</td>
<td>fig</td>
<td>apple</td>
</tr>
<tr>
<td>apple</td>
<td>fig</td>
<td>apple</td>
<td>grape</td>
</tr>
<tr>
<td>grape</td>
<td>apple</td>
<td>grape</td>
<td>fig</td>
</tr>
</tbody>
</table>
Properties of integers

If $b$ is a multiple of $a$ (or $a$ divides $b$), we write $a|b$. 
Properties of integers

If $b$ is a multiple of $a$ (or $a$ divides $b$), we write $a | b$. The greatest common divisor of $a$ and $b$, denoted $\gcd(a, b)$ or just $(a, b)$, is the largest integer dividing both $a$ and $b$. 

Theorem For any $a, b \in \mathbb{Z} > 0$, $\gcd(a, b) = xa + yb$ for some $x, y \in \mathbb{Z}$. In other words, the greatest common divisor is a $\mathbb{Z}$-linear combination of $a$ and $b$. 
Properties of integers

If \( b \) is a multiple of \( a \) (or \( a \) divides \( b \)), we write \( a \mid b \). The greatest common divisor of \( a \) and \( b \), denoted

\[
\gcd(a, b) \quad \text{or just} \quad (a, b)
\]

is the largest integer dividing both \( a \) and \( b \). We say \( a \) and \( b \) are relatively prime if \( (a, b) = 1 \).
Properties of integers

If \( b \) is a multiple of \( a \) (or \( a \) divides \( b \)), we write \( a \mid b \).

The greatest common divisor of \( a \) and \( b \), denoted

\[
gcd(a, b) \quad \text{or just} \quad (a, b)
\]

is the largest integer dividing both \( a \) and \( b \).

We say \( a \) and \( b \) are relatively prime if \( (a, b) = 1 \).

**Theorem**

*For any \( a, b \in \mathbb{Z}_{>0} \),*

\[
(a, b) = xa + yb \quad \text{for some} \ x, y \in \mathbb{Z}.
\]

*In other words, the greatest common divisor is a \( \mathbb{Z} \)-linear combination of \( a \) and \( b \).*
Theorem

Let $G$ be a group.

1. The identity element in $G$ is unique. We denote this element by $e$.
2. For a given $g \in G$, $g^{-1}$ is unique.
3. $(a^{-1})^{-1} = a$.
4. For any $x, y \in G$, there is a unique element $z \in G$ so that $xz = y$.
5. For any $x, y \in G$, $(xy)^{-1} = (y^{-1}x^{-1})$. 