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.

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

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
$A = \{1, 2, a, 5, c, 3\}$.

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

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 $A = \{1, 2, a, 5, c, 3\}$.

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:

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

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

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 $A = \{1, 2, a, 5, c, 3\}$.

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:

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

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.

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

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

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

Eg:

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

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

Eg:

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

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

Definition

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

Eg:

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

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

Definition

- $A \cap B = \{x \mid x \in A \wedge x \in B\}$ (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 $\vee$.

Eg:

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

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

Definition

- $A \cap B = \{x \mid x \in A \wedge x \in B\}$ (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: $A \cap B =$

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

1. $(A \cup B) \cap (A \cup C)$
2. $A \cap (B \cup C)$

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

1. $(A \cup B) \cap (A \cup C)$
2. $A \cap (B \cup C)$

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

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. $A \setminus B$
2. $A \setminus C$

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

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

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

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

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

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

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

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

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

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

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

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

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.

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 $\wedge, \vee, \neg$.

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

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

In set theory we could consider sets

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

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

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

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.

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

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

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

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

DE MORGAN (SET VERSION)

Lemma

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

Lemma

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

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

DE MORGAN (SET VERSION)

Lemma

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

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

Show it belongs to the RHS.

Lemma

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

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

Show it belongs to the RHS.

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

Lemma

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

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

Show it belongs to the RHS.

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

Repeat to get RHS$\subseteq$LHS, then LHS$=$RHS.

Lemma

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

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

Lemma

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

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

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

DE MORGAN (SET VERSION)

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.

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 $x \in \overline{A} \cup \overline{B}$.

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 $x \in \overline{A} \cup \overline{B}$.

Thus

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

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

YOUR TURN

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

$$A \cap (B \cup C) = (A \cup B) \cap (A \cup C).$$

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.**

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.

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.

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).*

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.

Lemma

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

Proof:

Lemma

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

Proof: Define $M = \{n - qd \mid q \in \mathbb{Z}\}$.

Lemma

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

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

Lemma

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

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

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).

Lemma

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

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

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).

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

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

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. $\square$

Definition

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

- $\gcd(3, 9)$
- $\gcd(6, 8)$

Definition

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

- $\gcd(3, 9)$

- $\gcd(6, 8)$

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

Input $54, 187$.

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

Input $54, 187$.

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

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

Repeat until you get $r_i = 0$.

Input $154, 287$.

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

Repeat until you get $r = 0$.

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.

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.

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

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.

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.

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.

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.

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

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 $\mathscr{A} \notin \mathscr{A}$?

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.

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 $\mathscr{A} \notin \mathscr{S}$.

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 $\mathscr{S} \notin \mathscr{S}$?

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.

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 $\mathscr{P}(A) \in \mathscr{P}(A)$?

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.

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 $\mathscr{P}(A)$?

- 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