Ideas of mathematical proof

Slides Week 20

Sets, operations with sets. Cartesian products.

2. Sets, relations, mappings, cardinalities.

Sets and operations with sets

A set $A = \{\dots\}$ of some objects (elements).

E.g.:
$$\mathbb{N} = \{1, 2, 3, \dots\}$$
, or $B = \{1, 2, 3\}$, etc.

Order of elements is irrelevant: $\{1,2,3\} = \{3,2,1\}$.

Repeats irrelevant: $\{1, 2, 2, 3, 3, 3\} = \{1, 2, 3\}.$

A set defined by a condition: $\{x \mid P(x) \text{ is true}\}\$,

read: the set of all x such that P(x) is true.

The same: $\{x : P(x) \text{ is true}\}$

Notation: $a \in A$, read: a is an element of A, or a belongs to A.

$$-2 \notin \mathbb{N}$$
, $-2 \in \mathbb{Z}$, $\sqrt{2} \notin \mathbb{Q}$.

Subsets: $A \subseteq B$ if every element of A is also in B;

read: A is contained in B (as a subset).

 $a \in A$ does not mean $a \subseteq A$, but rather $\{a\} \subseteq A$.

E.g.: $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$.

Standard notation for intervals (subsets of \mathbb{R}):

 $[a, b] = \{x \in \mathbb{R} \mid a \le x \le b\}, \text{ closed interval,}$

note: $a \in [a, b]$ and $b \in [a, b]$;

 $(a, b) = \{x \in \mathbb{R} \mid a < x < b\}, \text{ open interval,}$

 $a \not\in (a, b)$ and $b \not\in (a, b)$;

 $(a, b] = \{x \in \mathbb{R} \mid a < x \le b\}$, a semi-open interval, etc.

E.g.: $2 \in [-3, 8], \pi \in [3.14, 3.15], [0, 8) \subseteq (-1, 10].$

Infinite intervals: $(-\infty, b] = \{x \in \mathbb{R} \mid x \le b\}$, $(a, \infty) = \{x \in \mathbb{R} \mid a < x\}$, etc.

Note: ∞ is not a number, just notation.

Example

$${x \in \mathbb{R} \mid x^2 - 3x + 2 \le 0} = [1, 2]$$
 (solution set).

Principle:

a set is completely determined by its elements:

Two sets A, B are equal, A = B

if and only if $A \subseteq B$ and $B \subseteq A$

In other words:

$$A = B$$
 means that $x \in A \Leftrightarrow x \in B$.

Many results in maths are like A = B.

To prove "=", one must check

both $A \subseteq B$ and $B \subseteq A$.

Example

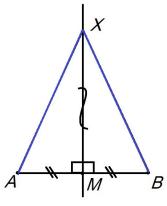
Given points A, B on the plane π ;

let
$$S = \{X \in \pi \mid AX = XB\}.$$

Then S = T, where T = the perpendicular bisector to AB.

Perpendicular bisector $\subseteq S$

Proof:



Hence AX = BX $T \subseteq S$ Let M be the midpoint of AB.

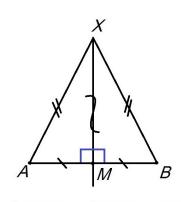
If $X \in T$, then in $\triangle XMA$ and $\triangle XMB$ we have AM = MB, $\angle XMA = 90^{\circ} = \angle XMB$, and XM is a common side; hence $\triangle XMA$ is congruent to $\triangle XMB$, and therefore XA = XB. (Or use Pythagoras.)

Thus, $X \in T \Rightarrow X \in S$.

But we only proved $T \subseteq S$.

Perpendicular bisector $\supseteq S$

Now prove reverse:



$$\angle AMX = \angle BMX = 90^{\circ}$$

$$S \subseteq T$$

if AX = XB, then in $\triangle XMA$ and $\triangle XMB$ we have AM = MB, AX = XB, and XM is a common side. Hence $\triangle XMA$ is congruent to $\triangle XMB$.

Then $\angle XMA = \angle XMB$, sum is 180° , so each is 90° .

Hence XM is perpendicular to AB, so $X \in T$.

That is, $X \in S \Rightarrow X \in T$, so we proved $S \subseteq T$. Together with $T \subseteq S$ means S = T. \square

Empty set

Definition

Ø is a unique **empty set**, with no elements.

Note $\varnothing \subseteq A$ for any set A.

Useful: $\{x \in \mathbb{Q} \mid x^2 = 2\} = \emptyset$.

Universal set

Definition

The **universal set** \mathscr{U} contains 'everything' (in a given context), so every set A in this context is $A \subseteq \mathscr{U}$.

Example: in geometry on the plane, $\mathscr U$ is this plane.

Instead of $\{x \mid P(x) \text{ is true}\}\$ we should better write $\{x \in \mathcal{U} \mid P(x) \text{ is true}\}\$; (but usually clear from the context, then \mathcal{U} is omitted).

Dangers of set theory: Russell paradox

```
Why not a universal set of really everything?
Because this is 'dangerous':
then so-called paradoxes arise (Russell paradox),
contradictions,
the whole of mathematics would collapse.....
```

Optional remark: Russell's paradox

(Why the 'super-universal' set of everything cannot be used.)

Russell's paradox

Consider the set S of all sets A such that $A \notin A$:

$$S = \{A \mid A \not\in A\}$$

Is $S \in S$?

If yes, then must have $S \not\in S$ by the definition of S.

If not, then must have $S \in S$ by the definition of S.

Contradiction! in each case.

Russell's paradox for a pub chat

The same **Russell's paradox** without sets:

call a phrase "self-describing"

if it applies to itself.

E.g.: "involves more than 5 letters" is self-describing.

Or: "non-monosyllabic" is self-describing.

Is "non-self-describing" self-describing or not?

If yes, then it is not; if not, then it is.

Contradiction!

Correct use of universal sets

To avoid such paradoxes, sets should be defined only by conditions like

$$S = \{x \in \mathcal{U} \mid P(x) \text{ is true}\},\$$

where \mathscr{U} is a universal set chosen beforehand.

(Often this $\mathscr U$ is assumed to be clear from context, like by $\{x\mid x^2>2\}$ we mean $\{x\in\mathbb R\mid x^2>2\}$, etc.)

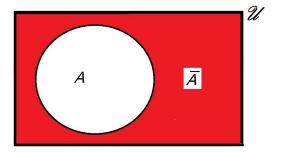
Operations on sets

Complement of a set A is $\overline{A} = \{x \in \mathcal{U} \mid x \notin A\}$ (sometime denoted by A^c , or A', etc.).

E.g.: if $\mathscr{U} = \mathbb{R}$ and $A = (-\infty, 7)$, then $\bar{A} = [7, \infty)$.

Euler-Venn diagrams

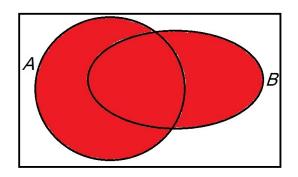
Euler–Venn diagrams show sets as shapes on the plane.



Here the rectangle represents the universal set, the oval a set A, and the difference is the complement \bar{A} .

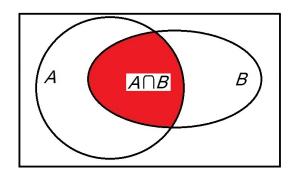
Union of two sets A and B is

 $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$ (here "or" includes "or both"):



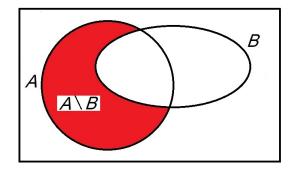
Intersection of two sets A and B is

$$A \cap B = \{x \mid x \in A \text{ and } x \in B\}$$
:



Difference of two sets A and B is

$$A \setminus B = \{x \mid x \in A \text{ and } x \notin B\}$$
:



For example, $\bar{A} = \mathscr{U} \setminus A$.

Use of set operations

Unions:

Example

$${x \mid x^2 - 3x + 2 > 0} = (-\infty, 1) \cup (2, \infty).$$

Example

$${x \mid (x+2)(x-|x|) = 0} = {-2} \cup [0,\infty).$$

Example

$$\{(x,y) \in \mathbb{R}^2 \mid |x| = |y|\}$$

 $= \{ \text{graph of } y = x \} \cup \{ \text{graph of } y = -x \}.$

Use of intersection

Use of intersection

For a system of $\underline{\text{simultaneous}}$ equations or inequalities, the solution set = the $\underline{\text{intersection}}$ of the solution sets of individual equations or inequalities in the system.

Solve the (simultaneous) system of inequalities

$$\begin{cases} x^2 \ge 4; \\ (x+3)(x-4) \le 0. \end{cases}$$

Solution of the first: $x \in (-\infty, -2] \cup [2, +\infty)$; of the second: $x \in [-3, 4]$.

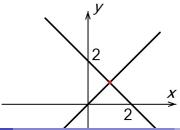
Simultaneously = the intersection (in red):

Answer: $x \in [-3, -2] \cup [2, 4]$.

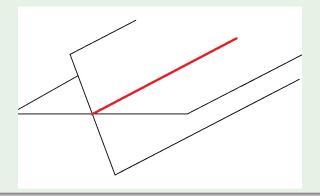
In two variables (on (x, y)-plane):

$$\begin{cases} x + y = 2 \\ x - y = 0. \end{cases}$$

Solution set of 1st eq'n: y = 2 - x, of the second: y = x. Simultaneously satisfy both eq'ns = intersection of the two: here (1,1), so solution is x = 1, y = 1.



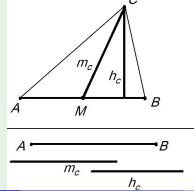
In three variables x, y, z, solution set of one linear equation is a plane in 3D. For a system of two linear equations, solution = intersection of two planes – in 'generic' case, a straight line.



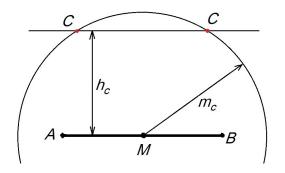
Geometric construction by intersection

Example

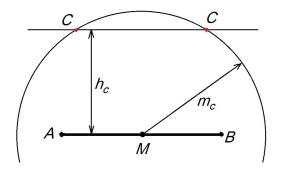
Construction with compass and straight edge of $\triangle ABC$ by the base AB, median m_c and height h_c means we are given these three segments and must reconstruct the triangle.



Fix the base AB; let M be the midpoint of AB.



Vertex C is at distance m_c from M. The set S of all such points is the circle with radius m_c centred at M. Also, vertex C is at distance h_c from the line AB. The set T of all such points is two parallel lines. (Both sets S and T can be easily constructed with compass and edge — assume these as known constructions.)



Idea: C must be <u>both</u> in S and in T, that is, in the intersection $S \cap T$.

Let
$$\mathscr{U} = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$$
,

$$A = \{x \in \mathcal{U} \mid x \text{ is a prime}\},\$$

$$B = \{x \in \mathcal{U} \mid x \text{ is even}\}.$$

Then
$$A \cap B = \{2\}$$
,

$$A \cup B = \{2, 3, 4, 5, 6, 7, 8\}$$
 (1 is not a prime),

$$\overline{A} \cup B = \{1, 2, 4, 6, 8, 9\}.$$

Distinguish: $a \neq \{a\}$

Remark: $a \neq \{a\}$; $a \in \{a\}$; $\{\emptyset\} \neq \emptyset$.

OPTIONAL REMARK: In foundations of mathematics, sets are used to build everything 'from scratch'. E.g., positive integers can be defined: $1 := \{\emptyset\}, \quad 2 := \{\emptyset, \{\emptyset\}\}, \text{ and so on, by induction, } n+1=n\cup\{n\}.$

Properties of operations on sets

Here, A,B,C are arbitrary sets.

(\cap 'kind of product'; \cup 'kind of sum').

Associativity:

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

Commutativity:

 $A \cup B = B \cup A$ and $A \cap B = B \cap A$.

Distributivity:

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

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

Properties of operations on sets cont'd

De Morgan Laws:

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

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

Universal set:

$$A \cup \mathscr{U} = \mathscr{U}$$
, $A \cap \mathscr{U} = A$, $A \cup \overline{A} = \mathscr{U}$.

Empty set:

$$A \cap \emptyset = \emptyset$$
, $A \cup \emptyset = A$, $A \cap \overline{A} = \emptyset$.

Complements:

$$\overline{\overline{A}} = A$$
, $\overline{\mathscr{U}} = \varnothing$, $\overline{\varnothing} = \mathscr{U}$.

Boolean algebra

(OPTIONAL) All subsets in \mathscr{U} form a so-called **Boolean algebra** under these operations and subject to these laws.

One can think of \cup as a kind of 'addition', and \cap as 'multiplication'. Then the laws for \varnothing are similar to the laws for 0 for the ordinary operations with numbers, and the laws for $\mathscr U$ are similar to the laws for 1 for the ordinary operations with numbers.

But there are of course differences: $A \cup A = A$, unlike addition of numbers!

Properties above must be proved:

either considering Venn diagrams, or 'from 1st principles', from definitions by logical reasoning.

Associativity and commutativity are obvious: $(A \cup B) \cup C$ consists of all elements in A, or in B, or in C (inclusive "or"), the same as $A \cup (B \cup C)$.

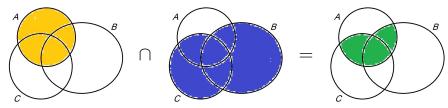
 $(A \cap B) \cap C$ consists of all elements that are simultaneously in A and in B and in C, the same as $A \cap (B \cap C)$.

Clearly, $A \cap B = B \cap A$ and $A \cup B = B \cup A$.

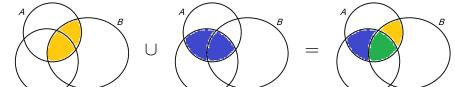
Prove by using Venn diagrams that

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

L.h.s.:



R.h.s.:



Prove 'from 1st principles', based on definitions that $A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$

Need both \subseteq and \supseteq .

" \subseteq ": $x \in I.h.s.$ means by def'n of union that $x \in A$ or $x \in B \cap C$.

If $x \in A$, then $x \in A \cup B$ by def. of union, and $x \in A \cup C$ for the same reason.

By def. of intersection $\Rightarrow x \in (A \cup B) \cap (A \cup C) =$ r.h.s., as required.

If $x \in B \cap C$, then by def. of intersection, $\Rightarrow x \in B$ and $x \in C$; $\Rightarrow x \in A \cup B$ and $x \in A \cup C$ by def. of union. By def. of intersection, then $x \in r.h.s.$, as req. s Week 20 (Sets, operations with sets. (Ideas of mathematical proof 36 / 61 Slides Week 20 (Sets, operations with sets. (

We have proved " \subseteq ".

Now we prove $A \cup (B \cap C) \supseteq (A \cup B) \cap (A \cup C)$.

 $x \in r.h.s.$ means by def. of intersection $x \in A \cup B$ and $x \in A \cup C$. If $x \in A$, then $x \in I.h.s.$ by def. of union.

Remaining case $x \notin A$. But then $x \in B$ and $x \in C$ by def. of union. Then $x \in B \cap C$ by def. of intersection, and then $x \in I$.h.s. by def. of union.

We have proved both \subseteq and \supseteq , so we have indeed proved this distributivity law:

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

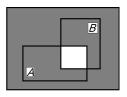
Example

 $\underline{\mathsf{Prove}}$ by $\underline{\mathsf{Venn}}$ diagram the de Morgan law

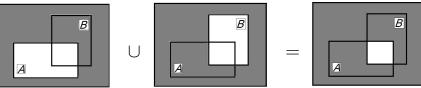
$$\overline{A \cap B} = \overline{A} \cup \overline{B}.$$

For clarity we draw the same sets separately.

(Set is question is shaded area) L.h.s.:



R.h.s.:



Results are the same for l.h.s. and r.h.s.

Other properties will be exercises: some by Venn diagrams, some by definitions and 'sheer reasoning'.

For example, $\varnothing \cap A = \varnothing$ for any set A. Indeed, nothing belongs to \varnothing , \Rightarrow nothing belongs to $\varnothing \cap A$ by def. of intersection.

Properties above can be applied to simplify more complicated constructions.

Example

Simplify $A \cap \overline{((\overline{B} \cup A) \cap B)}$.

By de Morgan law
$$= A \cap (\overline{(\overline{B} \cup A)} \cup \overline{B}) =$$

de Morgan $= A \cap ((\overline{\overline{B}} \cap \overline{A}) \cup \overline{B})$
 $= A \cap ((B \cap \overline{A}) \cup \overline{B}) =$
distributivity $= A \cap ((B \cup \overline{B}) \cap (\overline{A} \cup \overline{B}))$
 $= A \cap (\mathcal{U} \cap (\overline{A} \cup \overline{B})) =$
 $= A \cap (\overline{A} \cup \overline{B}) =$
distributivity $= (A \cap \overline{A}) \cup (A \cap \overline{B})$
 $= \emptyset \cup (A \cap \overline{B}) = A \cap \overline{B}.$

One more proved from definitions.

Example

For sets A and B, prove that $A \subseteq B \Leftrightarrow A \cap B = A$.

<u>"⇒":</u> Given $A \subseteq B$, must derive $A \cap B = A$.

As always, need \subseteq and \supseteq . First \subseteq : if $x \in A \cap B$, then by def. of intersection $x \in A$, as req.

Now \supseteq : if $x \in A$, then also $x \in B$ since $A \subseteq B$ by assumption. Then by def. of intersection $x \in A \cap B$, as req.

<u>" \Leftarrow ":</u> Given $A \cap B = A$, must derive $A \subseteq B$.

Let $x \in A$, but $A = A \cap B$ by assumption, so $x \in B$ by def. of intersection. Thus, $A \subseteq B$ as req.

Cardinality of a finite set

Notation. If A is a finite set, then |A| = the number of elements in A.

Often called the **cardinality** of A.

E.g.:
$$|\{a, b, c\}| = 3$$
, etc.

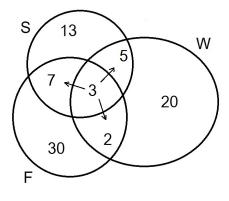
Venn diagrams used for counting

Example

Among 100 students, some study French, some Welsh, some Spanish (some two of these, some three, some none).

Given that
$$|S| = 28$$
, $|W| = 30$, $|F| = 42$, $|S \cap W| = 8$, $|S \cap F| = 10$, $|F \cap W| = 5$, $|S \cap W \cap F| = 3$,

how many do not study any of these languages? How many study only French?



$$|S| = 28,$$

 $|W| = 30,$
 $|F| = 42,$
 $|S \cap W| = 8,$
 $|S \cap F| = 10,$
 $|F \cap W| = 5,$
 $|S \cap W \cap F| = 3.$

Work from the 'centre': e.g., since $|S \cap W| = 8$ and $|S \cap W \cap F| = 3$, we get 8 - 3 = 5 in Welsh and Spanish but not French. ... We get total 80, so 20 students do not study any of these three languages. And it is 30 who study French but none of the other two.

Inclusion-exclusion formula

Theorem

Let A, B, C be any finite sets. Then

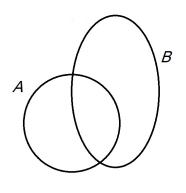
- (a) $|A \cup B| = |A| + |B| |A \cap B|$;
- (b) $|A \cup B \cup C| =$ $|A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|;$
- (c) (OPTIONAL) For any finite sets $A_1, ..., A_n$ the following "inclusion-exclusion formula" holds:

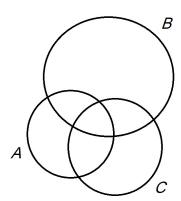
$$|A_1 \cup \cdots \cup A_n| = \sum_{\substack{\{i_1, ..., i_k\} \subseteq \{1, ..., n\} \ i_1 < \cdots < i_k}} (-1)^{k-1} |A_{i_1} \cap \cdots \cap A_{i_k}|.$$

Proof:

- (a) In the sum |A| + |B|, we count twice elements in $A \cap B$; therefore subtract $|A \cap B|$ to get the correct result: $|A \cup B| = |A| + |B| |A \cap B|$.
- (b) In the sum |A| + |B| + |C|, elements in $|A \cap B \cap C|$ are counted three times, and other elements in the pairwise intersections two times. Hence, when we subtract $\cdots - |A \cap B| - |A \cap C| - |B \cap C|$, we get correct count for the elements outside $A \cap B \cap C$. But elements in $A \cap B \cap C$ now have zero count: they were counted three times before, and now subtracted three times. Therefore adding $|A \cap B \cap C|$ restores the correct count for them.

Both parts (a) and (b) have clear illustration on Venn diagrams:





(c) (OPTIONAL) This formula can be proved by induction on n.

Power set

Definition.

For a set A, the **power set** $\mathcal{P}(A)$ is the set of all subsets of A (including \emptyset and A)

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

For example, if $A = \{a, b, c\}$, then

$$\mathscr{P}(A) =$$

$$\{\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\}.$$

Theorem

If A is a finite set with n = |A| elements, then $|\mathscr{P}(A)| = 2^n$.

Proof: Every element of A can be either included or not in a subset $B \subseteq A$, independently of each other – two independent choices, for each of n elements.

Therefore there are 2^n possibilities in total for forming a subset B.

(In particular, $B = \emptyset$ when none of the elements is included, and B = A when all are included.)

Cartesian products

Definition.

An ordered pair of two elements

is denoted by (a, b), where

a is the first element and b the second.

Note: this is <u>not</u> the set $\{a, b\}$.

$$(a,b)=(c,d)$$
 if and only if $a=c$ and $b=d$.

Thus, $(a, b) \neq (b, a)$ (unlike for sets $\{a, b\} = \{b, a\}$).

Optional remark: How to build pairs without informal "first" and "second", using sets only:

for example, $(a, b) := \{a, \{a, b\}\}.$

Definition

The **Cartesian product** of two sets A, B,

denoted $A \times B$,

is the set of all ordered pairs (a, b), $a \in A$, $b \in B$:

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

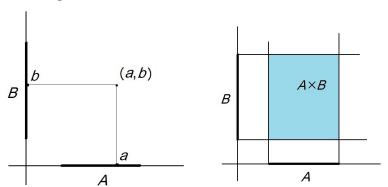
Example. Let $A = \{a, b, c\}$ and $B = \{1, 2\}$. Then $A \times B = \{(a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2)\}$.

Example. Well-known example is the Cartesian plane:

$$\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(a, b) \mid a, b \in \mathbb{R}\}.$$

Diagrams for Cartesian products

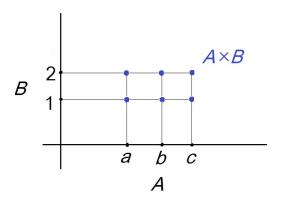
as illustrations drawn on the plane, depicting sets A and B as segments on 'coordinate axes', and the pairs (a,b) as points on the plane. Then $A \times B$ is visualised as the rectangle:



Traditionally: first elements placed on the horizontal axis.

For finite sets — only finitely many points.

Example: $A = \{a, b, c\}$, $B = \{1, 2\}$, Then $A \times B$:



Properties of Cartesian products

For any sets A, B, C, X, Y,

(1)
$$A \times B \neq B \times A$$
 (in general);

$$(2) A \times (B \cap C) = (A \times B) \cap (A \times C);$$

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

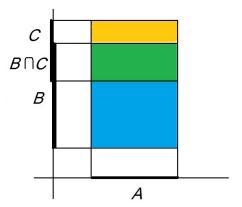
$$(4) (A \times B) \cap (X \times Y) = (A \cap X) \times (B \cap Y);$$

(5)
$$(A \times B) \cup (X \times Y) \subseteq (A \cup X) \times (B \cup Y)$$
, and usually $(A \times B) \cup (X \times Y) \neq (A \cup X) \times (B \cup Y)$.

These properties must be proved 'from 1st principles', based on definitions.

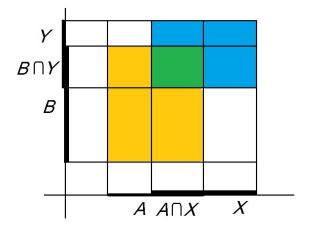
Diagrams can also illustrate the proofs.

E.g.: property (2):
$$A \times (B \cap C) = (A \times B) \cap (A \times C)$$
.



Yellow and green is $A \times C$, blue and green is $A \times B$, and green is $A \times (B \cap C)$. We see: l.h.s. \square

Property (4): $(A \times B) \cap (X \times Y) = (A \cap X) \times (B \cap Y)$:



Yellow and green is $A \times B$, blue and green is $X \times Y$, and green is $(A \times B) \cap (X \times Y)$ (I.h.s.)

- the same as $(A \cap X) \times (B \cap Y)$ (r.h.s.).

Proof from 1st principles:

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

$$\subseteq$$
: $(u, v) \in L.h.s.$ means

 $u \in A$ and $v \in B \cup C$, so $v \in B$ or $v \in C$, which means $(u, v) \in A \times B$ or $(u, v) \in A \times C$, resp.

By def. of union then $(u, v) \in R.h.s.$

$$\supseteq: (u, v) \in \mathsf{R.h.s.}$$
 means

$$(u, v) \in A \times B$$
 or $(u, v) \in A \times C$.

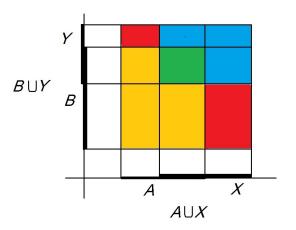
In either case, $u \in A$,

while $v \in B$ or $v \in C$, so $v \in B \cup C$ by def. of union.

So
$$(u, v) \in L.h.s.$$

By diagram:

$$(A \times B) \cup (X \times Y) \neq (A \cup X) \times (B \cup Y).$$



$$(A \times B) \cup (X \times Y) = \text{ yellow, blue and green.}$$

 $(A \cup X) \times (B \cup Y)$ is bigger, also includes red bits.

Theorem

If A and B are finite sets, then $|A \times B| = |A| \cdot |B|$.

Proof: For every of |A| elements $a \in A$,

there are |B| elements $b \in B$

to form a pair $(a, b) \in A \times B$.

Hence there are $|A| \cdot |B|$ choices for the pair (a, b).

Definition

An **ordered** *n***-tuple**

is denoted by (a_1, \ldots, a_n) , where

 a_1 is the first element, a_2 the second, ..., a_n the n-th element of the tuple.

E.g., ordered triples (a, b, c) for $a, b, c \in \mathbb{R}$ are coordinates of vectors in \mathbb{R}^3 .