Def) A set $X$ is a well-defined collection of objects.

For any object $x$ we can decide if $x \in X$ or $x \notin X$.

Example: $A = \left\{ \frac{p}{q} \mid p, q \in \mathbb{Z}, q \neq 0 \right\}$

Subsets

$A \subseteq B$, $A \subset B$

$A \cap B$

$\emptyset$ – Empty set

Set operations

Union: $A \cup B = \left\{ x \mid x \in A \text{ or } x \in B \right\}$

Intersection: $A \cap B = \left\{ x \mid x \in A \text{ and } x \in B \right\}$

Disjoint if $A \cap B = \emptyset$

Suppose $A \subseteq \mathcal{U}$

Complement: $A' = \left\{ x \mid x \in \mathcal{U} \text{ and } x \notin A \right\}$
Difference: \( A \setminus B = A \cap B' = \{ x \mid x \in A, x \notin B \} \frac{3}{2} \)

\( \mathbb{U} = \mathbb{R}^2 \)

\[ A = \{ (x, y) \mid y = x^2 \} \]

\[ B_M = \{ (x, y) \mid y = 1 \} \]

\[ A \cap B = \frac{3}{2} (1, 1), (-1, 1) \frac{3}{2} \]

\[ A \cup B = \frac{3}{2} \]

**Proposition 1.2.** Let \( A, B, \) and \( C \) be sets. Then

1. \( A \cup A = A, A \cap A = A, \) and \( A \setminus A = \emptyset; \)
2. \( A \cup \emptyset = A \) and \( A \cap \emptyset = \emptyset; \)
3. \( A \cup (B \cup C) = (A \cup B) \cup C \) and \( A \cap (B \cap C) = (A \cap B) \cap C; \)
4. \( A \cup B = B \cup A \) and \( A \cap B = B \cap A; \)
5. \( A \cup (B \cap C) = (A \cup B) \cap (A \cup C); \)
6. \( A \cap (B \cup C) = (A \cap B) \cup (A \cap C). \)

**Theorem 1.3** (De Morgan’s Laws). Let \( A \) and \( B \) be sets. Then

1. \( (A \cup B)' = A' \cap B'; \)
2. \( (A \cap B)' = A' \cup B'. \)

**Cartesian Product:**

\[ A \times B = \{ (a, b) \mid a \in A, b \in B \} \]
Mappings

A mapping or function from $A$ to $B$ is a relation

$f = \{ (a,b) \mid \text{for all } a \in A \exists \text{ unique } b \in B \}$

Note:

* Not all $b \in B$ need appear
* Different $a_1, a_2 \in A$ can pair with the same $b$ just not with multiple $b$.

$f : A \mapsto B$ or $A \xrightarrow{f} B$

$f(a) = b$ or $f : a \mapsto b$ (instead of $(a,b) \in f \subseteq A \times B$)

Ex)

<table>
<thead>
<tr>
<th>$A$</th>
<th>$f$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Rabbit</td>
</tr>
<tr>
<td>2</td>
<td>Cat</td>
</tr>
<tr>
<td>3</td>
<td>Umbrella</td>
</tr>
</tbody>
</table>

This is a function

\[\text{Not a function}\]

A relation can fail to be a function if it is not well-defined.

A relation is well-defined if each element in the domain is assigned to a unique element in the range.
Example: \( f: \mathbb{Q} \to \mathbb{Z} \) is not well defined
\[
\frac{p}{q} \mapsto p
\]
\[
\frac{1}{2} = \frac{2}{4}
\]
\[
f\left(\frac{1}{2}\right) = 1
\]
\[
f\left(\frac{3}{4}\right) = 2
\]

Onto/Surjective: \( f(A) = B \), i.e. \( \exists a \in A \) for each \( b \in B \) such that \( f(a) = b \)

Injective / 1-1: \( a_1 \neq a_2 \implies f(a_1) \neq f(a_2) \)

If \( f(a_1) = f(a_2) \) \( \implies a_1 = a_2 \)

Bijective = 1-1 and onto

Example: \( f: \mathbb{Z} \to \mathbb{Q} \)
\[
n \mapsto \frac{n}{1}
\]
\( \) is 1-1 but not onto

\( g: \mathbb{Q} \to \mathbb{Z} \)
\[
\frac{p}{q} \mapsto p \text{ where } \frac{p}{q} \text{ is expressed in lowest terms and } q > 0
\]
\( \) is onto, not 1-1

Composition:
\( f: A \to B \), \( g: B \to C \)
\( g \circ f: A \to C \)
\( x \mapsto g(f(x)) \)
Theorem 1.15. Let \( f : A \to B \), \( g : B \to C \), and \( h : C \to D \). Then

1. The composition of mappings is associative; that is, \((h \circ g) \circ f = h \circ (g \circ f)\);
2. If \( f \) and \( g \) are both one-to-one, then the mapping \( g \circ f \) is one-to-one;
3. If \( f \) and \( g \) are both onto, then the mapping \( g \circ f \) is onto;
4. If \( f \) and \( g \) are bijective, then so is \( g \circ f \).

Identity

\[ \text{id}_S : S \to S \]
\[ s \mapsto s \]

A map \( g : B \to A \) is an inverse mapping of \( f : A \to B \) if \( g \circ f = \text{id}_A \) and \( f \circ g = \text{id}_B \). Write \( g = f^{-1} \).

Ex. Suppose \( S = \{1, 2, 3\} \), define a map

\[ \Pi : S \to S \]
\[ \Pi(1) = 2, \quad \Pi(2) = 3, \quad \Pi(3) = 1 \]

\( \Pi \) is bijective

\[ \left( \begin{array}{ccc} 1 & 2 & 3 \\ \Pi(1) & \Pi(2) & \Pi(3) \end{array} \right) = \left( \begin{array}{ccc} 1 & 2 & 3 \\ 2 & 3 & 1 \end{array} \right) = (2 \, 3 \, 1) \]

\[ \Pi^{-1} = \left( \begin{array}{ccc} 1 & 2 & 3 \\ 3 & 1 & 2 \end{array} \right) \]

\( \Pi^{-1} : 2 \mapsto 1 \) \quad \Pi^{-1} : 3 \mapsto 2 \quad \Pi^{-1} : 1 \mapsto 3 \]
Theorem: A mapping is invertible if it is both 1-1 and onto.

Equivalence Relations

An equivalence relation \( \sim \) on a set \( X \) is a relation \( R \subseteq X \times X \)

- \((x, x) \in R \quad \forall x \in X \) (reflexive property)
  \[ x \sim x \]

- \((x, y) \in R \Rightarrow (y, x) \in R \) (symmetric property)
  \[ x \sim y \Rightarrow y \sim x \]

- \((x, y) \in R \) and \((y, z) \in R \Rightarrow (x, z) \in R \)
  \[ x \sim y \text{ and } y \sim z \Rightarrow x \sim z. \quad [\text{transitive property}] \]

A Partition \( P \) of set \( X \) is a collection of non-empty sets \( A_1, A_2, \ldots \), s.t. \( A_i \cap A_j = \emptyset \) for \( i \neq j \)
and \( \bigcup_{k} A_k = X \)

Equivalence class

\([x] = \{ y \in X \mid y \sim x \}\)
Theorem 1.25. Given an equivalence relation ~ on a set X, the equivalence classes of X form a partition of X. Conversely, if \( P = \{X_i\} \) is a partition of a set X, then there is an equivalence relation on X with equivalence classes \( X_i \).

**Cor** Two Eq. Classes are either disjoint or equal

**Ex.** Let \( r,s \) be in \( \mathbb{Z} \) suppose \( n \in \mathbb{N} \) \( n > 0 \)

\( r \) is congruent to \( s \) modulo \( n \)

\[ r \equiv s \pmod{n} \]

or

\[ r - s = n \cdot k \text{ for some } k \in \mathbb{Z} \]

(also \( r - s \) is divisible by \( n \))

**Ex.** \( 41 \equiv 17 \pmod{8} \) since \( 41 - 17 = 24 = 8 \cdot 3 \)

**Congruence mod \( n \) is an Eq. relation on \( \mathbb{Z} \).**

- \( r \equiv r \pmod{n} \) since \( r - r = 0 \cdot n \)

- \( r \equiv s \pmod{n} \) \( \Rightarrow \) \( r - s = n \cdot k \) (symmetric)

  \[ \Rightarrow s - r = n \cdot (-k) \Rightarrow s \equiv r \pmod{n} \]

- \( r \equiv s \pmod{n} \) and \( s \equiv t \pmod{n} \)

  \[ \Rightarrow r \equiv t \pmod{n} \] (transitive)
\[ r - s = kn \quad \text{and} \quad s - t = ln \quad (k, l \in \mathbb{Z}) \]

\[ r - s + s - t = kn + ln \]

\[ r - t = n(k + l) \implies r \equiv t \pmod{n} \]

\[ \mathbb{Z}/3\mathbb{Z} = \text{integers modulo 3} \]

\[ [0] = \{ \ldots, -3, 0, 3, 6, \ldots \} \]

\[ [1] = \{ \ldots, -2, 1, 4, \ldots \} \]

\[ [2] = \{ \ldots, -1, 2, 5, 8, \ldots \} \]

A non-empty subset \( S \) of \( \mathbb{Z} \) is well-ordered if it contains a least element.

\[ \mathbb{N} = \{ 1, 2, 3, \ldots \} \]

**Principle 2.6** (Principle of Well-Ordering). *Every nonempty subset of the natural numbers is well-ordered.*

The Principle of Well-Ordering is equivalent to the Principle of Mathematical Induction.

**Lemma 2.7.** *The Principle of Mathematical Induction implies that 1 is the least positive natural number.*

**Proof:**

\[ S = \{ n \in \mathbb{N} \mid n \geq 1 \} \implies 1 \in S \]

Assume \( n \in S \), \( n \geq 1 \)

\[ n + 1 \geq 1 \implies n + 1 \in S \]

By induction, all natural numbers are in \( S \) and \( \geq 1 \).
Theorem 2.8. The Principle of Mathematical Induction implies the Principle of Well-Ordering. That is, every nonempty subset of \( \mathbb{N} \) contains a least element.

Theorem 2.9 (Division Algorithm). Let \( a \) and \( b \) be integers, with \( b > 0 \). Then there exist unique integers \( q \) and \( r \) such that
\[
a = bq + r
\]
where \( 0 \leq r < b \).

\[
\text{Let } a, b \in \mathbb{Z}
\]
\[
\text{d} \text{ is a common divisor of } a, b \text{ if } d \mid a \text{ and } d \mid b
\]
\[
\gcd(a, b) = d \quad \text{s.t. all other common divisors of } a, b \text{ also divide } d
\]
\[
\text{If } \gcd(a, b) = 1 \implies a \text{ and } b \text{ are relatively prime.}
\]

Theorem 2.10. Let \( a \) and \( b \) be nonzero integers. Then there exist integers \( r \) and \( s \) such that
\[
\gcd(a, b) = ar + bs
\]
Furthermore, the greatest common divisor of \( a \) and \( b \) is unique.

Corollary. If \( a, b \) are relatively prime then \( \exists r, s \) s.t.
\[
l = ar + bs
\]

Prime
- \( p \) is a prime number if only if \( \gcd(p, a) = p \text{ and } p \mid a \).

Lemmas. Let \( a, b \in \mathbb{Z} \). If \( p \) prime then
- either \( p \mid a \) or \( p \mid b \).
Theorem \( a \in \mathbb{Z} \)

\[ a = p_1 \cdots p_r \quad \text{for } p_1, \ldots, p_r \text{ prime} \]

**Groups**

*(Informal Definition)*

A **Group** is a set \( G \) which is closed under an associative operation s.t. \( \exists \) an identity and inverse \( \forall a, b, c \in G \)

**Associative operation**

\[ a \cdot (b \cdot c) = (a \cdot b) \cdot c \]

**Identity** \( e = \text{identity is s.t.} \)

\[ a \cdot e = e \cdot a = a \]

**Inverse** \( a^{-1} = \text{inverse of } a \quad \text{if} \quad a \cdot a^{-1} = a^{-1} \cdot a = e = \text{identity} \)

**Is closed** \( a \cdot b \in G \) for all \( a, b \in G \)

The integers \( \mod n \)

Recall \( a \equiv b \pmod{n} \) \( \iff \) \( a - b = kn \), \( k \in \mathbb{Z} \)

- Integers \( \mod n \) partition \( \mathbb{Z} \) into \( n \) different equivalence classes

- \( \mathbb{Z}_n \) or \( \mathbb{Z} / n \mathbb{Z} \)

Operation is addition modulo \( n \)
\[ \mathbb{Z}_{12} = \{ \text{integers mod 12} \} \]

\[ \mathbb{Z}_{10} = \{ \ldots, -12, 0, 12, 24, \ldots \} \]

\[ \mathbb{Z}_{11} = \{ \ldots, -1, 11, 23, 35, \ldots \} \]

- Note that addition and multiplication are defined \( \mod n \):

\[
(a + b) \mod n = ((a \mod n) + (b \mod n)) \mod (n)
\]

\[
(a \cdot b) \mod n = (a \mod n \cdot b \mod n) \mod (n)
\]

**Example**

\[ 7 + 4 = 1 \mod 5 \]

\[ 7 \cdot 3 = 1 \mod 5 \]

\[
\begin{array}{c|cccccccc}
- & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\
2 & 0 & 2 & 4 & 6 & 0 & 2 & 4 & 6 \\
3 & 0 & 3 & 6 & 1 & 4 & 7 & 2 & 5 \\
4 & 0 & 4 & 0 & 4 & 0 & 4 & 0 & 4 \\
5 & 0 & 5 & 2 & 7 & 4 & 1 & 6 & 3 \\
6 & 0 & 6 & 4 & 2 & 0 & 6 & 4 & 2 \\
7 & 0 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \\
\end{array}
\]

**Table 3.3:** Multiplication table for \( \mathbb{Z}_8 \)

Not a group under multi.

\( \text{integer mod 8} \)
Prop. Let $\mathbb{Z}_n$ be the set of equivalence classes of integers mod $n$ and $a, b, c \in \mathbb{Z}_n$

1) Addition and multiplication are commutative

$$a + b \equiv b + a \pmod{n}$$

$$ab \equiv ba \pmod{n}$$

2) Addition and multiplication are associative

3) There are additive and multiplicative identities

$$a + 0 \equiv a \pmod{n}$$

$$a \cdot 1 \equiv a \pmod{n}$$

4) For every integer $a \in \mathbb{Z}$, there exists an additive inverse

$$-a \text{ s.t. } \quad a + (-a) \equiv 0 \pmod{n}$$

5) Let $a \neq 0$. Then $\gcd(a, n) = 1$ if and only if $a$ has a multiplicative inverse $b$ for $a \pmod{n}$, i.e. $\exists b \text{ s.t. } \quad ab \equiv 1 \pmod{n}$

$$\gcd(a, n) = 1 \iff \exists b, s \in \mathbb{Z} \text{ s.t. } \quad ab + ns = 0 \pmod{n}$$

$$\equiv ab \pmod{n}$$
Corollary 1: \( \mathbb{Z}_n \) is a group under addition.

- A symmetry of a geometric figure is a rearrangement of the figure which preserves the shape.

- A map from the plane to itself preserving the shape of an object is called a rigid motion.

Recall: a permutation of a set \( S \) is a 1-1 and onto map \( \pi : S \to S \).

- 3 vertices, this is our set \( S \)

\[ 3! = 6 \] permutation \( S \)

Think about composition of maps (which is associative)

\[ \begin{align*}
M_1 \circ \rho_1 & \quad M_1(\rho_1(A)) = M_1(B) = C \\
M_1A_1 & = \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix} = M_2 \\
\rho_1 \cdot M_1 & = \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix} = M_3 = M_1A_1
\end{align*} \]
Formal Definition of a Group

A binary operation on a set $G$ is a function $A \times G \rightarrow G$ that assigns to each pair $(a, b) \in A \times G$ a unique element $a \cdot b$ or $ab$ or $a \circ b$ or $a+b$.

A group $(G, \cdot)$ is a set $G$ with a (closed) binary operation $(a, b) \mapsto a \cdot b$ that satisfies the following axioms:

- The binary op. is associative, i.e.
  \[(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall a, b, c \in G\]

- There exists an element $e \in G$ called the identity element $s.t. b \cdot e = a \cdot e = a$

- For each element $a \in G$ there exists an inverse element in $G$, $a^{-1}$, s.t.
  \[a \cdot a^{-1} = a^{-1} \cdot a = e\]
Note that $a \cdot b \neq b \cdot a$ in general.

A group $G$ s.t. $a \cdot b = b \cdot a \ \forall a, b \in G$ is called an abelian or a commutative group.

Ex) $(\mathbb{Z}_n, \mathbb{1}^n)$ is a group

$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$

$\mathbb{Z}_n$ is not a group under mult.

$U(n) = \{ k \in \mathbb{Z}_n \mid \gcd(k, n) = 1 \}$ is a group

$U(8) = \{ 1, 3, 5, 7 \}$

<table>
<thead>
<tr>
<th>.</th>
<th>1 3 5 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1 3 5 7</td>
</tr>
<tr>
<td>3</td>
<td>3 1 7 5</td>
</tr>
<tr>
<td>5</td>
<td>5 7 1 3</td>
</tr>
<tr>
<td>7</td>
<td>7 5 3 1</td>
</tr>
</tbody>
</table>

Table 3.12: Multiplication table for $U(8)$
A matrix group

\[ GL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid \det(A) \neq 0 , a, b, c, d \in \mathbb{R}, a \neq 0 \right\} \]

The general linear group, operation is matrix multiplication

**Claim:** \( GL_2(\mathbb{R}) \) is a group

- The product of two invertible matrices is invertible since \( \det(AB) = \det(A) \cdot \det(B) \)
  
  or \( (AB)^{-1} = B^{-1}A^{-1} \)

- Matrix multiplication is associative \( \forall A, B, C \in GL_2(\mathbb{R}) \):
  \( (AB)C = A(BC) \)

- Identity is in \( GL_2(\mathbb{R}) \):
  \[ I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \]
  \[ JA = AJ = A \]

- Inverse exists \( \forall A \in GL_2(\mathbb{R}) \):
  \[ \left( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right)^{-1} = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \]

\[ \therefore GL_2(\mathbb{R}) \text{ is a group} \]

- Note \( GL_2(\mathbb{R}) \) is **not** abelian.

**Ex:** Let \[ I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad K = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \]

where \( i^2 = -1 \)
Then
\[ \mathcal{Q}_{6} = \{ 1, \pm 1, \pm J, \pm K \} \]
is a group.

To check see
\[ I^2 = J^2 = K^2 = -1, \ IJ = K, \ JK = I, \ KI = J \]
\[ JI = -K, \ KJ = -I, \ IK = -J. \]

\[ \therefore \ I^{-1} = -I \]
\[ J^{-1} = -J \]
\[ K^{-1} = -K \]

Basic properties of Groups

- Groups can be finite or infinite.

Let \( G \) be a group, write \( |G| = n \) of elements in \( G \), or the order of \( G \)

\[ |\mathbb{Z}_5| = 5 \quad , \quad |\mathbb{Z}| = \infty \]

**Proposition**
The identity element \( e \) of a group \( G \) is unique.

**Proof:** Suppose that \( e, \hat{e} \) are identities of \( G \).

\[ \Rightarrow \ eg = ge = g = \hat{e}g = \hat{g} \hat{e} \quad \forall g \in G \]

\[ \therefore \ eg = \hat{e}g \quad , \quad \text{mult. by } g^{-1} \]
Prop: If \( G \) is a group, \( g \in G \), then \( g^{-1} \) is unique.

Proof: Suppose \( \tilde{g}, g'' \) are both inverses of \( g \)

\[
g \cdot g'' = g'' \cdot g = e = g \cdot \tilde{g} = \tilde{g} \cdot g
\]

\[
g \cdot g'' = g \tilde{g}
\]

\[
g^{-1} g \cdot g'' = g^{-1} g \tilde{g}
\]

\[
e g'' = e \tilde{g}
\]

\[
g'' = \tilde{g} \quad \Box
\]

Prop: \( G \) is a group, \( a, b \in G \). Then \( (ab)^{-1} = b^{-1} a^{-1} \)