0 Communicating Mathematics in this Course and Beyond

Set and Logical Notation

Set Notation

Definition 1.1. A **set** is a collection of objects, which are called the **elements** of the set.

$x \in D$	"x is an element of the set D" (a proposition about x and its *domain* D)
$P(x)$	A proposition about the variable x; may be true or false depending on x
$\{x \in D : P(x)\}$ $\{x \in D \mid P(x)\}$	The set of all elements of D for which $P(x)$ is true (a subset of D). Note that the "rule" for set membership may be given in many ways, not just an algebraic rule. For example, graphical, table, list, description.
$A \subseteq B$	"A is a subset of B" (a proposition about sets A and B)
$A \subsetneq B$	"A is a strict subset of B", i.e., "$A \subseteq B$ and $A \neq B$"
$A \supseteq B$	"A is a superset of B" or "B is a subset of A"
$A \supsetneq B$	"A is a strict superset of B" or "B is a strict subset of A", i.e., "$A \supseteq B$ and $A \neq B$"
$A \cap B$	The intersection of the sets A and B (a set)
$A \cup B$	The union of the sets A and B (a set)
$\varnothing$	The *empty set* (the set with no elements); also known as *null set*
$\lvert A \rvert$	The cardinality ("size") of A. When A is finite, $\lvert A \rvert$ is the number of elements in A.

Note. The notation for subset (without the bottom line) is ambiguous: some people use it to mean $A \subseteq B$ and others use it to mean $A \subsetneq B$. So we don't use it here.

Definition 1.2. Given sets A and B. We say A **is equal to** B if $A \subseteq B$ and $B \subseteq A$.
Notation: $A = B$.

Logical notation

$\neg P(x)$	The negation of $P(x)$
$\forall x, P(x)$	The proposition "For all values of x, $P(x)$ is true."
$\exists x : P(x)$	The proposition "There exists a value of x such that $P(x)$ is true."
$\forall x, P(x) \Rightarrow Q(x)$	The proposition "For all values of x, if $P(x)$ is true then $Q(x)$ is true."
$\forall x, P(x) \Leftrightarrow Q(x)$	The proposition "For all values of x, $P(x)$ is true if and only if $Q(x)$ is true."

Proof structures

To show that …	Requires showing that …
$x \in A$	x satisfies set membership rules for A
$x \notin A$	x does not satisfy at least one set membership rule of A
$A \subseteq B$	If $x \in A$, then $x \in B$
$A \subsetneq B$	(1) $A \subseteq B$ (2) there is an element of B that is not in A
$A = B$	(1) $A \subseteq B$ (2) $B \subseteq A$

Sets of numbers

$\mathbb{N}$	The set of *natural numbers* (nonnegative whole numbers – positive or zero)
$\mathbb{Z}$	The set of *integers* (all whole numbers – positive, negative, and zero)
$\mathbb{Q}$	The set of *rational numbers* (any number that can be expressed as a fraction with integer numerators and denominators, where the denominator is not zero)
$\mathbb{R}$	The set of *real numbers* (all numbers on the real line; equivalently, all decimal numbers)
$\mathbb{C}$	The set of *complex numbers* (all numbers of the form $a + bi$, where a and b are real)

Properties of $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$

Operations are well-defined

Well-defined: There is an answer, and there isn't more than one answer.

Operations $+, -, \times$ on $\mathbb{R}$ and $\mathbb{C}$ are well-defined: This means that when we add two numbers, we get exactly one answer (we don't expect there two be two answers to "What is $a + b$?" and we expect that there is an answer); similarly, when we subtract one number from another, or multiply two numbers, we get exactly one answer.

Division by nonzero numbers is well-defined. (There is no good numerical answer to "What is $a/0$?")

Arithmetic Properties of $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$

We state them below for $\mathbb{Z}$. They also hold for $\mathbb{R}$.

1	$a, b \in \mathbb{Z} \implies a + b \in \mathbb{Z}$	$\mathbb{Z}$ is closed under addition
2	$a, b, c \in \mathbb{Z} \implies a + (b + c) = (a + b) + c$	Addition in $\mathbb{Z}$ is associative
3	$a, b \in \mathbb{Z} \implies a + b = b + a$	Addition in $\mathbb{Z}$ is commutative
4	$a \in \mathbb{Z} \implies a + 0 = a = 0 + a$	0 is an additive identity in $\mathbb{Z}$
5	$\forall a \in \mathbb{Z}$, the equation $a + x = 0$ has a solution in $\mathbb{Z}$	Additive inverses exist in $\mathbb{Z}$
6	$a, b \in \mathbb{Z} \implies ab \in \mathbb{Z}$	$\mathbb{Z}$ is closed under multiplication
7	$a, b, c \in \mathbb{Z} \implies a(bc) = (ab)c$	Multiplication in $\mathbb{Z}$ is associative
8	$a, b, c \in \mathbb{Z} \implies a(b + c) = ab + ac$ and $(a + b)c = ac + bc$	Distributive property
9	$a, b \in \mathbb{Z} \implies ab = ba$	Multiplication in $\mathbb{Z}$ is commutative
10	$a \in \mathbb{Z} \implies a \cdot 1 = a = 1 \cdot a$	1 is a multiplicative identity in $\mathbb{Z}$
11	$a, b \in \mathbb{Z}, ab = 0 \implies a = 0$ or $b = 0$	$\mathbb{Z}$ has no zero divisors

Divides, Divisor, Factor

- Given $a, b \in \mathbb{Z}$, not both zero, we say *b divides a* if $a = bc$ for some integer c. Notation: $b \mid a$
  These all mean the same thing:
  - b divides a
  - b is a divisor of a
  - b is a factor of a
  - $b \mid a$

  If we want to say that b does not divide a, we write $b \nmid a$.
- A factor of a number is *trivial* if it is ± 1 or the $\pm$ number. A *nontrivial* factor that is not trivial.
- All nonzero natural numbers have a finite number of factors.
- Let $a, b, c \in \mathbb{Z}$. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Prime, Composite

- An integer p is *prime* if $p \neq 0, \pm 1$ if the only divisors of p are ± 1 and $\pm p$.
  An integer n is *composite* if $n \neq 0, \pm 1$, and it is not prime.
- Let $a \in \mathbb{Z}$. If p, q are primes such that $p \mid a$ and $q \mid a$, and $p \neq q$, then $pq \mid a$.

Even number

An integer n is even if it is divisible by 2.

Fundamental Theorem of Arithmetic

There is only one way to write any whole number as a product of positive primes (reordering doesn't count as a different way).

Sample handwritten proof

Let's use a proof about sets as an example. We begin with the typed up version and then show one way that this same proof might be handwritten.

Claim. If $A = \{3n : n \in \mathbb{Z}\}$ and $B = \{6n : n \in \mathbb{Z}\}$, then $B \subsetneq A$.

Proof. Given $A = \{3n : n \in \mathbb{Z}\}$ and $B = \{6n : n \in \mathbb{Z}\}$.

1. *Why $B \subseteq A$*: This means showing: if $x \in B$, then $x \in A$.
   Given $x \in B$. Then:

$$\begin{aligned} x &= 6k, k \in \mathbb{Z}, \text{ by definition of } B \\ &= 3 \cdot 2k \\ &= 3n, n \in \mathbb{Z}, \text{ because } 2 \in \mathbb{Z}, k \in \mathbb{Z}, \text{ and } \mathbb{Z} \text{ is closed under multiplication} \end{aligned}$$

   Therefore x satisfies set membership rules of A, implying $x \in A$.
   We have shown that if $x \in B$, then $x \in A$. Thus $B \subseteq A$, by definition of subset. $\boxed{1}$

2. *Why there is an element of A that is not in B.* We find an element of A that is not in B. If $x \in B$, then x is an even number because if $x = 6k$ for some $k \in \mathbb{Z}$, then x as $x = 2 \cdot (3k)$. Closure of multiplication in $\mathbb{Z}$ implies $3k \in \mathbb{Z}$, so x satisfies the definition of even number.
   However, some members of A are odd numbers: $3, 9, 15, \ldots$.
   Hence there are elements of A that are not in B. $\boxed{2}$

Why this means $B \subsetneq A$: (1) and (2) show that B and A satisfy the definition of strict subset, and we have $B \subsetneq A$. $\square$

<u>Claim</u>. $\left.\begin{matrix} A = \{3n : n \in \mathbb{Z}\} \\ B = \{6n : n \in \mathbb{Z}\} \end{matrix}\right] \Rightarrow B \subsetneq A.$

<u>Proof</u>. Given $A = \{3n : n \in \mathbb{Z}\}$
$B = \{6n : n \in \mathbb{Z}\}$.

1 $\boxed{B \subseteq A}$ We show: $x \in B \Rightarrow x \in A$.

Given $x \in B$.

$$\circledast \left[\begin{aligned} x &= 6k, \quad k \in \mathbb{Z} && \text{by defn of membership in } B \\ &= 3 \cdot 2k \\ &= 3n, \ n \in \mathbb{Z}. && \text{by closure of mult in } \mathbb{Z} \\ & && (2, k \in \mathbb{Z} \Rightarrow 2k \in \mathbb{Z}) \end{aligned}\right.$$

Hence x satisfies membership rules for A
$\Rightarrow x \in A$.
By defn of subset, $B \subseteq A$. $\boxed{1}$

2 $\boxed{\exists x \in A \text{ s.t. } x \notin B}$ We find an elt of A not in B. Observe that <u>all $x \in B$</u> are <u>even</u> (by defn of even):

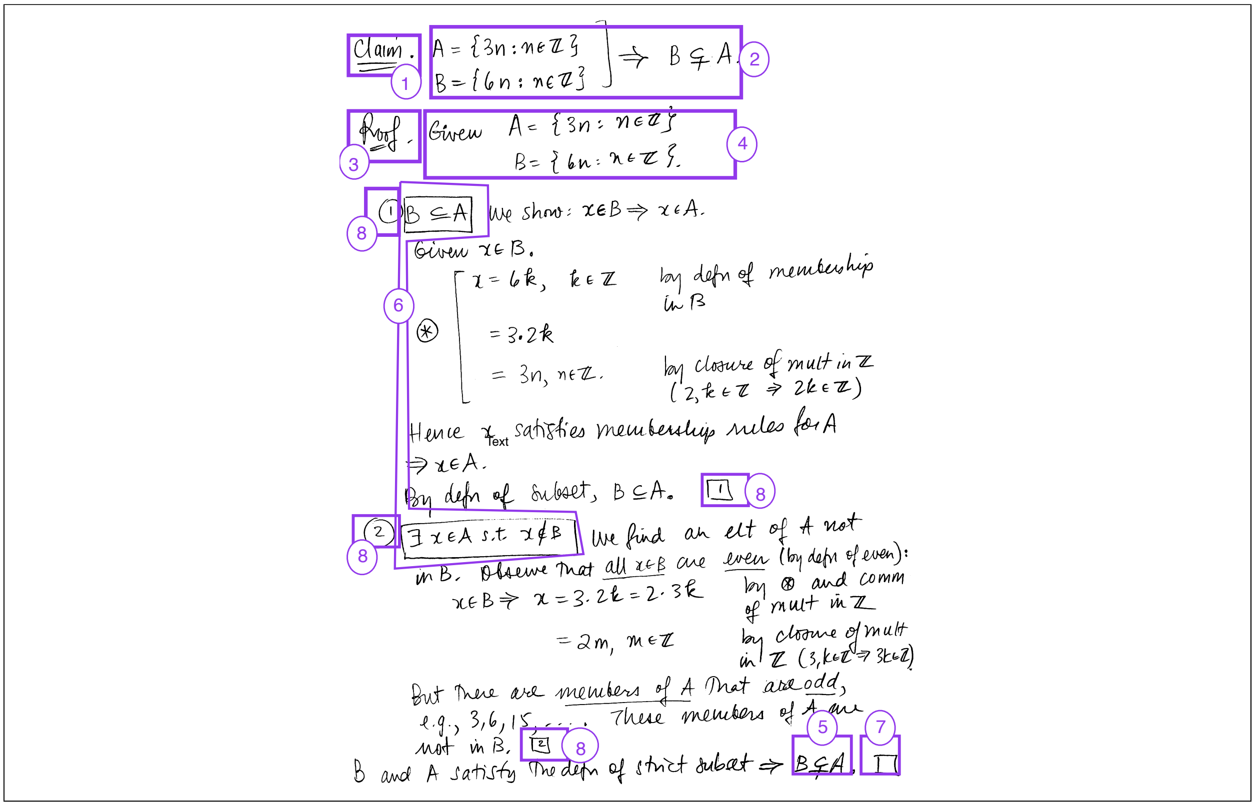
$$\begin{aligned} x \in B \Rightarrow x &= 3 \cdot 2k = 2 \cdot 3k && \text{by } \circledast \text{ and comm of mult in } \mathbb{Z} \\ &= 2m, \ m \in \mathbb{Z} && \text{by closure of mult in } \mathbb{Z} \ (3, k \in \mathbb{Z} \Rightarrow 3k \in \mathbb{Z}) \end{aligned}$$

But there are <u>members of A</u> that are <u>odd</u>, e.g., 3, 6, 15, ... These members of A are not in B. $\boxed{2}$

B and A satisfy the defn of strict subset $\Rightarrow B \subsetneq A$. $\square$

Good proof communication

Here is the same proof, with key features pointed out. These features are explained at the bottom. In general, you want to incorporate most if not all of these features into any proof you write. Even though it might seem strange at first, you may find eventually that you learn math better when you develop the habits of incorporating these features into your own writing and being aware of these features in proofs you encounter.



Features of communicating proof well:
(**Essential features in bold**)

1. **Label the claim.**
2. **State the claim precisely.**
3. **Label the proof beginning.**
4. Begin a proof by reminding yourself and readers of the starting point: the conditions of the claim.
5. **End the proof with where you need to go: the conclusions of the claim.**
6. Summarize your approach to the reader.
7. **Label the proof end.** A traditional way is to use a box.
8. **Write up parts within a proof properly. Label when they begin and end.**
   - Give them a name (e.g., Claim A) if it is a proof within a proof
   - **Use labels like [$\Rightarrow$] and [$\Leftarrow$] if doing an if and only if proof.**
9. Diagrams are good only if you explain what you are showing. Give a caption.