§ 1 Sets and Logic

Statement Calculus:

A statement is a sentence that is either true or false (truth value).

Example 1.1

(1) 2 is smaller than 3

(2) 4 is a prime number.

(3) $2^{n+1}-1$ is a prime number.

All of the above are statements, while (1) is true, (2) is false and whether (3) is true depends on the value of n (We denote the statement by $P(n)$, called statement function).

Definition 1.1

Let P, Q be two statements.

(1) The conjunction of P, Q, denoted by $P \wedge Q$ (read as "P and Q"), is defined as a statement which is true if both P, Q are true.

(2) The disjunction of P, Q, denoted by $P \vee Q$ (read as "P or Q"), is defined as a statement which is true if either P or Q is true, or both P and Q are true.

P	$\neg P$
T	F
F	T

Truth table of $\neg P$

P	Q	$P \wedge Q$	$P \vee Q$
T	T	T	T
T	F	F	T
F	T	F	T
F	F	F	F

Truth table of $P \wedge Q$, $P \vee Q$

(3) The negation of P, denoted by $\neg P$ (read as "not P"), is defined as a statement which has opposite truth value of P.

(4) The conditional statement, denote by $P \rightarrow Q$ (read as "if P then Q" or "P implies Q") is defined as a statement which is false only when P is true and Q is false.

P	Q	$P \to Q$
T	T	T
T	F	F
F	T	T
F	F	T

Truth table of $P \to Q$

How to understand ?

Example 1.2

Let P be the statement "John wins the Mark Six jackpot",

Q be the statement "John buys Mary a meal".

$P \to Q$ is the statement

"If John wins the Mark Six jackpot, then John buys Mary a meal".

Just like a promise, John breaks his promise only when he wins the Mark Six jackpot

(P is true) but he does not buy Mary a meal (Q is false)

Caution: When $P \to Q$ is true, it does mean P is true!

If we know the statement $P \to Q$ is always true, we say P implies Q

and denote it by $P \Rightarrow Q$

Example 1.3

Let P be the statement "ABCD is a rectangle",

Q be the statement "ABCD is a parallelogram".

P	Q	$P \to Q$
T	T	T
~~T~~	~~F~~	~~F~~
F	T	T
F	F	T

× This case never happens !

Truth table of $P \to Q$

$P \to Q$ is always true and we say ABCD is a rectangle implies ABCD is a parallelogram.

As we can see from the truth table of $P \to Q$, if we want to show $P \Rightarrow Q$, what we have to do is showing that when P is true, Q must be true!

Definition 1.2

Let P, Q be two statements.

The biconditional statement, $P \leftrightarrow Q$ (read as "P if and only if Q") is defined as $(P \to Q) \wedge (Q \to P)$

P	Q	$P \to Q$	$Q \to P$	$(P \to Q) \wedge (Q \to P)$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

Truth table of $P \leftrightarrow Q$

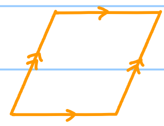
Example 1.4

Let P be the statement "ABCD is a rectangle",

Q be the statement "ABCD is a parallelogram"

P	Q	$P \leftrightarrow Q$
T	T	T
~~T~~	~~F~~	~~F~~
F	T	F
F	F	T

This case never happens!



$P \leftrightarrow Q$ is false when ABCD is a parallelogram but not a rectangle.

If we know the statement $P \leftrightarrow Q$ is always true, we say P is equivalent to Q and denote it by $P \Leftrightarrow Q$ or $P \equiv Q$.

From the truth table of $P \leftrightarrow Q$, we can see that it is true only when both $P \to Q$ and $Q \to P$ are true, i.e. $P \Rightarrow Q$ and $Q \Rightarrow P$.

In this case, we can see that P and Q always have the same truth value.

Example 1.5

In ΔABC,

Let P be the statement " $\angle A$ is a right angle",

Q be the statement " $AB^2 + AC^2 = BC^2$ ".

We have $P \Rightarrow Q$ (Pyth. Theorem) and $Q \Rightarrow P$ (Converse of Pyth. Theorem).

Therefore $P \Leftrightarrow Q$.

Remark:

There is a little bit difference between "English" and "Mathematics".

For example,

Theorem: In ΔABC, if $\angle A$ is a right angle, then $AB^2 + AC^2 = BC^2$.

should be understood as

"if $\angle A$ is a right angle, then $AB^2 + AC^2 = BC^2$ " is true.

When we know $P \Rightarrow Q$ and $Q \Rightarrow R$, $P \Rightarrow R$ (Hypothetical syllogism)

P	Q	R	$P \to Q$	$Q \to R$	$(P \to Q) \land (Q \to R)$	$P \to R$
T	T	T	T	T	T	T
~~T~~	~~T~~	~~F~~	~~T~~	~~F~~	~~F~~	~~F~~
~~T~~	~~F~~	~~T~~	~~F~~	~~T~~	~~F~~	~~T~~
~~T~~	~~F~~	~~F~~	~~F~~	~~T~~	~~F~~	~~F~~
F	T	T	T	T	T	T
~~F~~	~~T~~	~~F~~	~~T~~	~~F~~	~~F~~	~~T~~
F	F	T	T	T	T	T
F	F	F	T	T	T	T

In a proof, we usually write

$P_1 \Rightarrow P_2 \Rightarrow P_3 \Rightarrow \cdots \Rightarrow P_{k-1} \Rightarrow P_k$,

it actually means $P_1 \Rightarrow P_2$, $P_2 \Rightarrow P_3$, $\cdots$, $P_{k-1} \Rightarrow P_k$

Proposition 1.1

$P \to Q \equiv \neg P \vee Q$

proof :

P	Q	$\neg P$	$\neg P \vee Q$	$P \to Q$
T	T	F	T	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

always the same

Exercise 1.1

Let P, Q, R be three statements By constructing truth tables, show that :

(1) $\neg(\neg P) \equiv P$

(2) $P \wedge Q \equiv Q \wedge P$ (Commutative Law of Conjunction)

(3) $P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge R$ (Associative Law of Conjunction)

(4) $P \vee P \equiv P$ (Commutative Law of Conjunction)

(5) $P \vee Q \equiv Q \vee P$ (Associative Law of Conjunction idunction)

(6) $P \vee (Q \vee R) \equiv (P \vee Q) \vee R$ (Associative Law of Disjunction)

(7) $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$

(8) $P \wedge (Q \vee R) \equiv (P \vee Q) \wedge (P \vee R)$

(Distributive Laws)

(9) $\neg(P \wedge Q) \equiv (\neg P) \vee (\neg Q)$

(10) $\neg(P \vee Q) \equiv (\neg P) \wedge (\neg Q)$

(De Morgan's Laws)

(11) $P \to Q \equiv (\neg Q) \to (\neg P)$

(12) $P \leftrightarrow Q \equiv Q \leftrightarrow P$

(13) $P \leftrightarrow Q \equiv (\neg P) \leftrightarrow (\neg Q)$

Example 1.6

Recall $P \to Q \equiv \neg P \vee Q$, so

$$\begin{aligned} \neg(P \to Q) &\equiv \neg(\neg P \vee Q) \\ &\equiv \neg(\neg P) \wedge (\neg Q) \\ &\equiv P \wedge (\neg Q) \end{aligned}$$

Quantifier : specifies quantity of specimens.

Commonly used quantifiers : for all (denoted by $\forall$), there exists (denoted by $\exists$).

$\forall x, P(x)$ means "For all x, $P(x)$"

$\exists x, P(x)$ means "There exists x, $P(x)$".

Example 1.7

Let $P(x)$ be the statement "x studies math" where x is a student.

(1) $\forall x, P(x)$ means "For all students x, x studies math".

(2) $\exists x, P(x)$ means "There exists a student x such that x studies math".

(3) $\neg(\forall x, P(x))$ means "Not all students study math"

(4) $\neg(\exists x, P(x))$ means "There exists no student studying math".

(5) $\forall x, \neg P(x)$ means "For all students x, x does not study math"

(6) $\exists x, \neg P(x)$ means "There exists a student x such that x does not study math".

We can see that (3) $\equiv$ (5), (4) $\equiv$ (6).

Example 1.8

Let $P(x)$ be the statement "x studies math"

$Q(x)$ be the statement "x studies physics"

where x is a student

$\forall x, P(x) \to Q(x)$ means

"For all students x, if x studies math, then x studies physics".

Negation of the above :

$\neg(\forall x, P(x) \to Q(x)) \equiv \exists x, \neg(P(x) \to Q(x)) \equiv \exists x, P(x) \wedge (\neg Q(x))$ means

"There exists a student x such that x studies math and x does not study physics".

Naive Set Theory

A set is a well-defined collection of distinct objects (elements)

If x is an element of a set A, we denote it by $x \in A$

(read as "x belongs to A").

Definition 1.3

For two sets A, B, $A = B$ if and only if A contains every element of B and B contains every element of A

$(\forall x,\ x \in A \Leftrightarrow x \in B)$

Let A and B be sets. B is a subset of A (denoted by $B \subseteq A$) if and only if every element of B is an element of A.

$(\forall x,\ x \in B \Rightarrow x \in A)$

Example 1.9

$S = \{1, 2, 3\}$

That means S is a set containing 3 elements, namely 1, 2 and 3.

OR: $1, 2, 3 \in S$

If $T = \{1, 2, 3, 4\}$, then we say S is a subset of T, or $S \subseteq T$.

That means every element in S is also an element in T.

Notations often used:

$\mathbb{N}$: set of all natural numbers (nonnegative integers)

$\mathbb{Z}$ ($\mathbb{Z}^+$) : set of all (positive) integers

$\mathbb{Q}$: set of all rational numbers

$\mathbb{R}$: set of all real numbers

$\mathbb{C}$: set of all complex numbers

ϕ : empty set, i.e. $\phi = \{\ \}$ Nothing

$[a,b]$: set of all real numbers x such that $a \leq x \leq b$

(a,b) : set of all real numbers x such that $a < x < b$

$[a,\infty)$: set of all real numbers x such that $a \leq x$

Example 1.10

$\phi \subseteq A$ for any set A.

$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

Let $A = \{\{1\}, \{2\}, \{1,2\}\}$. A consists of 3 elements, but in fact each element is again a set

Proposition 1.2

Let A and B be sets. $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.

proof:

"$\Rightarrow$" Suppose $A = B$,

(Definition of $A = B$) $\forall x, x \in A \Rightarrow x \in B$ i.e. $A \subseteq B$

Similarly, $\forall x, x \in B \Rightarrow x \in A$ i.e. $B \subseteq A$

"$\Leftarrow$" Suppose $A \subseteq B$ and $B \subseteq A$

(Definition of $A \subseteq B$) $\forall x, x \in A \Rightarrow x \in B$

(Definition of $B \subseteq A$) $\forall x, x \in B \Rightarrow x \in A$

$\therefore \forall x, x \in A \Leftrightarrow x \in B$

Proposition 1.3

Show that

1) For every set A, $A \subseteq A$.

2) If $C \subseteq B$ and $B \subseteq A$, then $C \subseteq A$.

proof:

1) $\forall x, x \in A \Rightarrow x \in A$

$\therefore A \subseteq A$

2) $\forall x, x \in C \Rightarrow x \in B$ and $\forall x, x \in B \Rightarrow x \in A$

$\therefore \forall x, x \in C \Rightarrow x \in A$

Example 1.11

Set of all positive even integers

$= \{2, 4, 6, \dots\}$

$= \{2m : m \in \mathbb{Z}^+\}$

i.e this set consists of elements of the form $2m$ such that $m \in \mathbb{Z}^+$.

Set of all positive odd integers = ? (How to describe?)

Answer : $\{2m+1 : m \in \mathbb{N}\}$ or $\{2m-1 : m \in \mathbb{Z}^+\}$

In general, a set can be described as $\{x : P(x)\}$, so it consists of all x such that $P(x)$ is true.

$\{2m : m \in \mathbb{Z}^+\} = \{x : x = 2m \wedge m \in \mathbb{Z}^+\}$

Hence, ϕ can be described as $\{x : x \neq x\}$

Proposition 1.4

There is one and only one set which contains no element.

proof:

(Prove by contradiction)

Let A be a set which contains no element but $A \neq \phi$.

$(A = \phi \Leftrightarrow (\forall x, x \in A \Rightarrow x \in \phi) \wedge (\forall x, x \in \phi \Rightarrow x \in A))$

$$A \neq \phi \Leftrightarrow \neg\big((\forall x, x \in A \Rightarrow x \in \phi) \wedge (\forall x, x \in \phi \Rightarrow x \in A)\big)$$

$$\Leftrightarrow \big(\exists x, \neg(x \in A \Rightarrow x \in \phi)\big) \vee \big(\exists x, \neg(x \in \phi \Rightarrow x \in A)\big)$$

$$\Leftrightarrow (\exists x, x \in A \wedge x \notin \phi) \vee (\exists x, x \in A \wedge x \notin \phi)$$

Then there exists an element x in A but not in ϕ or there exists an element x in ϕ but not in A, which contradicts to the fact that both A and ϕ contain no element.

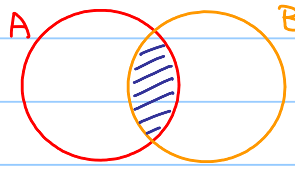
Exercise 1.2

Let A be a set. Show that $\phi \subseteq A$.

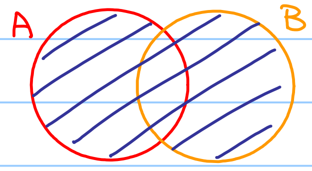
Definition 1.4

Let A and B be two sets.

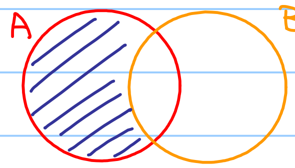
1) The intersection of A and B is the set $A \cap B = \{x : x \in A \land x \in B\}$
2) The union of A and B is the set $A \cup B = \{x : x \in A \lor x \in B\}$
3) The complement of B in A is the set $A \setminus B = \{x : x \in A \land x \notin B\}$ i.e. $\neg(x \in B)$



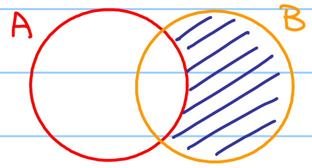
Intersection : $A \cap B$



Union : $A \cup B$



complement of B in A : $A \setminus B$



complement of A in B : $B \setminus A$

Venn diagrams

Example 1.12

Let $A = \{1,2\}$, $B = \{2,3\}$, $C = \{3\}$

- $A \cap B = \{2\}$ $\quad A \cap C = \phi$
- $A \cup B = A \cup C = \{1,2,3\}$

(Sometimes, we use $A \amalg C$ instead of $A \cup C$ to emphasize it is a disjoint union, i.e. $A \cap C = \phi$.)

- $A \setminus B = \{1\}$ $\quad B \setminus A = \{3\}$

Example 1.13

$\mathbb{R} \setminus \{2\}$: set of all real numbers except 2

(Caution : We cannot write $\mathbb{R} \setminus 2$ as 2 is not a set !)

Remark :

Let A , B be two sets. How to prove $A = B$?

Usually, two methods : (1) Showing $A \subseteq B$ and $B \subseteq A$.

(2) If $A = \{x : P(x)\}$, $B = \{x : Q(x)\}$, try to show $P(x) \equiv Q(x)$

Proposition 1.5

Let A, B, C be three sets.

1) $A \cap A = A$ $\quad (x \in A \Leftrightarrow (x \in A) \wedge (x \in A))$

2) $A \cap B = B \cap A$ $\quad ((x \in A) \wedge (x \in A) \Leftrightarrow (x \in B) \wedge (x \in A))$

3) $A \cap (B \cap C) = (A \cap B) \cap C$

4) $A \cap B \subseteq A$, $A \cap B \subseteq B$

5) $A \cap \phi = \phi$.

Proposition 1.6

Let A, B, C be three sets.

1) $A \cup A = A$

2) $A \cup B = B \cup A$

3) $A \cup (B \cup C) = (A \cup B) \cup C$

4) $A \subseteq A \cup B$, $B \subseteq A \cup B$

5) $A \cup \phi = A$.

Proposition 1.7

Let A, B be two sets.

1) $A \setminus A = \phi$

2) $A \setminus \phi = A$

3) $\phi \setminus A = \phi$

4) $B \setminus A = \phi$ if and only if $B \subseteq A$

5) $(A \setminus B) \cap (B \setminus A) = \phi$

6) $A \cap (B \setminus A) = \phi$

$A \times B$: Product of two sets A and B defined by $\{(a,b) : a \in A \text{ and } b \in B\}$

Example 1.14

- Let $A = \{1,2,3\}$, $B = \{4,5\}$.

  $A \times B = \{(1,4), (1,5), (2,4), (2,5), (3,4), (3,5)\}$

  $B \times A = \{(4,1), (4,2), (4,3), (5,1), (5,2), (5,3)\}$

- $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2 = \{(x,y) \; x, y \in \mathbb{R}\}$ = set of points on a plane

Examples :

Example 1.15

Let m be an integer.

Prove that if m is divisible by 4, then m is divisible by 2.

(Let P be the statement "m is divisible by 4"

Q be the statement "m is divisible by 2"

Actually, it means showing that $P \to Q$ is true, i.e. $P \Rightarrow Q$.

As we can see from the truth table of $P \to Q$, if we want to show $P \Rightarrow Q$, what we have to do is showing that when P is true, Q must be true!)

Let m be an integer divisible by 4,

i.e. $m = 4M$ where M is an integer. ← (Definition of divisibility ?)

$$m = 4M$$
$$= 2(2M)$$

Since $2M$ is an integer, m is divisible by 2.

(Think deeper : Definition of $\mathbb{Z}$, multiplication ?)

Example 1.16 (Prove by contradiction)

Prove that $\sqrt{2}$ is irration.

(Let P be the statement "$\sqrt{2}$ is irration".

Instead of showing P is true (i.e. $P \equiv T$), we are going to show $\neg P$ is false (i.e. $\neg P \equiv F$). Then $P \equiv \neg(\neg P) \equiv \neg(F) \equiv T$! It is called proving by contradiction.

How do we prove $\neg P$ is false ? We try to show $\neg P \Rightarrow Q$ where $Q \equiv F$

i.e. $\neg P$ leads something wrong !)

$\neg P$	Q	$\neg P \to Q$	
T	T	T	① Show $\neg P \Rightarrow Q$
~~T~~	~~F~~	~~F~~	i.e. show this case never happens.
F	T	T	② $Q \equiv F$, so $\neg P \equiv F$
F	F	T	

Assume $\sqrt{2}$ is rational, i.e. $\sqrt{2} = \frac{m}{n}$ for some positive integers m, n.
We can express $m = 2^k M$ and $n = 2^q N$ where k, q are nonnegative integers,
M, N are positive integers which are not divisible by 2.
Then $2n^2 = m^2$

$$2^{2q+1} N^2 = 2^{2k} M^2$$

Therefore, $2q+1 = 2k$ which is impossible. (Contradiction!)

Example 1.17 (Prove by contradiction)
Prove that there are infinitely many primes.
proof:
Assume there are finitely many primes.
Then we list out all primes $p_1, p_2, \cdots, p_n$, and let $N = p_1 p_2 \cdots p_n + 1$.
Since N is greater than all p_j and N is not divisible by all p_j,
N is a prime other than $p_1, p_2, \cdots, p_n$. (Contradiction)

Example 1.18 (Prove by contrapositive)
Prove that if x^2 is even then x is even.
(Let P be the statement "x^2 is even".
Q be the statement "x is even".
We are going to show $P \to Q$ is true. However, we know $P \to Q \equiv (\neg Q) \to (\neg P)$,
so we can show $(\neg Q) \to (\neg P)$ is true instead.)
Suppose that x is not even $(\neg Q)$,
then x is odd and $x = 2k+1$ for some integer k.

$$x^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$ where $2k^2 + 2k$ is an integer.

Therefore x^2 is odd, i.e. x^2 is not even.

Relation :

Definition 1.5

A relation R from a set A to a set B is a subset R of $A \times B$.

Also, we say that "a is related to b" if $(a,b) \in R$,

sometimes it can be denoted by aRb or $a \sim b$. We denote the relation by R or $\sim$.

In particular, if $A = B$, then R is said to be a relation defined on A.

Example 1.19

Let $A = \{2,3\}$, $B = \{3,4,5,6\}$.

Let R be a relation from A to B given by $R = \{(a,b) \in A \times B : b \text{ is divisible by } a\}$

Then $R = \{(2,4),(2,6),(3,3),(3,6)\}$

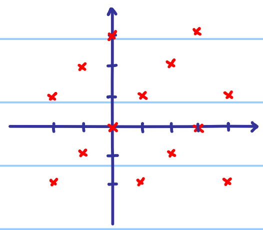
Remark : Given a relation R from a set A to a set B, R consists of pairs of (a,b) such that a and b are related in some sense.

However, let $R' = \{(2,3),(3,5)\} \subseteq A \times B$. The elements which are related may not have a particular meaning, but anyway R' is a relation from A to B.

Example 1.20

Let R be a relation defined on $\mathbb{Z}$ which is given by $(a,b) \in R$ if $b-a$ is divisible by 3.

Then the relation can be visualized as :



Example 1.21

Let "$|$" be a relation on $\mathbb{Z}^+$ such that $m,n \in \mathbb{Z}^+$ and $n|m$ if m is divisible by n.

Then 2 is related to 4 as 4 is divisible by 2, $(2,4) \in R \subseteq \mathbb{Z}^+ \times \mathbb{Z}^+$

but 4 is not related to 2 as 2 is not divisible by 4 $(4,2) \notin R \subseteq \mathbb{Z}^+ \times \mathbb{Z}^+$

Example 1.22

Let $M_n(\mathbb{R})$ be the set of all $(n \times n)$-matrices with real entities.

Define a relation $\sim$ on $M_n(\mathbb{R})$ by :

$A \sim B$ if there exists an invertible matrix P such that $A = PB$.

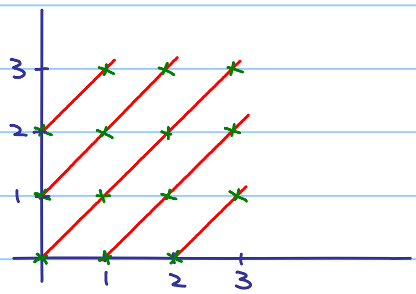
Then $I \sim B$ for all invertible matrices B as $I = (B^{-1})B$

Example 1.23

Define a relation $\sim$ on $\mathbb{N}^2 = \mathbb{N}\times\mathbb{N}$ (i.e. a subset of $\mathbb{N}^2\times\mathbb{N}^2$) by :

$(m,n)\sim(p,q)$ if $m+q=p+n$ (idea: $m-n=p-q$, but subtraction is not defined on $\mathbb{N}$)

Then, for example $(0,1)\sim(2,3)$ as $0+3=1+2$ (i.e. $((0,1),(2,3))\in R\subseteq \mathbb{N}^2\times\mathbb{N}^2$)



Lattice points on the same line $x-y=c$ are related.

Example 1.24

Define a relation R on $\mathbb{Z}\times\mathbb{Z}^*$ (i.e. $R\subseteq(\mathbb{Z}\times\mathbb{Z}^*)\times(\mathbb{Z}\times\mathbb{Z}^*)$) where $\mathbb{Z}^* = \mathbb{Z}\setminus\{0\}$, by

$(m,n)\sim(p,q)$ if $mq-np=0$.

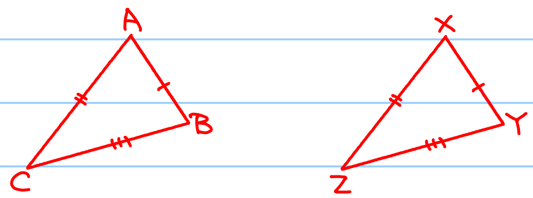
(Think: If we have two fractions $\frac{m}{n}$ and $\frac{p}{q}$ where $m,p\in\mathbb{Z}$ and $n,q\in\mathbb{Z}^*$,

they can be regarded as elements of $\mathbb{Z}\times\mathbb{Z}^*$

Also, they are the "same" if and only if $mq-np=0$.)

For example, if $x,y\in\mathbb{R}$, when we say "x equals to y ($x=y$)", what does it mean ?

(1) Meaning of "equality". In $\mathbb{R}$, in our mind, $x=y$ means both x,y have the same value. However, think :



Do they equal ?

(a) Equal as subsets of $\mathbb{R}^2$?

(b) Differ by translations and rotations ?

(c) Differ by translations, rotations and a reflection ?

(2) What our understanding to "equality" is a relation which satisfies :

(a) Everything equals to itself.

(b) If x equals to y, then y equals to x

(c) If x equals to y and y equals to z, then x equals to z.

Definition 1.6

Let $\sim$ be a relation defined on a set A.

Then $\sim$ is said to be an equivalence relation on A if

1) (reflexive) $a\sim a$ for all $a\in A$

2) (symmetric) if $a\sim b$, then $b\sim a$

3) (transitive) if $a\sim b$ and $b\sim c$, then $a\sim c$.

(What we try to do is abstraction of "equality":

Suppose we have a set A. Rather than defining what "equality" mean, we try to describe how it should behave!)

Example 1.25 / Exercise 1.3

Relations defined in example 1.20, 1.22 - 1.24 are equivalence relation but not for those in example 1.19 and 1.21.

Show that the relation in example 1.24 is an equivalence relation.

1) If $(m,n)\in\mathbb{Z}\times\mathbb{Z}^*$, then $(m,n)\sim(m,n)$ since $mn-mn=0$

2) If $(m,n),(p,q)\in\mathbb{Z}\times\mathbb{Z}^*$ and $(m,n)\sim(p,q)$, then $mq-np=0$ which means $pn-qm=0$ as well.

$\therefore (p,q)\sim(m,n)$

3) If $(m,n),(p,q),(r,s)\in\mathbb{Z}\times\mathbb{Z}^*$, $(m,n)\sim(p,q)$ and $(p,q)\sim(r,s)$ then $mq-np=ps-qr=0$.

$$q(ms-nr) = msq - nps - nrq + nps$$
$$= s(mq-np)+n(ps-qr) = 0$$
$$q\neq 0 \Rightarrow ms-nr=0$$

$\therefore (m,n)\sim(r,s)$

Definition 1.7

Let $\sim$ be an equivalence relation on the set A.

$[a]=\{b\in A.\ a\sim b\}$ is called the equivalence class of a by $\sim$.

Any element of an equivalence class is called a representative.

$A/\sim = \{[a] : a\in A\}$ is called the quotient set of A by $\sim$.

Example 1.25

If $\sim$ is the equivalence relation on $\mathbb{Z}$ which is given by $a \sim b$ if $b-a$ is divisible by 3.

Note that $\cdots = [0] = [3] = [6] = \cdots$ $(= \{3m : m \in \mathbb{Z}\})$

$\cdots = [1] = [4] = [7] = \cdots$ $(= \{3m+1 : m \in \mathbb{Z}\})$

$\cdots = [2] = [5] = [8] = \cdots$ $(= \{3m+2 : m \in \mathbb{Z}\})$

$\mathbb{Z}/3\mathbb{Z} = \mathbb{Z}/\sim = \{[0], [1], [2]\}$

There are only three equivalence classes and also we can observe that $\mathbb{Z} = [0] \amalg [1] \amalg [2]$.

We can generalize the above as the following.

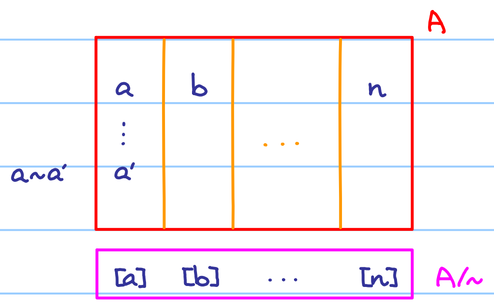
Proposition 1.8

Let $\sim$ be an equivalence relation on the set A. Then

1) $a \in [a]$ for all $a \in A$

2) $[a] = [a']$ if and only if $a \sim a'$

3) A equals to the disjoint union of equivalence classes.



proof:

1) Trivial, since $a \sim a$ for all $a \in A$

2) "$\Rightarrow$" Assume $[a] = [a']$

From 1, $a' \in [a'] = [a]$, so $a \sim a'$

"$\Leftarrow$" Assume $a \sim a'$.

Let $b \in [a']$. By definition $a' \sim b$.

$a \sim a'$ and $a' \sim b \Rightarrow a \sim b \Rightarrow b \in [a] \Rightarrow [a'] \subseteq [a]$

By similar argument, we can show that $[a] \subseteq [a']$.

$\therefore [a] = [a']$.

3) Since every equivalence class is a subset of A, so does the union of equivalence classes.

For all $a \in A$, by 1, $a \in [a]$, so a belongs to the union of equivalence classes

$\therefore$ union of equivalence classes $= A$ and what remains to show is the union is a disjoint union

It is equivalent to show if $c \in [a] \cap [b]$, then $[a] = [b]$.

$c \in [a] \cap [b] \Rightarrow a \sim c$ and $b \sim c$

$\Rightarrow a \sim b$ $(\because b \sim c \Rightarrow c \sim b)$

$\Rightarrow [a] = [b]$ (by 2)

Sometimes, we say that the equivalence classes form a partition of A.

Example 126

$\mathbb{Z}/3\mathbb{Z} = \mathbb{Z}/\sim = \{[0], [1], [2]\}$.

Question : Can we define addition on $\mathbb{Z}/3\mathbb{Z}$?

We know (assume) addition is defined on $\mathbb{Z}$, but how to make use of it ?

Try : $\underbrace{[a] \tilde{+} [b]}_{\text{addition to be defined}} := \underbrace{[a+b]}_{\text{addition on } \mathbb{Z}}$

$[1] \tilde{+} [1] = [1+1] = [2]$

$[2] \tilde{+} [1] = [2+1] = [3] = [0]$

but problem comes ! $[2] = [5]$, $[1] = [4]$, then $[2] \tilde{+} [1] = [5] \tilde{+} [4]$?

Fortunately, $[5] \tilde{+} [4] = [5+4] = [9] = [0]$

In general, if $[a] = [a']$, $[b] = [b']$, where $a, a', b, b' \in \mathbb{Z}$, $[a+b] = [a'+b']$?

$[a] = [a']$, $[b] = [b']$ means $a \sim a'$, $b \sim b'$, so

$a - a' = 3m$, $b - b' = 3n$ for some integers $m, n \in \mathbb{Z}$

then $(a+b) - (a'+b') = 3(m+n)$, so $[a+b] = [a'+b']$!

We say that addition $\tilde{+}$ on $\mathbb{Z}/3\mathbb{Z}$ is induced from addition $+$ on $\mathbb{Z}$.

(Usually, we simply write $+$ instead of $\tilde{+}$)

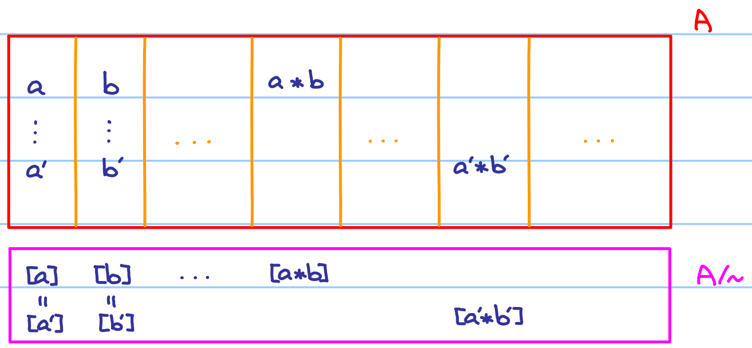
Suppose $\sim$ is an equivalence relation on A and $*$ is a binary operation on A.

Main question: Does $*$ induce a binary operation $\tilde{*}$ on $A/\sim$?

Naturally : We try to define $[a] \tilde{*} [b] = [a * b]$.

Trouble : It may happen that $a' \in [a]$, $b' \in [b]$ (i.e. $a \sim a'$ and $b \sim b'$)

but $[a' * b'] \neq [a * b]$ (i.e. $a * b \nsim a' * b'$).



What we require: If $a \sim a'$, $b \sim b'$, then $a * b \sim a' * b'$.

$*$ induces a binary operation $\tilde{*}$ on $A/\sim$ if the above condition holds.

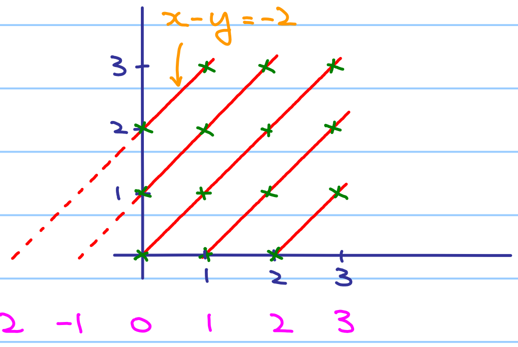
For simplicity, we denote the binary operation on $A/\sim$ by $*$ again.

Example 1.27

The relation $\sim$ on $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$ defined by $(m,n) \sim (p,q)$ if $m+q = p+n$ in example 1.23 is an equivalence relation. What is $\mathbb{N}^2/\sim$?

$\mathbb{N}^2/\sim \; = \{ \cdots, [(0,2)], [(0,1)], [(0,0)], [(1,0)], [(2,0)], \cdots \}$

denote $\quad -2 \quad -1 \quad 0 \quad 1 \quad 2$



$\mathbb{Z}$ can be defined as $\mathbb{N}^2/\sim$!

Addition on $\mathbb{N}^2$ is naturally defined.

$(m,n) + (p,q) = (m+p, n+q)$

Question: Does addition on $\mathbb{N}^2$ induce an addition on $\mathbb{N}^2/\sim$?

If $(m,n) \sim (m',n')$ and $(p,q) \sim (p',q')$, then $m+n' = m'+n$ and $p+q' = p'+q$

$\quad (m+p) + (n'+q') = (m'+p') + (n+q)$ and so

$(m+p) + (n+q) = (m+n, p+q) = (m'+n', p'+q') = (m'+p') + (n'+q')$

$\therefore$ We can define addition on $\mathbb{Z} = \mathbb{N}^2/\sim$

$-5 = [(0,5)]$, $3 = [(3,0)] \in \mathbb{Z} = \mathbb{N}^2/\sim$

$(-5)+(3) = [(0,5)] + [(3,0)] = [(0,5)+(3,0)] = [(3,5)] = [(0,2)] = -2$

$5 = [(5,0)]$, $3 = [(3,0)] \in \mathbb{Z} = \mathbb{N}^2/\sim$

$5+3 = [(5,0)] + [(3,0)] = [(5,0)+(3,0)] = [(8,0)] = 8$

Further: How to define subtraction on $\mathbb{Z}$?

Exercise 1.4

Define $\cdot$ on $\mathbb{N}^2$ as $(m,n)\cdot(p,q) = (mp+nq, np+mq)$

(Idea: (m,n) is actually representing $m-n$ in $\mathbb{Z}$,

$\quad (m-n)\cdot(p-q) = (mp+nq) - (mq+np)$ which is represented by $(mp+nq, np+mq)$.)

Does $\cdot$ on $\mathbb{N}^2$ induce $\cdot$ on $\mathbb{N}^2/\sim$?

Example 1.28

Define a relation R on $\mathbb{Z}\times\mathbb{Z}^*$ as in example 1.24

addition defined on $\mathbb{Z}\times\mathbb{Z}^*$

Define a binary operation (addition $+$) on $\mathbb{Z}\times\mathbb{Z}^*$ by $(m,n)+(p,q)=(mq+np,nq)$.

ordinary addition on $\mathbb{Z}$

(Think: Regard (m,n) as $\frac{m}{n}$, $(m,n)+(p,q)$ is defined as $\frac{mq+np}{nq}$)

If $(m,n)\sim(m',n')$ and $(p,q)\sim(p',q')$, i.e $mn'-nm'=pq'-qp'=0$

$(m',n')+(p',q')=(m'q'+n'p',n'q')$.

Then $(mq+np)n'q'-nq(m'q'+n'p')=0 \Rightarrow (m,n)+(p,q)\sim(m',n')+(p',q')$

$\therefore$ We can define addition on $\mathbb{Q}=\mathbb{Z}\times\mathbb{Z}^*/\sim$

Usually, we say $\frac{1}{2},\frac{3}{4}\in\mathbb{Q}$. To be precise, it should be $[\frac{1}{2}],[\frac{3}{4}]\in\mathbb{Q}$

$[\frac{1}{2}]+[\frac{3}{4}]=[\frac{1}{2}+\frac{3}{4}]$ ($+$ is defined on $\mathbb{Q}$, $+$ is defined on $\mathbb{Z}\times\mathbb{Z}^*$)

$=[\frac{1\times4+3\times2}{2\times4}]=[\frac{10}{8}]=[\frac{5}{4}]$ ($\because \frac{10}{8}\sim\frac{5}{4}$)

However, we can freely take other representatives in $[\frac{1}{2}],[\frac{3}{4}]$, say $\frac{3}{6}\in[\frac{1}{2}]$ and $\frac{9}{12}\in[\frac{3}{4}]$ and

$[\frac{1}{2}]+[\frac{3}{4}]=[\frac{3}{6}+\frac{9}{12}]=[\frac{3\times12+9\times6}{6\times12}]=[\frac{90}{72}]=[\frac{5}{4}]$

Exercise 1.5

Define $\cdot$ on $\mathbb{Z}\times\mathbb{Z}^*$ as $(m,n)\cdot(p,q)=(mp,nq)$

Does $\cdot$ on $\mathbb{Z}\times\mathbb{Z}^*$ induce $\cdot$ on $(\mathbb{Z}\times\mathbb{Z}^*)/\sim$?

Further: How to define division on $\mathbb{Q}$?

Summary:

Assume we know the definition of $\mathbb{N}$,

we can define $\mathbb{Z}$ and then define $\mathbb{Q}$.

Also, assume we know the definition of addition and multiplication on $\mathbb{N}$,

we can define addition and multiplication on $\mathbb{Z}$ and then define on $\mathbb{Q}$.

Remark:

For more detail of $\mathbb{N}$, see ch.6 of [3].

Functions :

Definition 1.8

A function f from A to B is a relation from A to B (i.e. $f \subseteq A \times B$) such that

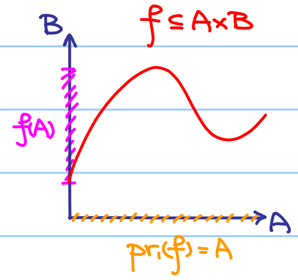
1) $pr_1(f) := \{a \in A : (a,b) \in f\} = A$

2) If $(a,b_1), (a,b_2) \in f$, then $b_1 = b_2$.

The sets A and B are said to be the domain and codomain of the function f respectively.

$(\text{range}(f) = f(A) =)\ pr_2(f) := \{b \in B : (a,b) \in f\}$ is said to be the range of f.

We denote it by $f : A \to B$ and we write $f(a) = b$ or $a \overset{f}{\mapsto} b$ if $(a,b) \in f$.



Remark : (1) guarantees that $f(a)$ is well-defined and

(2) guarantees that $a \in A$ is sent to

a unique element in B

Example 1.29

Addition of real numbers can also be regarded as a function $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ defined by $f(a,b) = a + b$.

In general, let S be a set, a function $f : S \times S \longrightarrow S$ is said to be a binary operation on S. Sometimes, we simply write $a * b$ to denote $f(a,b)$.

Definition 1.9

Let $f : A \to B$ be a function.

1) f is said to be an injective function if $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$

(Explanation : Once the output are the same, the inputs must be the same !)

2) f is said to be a surjective function if $\forall y \in B, \exists x \in A\ f(x) = y$ $(f(A) = B)$

If f is both injective and surjective, then it is said to be bijective.

Definition 1.10

Let $f : A \to B$ be a function. If $g : B \to A$ is a function such that

1) $g(f(x)) = x \quad \forall x \in A$

2) $f(g(y)) = y \quad \forall y \in B$

Then g is said to be an inverse of f.

Proposition 1.9

1) If an inverse of f exists, it is unique, so we denote it by f^{-1}.

2) f has an inverse if and only if f is bijective.

Example 1.30

$f: \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$ is neither injective nor surjective.

$f: [0,\infty) \to [0,\infty)$ defined by $f(x) = x^2$ is bijective.

Its inverse $f^{-1}: [0,\infty) \to [0,\infty)$ is denoted by $f^{-1}(x) = \sqrt{x}$.

Example 1.31

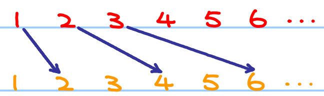
Let $A = \{1,2,3\}$, $B = \{a,b,c\}$ and let $f: A \to B$ defined by $f(1) = a$, $f(2) = b$, $f(3) = c$.

It can be check directly that f is bijective.

Remark: Naively, if $f: A \to B$ is a bijective function, then the "number" of elements in A and B are the same.

Example 1.32

Let $E = \{2n \in \mathbb{Z}^+ : n \in \mathbb{Z}^+\}$ and let $f: \mathbb{Z}^+ \to E$ defined by $f(n) = 2n$. Then f is bijective.



Remark: f is a bijective function mapping a set to its proper subset ($E \subseteq \mathbb{Z}^+$ but $E \neq \mathbb{Z}^+$)

Axiomatic Set Theory :

Third crisis (see three crises in mathematics) :

- (Naive) set theory was used in the discussion of the foundations of mathematics.
- According to naive set theory, if $P(x)$ is a statement,

  $\exists y \; \forall x \; (x \in y \Leftrightarrow P(x))$

  but Russell's paradox was proposed (Bertand Russell, 1901) :

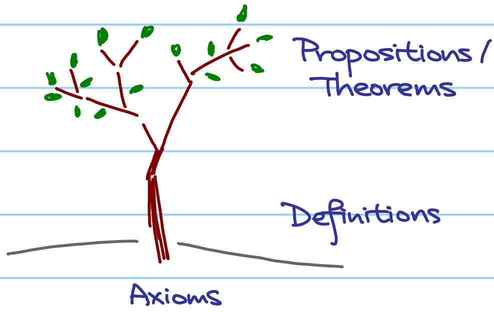
  Let $y = \{x : x \notin x\}$, then $y \in y \Leftrightarrow y \notin y$ (Contradiction!)

  $\rightsquigarrow$ Axiomatic set theory (20 th century)

Axiom : A statement that is taken to be true, to serve as a starting point for further reasoning.

Too few axioms : Cannot deduce much

Too many axioms : Cause redundancies or even contradictions



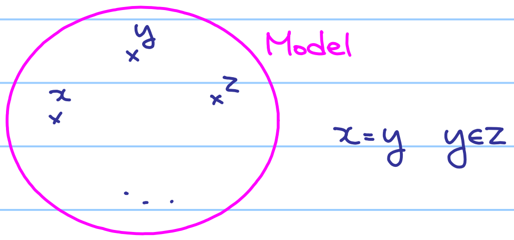
What we want to do :

1) Develop set theory in axiomatic approach

2) Different branches of mathematics are developed in terms of language of sets.

Idea of axiomatic set theory :

- NOT to ask what a set is, what the meaning of belonging / equality is. (Let them to be undefined objects!)
- For a model with something called sets, elements, concepts of belonging and equality, we describe how they behave (imposing axioms).
  As long as no contradicts / paradoxes occur, the model is a well-established theory.
- Different sets of axioms may lead to different set theories.



Zermelo-Fraenkel set theory is one of several axiomatic systems which were proposed in early 20th century to formulate a theory of sets free of paradoxes.

Zermelo-Fraenkel Set Theory:

1) (Axiom of existence)

There exists at least one set.

2) (Axiom of extension)

Two sets X and Y are equal if and only if X contains every element of Y and Y contains every element of X.

3) (Axiom schema of specification)

Given any set X and any statement $P(x)$ on elements x of X, there exists a set Y whose elements are exactly those elements in X for which $P(x)$ is true.

4) (Axiom of pairing)

If X and Y are sets, then there exists a set which contains X and Y.

5) (Axiom of union)

For any set of sets $\mathcal{F}$, there exists a set X containing every element which is in a member of $\mathcal{F}$

6) (Axiom of power set)

For any set X, there exists a set Y that contains every subset of X.

7) (Axiom of infinity)

There exists a set I such that I contains ϕ and for all x in I, $x \cup \{x\}$ is also in I.

8) (Axiom of substitution)

The image of the domain set X under a definable function falls inside a set Y.

9) (Axiom of regularity)

For any nonempty set X, there exists Y in X such that $X \cap Y$ is empty.

10) (Axiom of choice)

For any nonempty set X, there exists a choice function f defined on X.

The theory with axiom 1-9 is denoted by ZF.

ZF theory together with axiom of choice is denoted by ZFC.

Have a taste!

Question : Why does "empty set" exist ?

Proposition 1.10

There exists a set which contains no element.

proof:

By axiom 1, there exists a set A.

By axiom 3, $\{x \in A : x \neq x\}$ is a set as "$x \neq x$" is a statement for all x in A,

we denote it by ϕ.

(ϕ contains no element, otherwise there exists x in A such that $x \neq x$)

Question : Let A, B be sets. Why can we construct the intersection of A and B ?

By axiom 3, $\{x \in A : x \in B\}$ is a set and we denote it by $A \cap B$.

Similarly, $B \cap A = \{x \in B : x \in A\}$ is also a set, but $A \cap B = B \cap A$?

$\forall x,\ x \in A \cap B \Leftrightarrow x \in A \wedge x \in B \Leftrightarrow x \in B \wedge x \in A \Leftrightarrow x \in B \cap A$.

Therefore, $\{x \in A : x \in B\} = \{x \in B : x \in A\}$ and we denote it by $\{x : x \in A \wedge x \in B\}$.

Without the above, we do not know if $\{x : x \in A \wedge x \in B\}$ constitues a set!

Question : Does it exist an universal set, i.e. it contains everything ?

Proposition 1.11

There exists no universal set.

proof:

Suppose the contrary, V is a universal set.

By axiom 3, $\{x \in V : x \notin x\}$ is a set.

However, both cases $V \in \{x \in V : x \notin x\}$ and $V \notin \{x \in V : x \notin x\}$ lead contradiction!