International Baccalaureate

MATHEMATICS HL

OPTION: Sets, Relations and Groups

Lecture Notes

by

Christos Nikolaidis

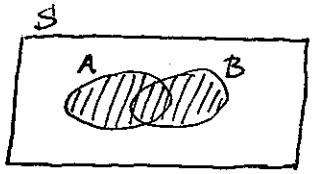
January 2015

CONTENTS

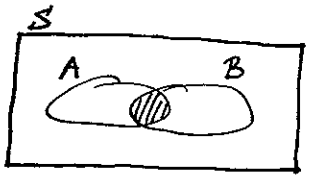
1. SETS

▶ BASIC OPERATIONS (USING VENN DIAGRAMS)

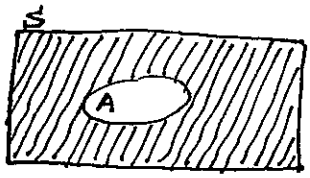
We already know:



UNION $A \cup B$ (A or B)

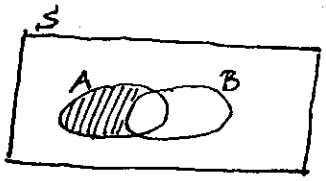


INTERSECTION $A \cap B$ (A and B)



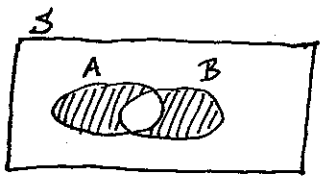
COMPLEMENT A' (not A)

We also define:



DIFFERENCE $A-B$ (A but not B)

Notice that $\boxed{A-B = A \cap B'}$



SYMMETRIC DIFFERENCE $A \triangle B$

(A or B but not both)

Notice that $\boxed{A \triangle B = (A \cup B) - (A \cap B)}$

or $\boxed{A \triangle B = (A - B) \cup (B - A)}$

EXAMPLE (Using explicit sets)

Let $S = \{1,2,3,4,5,6,7,8,9\}$ be our universal set

Consider the subsets $A = \{2,3,4,5\}$ $B = \{4,5,6\}$

Then

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

$A \cap B = \{4,5\}$

$A' = \{1,6,7,8,9\}$ $B' = \{1,2,3,7,8,9\}$

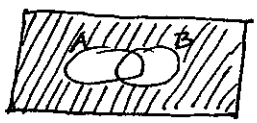
$A - B = \{2,3\}$ $B - A = \{6\}$

$A \triangle B = \{2,3,6\}$

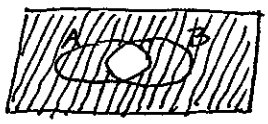
▶ USE OF VENN DIAGRAMS

We can easily verify, by using Venn diagrams, if a property of sets holds or not

EXAMPLE Show that $(A \cup B)' \neq A' \cup B'$

LHS: 

$(A \cup B)'$

RHS: 

$A' \cup B'$

In fact

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

De Morgan Laws

We can easily verify these laws by Venn Diagrams

▶ PROPERTIES OF SET OPERATIONS (LAWS)

① $A \cup B = B \cup A$
$A \cap B = B \cap A$ (COMMUTATIVE LAWS)

② $(A \cap B) \cap C = A \cap (B \cap C)$
$(A \cup B) \cup C = A \cup (B \cup C)$ (ASSOCIATIVE LAWS)

NOTICE: This property implies that we can remove brackets and write

$A \cap B \cap C$ and $A \cup B \cup C$ respectively.

(There is no confusion!)

③ What about $A \cap (B \cup C)$ and $A \cup (B \cap C)$?

HINT: If you imagine that in both cases we have

$A \cdot (B + C)$

you may obtain the result!

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

④ Notice also the following properties:

$A \cap A' = \emptyset$	$A \cap \emptyset = \emptyset$	$A \cap S = A$
$A \cup A' = S$	$A \cup \emptyset = A$	$A \cup S = S$

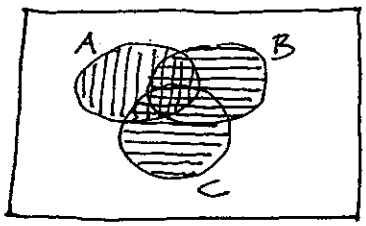
where $\emptyset$ = empty set, S = universal set.

EXAMPLE Let us verify the first distributive law

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

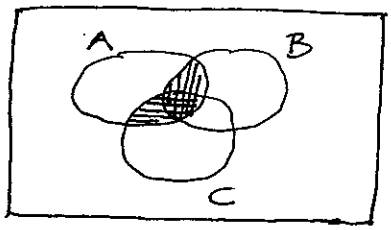
by using Venn diagrams.

LHS:



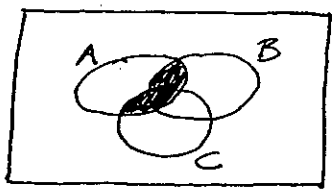
$A \cap (B \cup C)$

RHS:



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

Both sides give:



▶ PROOFS BY USING THE LAWS

EXAMPLE Prove that A-B and B-A are mutually exclusive (without using Venn diagrams)

We have to show that $(A-B) \cap (B-A) = \emptyset$

Remember that: $A-B = A \cap B'$ ⊛

Indeed,

$$\begin{aligned}
(A-B) \cap (B-A) &= (A \cap B') \cap (B \cap A') && [\text{by } ⊛] \\
&= A \cap B' \cap B \cap A' && [\text{Associative Law}] \\
&= A \cap A' \cap B \cap B' && [\text{Commutative Law}] \\
&= \emptyset \cap \emptyset \\
&= \emptyset
\end{aligned}$$

EXAMPLE By using the fact $A-B=A\cap B'$ (*)

prove $(A-B)\cup(B-A)=(A\cup B)-(A\cap B)$

(i.e. the two expressions of the symmetric difference $A\Delta B$ are equal)

$LHS=(A-B)\cup(B-A)=(A\cap B')\cup(B\cap A')$ [by *]

$=(A\cup B)\cap(A\cup A')\cap(B'\cup B)\cap(B'\cup A')$ [by Distributive Law]

$=(A\cup B)\cap S\cap S\cap(A'\cup B')$ [S → universal set]

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

$=(A\cup B)\cap(A\cap B)'$ [by De Morgan]

$=(A\cup B)-(A\cap B)$ [by *]

$=RHS$

▶ PROOFS BY INCLUSION

In order to prove $A=B$ we can prove

$A\subseteq B$ $(x\in A\Rightarrow\cdots\Rightarrow x\in B)$

and $B\subseteq A$ $(x\in B\Rightarrow\cdots\Rightarrow x\in A)$

EXAMPLE Prove the distributive law:

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

For "$\subseteq$". Let $x\in A\cap(B\cup C)\Rightarrow x\in A$ and $x\in B\cup C$

$\Rightarrow x\in A$ and $(x\in B$ or $x\in C)$

$\Rightarrow(x\in A$ and $x\in B)$ or $(x\in A$ and $x\in C)$

$\Rightarrow x\in A\cap B$ or $x\in A\cap C$

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

For "$\supseteq$" we work similarly.

In fact, we can use "$\Leftrightarrow$" instead of "$\Rightarrow$"

EXAMPLE Prove $(A \cup B)' = A' \cap B'$ [De Morgan]

For both directions we use "$\Leftrightarrow$"

$x \in (A \cup B)' \Leftrightarrow x \notin A \cup B$

$\Leftrightarrow x \notin A$ and $x \notin B$

$\Leftrightarrow x \in A'$ and $x \in B'$

$\Leftrightarrow x \in A' \cap B'$

EXAMPLE Prove that $A-B$ and $B-A$ are mutually exclusive

i.e. $(A-B) \cap (B-A) = \emptyset$.

Let $x \in (A-B) \cap (B-A) \Rightarrow x \in A-B$ and $x \in B-A$

$\Rightarrow x \in A$ and $x \notin B$ and $x \in B$ and $x \notin A$

$\Rightarrow x \in A$ and $x \notin A$ and $x \in B$ and $x \in B$

This is impossible. Thus the set is empty.

EXAMPLE Show that $A \cap (B \cup C) \subseteq (A \cap B) \cup C$

(only one direction holds)

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

$\Rightarrow x \in A$ and ($x \in B$ or $x \in C$)

$\Rightarrow$ { either $x \in B$ (and $x \in A$) so $x \in A \cap B$
or $x \in C$

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

▶ NUMBER OF SUBSETS

Let A be a set; a subset B consists of some, none or all elements of A.
We write $\boxed{B \subseteq A}$

For example, if $A = \{a, b, c\}$ we obtain the following subsets:

$\{a, b, c\}$ ← A itself
$\{a, b\}$ $\{a, c\}$ $\{b, c\}$ ← 2-element sets
$\{a\}$ $\{b\}$ $\{c\}$ ← 1-element set
$\emptyset$ ← the empty set

NOTICE: All subsets except A itself are called proper subsets. To emphasise that B is a proper subset of A we write $B \subset A$.

We observe that the number of subsets of $A = \{a, b, c\}$ is 8 (it is 2^3). In general:

PROPOSITION If A consists of n elements there exist 2^n subsets

---

PROOF. There exist $\binom{n}{0}$ subsets of no elements
$\binom{n}{1}$ subsets of 1 element
$\vdots$
$\binom{n}{n}$ subsets of n elements

TOTAL NUMBER $= \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = (1+1)^n$ [binomial thm]
$= 2^n$

---

2. CARTESIAN PRODUCT $A \times B$ - RELATIONS

▶ Let A and B be two sets

The <u>cartesian product $A \times B$</u> consists of all ordered pairs (a,b) where $a \in A$ and $b \in B$

<u>An example will clarify the definition</u>

<u>EXAMPLE</u> Let $A = \{a, b, c\}$ $B = \{1, 2\}$

The cartesian product $A \times B$ is a new set of six pairs:

$$A \times B = \{(a,1), (a,2), (b,1), (b,2), (c,1), (c,2)\}$$

Notice that $B \times A$ is a different set

$$B \times A = \{(1,a), (1,b), (1,c), (2,a), (2,b), (2,c)\}$$

<u>(since for example $(a,1) \neq (1,a)$)</u>

Thus in general $A \times B \neq B \times A$

▶ The cartesian product $A \times A$ is also denoted by A^2

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

$$A^2 = A \times A = \{(a,a), (a,b), (b,a), (b,b)\}$$

Always remember that the nature of an element in $A \times B$ or in $A^2 = A \times A$ is a PAIR

We can say for example that $(x,y) \in A \times B$ but not $x \in A \times B$ or $y \in A \times B$

The set $A \times (B \cap C)$ contains pairs (x,y) where $x \in A$ and $y \in B \cap C$
Let's prove the following

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

[Notice: here, we cannot use Venn diagrams or known properties. Only inclusion "$\subseteq$".]

$(x,y) \in LHS \Leftrightarrow (x,y) \in A \times (B \cap C)$
$\Leftrightarrow x \in A$ and $y \in B \cap C$
$\Leftrightarrow x \in A$ and $y \in B$ and $y \in C$
$\Leftrightarrow (x,y) \in A \times B$ and $(x,y) \in A \times C$
$\Leftrightarrow (x,y) \in (A \times B) \cap (A \times C)$
$\Leftrightarrow (x,y) \in RHS$

In exactly the same way we can show that

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

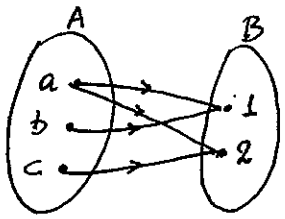
▶ RELATIONS FROM A TO B

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

For example, let $A = \{a, b, c\}$ $B = \{1, 2\}$

Let us define some relations from A to B

(a) $R = \{(a,1), (a,2), (b,1), (c,2)\}$

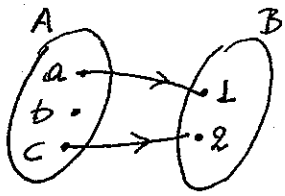


In order to express that "a is related to 1" we write

$(a,1) \in R$ or $aR1$

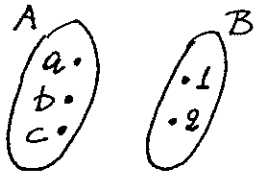
On the contrary $(b,2) \notin R$ or $b \not R 2$

(b) $S = \{(a,1), (c,2)\}$



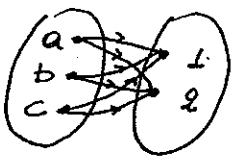
(only $aS1$ $cS2$)

(c) $T = \emptyset$
"empty relation"



(It is the most "frigid" relation!!!)

(d) $U = A \times B$



(It is the "warmest" relation!!!)

▶ A nice way to represent a relation is by a matrix of 0's and 1's

e.g. for $R = \{(a,1),(a,2),(b,1),(c,2)\}$

R	1	2
a	1	1
b	1	0
c	0	1

since $aR1$ $b\not R2$ the corresponding entries are 1 and 0 respectively.

▶ RELATIONS ON A

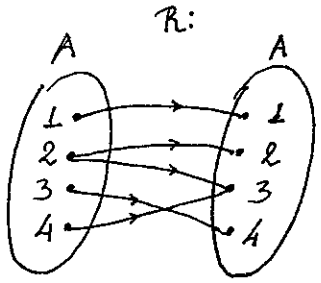
A relation from A to A is said to be a relation on A. (It is simply a subset of $A^2 = A \times A$)

EXAMPLE $A = \{1, 2, 3, 4\}$

Let R be relation on A, given by

$$R = \{(1,1),(2,2),(2,3),(3,4),(4,3)\}$$

R may also be described as follows:



or

R	1	2	3	4
1	1	0	0	0
2	0	1	1	0
3	0	0	0	1
4	0	0	1	0

A relation could also be given by a statement:

EXAMPLE Let $A = \{1, 2, 3, 4\}$

We define the relations: R, S, T, U as follows

xRy if and only if $x = y$
xSy if and only if $x < y$
xTy if and only if $x \leq y$
xUy if and only if $x - y$ is even

Clearly, $R = \{(1,1), (2,2), (3,3), (4,4)\}$
$S = \{(1,2), (1,3), (1,4), (2,3), (2,4), (3,4)\}$
$T = R \cup S$
$U = \{(1,1), (2,2), (3,3), (4,4), (1,3), (3,1), (2,4), (4,2)\}$

Let us also see the corresponding matrices

R	1	2	3	4
1	1	0	0	0
2	0	1	0	0
3	0	0	1	0
4	0	0	0	1

↓ the relation $=$

S	1	2	3	4
1	0	1	1	1
2	0	0	1	1
3	0	0	0	1
4	0	0	0	0

↓ the relation $<$

T	1	2	3	4
1	1	1	1	1
2	0	1	1	1
3	0	0	1	1
4	0	0	0	1

↓ the relation $\leq$

U	1	2	3	4
1	1	0	1	0
2	0	1	0	1
3	1	0	1	0
4	0	1	0	1

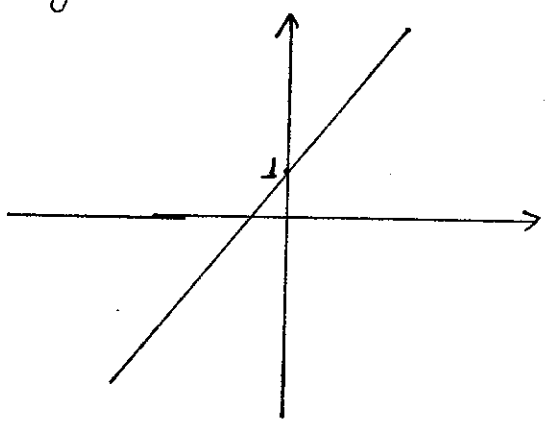
[You see, instead of $(1,2) \in <$ we usually write $1 < 2$.]

▶ RELATIONS ON THE CARTESIAN PLANE

A relation on $\mathbb{R}$ is a subset of $\mathbb{R}\times\mathbb{R}$.
Thus, we may represent such relations on the Cartesian plane.

EXAMPLE We define the following relations on $\mathbb{R}$ and sketch a corresponding graph.

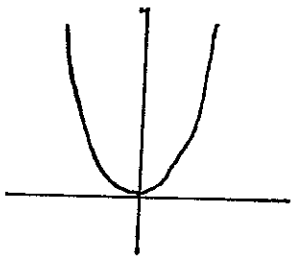
- $xRy \Leftrightarrow y = 2x+1$



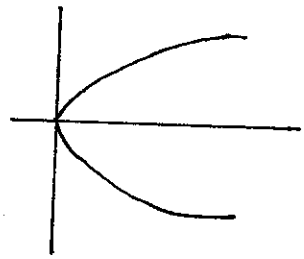
i.e. this relation consists of all pairs (x,y) that satisfy $y=2x+1$.
In that sense, all functions you already know are relations!

later on, we will give a formal definition of a function based on relations
At the moment let's see other relations

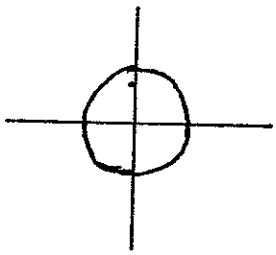
- $x R y \Leftrightarrow y = x^2$



$x R y \Leftrightarrow x = y^2$

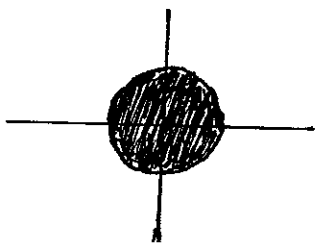


- $x R y \Leftrightarrow x^2 + y^2 = 1$



i.e. unit circle

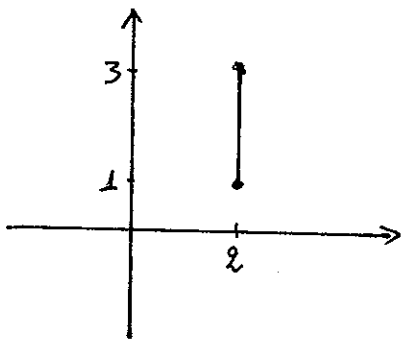
$x R y \Leftrightarrow x^2 + y^2 \leq 1$



i.e. circular disk of radius 1

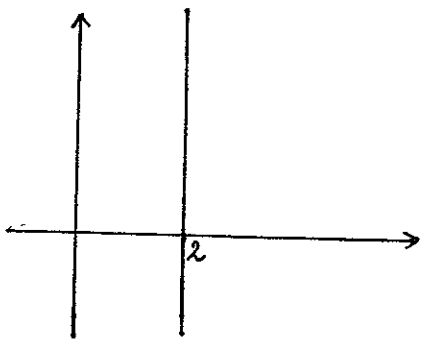
(remember: $x^2 + y^2 = a^2$ is a circle of radius a)

- $x R y \Leftrightarrow x = 2, 1 \leq y \leq 3$



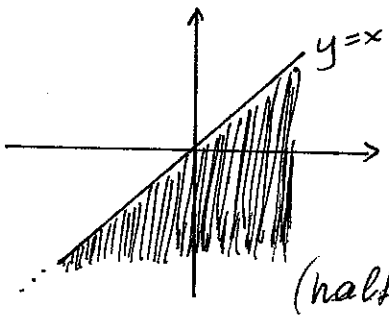
segment

$x R y \Leftrightarrow x = 2$



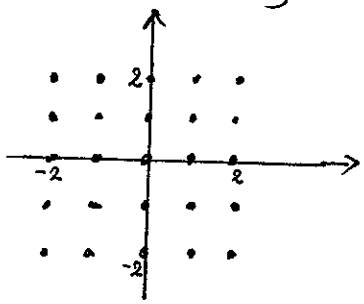
line $x = 2$

- $xRy \Leftrightarrow x > y$



(half-plane)

- $xRy \Leftrightarrow -2 \leq x \leq 2, -2 \leq y \leq 2$ and $x, y \in \mathbb{Z}$



(for $y \leq ax+b$ or $y \geq ax+b$, you draw $y = ax+b$ and pick a point outside the line to see which half-plane to shade)

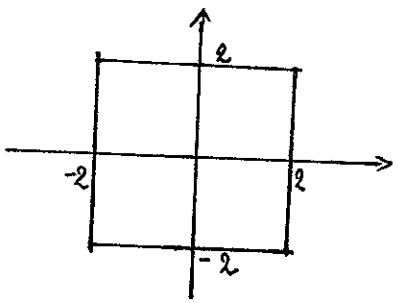
- An interesting relation is the following.

By $\max\{a,b\}$ we denote the greatest value between a and b. For example, $\max\{2,3\} = 3$

Let's define

$xRy \Leftrightarrow \max\{|x|, |y|\} = 2$

Thus, either $|x| = 2$ and $|y| \leq 2$
or $|y| = 2$ and $|x| \leq 2$



It is a square of side 4.

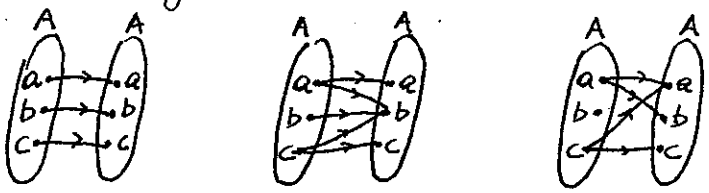
▶ PROPERTIES OF RELATIONS ON A

The relation R on a set A is said to be

- REFLEXIVE if $(a,a) \in R$ for all $a \in A$
- SYMMETRIC if $(a,b) \in R \Rightarrow (b,a) \in R$
- TRANSITIVE if $(a,b) \in R$ and $(b,d) \in R \Rightarrow (a,c) \in R$

In other words

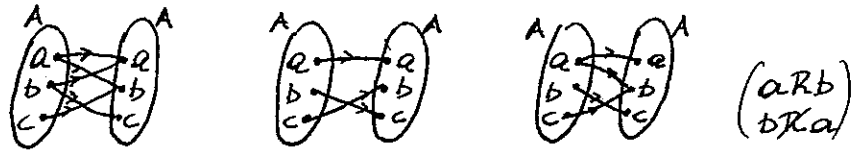
REFLEXIVE means that aRa for all a
i.e. every element is related to itself.



reflexive reflexive not reflexive since $b \not R b$

Don't mind if pairs other than $(a,a),(b,b),(c,c)$ are also appear!

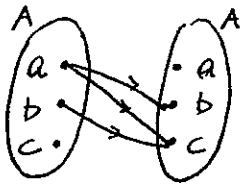
SYMMETRIC means that aRb implies that also bRa
i.e. whenever a is related to b we observe that b is also related to a.



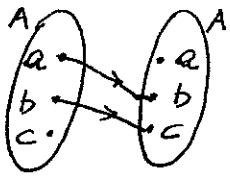
symmetric symmetric not symmetric

TRANSITIVE means that aRb and bRc imply that aRc

i.e. whenever we see consecutive pairs aRb, bRc we must also see aRc.



transitive



not transitive
since aRb and bRc
but aRc

NOTICE: Transitivity is the most difficult to check! Fortunately, they will never ask difficult cases!

It is much easier though to check the three properties if the relation is given as an explicit statement:

The relation $\leq$ on the set $\mathbb{R}$ of real numbers is

- REFLEXIVE since $x \leq x$ for all $x \in \mathbb{R}$
- NOT SYMMETRIC since for example $1 \leq 3$ but $3 \not\leq 1$
  (in such a case a counterexample helps!)
- TRANSITIVE since $x \leq y$ and $y \leq z \Rightarrow x \leq z$

The relation $=$ on $\mathbb{R}$ has all three properties (easy to check!)

▶ MATRIX REPRESENTATION AND PROPERTIES

As far as the REFLEXIVE and the SYMMETRIC properties are concerned, the matrix representation is very clear:

R_1	a	b	c	d
a	1	1	0	1
b	1	0	0	0
c	0	0	1	0
d	1	0	0	1 ↖

R_2	a	b	c	d
a	1	1	0	0
b	0	1	0	0
c	0	0	1	1
d	0	0	1	1 ↖

For R_1

- It is NOT REFLEXIVE
  since the main diagonal contain 0's (↖)
- It is SYMMETRIC
  since the matrix is symmetric
  (about the main diagonal)

For R_2

- It is REFLEXIVE
  since the main diagonal has only 1's
- It is NOT SYMMETRIC
  since the matrix is not symmetric
  (aR_2b but $b\not R_2a$)

TRANSITIVITY is more difficult to check!
We can see though that R_1 is not transitive since bR_1a, aR_1b but $b\not R_1b$.

3. EQUIVALENCE RELATION

A relation on a set A which is

- REFLEXIVE
- SYMMETRIC
- TRANSITIVE

is said to be an EQUIVALENCE RELATION

The most trivial equivalence relation is the equality "=" on a set of numbers

---

EXAMPLE Let $A = \{1, 2, 3, \ldots, 100\}$

We define

$aRb \Leftrightarrow$ a and b have the same number of digits

for example $2R7$, $31R64$ but $5\not R27$

The relation R is an EQUIVALENCE RELATION:

- REFLEXIVE: it holds aRa for any $a \in A$
  since any number has the same number of digits with itself.
- SYMMETRIC: since
  $aRb \Rightarrow$ a and b have the same number of digits
  $\Rightarrow$ b and a have the same number of digits
  $\Rightarrow bRa$
- TRANSITIVE: since
  aRb and $bRc \Rightarrow$ (similar process) $\Rightarrow aRc$

▶ EQUIVALENCE CLASS – PARTITION

An equivalence relation is very often denoted by $\sim$ (instead of R). In the last example we could define the relation as follows

$a \sim b \Leftrightarrow$ a and b have the same number of digits

Related elements are said to be equivalent.

The <u>EQUIVALENCE CLASS</u> of some element a consists of all the elements related to a (i.e. the equivalent elements of a).
This set is denoted by $[a]$.

Formally $\quad [a] = \{ x \in A \mid x \sim a \}$

In the last example, the equivalence class of 1 is

$$[1] = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

Of course, this is also $[2]$ or $[3]$ etc. In fact, we can select any 1-digit number as a representative
We have 3 equivalence classes:

$[1] = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ (one-digit numbers)
$[10] = \{10, 11, 12, \ldots, 99\}$ (two-digit numbers)
$[100] = \{100\}$ (three-digit numbers)

In this way we obtain a PARTITION of set A (i.e. we split A into disjoint subsets)

Formally, a partition of a set A is a collection of subsets $A_1, A_2, \dots, A_n$ of A such that

- the subsets are mutually exclusive pairwise
  i.e $A_i \cap A_j = \emptyset$ for any pair A_i, A_j
- the union of the subsets is A
  i.e $A_1 \cup A_2 \cup \dots \cup A_n = A$

EXAMPLE Let $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

We define

$$a \sim b \Leftrightarrow a - b \text{ is even}$$

We show that this is an equivalence relation

- REFLEXIVE : $a \sim a$ for any $a \in A$
  since $a - a = 0$ is even.
- SYMMETRIC: $a \sim b \Rightarrow a - b$ is even
  $\Rightarrow b - a$ is even
  $\Rightarrow b \sim a$
- TRANSITIVE: $a \sim b$ and $b \sim c$
  $\Rightarrow a - b$ is even, $b - c$ is even
  $\Rightarrow (a - b) + (b - c)$ is even
  $\Rightarrow a - c$ is even
  $\Rightarrow a \sim c$

The equivalence class of 1 is

$[1] = \{1, 3, 5, 7, 9\}$ · (odd numbers)

The equivalence class of 2 is

$[2] = \{2, 4, 6, 8, 10\}$ (even numbers)

Thus, we obtain a partition of A into two equivalence classes, [1] and [2] (odd and even)

NOTICE: If we are given a partition of A

say $A_1, A_2, A_3, \ldots, A_n$

an equivalence relation is automatically defined

$x \sim y \Leftrightarrow x$ and y lie in the same subset A_i

It is easy to check that $\sim$ is reflexive, symmetric and transitive.

The equivalence classes are the subsets $A_1, A_2, \ldots$

e.g. For $A = \{a, b, c, d, e\}$

the partition $A_1 = \{a, b\}$ $A_2 = \{c, d\}$ $A_3 = \{e\}$

defines

R	a	b	c	d	e
a	1	1	0	0	0
b	1	1	0	0	0
c	0	0	1	1	0
d	0	0	1	1	0
e	0	0	0	0	1

← observe the equivalence classes! {a, b} {c, d} {e}

▶ THE EQUIVALENCE RELATION $a \equiv b \pmod n$

We have already seen the relation

$$a \sim b \Leftrightarrow a-b \text{ is even}$$

i.e $a-b$ is divisible by 2

This relation on the set $\mathbb{Z}$ of integers is also denoted by $a \equiv b \pmod 2$. i.e,

$$a \equiv b \pmod 2 \Leftrightarrow a-b \text{ is even}$$

(we read, "a is equivalent to b modulo 2")

There are two equivalence classes:

$[0] = \{0, \pm 2, \pm 4, \dots\}$ (even numbers : $2n$, $n \in \mathbb{Z}$)

$[1] = \{\pm 1, \pm 3, \pm 5, \dots\}$ (odd numbers : $2n+1$, $n \in \mathbb{Z}$)

In general, the relation

$$a \equiv b \pmod n \Leftrightarrow a-b \text{ is divisible by } n$$

is an equivalence relation on $\mathbb{Z}$.

Indeed,

- REFLEXIVE : $a \equiv a \pmod n$ for any $a \in \mathbb{Z}$
  since $a-a=0$ is divisible by n

• SYMMETRIC:

$a \equiv b \pmod n \Rightarrow a-b$ is divisible by n
$\Rightarrow b-a$ is divisible by n
$\Rightarrow b \equiv a \pmod n$

• TRANSITIVE:

$a \equiv b \pmod n$ and $b \equiv c \pmod n$
$\Rightarrow a-b$ and $b-c$ are divisible by n
$\Rightarrow (a-b)+(b-c)$ is divisible by n
$\Rightarrow a-c$ is divisible by n
$\Rightarrow a \equiv c \pmod n$

The are n equivalence classes.
An example will clarify the concept!

EXAMPLE The equivalence relation

$a \equiv b \pmod 5 \Leftrightarrow a-b$ is divisible by 5

determines the following equivalence classes:

$[0] = \{\dots, 0, 5, 10, \dots\} = \{5k / k \in \mathbb{Z}\}$ (multiples of 5)
$[1] = \{\dots, 1, 6, 11, \dots\} = \{5k+1 / k \in \mathbb{Z}\}$
$[2] = \{\dots, 2, 7, 12, \dots\} = \{5k+2 / k \in \mathbb{Z}\}$
$[3] = \{\dots, 3, 8, 13, \dots\} = \{5k+3 / k \in \mathbb{Z}\}$
$[4] = \{\dots, 4, 9, 14, \dots\} = \{5k+4 / k \in \mathbb{Z}\}$

Thus, we obtain a partition of $\mathbb{Z}$

This equivalence relation may also be defined as follows

$a \equiv b \pmod 5 \Leftrightarrow$ a and b have the same remainder when divided by 5

Indeed, if both a and b have remainder r,

i.e $\left.\begin{aligned} a &= 5k_1 + r \\ b &= 5k_2 + r \end{aligned}\right\} \Rightarrow a - b = 5k_1 - 5k_2 = 5(k_1 - k_2)$

$\Rightarrow a - b$ is divisible by 5

(the opposite direction is similar)

Thus we have two definitions for $a \equiv b \pmod n$:

$a \equiv b \pmod n \Leftrightarrow a - b$ is divisible by n

$\Leftrightarrow a, b$ have the same remainder when divided by n.

We can easily verify that

$128 \equiv 3 \pmod 5$, $71 \equiv 1 \pmod 7$, $2015 \equiv 8 \pmod 9$

EXAMPLE Let $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

Let's define $a \sim b \Leftrightarrow a^2 \equiv b^2 \pmod 5$

It is easy to check that $\sim$ is an equiv. relation

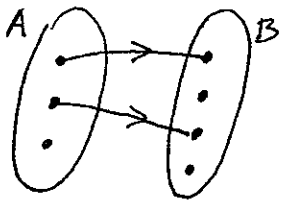
Equivalence classes: $[1] = \{1, 4, 6, 9\}$
$[2] = \{2, 3, 7, 8\}$
$[5] = \{5, 10\}$ (Why?)

---

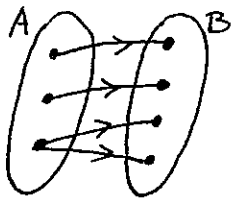
4. FUNCTIONS

Some relations from A to B are called FUNCTIONS:

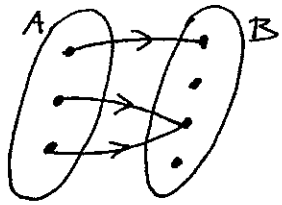
if <u>each element of A</u> corresponds to <u>a unique element of B</u>



it is NOT a function



it is NOT a function



it is a function

(Why?)

For such a relation $f \subseteq A \times B$ we write

$$f: A \to B$$

Instead of $(a,b) \in f$ or afb (a is related to b) we write

$$f(a)=b \quad \text{or} \quad f: a \mapsto b$$

As we know, some functions are defined by a formula. For example, we define the function

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

given by $f(x)=2x+1$ (or $f: x \mapsto 2x+1$)

For a function $f: A \to B$

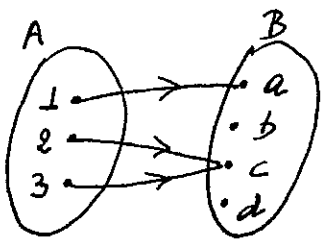
A is called DOMAIN

B is called CODOMAIN

If $f(a)=b$, we say that b is the image of a

The set of all images is a subset of B;
it is called RANGE of f.
It is denoted by $f(A)$.

EXAMPLE $f: A \to B$



DOMAIN $A = \{1, 2, 3\}$

CODOMAIN $B = \{a, b, c, d\}$

RANGE $f(A) = \{a, c\}$

EXAMPLE $f: \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$

DOMAIN $\mathbb{R}$

CODOMAIN $\mathbb{R}$

RANGE $f(\mathbb{R}) = [0, +\infty)$

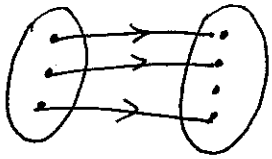
For the range we can also write

$f(\mathbb{R}) = \{y \mid y \geq 0\}$

or simply Range: $y \geq 0$

▶ "ONE-TO-ONE" OR INJECTION

A function f is "one-to-one" (or "1-1") or injection (or injective function) if different x's have different images:



DEFINITION: $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$

EQUIVALENT DEFINITION (and more practical)

$$\boxed{f(x_1) = f(x_2) \Rightarrow x_1 = x_2}$$

EXAMPLE Show that $f: \mathbb{R} \to \mathbb{R}$ with $f(x) = 3x + 5$ is "1-1".

$f(x_1) = f(x_2) \Rightarrow 3x_1 + 5 = 3x_2 + 5 \Rightarrow 3x_1 = 3x_2 \Rightarrow x_1 = x_2$.

EXAMPLE Show that $f: \mathbb{R} \to \mathbb{R}$ with $f(x) = x^2$ is not "1-1".

$f(x_1) = f(x_2) \Rightarrow x_1^2 = x_2^2 \Rightarrow x_1 = \pm x_2$ (so $\not\Rightarrow x_1 = x_2$)

In this case, it is better to find a COUNTEREXAMPLE

e.g. $f(2) = 4$ and $f(-2) = 4$, so f is not "1-1".

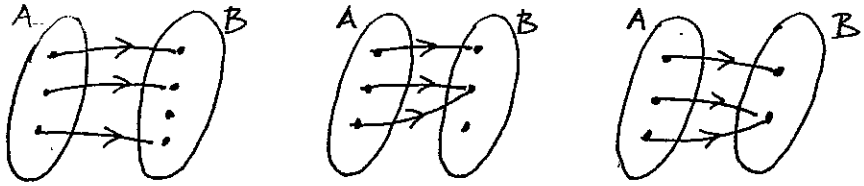
▶ "ONTO" OR SURJECTION

A function f is "onto" or surjection (or surjective function)

if RANGE = CODOMAIN

i.e $\boxed{f(A) = B}$

i.e every element of B is an image (of some element of A)



not ONTO not ONTO ONTO

(Why?)

EQUIVALENT DEFINITION:

$\boxed{\text{For any } b \in B, \text{ there exists } a \in A \text{ s.t } f(a)=b}$

IN PRACTICE: we solve $f(a)=b$ for a, to find a.

EXAMPLE $f: \mathbb{R} \to \mathbb{R}$, $f(x)=x^2$

It is not "onto" since range $\neq \mathbb{R}$ $(f(A)=[0,+\infty) \neq \mathbb{R})$

EXAMPLE $f: \mathbb{R} \to [0,+\infty)$ $f(x)=x^2$

It is "onto" since range $=[0,+\infty)$ $(f(A)=[0,+\infty))$

This explanation is enough! However, let us see

the equivalent definition:

Let $y \in [0, +\infty)$. We solve $f(x) = y$ for x

$f(x) = y \Leftrightarrow x^2 = y \Leftrightarrow x = \sqrt{y}$ (since $y \geq 0$)

Thus, for $y \in [0, +\infty)$, there exists $x = \sqrt{y} \in \mathbb{R}$, s.t. $f(x) = y$.

EXAMPLE $f: \mathbb{Z} \to \mathbb{Z}$, $f(n) = n+1$. It is "onto":

Let $m \in \mathbb{Z}$. We solve $f(n) = m$ for n

$f(n) = m \Leftrightarrow n+1 = m \Leftrightarrow n = m-1 \in \mathbb{Z}$

Thus, for $m \in \mathbb{Z}$, there exists $n = m-1 \in \mathbb{Z}$, s.t. $f(n) = m$.

EXAMPLE $f: \mathbb{Z} \to \mathbb{Z}$ $f(n) = 3n+1$. It is not "onto".

Let $m \in \mathbb{Z}$. We solve $f(n) = m$ for n.

$$f(n) = m \Leftrightarrow 3n+1 = m \Leftrightarrow n = \frac{m-1}{3}$$

but this is <u>not</u> always in $\mathbb{Z}$.

Again, a counterexample helps:

For $m = 5$, there is no $n \in \mathbb{Z}$, s.t $f(n) = 5$

since $3n+5 = 5 \Leftrightarrow n = \frac{4}{3} \notin \mathbb{Z}$.

EXAMPLE $f: \mathbb{N} \to \mathbb{N}$ $f(n) = n+1$ is not "onto".

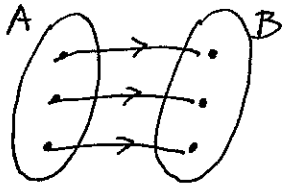
Indeed, $m = 0$ is not an image of some $n \in \mathbb{N}$

NOTICE: It would be onto if it was given as

$f: \mathbb{N} \to \mathbb{N}^*$, $f(n) = n+1$. (Why?)

▶ "1-1" AND "ONTO" OR BIJECTION

If f is "1-1" and "onto", that is injective and surjective, we say that f is a <u>bijection</u> (or a bijective function)



ONLY in this case we may define the inverse function $f^{-1}: B \to A$

$$f(x) = y \iff f^{-1}(y) = x$$

<u>NOTICE</u>: In fact

- we first check if f is "1-1"
- we try to solve $f(x)=y$ for x
- if we can solve it and $x \in A$, f is "onto"
- at the same time we obtain f^{-1}.

<u>EXAMPLE</u>: $f: \mathbb{R} \to \mathbb{R}$, $f(x) = 3x+5$

- $f(x_1) = f(x_2) \Rightarrow 3x_1+5 = 3x_2+5 \Rightarrow x_1 = x_2$, f is "1-1"
- We solve $f(x)=y \iff 3x+5=y \iff x = \frac{y-5}{3} \in \mathbb{R}$.
- Thus f is onto
- f is a bijection and $f^{-1}(x) = \frac{x-5}{3}$

EXAMPLE: Let $A=\mathbb{R}-\{2\}$, $B=\mathbb{R}-\{3\}$

$f: A \to B$, $f(x)=\dfrac{3x+1}{x-2}$

- f is "1-1":

$$f(x_1)=f(x_2) \Rightarrow \frac{3x_1+1}{x_1-2}=\frac{3x_2+1}{x_2-2}$$

$$\Rightarrow 3x_1x_2-6x_1+x_2-2=3x_1x_2+x_1-6x_2-2$$

$$\Rightarrow 7x_2=7x_1 \Rightarrow x_1=x_2$$

(OR)

from the graph of f: any horizontal line has at most one intersection point with the graph.

- We solve $f(x)=y$ for x:

$$\frac{3x+1}{x-2}=y \Leftrightarrow 3x+1=xy-2y \Leftrightarrow (y-3)x=2y+1$$

$$\Leftrightarrow x=\frac{2y+1}{y-3} \quad (\text{since } y\in B, \text{ so } y\neq 3)$$

Hence f is "onto"

(OR) range $=\mathbb{R}-\{3\}=B$, so f is "onto"

- Therefore, f is a bijection

The inverse function is $f^{-1}: B \to A$

$$f^{-1}(x)=\frac{2x+1}{x-3}$$

▶ FUNCTIONS OF TWO VARIABLES

(a) We may have functions of the form

$$f: \mathbb{R}\times\mathbb{R} \longrightarrow \mathbb{R}$$

for example $f(x,y) = 2x+y$. e.g. $f(1,2)=4$

(b) We may have functions of the form

$$f: \mathbb{R}\times\mathbb{R} \longrightarrow \mathbb{R}\times\mathbb{R}$$

for example $f(x,y)=(x+y, x-y)$. e.g $f(1,2)=(3,-1)$

EXAMPLE (OF A BIJECTION)

Let $f:\mathbb{R}\times\mathbb{R}\to\mathbb{R}\times\mathbb{R}$, $f(x,y)=(2x+y, x+2y)$

Show that f is a bijection. Find f^{-1}.

- f is "1-1": $\boxed{f(x_1,y_1)=f(x_2,y_2) \Rightarrow (x_1,y_1)=(x_2,y_2)}$

$$f(x_1,y_1)=f(x_2,y_2) \Rightarrow (2x_1+y_1,\ x_1+2y_1)=(2x_2+y_2,\ x_2+2y_2)$$

$$\Rightarrow \begin{cases} 2x_1+y_1 = 2x_2+y_2 & (a) \\ x_1+2y_1 = x_2+2y_2 & (b) \end{cases}$$

(a) - 2(b) : $-3y_1 = -3y_2 \Rightarrow y_1 = y_2$

Then

(b) gives $x_1 = x_2$

Hence $(x_1,y_1)=(x_2,y_2)$.

- f is "onto":

Let $(a,b) \in \mathbb{R}\times\mathbb{R}$. We solve $f(x,y)=(a,b)$ for (x,y).

$$(2x+y,\ x+2y)=(a,b) \iff \begin{array}{ll} 2x+y=a & (a) \\ x+2y=b & (b) \end{array}$$

$2(a)-(b)$: $3x=2a-b \Rightarrow x=\frac{2a-b}{3}$

$2(b)-a$: $3y=2b-a \Rightarrow y=\frac{2b-a}{3}$

Thus, we found $(x,y)\in\mathbb{R}\times\mathbb{R}$, s.t $f(x,y)=(a,b)$

- f is a bijection. The inverse function is

$$f^{-1}(a,b)=\left(\frac{2a-b}{3},\ \frac{2b-a}{3}\right)$$

or otherwise

$$f^{-1}(x,y)=\left(\frac{2x-y}{3},\ \frac{2y-x}{3}\right)$$

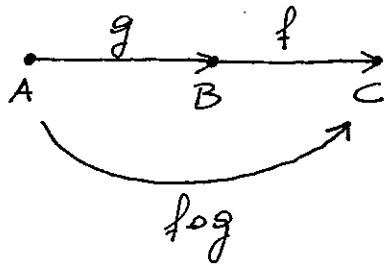
We can easily verify that

$$f\left(\frac{2x-y}{3},\ \frac{2y-x}{3}\right)=(x,y)$$

(i.e. $(f\circ f^{-1})(x,y)=(x,y)$: Exercise!)

▶ PROOFS FOR $f \circ g$

Let $g: A \to B$ and $f: B \to C$



Then $f \circ g: A \to C$ is defined by

$$(f \circ g)(a) = f(g(a))$$

(Notice that g is applied first, then f:
$a \longmapsto g(a) \longmapsto f(g(a))$)

PROPOSITIONS:

(a) f, g injective $\Rightarrow f \circ g$ injective

(b) f, g surjective $\Rightarrow f \circ g$ surjective

(c) f, g bijective $\Rightarrow f \circ g$ bijective

In the opposite direction

(d) $f \circ g$ injective $\Rightarrow g$ injective

(e) $f \circ g$ surjective $\Rightarrow f$ surjective

PROOFS:

(a) Let f, g be injective. We show that $f \circ g$ is injective:

$$(f\circ g)(a_1) = (f\circ g)(a_2) \Rightarrow f(g(a_1)) = f(g(a_2))$$
$$\Rightarrow g(a_1) = g(a_2) \quad \text{[since } f \text{ injective]}$$
$$\Rightarrow a_1 = a_2 \quad \text{[since } g \text{ injective]}$$

(b) Let f, g be surjective. We show that $f \circ g$ is surjective:

Let $c \in C$. We seek $a \in A$ such that $(f\circ g)(a) = c$.

But

there exists $b \in B$, s.t. $f(b) = c$ [since f surjective]

there exists $a \in A$, st. $g(a) = b$ [since g surjective]

Thus, we found $a \in A$, s.t. $(f\circ g)(a) = f(g(a)) = f(b) = c$.

(c) This is (a) and (b) together!

(d) Let $f \circ g$ be injective. We show that g is injective:

$$g(a_1) = g(a_2) \Rightarrow f(g(a_1)) = f(g(a_2)) \quad \text{[just apply } f\text{]}$$
$$\Rightarrow (f\circ g)(a_1) = (f\circ g)(a_2)$$
$$\Rightarrow a_1 = a_2 \quad \text{[since } f\circ g \text{ injective]}$$

(e) Let $f \circ g$ be surjective. We show that f is surjective:

Let $c \in C$. We seek $b \in B$, s.t. $f(b) = c$

But

there exists $a \in A$, s.t. $(f\circ g)(a) = c \Rightarrow f(g(a)) = c$

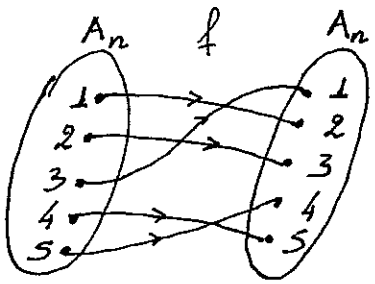
Thus, we found $b = g(a)$, s.t. $f(b) = f(g(a)) = c$.

---

5. THE SET OF PERMUTATIONS: S_n

▶ IN GENERAL

Consider the set $A_n = \{1, 2, 3, \ldots, n\}$
We deal with bijections from A_n to A_n
For example



is a bijection on $A_5 = \{1, 2, 3, 4, 5\}$
Such a bijection is called PERMUTATION
Instead of $f(1)=2$, $f(2)=3$, etc we write

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$$

How many permutations are there? $\rightarrow 5!$

In fact, in the second row we rearrange (otherwise permute) n elements in all possible ways. Hence

---

There are $n!$ permutations on A_n. The set of all these permutations is denoted by S_n

---

▶ THE SET S_3

It contains $3! = 6$ permutations

$$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \qquad f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \qquad f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

- The composition of two permutations gives also a permutation in S_3.
  For example

$$f_2 \circ f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ ? & & \end{pmatrix}$$

Mind that f_4 is applied first and then f_2.

Hence

$$1 \mapsto 1 \mapsto 3$$
$$2 \mapsto 3 \mapsto 2$$
$$3 \mapsto 2 \mapsto 1$$

Therefore,

$$f_2 \circ f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = f_5$$

EXAMPLE. Similarly in S_4 we have

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$$

- The inverse function of a permutation is also a permutation

For example, consider

$$f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

The inverse function f_2^{-1} maps

$$3 \mapsto 1$$
$$1 \mapsto 2$$
$$2 \mapsto 3$$

Thus

$$f_2^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \rightarrow \text{This is } f_3$$

- The identity permutation is $f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$

It is usually denoted by $e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$

For any permutation f in S_3, it is easy to verify that

$$\boxed{\begin{aligned} e \circ f &= f \\ f \circ e &= f \end{aligned}} \qquad \text{and} \qquad \boxed{\begin{aligned} f \circ f^{-1} &= e \\ f^{-1} \circ f &= e \end{aligned}}$$

NOTICE: These properties hold in general is S_n where

$$e = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix} \in S_n$$

It will be interesting to see all possible compositions in S_3 in the following table
We rename the permutations as follows:

$$e=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} \qquad \sigma_1=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} \qquad \sigma_2=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$$

$$\tau_1=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} \qquad \tau_2=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} \qquad \tau_3=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$$

In fact, σ_1 permutes 1,2,3 cyclically: $\begin{matrix}1\to2\\2\to3\\3\to1\end{matrix}$
σ_2 does the same twice
and τ_1 keeps 1, interchanges 2 and 3: $\begin{matrix}1\\2\rightleftarrows3\end{matrix}$
Similarly for τ_2, τ_3

Then

$\circ$	e	σ_1	σ_2	τ_1	τ_2	τ_3
e	e	σ_1	σ_2	τ_1	τ_2	τ_3
σ_1	σ_1	σ_2	e	τ_2	τ_3	τ_1
σ_2	σ_2	e	σ_1	τ_3	τ_1	τ_2
τ_1	τ_1	τ_3	τ_2	e	σ_2	σ_1
τ_2	τ_2	τ_1	τ_3	σ_1	e	σ_2
τ_3	τ_3	τ_2	τ_1	σ_2	σ_1	e

NOTICE: This is a "taste" of a nice GROUP, a concept we deal with in the next section!

▶ Cyclic Notation

The permutation

$$p=\begin{pmatrix}1&2&3&4&5\\2&3&1&5&4\end{pmatrix}$$

can also be written as

$$p=(1\ 2\ 3)(4\ 5)$$

i.e $1\to 2\to 3$ $\quad 4\to 5$

In this way any permutation can be expressed in disjoint cycles

e.g $\begin{pmatrix}1&2&3&4&5\\2&3&4&5&1\end{pmatrix} \to (1\ 2\ 3\ 4\ 5)$

$\begin{pmatrix}1&2&3&4&5\\3&2&5&1&4\end{pmatrix} \to (1\ 3\ 5\ 4)(2)$

$\begin{pmatrix}1&2&3&4&5\\2&1&3&5&4\end{pmatrix} \to (1\ 2)(3)(4\ 5)$

$\begin{pmatrix}1&2&3&4&5\\1&2&3&4&5\end{pmatrix} \to (1)(2)(3)(4)(5)$

This notation is more appropriate for "powers" of permutations, (e.g. $p^3 = p\circ p\circ p$).

For example, if $p=(1\ 2\ 3)(4\ 5)$

then $p^3=(1)(2)(3)(4\ 5)$, $p^6=(1)(2)(3)(4)(5)$ (Why?)

6. BINARY OPERATIONS

Let S be a non-empty set. A <u>binary operation</u> $*$ on S is defined if

$$\boxed{x,y \in S \Rightarrow x*y \in S} \quad \text{for all } x,y \in S$$

(i.e. $x*y$ is another element of S)

EXAMPLES

- Addition $(+)$ on $\mathbb{R}$: for $x,y \in \mathbb{R}$, $x+y \in \mathbb{R}$
- Multiplication $(\cdot)$ on $\mathbb{R}$: for $x,y \in \mathbb{R}$, $x \cdot y \in \mathbb{R}$
- Operations $+,-$ on the set V of 3D vectors

  for $\vec{u},\vec{v} \in V$, $\vec{u}+\vec{v} \in V$ and $\vec{u}-\vec{v} \in V$
- Composition on functions:

  f, g functions, $f \circ g$ is a function
- An unusual operation $*$ may be given by a formula:

  For $m,n \in \mathbb{Z}$ we define $m*n = m+n+2$

  For example: $2*3=7$, $1*1=4$
- An unusual operation $*$ on a small set S may be given by a table:

  $S=\{a,b,c,d\}$

$*$	a	b	c	d
a	b	c	a	d
b	a	b	b	b
c	a	b	d	c
d	c	d	a	b

e.g. $a*b=c$

$b*a=a$

NOTICE In fact, a binary operation $*$ on S is a function $*: S \times S \to S$

Instead of $*(x,y)$ we write $x*y$

We also say that S is CLOSED under $*$ if

$$x,y \in S \Rightarrow x*y \in S$$

The concept of "CLOSURE" is mainly appropriate for subsets:

Let $*$ be a binary operation on S
T be a subset of S $(T \subseteq S)$
We say that T is CLOSED under $*$ if

$$x,y \in T \Rightarrow x*y \in T$$

EXAMPLE Consider the binary operation $+$ on $\mathbb{R}$

- $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ are closed under $+$

  e.g. $x,y \in \mathbb{N} \Rightarrow x+y \in \mathbb{N}$

- The subset $\bar{\mathbb{Q}}$ of irrational numbers is NOT CLOSED

  Indeed, $-\sqrt{2}, \sqrt{2} \in \bar{\mathbb{Q}}$ but $-\sqrt{2}+\sqrt{2} = 0 \notin \bar{\mathbb{Q}}$

- The subset $C = \{0,1,2,3\}$ in NOT CLOSED (Why?)

- The subset $A=\{2n \mid n\in\mathbb{Z}\}$ (even integers) is CLOSED:

  if $x=2n\in A$, $y=2m\in A$, $x+y=2n+2m=2(n+m)\in A$

- The subset $B=\{2n+1 \mid n\in\mathbb{Z}\}$ (odd integers) is NOT CLOSED:

  for example $3, 5 \in B$ but $3+5=8\notin B$.

➤ PROPERTIES OF BINARY OPERATIONS

For a binary operation $*$ on S, we say

(a) $*$ is COMMUTATIVE

if $\boxed{x*y = y*x}$ for all $x,y\in S$

(b) $*$ is ASSOCIATIVE

if $\boxed{(x*y)*z = x*(y*z)}$ for all $x,y,z\in S$

(c) an IDENTITY ELEMENT e exists

if $\boxed{x*e = x = e*x}$ for all $x\in S$

(d) each x in S has an INVERSE (or SYMMETRIC) x'

if $\boxed{x*x' = e = x'*x}$

(provided that an identity e exists)

NOTICE

- ASSOCIATIVITY in practice means that brackets are not necessary!

  $(x*y)*z$ and $x*(y*z)$ may be written $x*y*z$ since the operations can be performed in any order.

- COMMUTATIVITY in practice means that we can swap elements as we wish!

  e.g. $x*a*c*y*b = x*y*a*b*c$

- If $*$ is commutative

  $x*e = x$ is enough for the identity elt.

  $x*x' = e$ is enough for the inverse.

We prove two results

PROPOSITION 1

If an identity element exists it is UNIQUE

PROOF

Suppose that two distinct identities e_1, e_2 exist.

$e_1 * e_2 = e_1$ [since e_2 is an identity]

$e_1 * e_2 = e_2$ [since e_1 is an identity]

Hence $e_1 = e_2$, contradiction.

PROPOSITION 2 Suppose that $*$ is associative and e is the identity element in S
If x has an inverse, this is UNIQUE

PROOF Suppose that x' and x'' are two distinct inverses of x. Then

$$\begin{aligned} x' &= x'*e && \text{[since } e \text{ is the identity]} \\ &= x'*(x*x'') && \text{[since } x*x''=e\text{]} \\ &= (x'*x)*x'' && \text{[associativity]} \\ &= e*x'' && \text{[since } x'*x=e\text{]} \\ &= x'' && \text{[since } e \text{ is the identity]} \end{aligned}$$

That is $x'=x''$, contradiction!

EXERCISE We define $x*y=x+y+3$ on $\mathbb{R}$

(a) Is $*$ COMMUTATIVE?

$x*y=x+y+3=y+x+3=y*x$ YES!

(b) Is $*$ ASSOCIATIVE?

$(x*y)*z=(x+y+3)*z=x+y+z+6$
$x*(y*z)=x*(y+z+3)=x+y+z+6$ YES!

(c) Is there an IDENTITY element e? (we solve for e)

$x*e=x \Leftrightarrow x+e+3=x \Leftrightarrow e=-3$
Clearly $e*x=x$ as well. IDENTITY: $\boxed{e=-3}$

(d) What is the INVERSE of $x\in\mathbb{R}$? (we solve for x')

$x*x'=e \Leftrightarrow x+x'+3=-3 \Leftrightarrow x'=-x-6$
Clearly $x'*x=e$ as well. INVERSE OF x: $\boxed{x'=-x-6}$
