37181: WEEK 3: EUCLIDEAN ALGORITHM, SET THEORY

A/Prof Murray Elder, UTS

Wednesday 7 August 2019

PLAN

- introduction to set theory notation
- Division and remainder lemma
- Euclidean algorithm
- power set

$\{\ .\ ,\ .\ ,\ .\ ,\ \}$

A *set* is a well-defined collection of objects. [1] The objects are called *elements* of the set, or *members* of the set.

We can represent a set using brackets, for example $A = \{1, 2, a, 5, c, 3\}$.

$\{\ x \mid \_\_\_\_\_\_$

The elements are the five symbols you see listed inside the brackets. We could also describe a set using variables satisfying some conditions, for example:

1 2 3 ~~4~~ 5

$$A = \{x \mid ((x \in \mathbb{N}) \wedge (1 \leqslant x \leqslant 5) \wedge (x \neq 4)) \vee (x = a) \vee (x = c)\}\,.$$

such that

The set $\{1, 5, 3, c, a, 1, 2\}$ is the same as the set A, since a set is defined only by the elements it contains, no matter how they are listed or displayed.

[1] Carefully defining what *well-defined* means will take us beyond the scope of this course, into axiomatic set theory and foundations of mathematics.

belongs to \in

The notation $x \in A$ means x *is an element of* A and $x \notin A$ means $\neg(x \in A)$.

Formally, if A, B are sets we define $A = B$ if

$$\neg\left(\forall x [x \in A \leftrightarrow x \in B] \right)$$

$p \to q$

$\neg p \vee q$

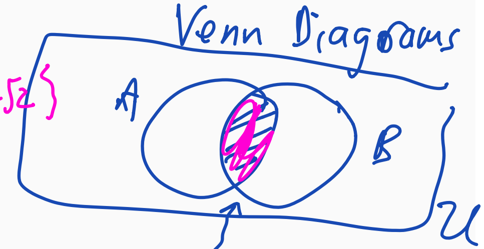
$(x \in A \to x \in B) \wedge$

$(x \in B \to x \in A)$

Eg:

- $A = \{x \mid x \in \mathbb{Q}, x < 0\}$
- $B = \{y \mid y \in \mathbb{R}, y^2 = 2\}$ $= \{\sqrt{2}, -\sqrt{2}\}$

Test: where does $-\sqrt{2}$ live?



Definition A, B sets.

- $A \cap B = \{x \mid x \in A \wedge x \in B\}$ (intersection)
- $A \cup B = \{x \mid x \in A \vee x \in B\}$ (union)

Note the similarity of notation for $\cap$ and $\wedge$, and $\cup$ and $\vee$.

In our Eg: $A \cap B = \emptyset$

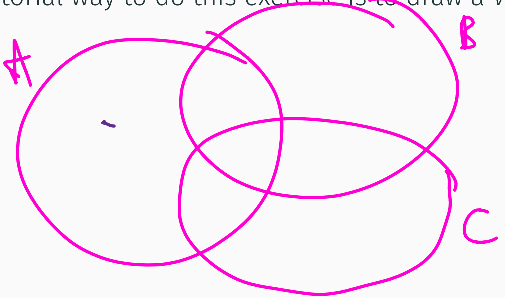
$\wedge$ $\cap$

Let $A = \{a, b, c, d, e\}$, $B = \{b, d, e\}$, $C = \{f, g, a\}$. Find

1. $(A \cup B) \cap (A \cup C)$ $= \{a\,b\,c\,d\,e\}$
2. $A \cap (B \cup C)$ $= \{a, b, d, e\}$

?

A pictorial way to do this exercise is to draw a *Venn diagram*.



$A \cap (B \cup C)$

$\{a, b$

If A, B are sets then $A \setminus B = \{x \mid x \in A \wedge x \notin B\}$.

Eg: $A = \{a, b, c, d, e\}, B = \{b, d, e\}, C = \{f, g, a\}$. Find

1. $A \setminus B$ $\{a, c\}$
2. $A \setminus C$

$\{\cancel{a} \quad \{b, c, d, e\}$

If A, B are sets we say A is a *subset* of B if $\forall x \in A, x \in B$, or $\forall x \, [(x \in A) \to (x \in B)]$. Notation $A \subseteq B$.

The notation $A \subsetneq B$ means *strictly contains*:

$$((x \in A) \to (x \in B)) \wedge (\exists y[y \in B \wedge y \notin A]).$$

-1 $\quad \frac{1}{2}$ $\quad 0.33333$

So $\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R}$.

$\sqrt{2}$

Let $\mathscr{U}$ be some large "universal" set, so we assume all sets we speak about are subsets of $\mathscr{U}$. Then $\overline{A} = \{x \mid x \notin A\} = \mathscr{U} \setminus A$ means the set of elements in $\mathscr{U}$ that are not in A.

$\overline{A}$

LOGIC VS. SET THEORY

complement

There is a strong connection to the logic we covered before. We have three operations on sets: $\cap, \cup, ^{-}$ which we can use to build new sets from old ones, and in logic we have three connectives $\wedge, \vee, \neg$.

Recall the tautologies in logic such as

$$\neg(p \wedge q) \leftrightarrow \neg p \vee \neg q$$

De Morgan

In set theory we could consider sets

$$\overline{A \cap B} \text{ and } \overline{A} \cup \overline{B}.$$

How do we show two sets are the same? We show they contain exactly the same elements.

Formally, if A, B are sets we define $A = B$ if

$$\forall x[x \in A \leftrightarrow x \in B]$$

$$\forall x((x \in A \to x \in B) \wedge (x \in B \to x \in A))$$

$\overline{A \cap B} \subseteq \bar{A} \cup \bar{B}$

Lemma

$\overline{A \cap B} = \bar{A} \cup \bar{B}$.

let $x \in \overline{A \cap B}$

The proof goes: pick some arbitrary element of the LHS.

Show it belongs to the RHS.

$\rightarrow x \in \bar{A}$ or $x \in \bar{B}$

Since we picked an arbitrary thing, this shows everything in the LHS is also in the RHS, so LHS⊆RHS.

$\rightarrow x \in \bar{A} \cup \bar{B}$

Repeat to get RHS⊆LHS, then LHS=RHS.

Lemma

$\overline{A \cap B} = \overline{A} \cup \overline{B}$.

Proof. Suppose $x \in \overline{A \cap B}$.

Then x is not in $A \cap B$.

Now either $x \in A$ or not. If $x \in A$ then since $x \notin A \cap B$ we must have x is not in B.

So either $x \in \overline{A}$ or $x \in \overline{B}$, so $x \in \overline{A} \cup \overline{B}$.

Thus

$$\overline{A \cap B} \subseteq \overline{A} \cup \overline{B}.$$

Next, start over and suppose $x \in \overline{A} \cup \overline{B}$.

$x \in \overline{A}$ or $x \in \overline{B}$

Suppose $x \in A \cap B$

$\rightarrow x \in A$, but since $x \in \overline{A}$ or $x \in \overline{B}$

$\rightarrow$ ~~aoo~~ $x \in \overline{B}$, but $x \in A \cap B$

$\rightarrow x \in B$

$\rightarrow$ contradiction.

therefore $x \notin A \cap B$.

Thus

$$\overline{A} \cup \overline{B} \subseteq \overline{A \cap B}.$$

Since each set is contained in the other, they are equal. $\square$

Prove or disprove,

~~Show~~ that for any sets $A, B, C \subseteq \mathscr{U}$

$$A \cap (B \cup C) \cancel{=} (A \cup B) \cap (A \cup C).$$

LHS $= \emptyset$

RHS $= \{1\}.$

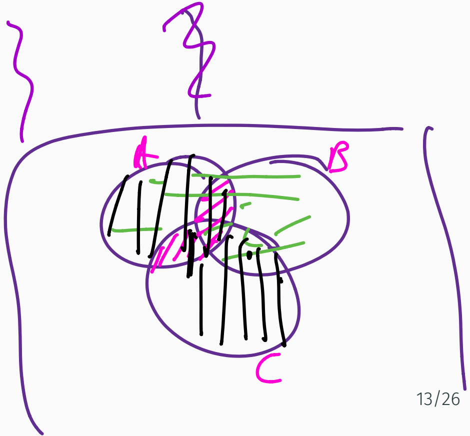
$\boxed{\text{False}}$

Let $\mathscr{U} = \{1,\}$

$A = \emptyset$

$B = \{1\}$

$C = \{1\}$



Note: a *Venn diagram* can be useful to check if a statement about sets looks correct, or to find a counterexample.

But **drawing a picture of a Venn diagram does not constitute a proof – you must do the LHS, RHS proof.**

Eg: check if you think $A \cup (B \cap C) = (A \cup B) \cap C$ is true or not.

PAUSE

RECALL

An element s in a subset $S \subseteq \mathbb{N}$ is called a *first element* in S if $s \leqslant x$ for every $x \in S$.

Eg: $\{5, 4, 6, 7\}$ has a first element, 4.

Lemma

First elements are unique. *(So we can say "the" first element).*

Axiom (Well ordering principle)

Every non-empty subset of $\mathbb{N}$ has a first element.

axiom = fact which does not follow from other facts.

$n=50$, $d=7$

$50 = 7 \cdot 7 + 1$

Lemma $n = 13$ $d = 7$

Let $n, d \in \mathbb{Z}$ with $d > 0$. Then there exist $q, r \in \mathbb{Z}$ with $0 \leqslant r < d$ such that $n = qd + r$.

$13 = 1 \cdot 7 + 6$

Proof: Define $M = \{n - qd \mid q \in \mathbb{Z}\}$. Then $M \cap \mathbb{N}$ is a subset of $\mathbb{N}$. $= \{0, 1, 2, \ldots$

It is non-empty because if $n \geqslant 0$ you can take $q = 0$ and if $n < 0$ take $q = 100n$ (which is a negative number, so $-qd$ is a big positive number).

$n - 100nd = n(1 - 100d)$

Therefore by the well ordering principle $M \cap \mathbb{N}$ has a first element, call it r.

$r = d$

Since $r \in M \cap \mathbb{N}$ we have $r \geqslant 0$ and $r = n - qd$ for some $q \in \mathbb{Z}$.

If $r \geqslant d$ (for contradiction) then $r - d \geqslant 0$ and $r - d = n - (q + 1)d$ so belongs to $M \cap \mathbb{N}$, and is smaller than r, contradicting our choice of r as first element. $\square$

APPLICATION OF DIVISION LEMMA

? 0

Definition

≥ 0

Let $a, b \in \mathbb{Z}$. Then $d \in \mathbb{N}$ is called the *greatest common divisor* of a and b if $d \mid a$, $d \mid b$, and if $c \mid a$, $c \mid b$ then $c \mid d$.

Eg: compute

- $\gcd(3, 9)$ $= \cancel{\pm} 3$, $\cancel{-3}$
- $\gcd(6, 8)$ $= \cancel{\pm} 2$

The following algorithm claims to compute gcd. It is called the *Euclidean algorithm*. We should not believe this claim, until we know how to prove algorithms are correct (lecture 6):
1. stops 2. gives the correct output

Euclid

$\gcd(187, 54)$

187
162
25

Input 54, 187.

Use the lemma to write $187 = q_1 \cdot 54 + r_1$.   3   25

Use the lemma to write $54 = q_2 \cdot r_1 + r_2$.   2   25   4

Repeat until you get $r_i = 0$.

$25 = 6 \cdot 4 + 1$

$4 = 4 \cdot 1 + 0$

$\gcd(m,n) = r_{i-1}$

YOUR TURN

7

166

7

Input 154, 287.

$0 \leq r < d$

Use the lemma to write $287 = q \cdot 154 + r$.

Repeat until you get $r = 0$.

$$287 = 1 \cdot 154 + 133$$

$$154 = 1 \cdot 133 + 21$$

$$133 = 6 \cdot 21 + 7$$

$$21 = 3 \cdot 7 + 0$$

Lemma

Let $n, d \in \mathbb{Z}$ with $d > 0$. Then there exist unique *integers q, r with $0 \leqslant r < d$ such that $n = qd + r$.*

Proof.

We already proved some q, r values exist. Suppose they are not unique.

Then we have q_1, q_2, r_1, r_2 and $n = q_1 d + r_1 = q_2 d + r_2$ so $r_1 - r_2 = d(q_2 - q_1)$.

This means d divides $r_1 - r_2$, but since they are both between 0 and $d - 1$ we must have $r_1 - r_2 = 0$, so $r_1 = r_2$ and then $q_1 - q_2 = 0$ so $q_1 = q_2$.

$\square$

BACK TO THE DEFINITION OF “SET”

The next exercise explains why *well-defined collection of objects* is not quite good enough.

Let $P(S)$ be the property (of sets) that S does not contain itself. For example, $P(\mathbb{N})$ is true because $\mathbb{N}$ contains numbers, it does not contain sets so it cannot contain itself.

Another example: the *empty set* $\emptyset$ is the set that has no elements, $\emptyset = \{\}$. So it contains nothing so cannot contain itself.

(a) Give some more examples.

BACK TO THE DEFINITION OF "SET"

Consider the set of all abstract concepts. Call it $\mathscr{A}$. Then A contains things like art, postmodernism, democracy, imaginary numbers.

(b) Which is true: $\mathscr{A} \in \mathscr{A}$ or $\mathscr{A} \notin \mathscr{A}$?

Let $\mathscr{S} = \{S \mid P(S)\}$ be the set of all sets that do not contain themselves.

So $\mathbb{N} \in \mathscr{S}$ and $\mathscr{A} \notin \mathscr{S}$.

(c) Which is true: $\mathscr{S} \in \mathscr{S}$ or $\mathscr{S} \notin \mathscr{S}$?

The moral of this story: you cannot define a set using a condition, in general. *i.e.* $\{x \mid P(x)\}$ may not actually be a well-defined collection of objects.

POWER SET

Let A be a set. Then (axiom)

$$\mathscr{P}(A) = \{B \mid B \subseteq A\}$$

is a set. Its called the *power set* of A.

Questions:

- is $\emptyset \in \mathscr{P}(A)$?
- is $A \in \mathscr{P}(A)$?
- is $\mathscr{P}(A) \in \mathscr{P}(A)$?

Another axiom: $\emptyset$ is a set.

What can you build with just these two axioms?

YOUR TURN

- Given $A = \{1, 2, 3\}$ is a set, what is $\mathscr{P}(A)$?
- Prove that if A is a set then $A \subsetneq \mathscr{P}(A)$

NEXT

Next lecture:

- induction
- correctness of computer code
- relations and functions