Lecture 1.

Sets

For most mathematical purposes we can think of a set intuitively, as a collection of elements.

Examples. a) I is a set of all integers from 1 to 50

b) C is a set of all European countries.

c) P is a set of all prime numbers (2, 3, 13 belong to P, but 12, 81 are not primes).

Set Notation

If S is a set, the notation $x \in S$ means that x is an element of S

A set may be specified using the standard set-roster notation by writing all of its elements between braces:

$I = \{1, 2, \ldots, 49, 50\}$

$P = \{2, 3, 5, 7, \ldots\}$ → and so for.

Sets can be finite and infinite.

Important. For any set we should have a possibility to test if some element x belongs to S (the answer should be Yes or No)

The axiom of extension. A set is completely determined by what its elements are - not the order in which they are listed or the fact that some elements might be listed more than once.

Def. Two sets are equal if and only if (iff) they have the same elements.

Thus: $\{a, a\} = \{a\}$.

Ex 2. $\{0\} \neq \{0, \{0\}\}$

$\{0\}$ has one element, namely 0.

$\{0, \{0\}\}$ has two elements: 0 and the set whose only element is 0.

Some important sets:

$\mathbb{R}$ - the set of all real numbers

$\mathbb{Z}$ - the set of all integers

$\mathbb{Q}$ - the set of rational numbers, quotients of integers

$\mathbb{N}$ - the set of natural numbers (non-negative integers)

$$\mathbb{N} = \{ x \in \mathbb{Z} \mid x \geq 0 \}$$

$\emptyset = \{\}$ an empty set.

A new set can be defined as the set of all elements x in S such that the property $P(x)$ is true:

$$S_1 = \{ x \in S \mid P(x) \}$$

Logic

Barber paradox (Russell's paradox).

Let's define

The barber is the "one who shaves all those, and only those, who do not shave themselves".

The question: does the barber shaves himself?

The barber can't shave himself, as he only shaves those who don't shave themselves.

Compare:

$$\{ x \in \mathbb{Z} \mid -3 < x < 7 \}$$

and

$$\{ x \in \mathbb{R} \mid -3 < x < 7 \}.$$

Definition of Subsets.

If A and B are sets, then A is called a subset of B ($A \subseteq B$), if and only if, every element of A is also an element of B.

$A \not\subseteq B$ not to be a subset of a set B means that there is at least one element of A that is not an element of B.

A is a proper subset of B, iff every element of A is in B but there is at least one element of B that is not in A.

Cartesian Products

Given elements a and b, the symbol (a, b) denotes the ordered pair, consisting of a and b together with the specification that

a is the first element of the pair
b is the second element

$(a, b) = (c, d)$ iff $a = c$, $b = d$

Question. Is $(1, 2) = (2, 1)$?

Generalization for an ordered n-tuple

Let n be a positive integer and let $x_1, x_2, \cdots, x_n$ be (not necessarily distinct) elements.

The ordered n-tuple, $(x_1, x_2, \cdots, x_n)$ consist of $x_1, x_2, \cdots, x_n$ together with the ordering.

An ordered 2-tuple is called ordered pair
3-tuple is called an ordered triple.

$(x_1, \cdots, x_n) = (y_1, \cdots, y_n) \Leftrightarrow x_1 = y_1, x_2 = y_2, \cdots, x_n = y_n$.

Given sets $A_1, A_2, \cdots, A_n$ the Cartesian product of $A_1, A_2, \cdots, A_n$, denoted $A_1 \times A_2 \times \cdots \times A_n$ is the set of all ordered n-tuples $(a_1, a_2, \cdots, a_n)$ where $a_j \in A_j$, $j = 1, \cdots, n$.

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \cdots, a_n) \mid a_1 \in A_1, a_2 \in A_2, \cdots, a_n \in A_n\}.$$

$$A_1 \times A_2 = \{(a_1, a_2) \mid a_1 \in A_1, a_2 \in A_2\}$$

is the Cartesian product of A_1 and A_2.

Example 1.

$$A = \{x, y\}, \quad B = \{1, 2, 3\}.$$

$$A \times B = \{(x,1), (x,2), (x,3), (y,1), (y,2), (y,3)\}$$

Example 2. Formally

$$(A \times B) \times C \neq A \times B \times C.$$

a set of ordered pairs of which one element itself is an ordered set

a set of ordered triples.

Example 3.

$$A \times B \neq B \times A.$$

In many cases we use another def

$$(A \times B) \times C = A \times (B \times C) = A \times B \times C$$

$$= \{(a, b, c) \mid a \in A, b \in B, c \in C\}$$

The order of a set S is equal to the number of its elements $n(S)$

$$n(A \times B) = n(A) \times n(B)$$

Example $A = \{x, y\}$, $B = \{1, 3, 5\}$

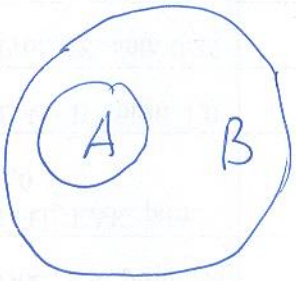
$$n(A) = 2, \quad n(B) = 3$$

$$n(A \times B) = 6.$$

Venn diagrams

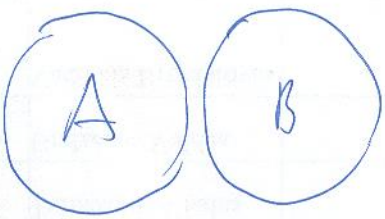
If A and B are represented as regions in the 2D plane, relationships between sets A and B can be represented by Venn diagrams.

1. $A \subset B$

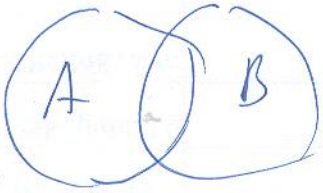


2. $A = B$

3. $A \not\subset B$.



a)



b)

c).

Operations on Sets

If all sets being considered are subsets of some set U, then U is called a **universal set**.

Let A and B are subsets of a universal set U.

1. The **union** of A and B, denoted $A \cup B$, is the set of all elements that are in **at least** one of A or B.

2. The **Intersection** of A and B, denoted $A \cap B$, is the set all elements that are common to both A and B.

3. The **difference** of B minus A, denoted by $B - A$, is the set of all elements that are in B and **not** in A.
(it can be denoted also by $B \setminus A$).

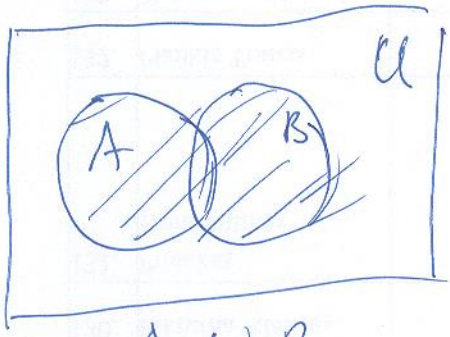
4. The complement of A, denoted by A^c or $\bar{A}$, is the set of all elements in U that are not in A.

$$A \cup B = \{x \in U \mid x \in A \text{ or } x \in B\}$$

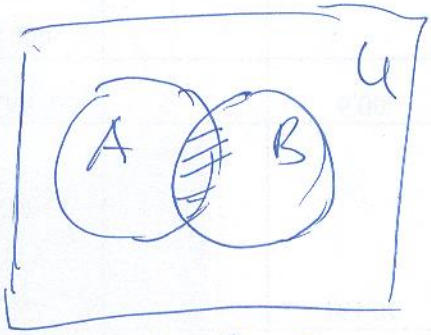
$$A \cap B = \{x \in U \mid x \in A \text{ and } x \in B\}$$

$$B - A = \{x \in U \mid x \in B \text{ and } x \notin A\}$$

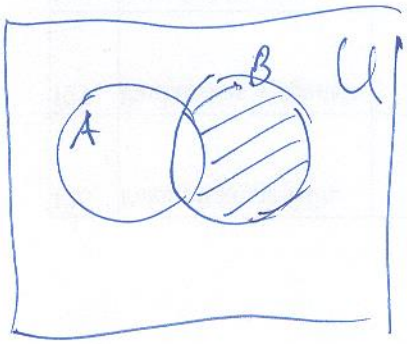
$$A^c = \{x \in U \mid x \notin A\}.$$



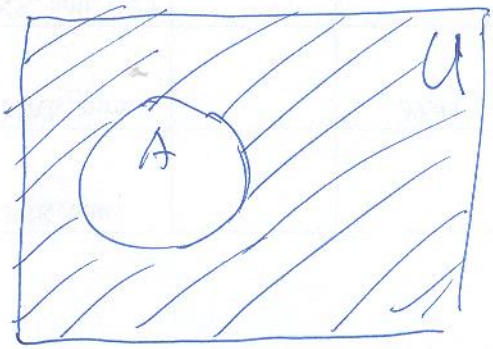
$A \cup B$



$A \cap B$



$B \setminus A$



A^c

Theorem. Some subsets relations.

1. For all sets A and B,
   $A \cap B \subseteq A$ and $A \cap B \subseteq B$.

2. For all sets A and B
   $A \subseteq A \cup B$ and $B \subseteq A \cup B$.

3. Transitive Property of subsets
   For all sets A and B, and C
   if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Proof. For example we try to prove 1.
Suppose that A and B are any (particular but arbitrarily chosen) sets.
We must show that
$\forall x$, if $x \in A \cap B$, then $x \in A$.

$x \in A \cap B \iff x \in A$ and $x \in B$.

in particular, x is in A.

Because x could be any element of $A \cap B$, thus every element in $A \cap B$ is in A.

Therefore, $A \cap B \subseteq A$.

Functions and Set identities

Theorem 2. Set identities

1. Commutative Laws

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

2. Associative Laws

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

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

3. Distributive Laws

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

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

4. Identity Laws: for every set A,

a) $A \cup \emptyset = A$ and b) $A \cap U = A$

5. Complement Laws

$$A \cup A^c = U \quad , \quad A \cap A^c = \emptyset$$

6. Double Complement Law

$$(A^c)^c = A$$

7. $A \cup U = U \quad , \quad A \cap \emptyset = \emptyset$

8. De Morgan's Laws:

$$(A \cup B)^c = A^c \cap B^c$$

$$(A \cap B)^c = A^c \cup B^c$$

12. Set Difference Law:

$$A - B = A \cap B^c.$$

Proof. Show that one set (on left) equals another set (on right).

Two sets are equal $\Leftrightarrow$ each is a subset of the other.

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

The following two statements must be proved

$$A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$$

and

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

Let's show how to prove the first condition

$\forall x$, if $x \in A \cup (B \cap C)$ then

$x \in (A \cup B) \cap (A \cup C)$

Case 1. $x \in A$, then both statements $x \in A \cup B$ and $x \in A \cup C$ are true by definition of union $\cup$ operation.

Hence $x \in (A \cup B) \cap (A \cup C)$.

Case 2. $x \in B \cap C$, then $x \in B$ and $x \in C$. by definition of $\cap$.

Since $x \in B$, then $x \in A \cup B$,

since $x \in C$, then $x \in A \cup C$.

Hence $x \in (A \cup B) \cap (A \cup C)$.

In both cases the required result is valid.

Functions defined on General Sets (Ch 07)

A function from a set X to a set Y is a relation from X, the domain of f (or definition domain) to Y, the co-domain, that satisfies two properties:

1. Every element in X is related to some element in Y
2. No element in X is related to more than one element in Y.

(related to one and only one element in Y).

f maps x to $y \in Y$.
sends x to $y \in Y$

Notations

$x \xrightarrow{f} y$ or $f: X \to Y$

or $y = f(x)$. (the value of f at x, the image of x under f)

The range of f (or the image of X under f) is defined by

$$f(X) = \{ y \in Y \mid y = f(x) \text{ for some } x \in X \}.$$

When x is an element such that

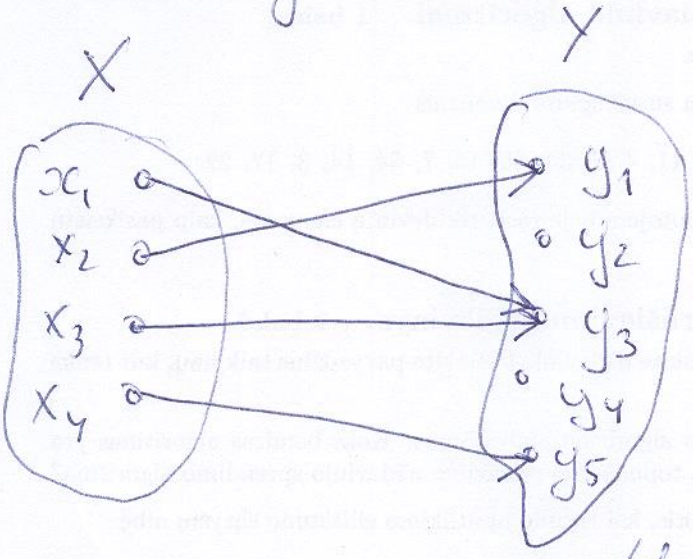
$$f(x) = y,$$

then x is called a <u>preimage</u> of y or an <u>inverse</u> image of y.

The inverse image of $y = \{x \in X \mid f(x) = y\}$

Arrow Diagrams

If X and Y are finite sets, we can define a function from X to Y by drawing an arrow diagram.



(i) Every element of X has an arrow

(ii) No element of X has two arrows that point to two different elements of Y.

Example 1. The identity function from X to X:

$I_X(x) = x$ for each $x \in X$.

Example 2. Sequences

Take a sequence

$1, -\frac{1}{2}, \frac{1}{3}, -\frac{1}{4}, \frac{1}{5}, \ldots$

It can be thought of as a function

$$f(n) = \frac{(-1)^n}{n+1}$$ for each integer $n \geq 0$.

Functions acting on sets

X and Y are sets

If $f: X \to Y$ is a function and $A \subseteq X$ and $C \subseteq Y$, then

$$f(A) = \{ y \in Y \mid y = f(x) \text{ for some } x \text{ in } A \}$$

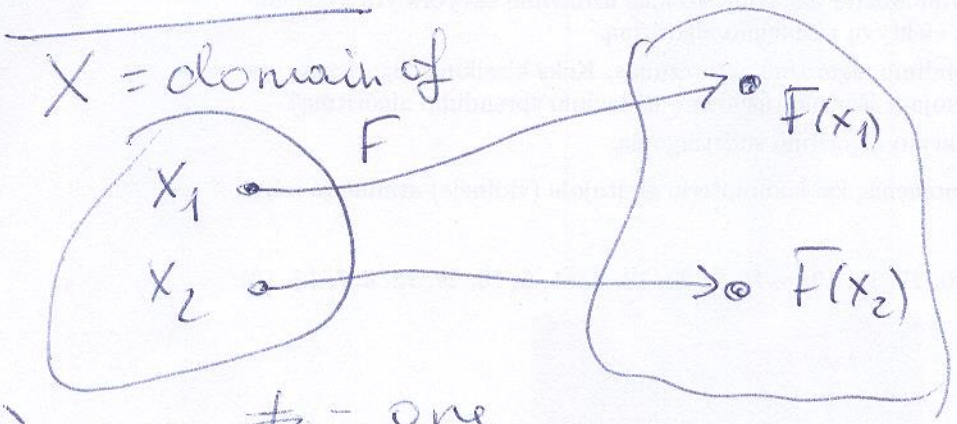
$f(A)$ is called the image of A.

$$f^{-1}(C) = \{ x \in X \mid f(x) \in C \}$$

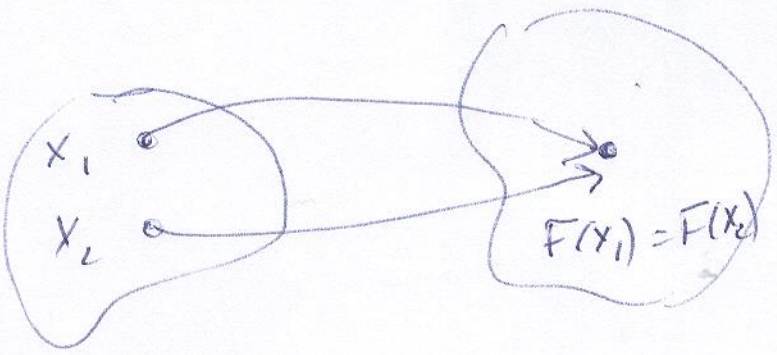
$f^{-1}(C)$ is called the inverse image of C.

Definition. Let F be a function from a set X to a set Y. F is injective (one-to-one) iff for all elements x_1 and x_2 in X

if $F(x_1) = F(x_2)$, then $x_1 = x_2$.



a) one-to-one



b) F is not One-to-one. $F(x) = x^2$.

Example. $f: \mathbb{R} \to \mathbb{R}$

$$f(x) = 4x - 1.$$

How to prove that f is one-to-one.

Proof. Suppose that x_1 and x_2 are any real numbers such that

$$4x_1 - 1 = 4x_2 - 1$$

Then

$$4x_1 = 4x_2 \Rightarrow x_1 = x_2.$$

Example 2 Hash functions Cryptography.

Definition $F: X \to Y$ is surjective (or onto) iff given any element y in Y, it is possible to find $x \in X$ such that $y = F(x)$.

$F: X \to Y$ is onto $\Leftrightarrow \forall y \in Y, \exists x \in X$ such that $y = F(x)$

T1. Show this definition in terms of arrow diagrams

Definition. If $F: X \to Y$ is injective and surjective it is called bijective. (or one-to-one correspondence).

Each element of X matches with exactly one element of Y and each element of Y matches with exactly one element of X.

Thus a bijection from a set X to a set Y is a function $F: X \to Y$ that is both one-to-one and onto
injection surjection.