Preamble

Remark: Math is a language. We write math just like we write English, with full sentences and correct grammer.

Board Work - Not always full sentences. Attempt to communicate ideas.
Homework - Always write in full sentences. Trying to learn how to write proofs.

Math writing must be precise in order to say exactly what one means.
There is a lot of notation to clearly and succintly express what is being said.

Notation

Logic

- $P \Rightarrow Q$ means P implies Q. = if P is true then Q is true.
- $P \Leftrightarrow Q$ means P is true if and only if (iff) Q is true
- $\forall$ - for all
- $\exists$ - there exists, $\exists!$ - there exists a unique

Sets: A set is a collection of objects

S, T - two sets

1. $x \in S$ = x is an element/member of S
   $x \notin S$ = x is not an element/member of S

2. $|S|$ = cardinality of S. If S is finite, $|S|$ is the number of elements in S.

3. Curly bracket notation:

$S = \{$ Notation for elements of S $\mid$ or $:$ Property that defines being in S $\}$

$\mid$ or $:$ read as such that

$S = \{$ list of elements of $S \}$

Examples:

(i) $S = \{x \in \mathbb{Z} : 2$ divides $x\}$, S is the set of even integers.

(ii) $S = \{1, 2, 3\}$

4. $S \subseteq T$ = S is a subset of T
means if $x \in S$, then $x \in T$

(*) If $S \subseteq T$ and $T \subseteq S$, then $S = T$.

5. If $S \subseteq T$, then $T \setminus S$ = complement of S in T

$$T \setminus S = \{t \in T : t \notin S\}$$

6. $S \cap T$ = intersection of S and T

$$S \cap T = \{x : x \in S \text{ and } x \in T\}$$

7. $S \cup T$ = union of S and T

$$S \cup T = \{x : x \in S \text{ or } x \in T\}$$

8. $S \times T$ = cartesian product of S and T

$$S \times T = \{(s,t) : s \in S, t \in T\}$$

9. ϕ = empty set
S and T are <u>disjoint</u> iff $S \cap T = \phi$

Def: Let S and T be sets. A function (or map) from S to T is a "rule", f, which associates to each $x \in S$ a single element $f(x) \in T$.

Notation:

$$f: S \longrightarrow T$$
$$x \longmapsto f(x)$$

Examples

(i) $S = T = \mathbb{R}$

$f(x) = e^x, \sin(x), \cos(x), x^2+4$

single variable calculus = study of certain classes of functions $f: \mathbb{R} \to \mathbb{R}$

i.e. continuous/differentiable/integrable

(ii) $A \in M_{m\times n}(\mathbb{R})$ = $m\times n$ matrices with real coefficients

get a map $\phi_A : \mathbb{R}^n \longrightarrow \mathbb{R}^m$

$$\underset{\text{vector}}{v} \longmapsto \underset{\text{matrix multiplication}}{Av}$$

$M_{m\times n}(\mathbb{R})$ = set of linear maps from $\mathbb{R}^n$ to $\mathbb{R}^m$

Linear Algebra = study of linear maps between vectorspaces

(iii) Addition and multiplication can be thought of as functions:

$$+ : \mathbb{Z}\times\mathbb{Z} \longrightarrow \mathbb{Z} \qquad \cdot : \mathbb{Z}\times\mathbb{Z} \longrightarrow \mathbb{Z}$$
$$(a,b) \longmapsto a+b \qquad (a,b) \longmapsto a\cdot b$$

Definitions and properties of functions:

1. $f: S \to T$ is a function from S to T.

   S - called the domain

   T - called the codomain

2. $\mathrm{Im}(f) = \{t \in T : \exists s \in S \text{ with } f(s) = t\}$ - the image of f
   $\mathrm{im}(f)$

3. f is <u>surjective</u> (onto) if $\mathrm{im}(f) = T$ or equiv. if

   $\forall t \in T, \exists s \in S$ s.t. $f(s) = t$.

4. f is <u>injective</u> (1-1) if $\forall a, b \in S$, $f(a) = f(b)$ implies $a = b$.

5. f is <u>bijective</u> (1-1 correspondence) if f is injective and surjective.

<u>Examples</u>

(i) $S = \{1, 2, 3\}$, $T = \{a, b, c\}$

$$\left.\begin{aligned} f: S &\to T \\ 1 &\mapsto a \\ 2 &\mapsto b \\ 3 &\mapsto c \end{aligned}\right\} \text{bijection}$$

$$\left.\begin{aligned} f: S &\to T \\ 1 &\mapsto a \\ 2 &\mapsto a \\ 3 &\mapsto c \end{aligned}\right\} \begin{array}{l} \text{not a bijection} \\ \text{not surj: } b \notin \mathrm{im}(f) \\ \text{not inj: } f(1) = f(2) \text{ and} \\ \qquad 1 \neq 2 \end{array}$$

(ii) $S = T = \mathbb{R}$

$f: \mathbb{R} \to \mathbb{R}$
$f(x) = x^3$
bijection

$f: \mathbb{R} \to \mathbb{R}$
$f(x) = e^x$
injective, not surjective

$f: \mathbb{R} \to \mathbb{R}$
$f(x) = x^2$
not injective and not surjective

$f: \mathbb{R} \to \mathbb{R}$
$f(x) = x^3 - x$
surjective, not injective

6. For every set S, there is the identity function Id_S from S to S

$$Id_S : S \longrightarrow S$$
$$x \longmapsto x$$

7. Composition of functions

$$f : S \to T, \quad g : T \to V$$

$$g \circ f : S \to V$$
$$g \circ f(s) = g(f(s))$$

$$\begin{tikzcd} S \arrow[r, "f"] \arrow[rr, bend left, "g\circ f"] & T \arrow[r, "g"] & V \end{tikzcd}$$

<u>Fact/Exercise</u>: $f : S \to T$ is a bijection iff $\exists$ function $g : T \to S$ such that $g \circ f = Id_S$ <u>and</u> $f \circ g = Id_T$.
g is called the <u>inverse</u> of f.

<u>Equivalence Relations</u>

<u>Def</u>: Let S be a set. An <u>equivalence relation</u> on S is a subset $U \subseteq S \times S$ such that

(i) (reflexivity) $(x,x) \in U$ for all $x \in S$.
(ii) (symmetry) if $(x,y) \in U$, then $(y,x) \in U$.
(iii) (transitivity) if $(x,y), (y,z) \in U$, then $(x,z) \in U$.

<u>Notation</u>. The equivalence relation is sometimes denoted by $\sim$, meaning

$$(x,y) \in U \quad \text{iff} \quad x \sim y$$

$x \sim y$ is read x is equivalent to y.

Def: Let $\sim$ be an equivalence relation on a set S. Given $x \in S$, we define the <u>equivalence class containing x</u> to be the set

$$[x] = \{ y \in S : x \sim y \}$$

We denote the set of equivalence classes by $S/\sim$.

<u>Fact/Exercise:</u> Let $\sim$ be an equivalence relation on S.

(i) If $y \in [x]$, $[x] = [y]$.

(ii) If $y \notin [x]$, $[x] \cap [y] = \phi$.

<u>Remark:</u> Given an equivalence class $[x]$, if $y \in [x]$, we say that y is a representative for the equivalence class $[x]$.

<u>Example:</u> Modular Arithmetic

Fix a positive integer n.

$S = \mathbb{Z}$ and $U = \{ (a,b) \in \mathbb{Z} \times \mathbb{Z} : n \text{ divides } b-a \}$

<u>Exercise:</u> Show that U is an equivalence relation.

<u>Notation</u>

$a \equiv b \bmod n$ denotes $(a,b) \in U$

$\mathbb{Z}/n\mathbb{Z}$ denotes the set of equivalence classes mod n

$a + n\mathbb{Z}$ or $\bar{a}$ denotes the equivalence class represented by a, for $a \in \mathbb{Z}$

We have that the equivalence class $a+n\mathbb{Z}$ is the set

$$a+n\mathbb{Z} = \{a+kn : k \in \mathbb{Z}\}$$

That is, $a+n\mathbb{Z}$ is the set of all integers, which are a more than a multiple of n.

<u>Prop</u>: $|\mathbb{Z}/n\mathbb{Z}| = n$. That is, there are n equivalence classes mod n.

<u>proof</u>: We show

(1) Every $a \in \mathbb{Z}$ is equivalent to some $r \in \mathbb{Z}$ with $0 \le r \le n-1$.

(2) If $0 \le r, s \le n-1$, then $r \equiv s \mod n$ iff $r = s$.

Let $a \in \mathbb{Z}$. By division algorithm, $\exists q, r \in \mathbb{Z}$ ~~st~~ such that

$$a = qn + r \quad \text{and} \quad 0 \le r \le n-1$$

Then $qn = a - r$, so n divides $a - r$ meaning that $a \equiv r \mod n$.

Part (1) is done.

Now let $r, s \in \mathbb{Z}$ be s.t. $0 \le r, s \le n-1$. WLOG assume $r \le s$. We have

$$r \equiv s \mod n \quad \text{iff} \quad n \text{ divides } s - r$$

$0 \le r \le s \le n-1$ implies $0 \le s - r < n$, so

$$n \text{ divides } s - r \quad \text{iff} \quad s - r = 0$$

$$\text{iff} \quad r = s \qquad \square$$

The representatives $0, 1, 2, \dots, n-1$ for the n distinct equivalence classes mod n are called the <u>standard representatives</u> modulo n.

<u>Remark</u>: Addition and multiplication are defined on $\mathbb{Z}/n\mathbb{Z}$ by taking any representatives of equivalence classes and using addition and multiplication in $\mathbb{Z}$:

$$+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$$
$$(a+n\mathbb{Z},\ b+n\mathbb{Z}) \longmapsto (a+b)+n\mathbb{Z}$$

$$\cdot : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$$
$$(a+n\mathbb{Z},\ b+n\mathbb{Z}) \longmapsto a\cdot b+n\mathbb{Z}$$