

International Baccalaureate

MATHEMATICS HL

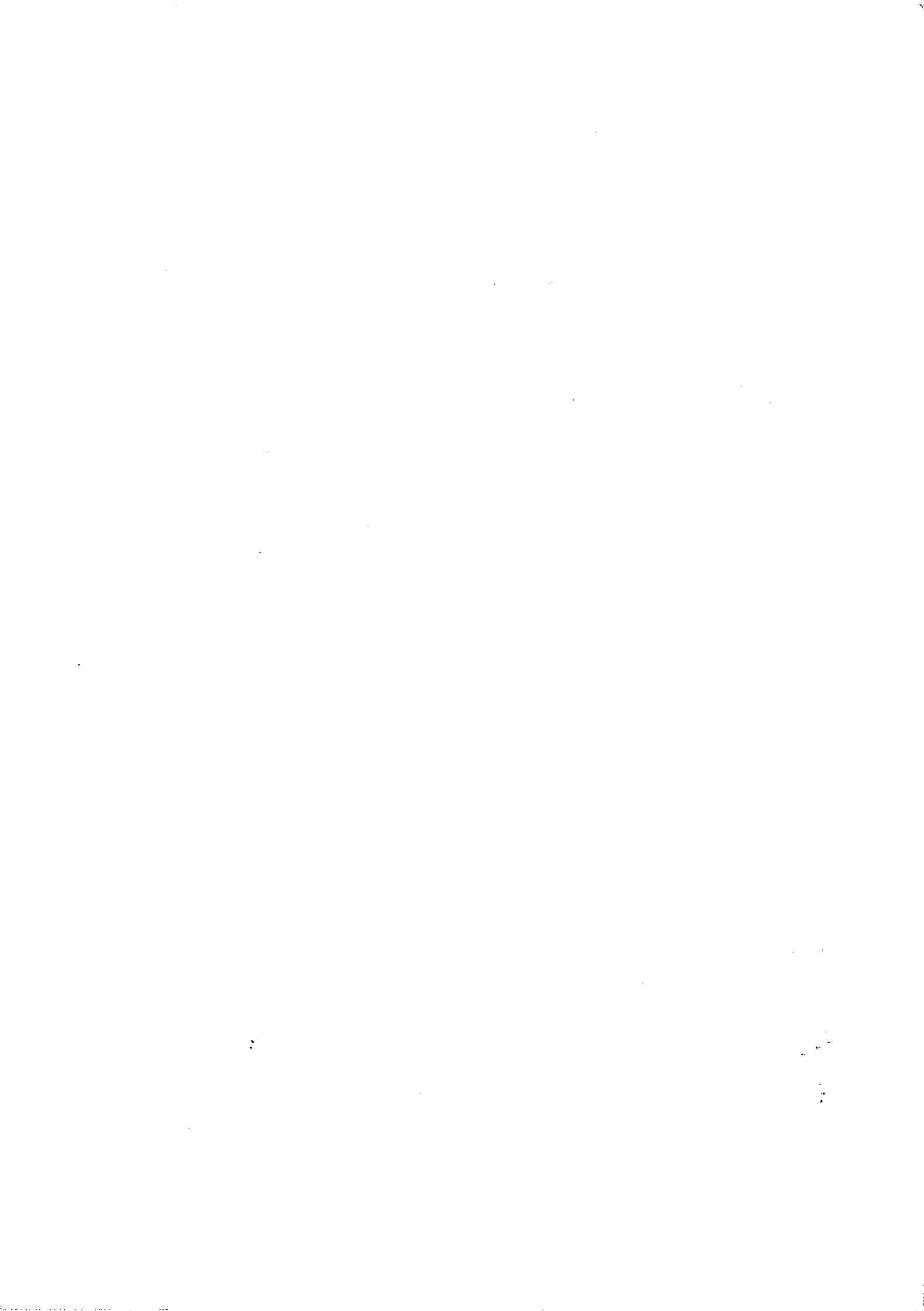
OPTION: Sets, Relations and Groups

Lecture Notes

by

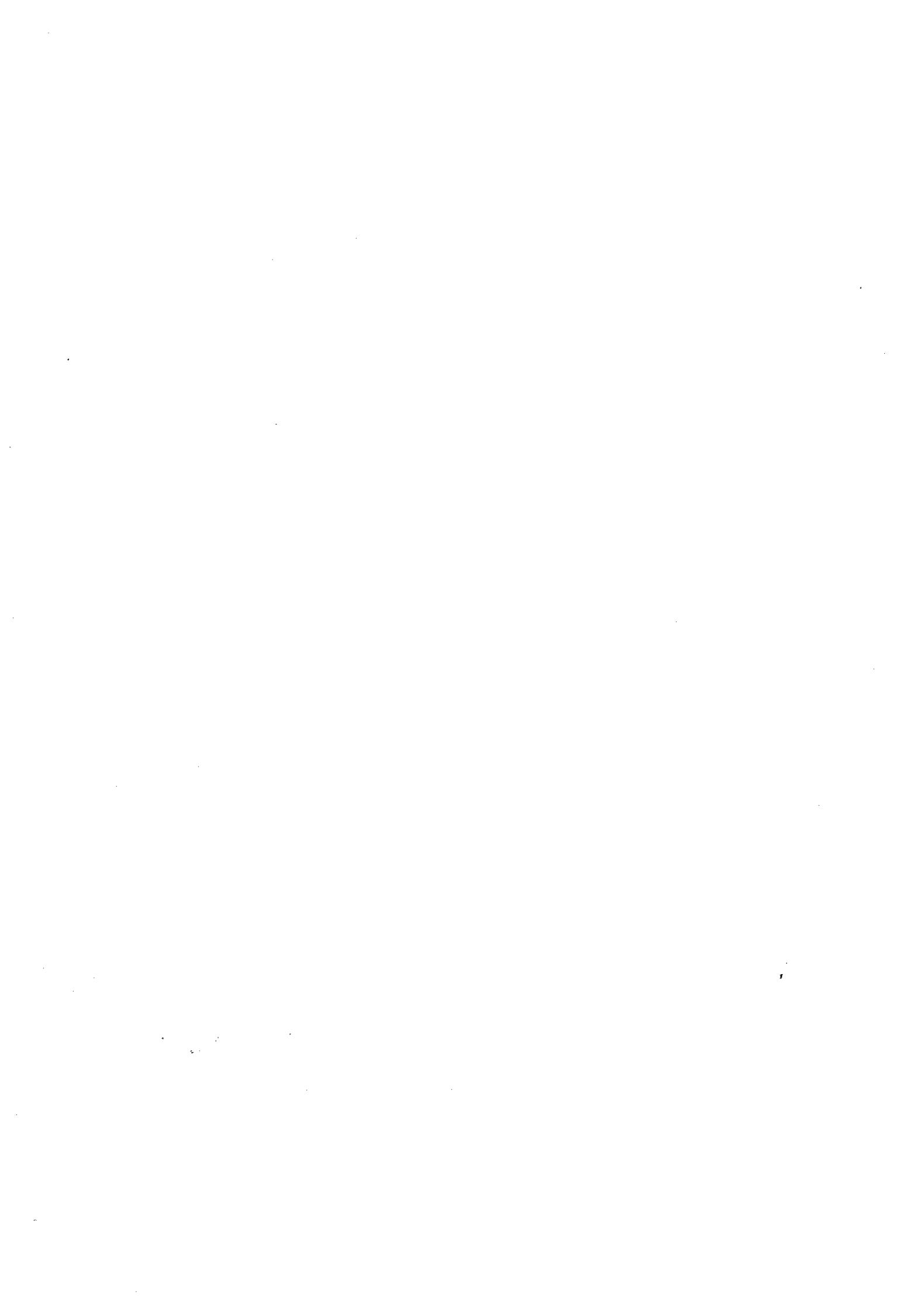
Christos Nikolaidis

January 2015



CONTENTS

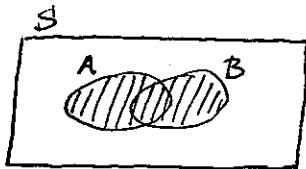
1. SETS	1
Basic operations - Venn diagrams	
Laws of sets	
2. CARTESIAN PRODUCT $A \times B$ - RELATIONS	8
Relations on a set A	
Properties of relations	
3. EQUIVALENCE RELATIONS	19
Equivalence class - Partition	
The equivalence relation $a \equiv b \pmod{n}$	
4. FUNCTIONS	26
Injection - Surjection - Bijection	
Functions of two variables	
5. THE SET OF PERMUTATIONS S_n	37
6. BINARY OPERATIONS	42
7. GROUPS	47
Finite groups, Infinite groups, $(\mathbb{Z}_n, +)$, (\mathbb{Z}_p^*, \cdot)	
8. SUBGROUPS - LAGRANGE THEOREM	56
Cyclic groups, order of G, order of a in G.	
9. COSETS	69
10. HOMOMORPHISMS	73
Isomorphism, kernel, range	



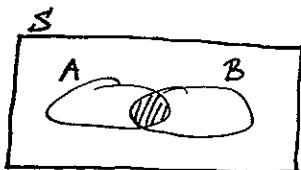
1. SETS

► BASIC OPERATIONS (USING VENN DIAGRAMS)

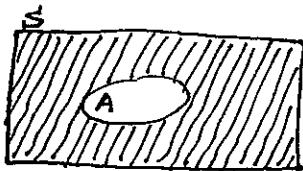
We already know:



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

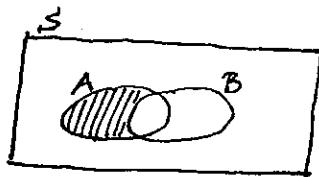


INTERSECTION $A \cap B$ (A and B)



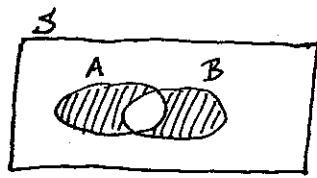
COMPLEMENT A' (not A)

We also define:



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

Notice that $A - B = A \cap B'$



SYMMETRIC DIFFERENCE $A \Delta B$

(A or B but not both)

Notice that

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

or

$$A \Delta B = (A - B) \cup (B - A)$$

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

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

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

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

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

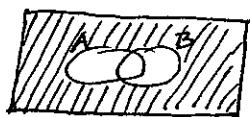
$$A \Delta B = \{2, 3, 6\}$$

► USE OF VENN DIAGRAMS

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

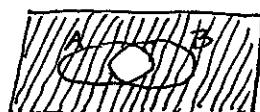
EXAMPLE Show that $(A \cup B)' \neq A' \cup B'$

LHS:



$$(A \cup B)'$$

RHS:



$$A' \cup B'$$

In fact

$$\begin{array}{|c|} \hline (A \cup B)' = A' \cap B' \\ \hline (A \cap B)' = A' \cup B' \\ \hline \end{array}$$

De Morgan Laws

We can easily verify these laws by Venn Diagrams

► PROPERTIES OF SET OPERATIONS (LAWS)

$$\textcircled{1} \quad A \cup B = B \cup A \quad (\text{COMMUTATIVE LAWS})$$

$$A \cap B = B \cap A$$

$$\textcircled{2} \quad (A \cap B) \cap C = A \cap (B \cap C) \quad (\text{ASSOCIATIVE LAWS})$$

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

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!

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \quad (\text{DISTRIBUTIVE LAWS})$$

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

(4) Notice also the following properties:

$$A \cap A' = \emptyset$$

$$A \cap \emptyset = \emptyset$$

$$A \cap S = A$$

$$A \cup A' = S$$

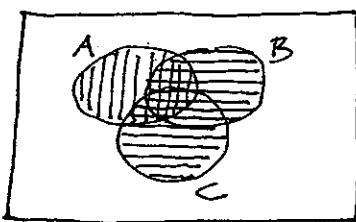
$$A \cup \emptyset = A$$

$$A \cup S = S$$

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

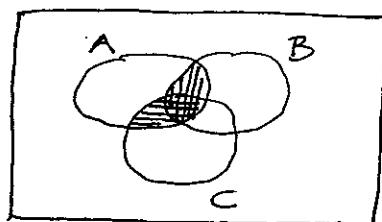
EXAMPLE Let us verify the first distributive law
 $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
by using Venn diagrams.

LHS:



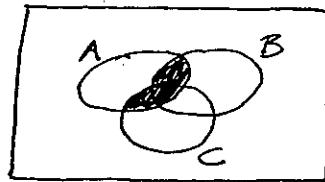
$$A \cap (B \cup C) \\ \equiv$$

RHS:



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

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: $A-B = A \cap B'$ $\textcircled{*}$

Indeed, $(A-B) \cap (B-A) = (A \cap B') \cap (B \cap A')$ [by $\textcircled{*}$]

$$= A \cap B' \cap B \cap A' \quad [\text{Associative Law}]$$

$$= A \cap A' \cap B \cap B' \quad [\text{Commutative Law}]$$

$$= \emptyset \cap \emptyset$$

$$= \emptyset$$

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)

$$\begin{aligned} LHS &= (A - B) \cup (B - A) = (A \cap B') \cup (B \cap A') \quad [\text{by } *] \\ &= (A \cup B) \cap (A \cup A') \cap (B' \cup B) \cap (B' \cap A') \quad [\text{by Distributive Law}] \\ &= (A \cup B) \cap S \cap S \cap (A' \cup B') \quad [S \rightarrow \text{universal set}] \\ &= (A \cup B) \cap (A' \cup B') \\ &= (A \cup B) \cap (A \cap B)' \quad [\text{by De Morgan}] \\ &= (A \cup B) - (A \cap B) \quad [\text{by } *] \\ &= RHS \end{aligned}$$

► PROOFS BY INCLUSION

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

$$A \subseteq B \quad (x \in A \Rightarrow \dots \Rightarrow x \in B)$$

$$\text{and } B \subseteq A \quad (x \in B \Rightarrow \dots \Rightarrow x \in A)$$

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 $x \in B \cup C$

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

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

$$\Rightarrow x \in A \cap B \text{ or } x \in A \cap C$$

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

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 "

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

$$\Leftrightarrow x \notin A \text{ and } x \notin B$$

$$\Leftrightarrow x \in A' \text{ and } x \in B'$$

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

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

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

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

$$\Rightarrow x \in A \text{ and } x \notin B \text{ and } x \in B \text{ and } x \notin A$$

$$\Rightarrow x \in A \text{ and } x \notin A \text{ and } x \in B \text{ and } x \notin B$$

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)

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

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

$$\Rightarrow \begin{cases} \text{either } x \in B \text{ (and } x \in A) \text{ so } x \in A \cap B \\ \text{or } x \in C \end{cases}$$

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

► NUMBER OF SUBSETS

Let A be a set; a subset B consists of some, none or all elements of A .

We write

$$B \subseteq A$$

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

we obtain the following subsets:

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

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

$$\begin{aligned} \text{TOTAL NUMBER} &= \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \dots + \binom{n}{n} = (1+1)^n \quad [\text{binomial thm}] \\ &= 2^n \end{aligned}$$

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

- Let A and B be two sets

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

An example will clarify the definition

EXAMPLE 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

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

(since for example $(a, 1) \neq (1, a)$)

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

$$\text{EXAMPLE} \quad A \times (B \cap C) = (A \times B) \cap (A \times C)$$

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

$$\begin{aligned} (x, y) \in \text{LHS} &\Leftrightarrow (x, y) \in A \times (B \cap C) \\ &\Leftrightarrow x \in A \text{ and } y \in B \cap C \\ &\Leftrightarrow x \in A \text{ and } y \in B \text{ and } y \in C \\ &\Leftrightarrow (x, y) \in A \times B \text{ and } (x, y) \in A \times C \\ &\Leftrightarrow (x, y) \in (A \times B) \cap (A \times C) \\ &\Leftrightarrow (x, y) \in \text{RHS} \end{aligned}$$

In exactly the same way we can show that
 $A \times (B \cup C) = (A \times B) \cup (A \times C)$

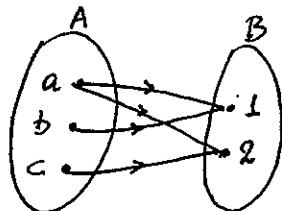
► RELATIONS FROM A TO B

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

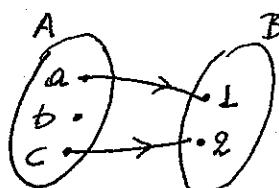
$$(a) R = \{(a, 1), (a, 2), (b, 1), (c, 2)\}$$



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 $b \not R 2$

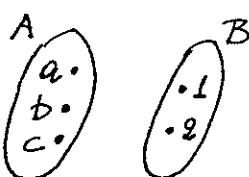
$$(b) S = \{(a, 1), (c, 2)\}$$



(only
 $aS1$
 $cS2$)

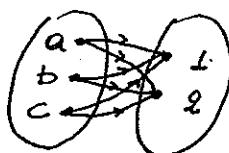
$$(c) T = \emptyset$$

"empty relation"



(It is the
 most "rigid"
 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 $aR1$ & $bR2$
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

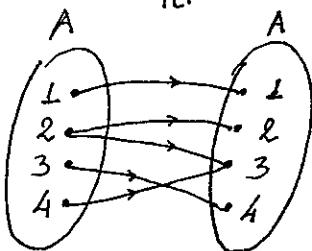
$$A = \{1, 2, 3, 4\}$$

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:

$R:$



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

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

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

$$T = R \cup S$$

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

Let us also see the corresponding matrices

<u>R</u>	<u>1</u> <u>2</u> <u>3</u> <u>4</u>
1	1 0 0 0
2	0 1 0 0
3	0 0 1 0
4	0 0 0 1

\downarrow
the relation

=

<u>S</u>	<u>1</u> <u>2</u> <u>3</u> <u>4</u>
1	0 1 1 1
2	0 0 1 1
3	0 0 0 1
4	0 0 0 0

\downarrow
the relation

<

<u>T</u>	<u>1</u> <u>2</u> <u>3</u> <u>4</u>
1	1 1 1 1
2	0 1 1 1
3	0 0 1 1
4	0 0 0 1

\downarrow
the relation

\leq

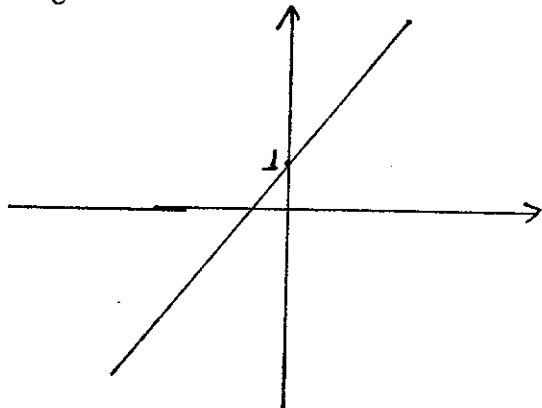
[You see, instead of $(1,2) \in <$ we usually write $1 < 2$.]

► 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.

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

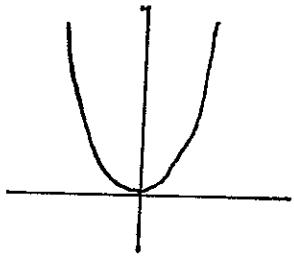


i.e. this relation consists of all pairs (x,y)
that satisfy $y = 2x + 1$.

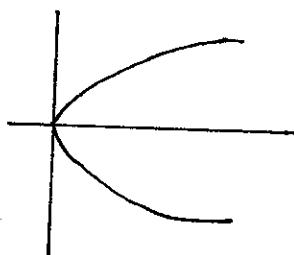
In that sense, all functions you already
know are relations!

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

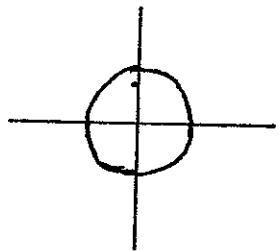
- $xRy \Leftrightarrow y = x^2$



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

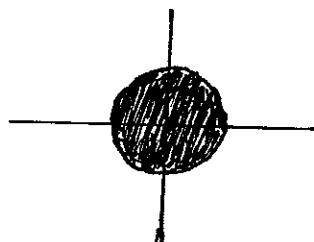


- $xRy \Leftrightarrow x^2 + y^2 = 1$



i.e. unit circle

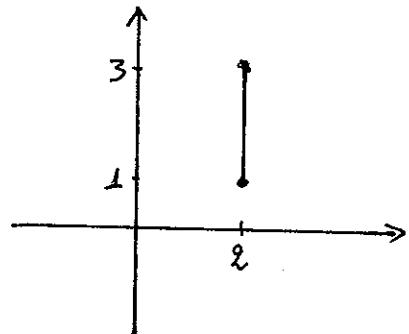
$$xRy \Leftrightarrow x^2 + y^2 \leq 1$$



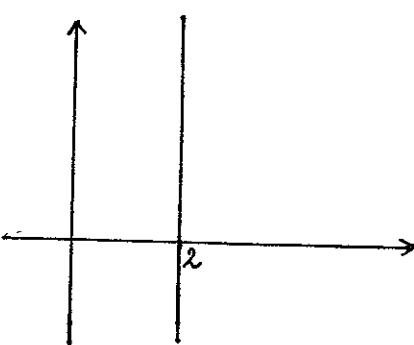
i.e. circular disk
of radius 1

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

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

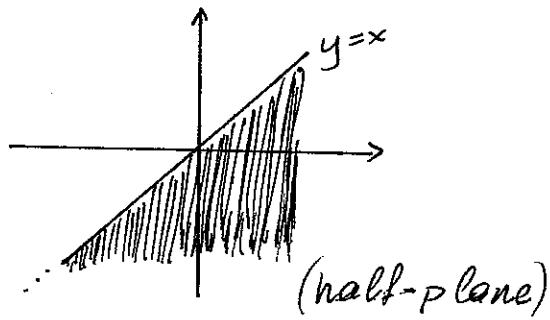


segment

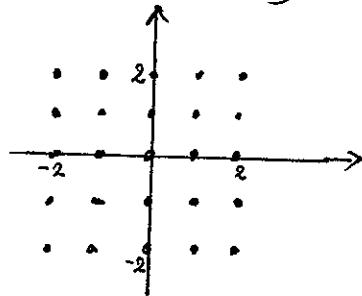


line $x = 2$

- $xRy \Leftrightarrow x > y$



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



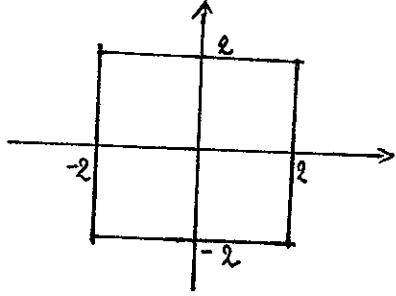
(for $y \leq ax+b$ or $y \geq ax+b$, you draw $y = ax+b$ and pick a point outside the line to see which half-plane to shade)

- 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.

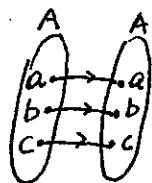
► PROPERTIES OF RELATIONS ON A

The relation R on a set A is said to be

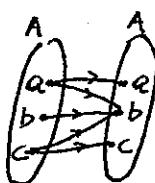
- REFLEXIVE if $(a,a) \in R$ for all $a \in A$
- SYMMETRIC if $(a,b) \in R \Rightarrow (b,a) \in R$
- TRANSITIVE if $(a,b) \in R$ and $(b,c) \in R \Rightarrow (a,c) \in R$

In other words

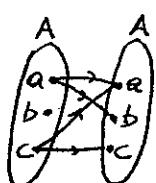
REFLEXIVE means that aRa for all a
i.e. every element is related to itself.



reflexive



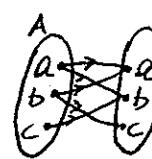
reflexive



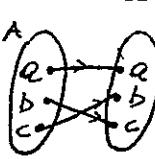
not reflexive
since bRb

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

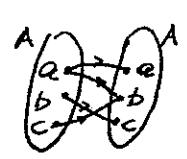
SYMMETRIC means that aRb implies that also bRa
i.e. whenever a is related to b we observe that b is also related to a.



symmetric



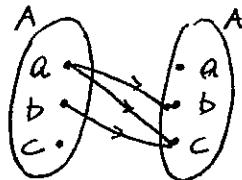
symmetric



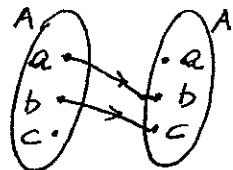
not symmetric

(aRb)
 bRa

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 $3 \neq 1$
 (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. (\nwarrow)
- 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 $bR_2'a$)

TRANSITIVITY is more difficult to check!
We can see though that R_1 is not transitive
since bR_1a, aR_1b but $bR_1'b$.

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 $A = \{1, 2, 3, \dots, 100\}$

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 $bRc \Rightarrow \dots \stackrel{\text{(similar process)}}{\dots} \Rightarrow aRc$

► 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 EQUIVALENCE CLASS 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 $[a] = \{x \in A \mid x \sim a\}$

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:

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

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: $a \sim b \Rightarrow a - b \text{ is even}$
 $\Rightarrow b - a \text{ is even}$
 $\Rightarrow b \sim a$
- TRANSITIVE: $a \sim b$ and $b \sim c$
 $\Rightarrow a - b \text{ is even, } b - c \text{ is even}$
 $\Rightarrow (a - b) + (b - c) \text{ is even}$
 $\Rightarrow a - c \text{ is even}$
 $\Rightarrow a \sim c$

The equivalence class of 1 is

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

The equivalence class of 2 is

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

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 $A_1, A_2, A_3, \dots, A_n$

an equivalence relation is automatically defined

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

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

The equivalence classes are the subsets A_1, A_2, \dots

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

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

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:

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

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

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:

$$\begin{aligned}a \equiv b \pmod{n} &\Rightarrow a-b \text{ is divisible by } n \\&\Rightarrow b-a \text{ is divisible by } n \\&\Rightarrow b \equiv a \pmod{n}\end{aligned}$$

• TRANSITIVE:

$$\begin{aligned}a \equiv b \pmod{n} \text{ and } b \equiv c \pmod{n} &\Rightarrow a-b \text{ and } b-c \text{ are divisible by } n \\&\Rightarrow (a-b)+(b-c) \text{ is divisible by } n \\&\Rightarrow a-c \text{ is divisible by } n \\&\Rightarrow a \equiv c \pmod{n}\end{aligned}$$

There are n equivalence classes.

An example will clarify the concept!

EXAMPLE The equivalence relation

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

determines the following equivalence classes:

$$[0] = \{\dots, 0, 5, 10, \dots\} = \{5k \mid k \in \mathbb{Z}\} \quad (\text{multiples of } 5)$$

$$[1] = \{\dots, 1, 6, 11, \dots\} = \{5k+1 \mid k \in \mathbb{Z}\}$$

$$[2] = \{\dots, 2, 7, 12, \dots\} = \{5k+2 \mid k \in \mathbb{Z}\}$$

$$[3] = \{\dots, 3, 8, 13, \dots\} = \{5k+3 \mid k \in \mathbb{Z}\}$$

$$[4] = \{\dots, 4, 9, 14, \dots\} = \{5k+4 \mid k \in \mathbb{Z}\}$$

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 ,

$$\text{i.e. } \begin{cases} a = 5k_1 + r \\ b = 5k_2 + r \end{cases} \Rightarrow a - b = 5k_1 - 5k_2 = 5(k_1 - k_2)$$

$\Rightarrow a - b$ 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

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

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

let's define $a \sim b \Leftrightarrow a^2 \equiv b^2 \pmod{5}$

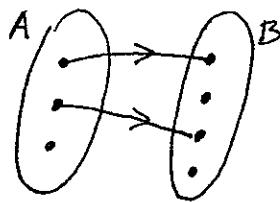
It is easy to check that \sim is an equiv. relation

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

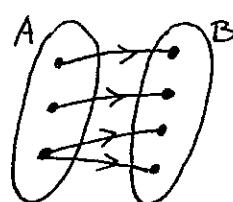
A. FUNCTIONS

Some relations from A to B are called FUNCTIONS:

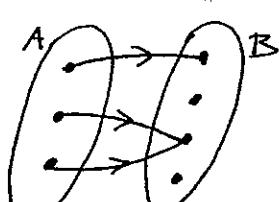
if each element of A corresponds to a unique element of B



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

$$f: A \rightarrow B$$

Instead of $(a, b) \in f$ or $a f b$ (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

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

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

For a function $f: A \rightarrow B$

A is called DOMAIN

B is called CODOMAIN

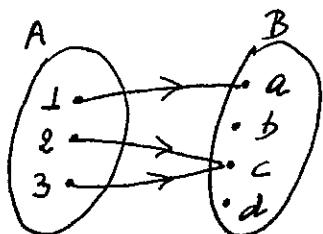
If $f(a)=b$, we say that b is the image of a

The set of all images is a subset of B ;

it is called RANGE of f .

It is denoted by $f(A)$.

EXAMPLE $f: A \rightarrow B$



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

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

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

EXAMPLE $f: \mathbb{R} \rightarrow \mathbb{R}$ 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

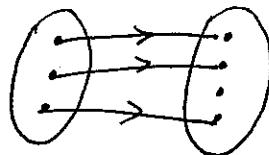
$$f(\mathbb{R}) = \{y \mid y \geq 0\}$$

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

$$f(x_1) = f(x_2) \Rightarrow x_1^2 = x_2^2 \Rightarrow x_1 = \pm x_2 \quad (\text{so } \nRightarrow x_1 = x_2)$$

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".

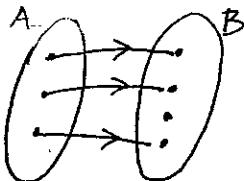
► "ONTO" OR SURJECTION

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

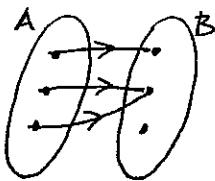
if $\text{RANGE} = \text{CODOMAIN}$

i.e $f(A) = B$

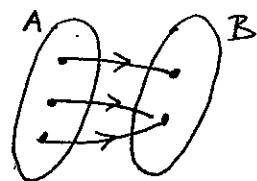
i.e every element of B is an image
(of some element of A)



not onto



not onto



onto

(Why?)

EQUIVALENT DEFINITION:

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

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

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

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

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

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

This explanation is enough! However, let us see

the equivalent definition:

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

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

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

EXAMPLE $f: \mathbb{Z} \rightarrow \mathbb{Z}$, $f(n) = n+1$. 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 $f: \mathbb{Z} \rightarrow \mathbb{Z}$ $f(n) = 3n+1$. 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 not always in \mathbb{Z} .

Again, a counterexample helps:

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

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

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

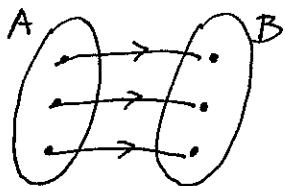
Indeed, $m=0$ is not an image of some $n \in \mathbb{N}$

NOTICE: It would be onto if it was given as

$$f: \mathbb{N} \rightarrow \mathbb{N}^*, f(n) = n+1. \quad (\text{why?})$$

► "1-1" AND "ONTO" OR BIJECTION

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



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

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

NOTICE: 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} .

EXAMPLE: $f: \mathbb{R} \rightarrow \mathbb{R}$, $f(x) = 3x + 5$

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

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

$$f: A \rightarrow B, \quad f(x) = \frac{3x+1}{x-2}$$

- 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 $f^{-1}: B \rightarrow A$

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

► FUNCTIONS OF TWO VARIABLES

(a) We may have functions of the form

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

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

(b) We may have functions of the form

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

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

EXAMPLE (OF A BIJECTION)

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

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

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

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

$$\Rightarrow \begin{cases} 2x_1 + y_1 = 2x_2 + y_2 & (1) \\ x_1 + 2y_1 = x_2 + 2y_2 & (2) \end{cases}$$

$$(1) - 2(2) : -3y_1 = -3y_2 \Rightarrow y_1 = y_2$$

Then

$$(1) \text{ gives } x_1 = x_2$$

$$\text{Hence } (x_1, y_1) = (x_2, y_2).$$

- f is "onto":

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

$$\begin{aligned} (2x+y, x+2y) = (a, b) &\Leftrightarrow 2x+y = a \quad (1) \\ &\quad x+2y = b \quad (2) \end{aligned}$$

$$2(1)-(2): 3x = 2a - b \Rightarrow x = \frac{2a-b}{3}$$

$$2(2)-1: 3y = 2b - a \Rightarrow y = \frac{2b-a}{3}$$

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

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

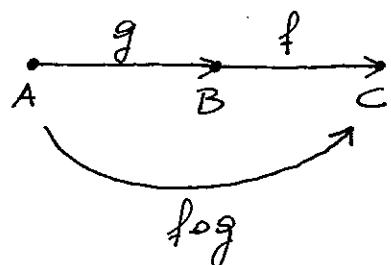
We can easily verify that

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

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

► PROOFS FOR $f \circ g$

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



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

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

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

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:

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

(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 $a \in A$, s.t. $g(a) = b$ [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:

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

(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. $f(b) = f(g(a)) = c$.

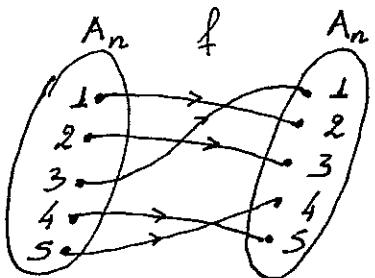
5. THE SET OF PERMUTATIONS: S_n

► IN GENERAL

Consider the set $A_n = \{1, 2, 3, \dots, n\}$

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

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

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

- 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

$$\begin{aligned} 1 &\mapsto 1 \mapsto 3 \\ 2 &\mapsto 3 \mapsto 2 \\ 3 &\mapsto 2 \mapsto 1 \end{aligned}$$

Therefore,

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

EXAMPLE: Similarly if 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

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

- 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

$$\boxed{\begin{aligned} e \circ f &= f \\ f \circ e &= f \end{aligned}}$$

and

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

NOTICE: These properties hold in general in 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:

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

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

In fact, σ_1 permutes 1,2,3 cyclically: $\boxed{\begin{matrix} 1 & 2 \\ 2 & 3 \end{matrix}}$
 σ_2 does the same twice
 and τ_1 keeps 1, interchanges 2 and 3: $\boxed{\begin{matrix} 1 \\ 2 & 3 \end{matrix}}$
 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	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. $\underbrace{1 \rightarrow 2 \rightarrow 3}_{\curvearrowright} \quad \underbrace{4 \rightarrow 5}_{\curvearrowright}$

In this way any permutation can be expressed in disjoint cycles

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

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

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

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

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 binary operation * on S is defined if

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

(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 $+, -, \cdot$ 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 $*: S \times S \rightarrow S$
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 $\overline{\mathbb{Q}}$ of irrational numbers is NOT CLOSED
Indeed, $-\sqrt{2}, \sqrt{2} \in \overline{\mathbb{Q}}$ but $-\sqrt{2} + \sqrt{2} = 0 \notin \overline{\mathbb{Q}}$
- The subset $C = \{0, 1, 2, 3\}$ is NOT CLOSED (Why?)

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

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

- The subset $B = \{2n+1 | n \in \mathbb{Z}\}$ (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
$$x * y = y * x \quad \text{for all } x, y \in S$$

- (b) $*$ is ASSOCIATIVE

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

- (c) an IDENTITY ELEMENT e exists

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

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

if
$$x * x' = e = x' * x$$

(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.

$$e_1 * e_2 = e_1 \quad [\text{since } e_2 \text{ is an identity}]$$

$$e_1 * e_2 = e_2 \quad [\text{since } e_1 \text{ is an identity}]$$

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

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

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

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

(a) Is $*$ COMMUTATIVE?

$$x*y = x+y+3 = y+x+3 = y*x \quad \text{YES!}$$

(b) Is $*$ ASSOCIATIVE?

$$\begin{aligned}(x*y)*z &= (x+y+3)*z = x+y+z+6 \\x*(y*z) &= x*(y+z+3) = x+y+z+6\end{aligned} \quad \text{YES!}$$

(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: $e = -3$

(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 : $x' = -x-6$

7. GROUPS

Let G be a set

* be a binary operation on G

DEFINITION: G is a GROUP under *
or simply $(G, *)$ is a GROUP if

(a) G is CLOSED under * : $a, b \in G \Rightarrow a * b \in G$.

(b) * is ASSOCIATIVE:

$$(a * b) * c = a * (b * c) \text{ for all } a, b, c \in G$$

(c) an IDENTITY element e exists:

$$a * e = a = e * a \quad \text{for all } a \in G$$

(d) each element a has an INVERSE a'

$$a * a' = e = a' * a$$

Furthermore, if

(e) * is COMMUTATIVE:

$$a * b = b * a \quad \text{for all } a, b \in G$$

we say that G is an ABELIAN (or COMMUTATIVE) GROUP

EXAMPLE \mathbb{I} , \mathbb{R} and \mathbb{Z} are (Abelian) groups under +

(a) CLOSURE is obvious for addition +

(b) ASSOCIATIVITY : $(a + b) + c = a + (b + c)$ for all a, b, c

(c) IDENTITY = 0 : $a + 0 = a = 0 + a$ for all a

(d) INVERSE of a : $a' = -a$ since $a + (-a) = 0 = (-a) + a$

(e) COMMUTATIVITY : $a + b = b + a$ for all a, b

EXAMPLE \mathbb{N} is not a group under $+$

Properties (a),(b),(c),(e) hold. Identity = 0

However (d) does not hold

e.g. 2 has no inverse ($-2 \notin \mathbb{N}$)

EXAMPLE \mathbb{R}^* and \mathbb{Q}^* are (abelian) groups under \cdot

(a) CLOSURE is obvious for multiplication.

(b) ASSOCIATIVITY holds : $(ab)c = a(bc)$

(c) IDENTITY = 1 : $a \cdot 1 = a = 1 \cdot a$ for all a .

(d) INVERSE of a : $a' = a^{-1} = \frac{1}{a}$ since $a a' = 1 = a' a$

(e) COMMUTATIVITY is known for \cdot : $a b = b a$ for all a, b .

NOTICE \mathbb{R}, \mathbb{Q} are not groups under \cdot

since 0 has no inverse.

$\mathbb{Z}^*, \mathbb{N}^*$ are not groups

e.g. 2 has no inverse (as $2^{-1} \notin \mathbb{Z}^*$, $2^{-1} \notin \mathbb{N}^*$)

REMARK

If the operation is $+$ (ADDITION)

the inverse of a is $-a$ (the opposite)

If the operation is \cdot (MULTIPLICATION)

the inverse of a is a^{-1} (inverse indeed!!!)

In general, we assume that an operation $*$ behaves as multiplication; the inverse is denoted a^{-1}

EXAMPLE $G = \text{all bijections } f: \mathbb{R} \rightarrow \mathbb{R}$ ("1-1" and "onto")

G is a group under composition \circ .

(a) CLOSURE : f, g bijections $\Rightarrow f \circ g$ bijection

(b) ASSOCIATIVITY holds: $(f \circ g) \circ h = f \circ (g \circ h)$

(c) IDENTITY is the identity function I with $I(x) = x$
since $f \circ I = f = I \circ f$

(d) The INVERSE of $f \in G$ is the inverse function f^{-1}

since $f \circ f^{-1} = I = f^{-1} \circ f$

The group G is NOT ABELIAN since

$f \circ g \neq g \circ f$ in general.

DETAILED PROOFS:

Mind that $f = g$ means $f(x) = g(x)$ for any x

$$(b) \text{ LHS: } [(f \circ g) \circ h](x) = (f \circ g)(h(x)) = f(g(h(x))) \Rightarrow \text{LHS} = \text{RHS}$$

$$\text{RHS: } [f \circ (g \circ h)](x) = f((g \circ h)(x)) = f(g(h(x)))$$

$$(c) (f \circ I)(x) = f(I(x)) = f(x) \Rightarrow f \circ I = f$$

$$(I \circ f)(x) = I(f(x)) = f(x) \Rightarrow I \circ f = f$$

Property (d) is known by the definition of f^{-1}

PROPOSITION (Left and Right cancellation)

In a group $(G, *)$

$$(1) \quad a * x = a * y \Rightarrow x = y$$

$$(2) \quad x * a = y * a \Rightarrow x = y$$

PROOF

(1) We "multiply" by a^{-1} from the left:

$$a * x = a * y \Rightarrow a^{-1} * (a * x) = a^{-1} * (a * y)$$

$$\Rightarrow (a^{-1} * a) * x = (a^{-1} * a) * y \quad [\text{ASSOCIATIVITY}]$$

$$\Rightarrow e * x = e * y \quad [\text{INVERSE}]$$

$$\Rightarrow x = y \quad [\text{IDENTITY}]$$

(2) We "multiply" by a^{-1} from the right

Similar proof.

For example,

$$\text{in addition} \quad a + x = a + y \Rightarrow x = y$$

$$\text{in multiplication} \quad a x = a y \Rightarrow x = y \quad (a \neq 0)$$

$$\text{in composition} \quad f \circ g = f \circ h \Rightarrow g = h$$

$$g \circ f = h \circ f \Rightarrow g = h$$

► FINITE GROUPS

They are usually given by a table

EXAMPLE: Let $G = \{e, a, b\}$ and * given by

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

(a) CLOSURE : The results are e,a,b (belong to G)

(b) ASSOCIATIVITY is usually given in such a case;

it is time-consuming to verify for all possible triads

(c) IDENTITY is e : row and column of e unchanged

(d) INVERSE : inverses meet at e, thus

inverse of e is e

inverse of a is b (i.e. $a^{-1}=b$)

inverse of b is a ($b^{-1}=a$)

(e) COMMUTATIVITY : The table is symmetric about the main diagonal.

Therefore, $(G, *)$ is an abelian group

NOTICE:

- The table of a group is called CAYLEY TABLE
- The table must be a LATIN SQUARE i.e.
"every element appears exactly once in each row and each column"

(Why? use the fact $ax=ay \Rightarrow x=y$)

► UNUSUAL BINARY OPERATIONS

EXAMPLE: We define $*$ on \mathbb{R} by

$$x * y = x + y + 3$$

(a) CLOSURE is obvious

We have already seen in page 46 that

(b) ASSOCIATIVITY holds

(c) The IDENTITY element is $e = -3$

(d) The INVERSE of x is $x' = -x - 6$

(e) $*$ is COMMUTATIVE

Hence $(\mathbb{R}, *)$ is a group

EXAMPLE: We define $*$ on \mathbb{R} by

$$x * y = \frac{xy}{x+y}$$

Show that (i) $*$ is COMMUTATIVE

(ii) $*$ is ASSOCIATIVE

(iii) $(\mathbb{R}, *)$ is not a group.

$$(i) \text{ Trivial: } x * y = \frac{xy}{x+y} = \frac{yx}{y+x} = y * x$$

$$(ii) (x * y) * z = \left(\frac{xy}{x+y} \right) * z = \frac{\frac{xy}{x+y} \cdot z}{\frac{xy}{x+y} + z} = \frac{\frac{x y z}{x+y}}{\frac{xy+yz(x+y)}{x+y}} = \frac{x y z}{x y + y z + z x}$$

$x * (y * z)$ gives the same result (similarly)

$$(iii) \text{ If IDENTITY} = e, \quad x * e = x \Leftrightarrow \frac{xe}{x+e} = x \Leftrightarrow xe = x^2 + ex \Leftrightarrow x^2 = 0 \Leftrightarrow x = 0$$

We should find some error. Thus $(\mathbb{R}, *)$ is not a group.

► ADDITION AND MULTIPLICATION modulo n

Let us work with modulus 5

Remember the relation $a \equiv b \pmod{5}$

Equivalence classes $[0], [1], [2], [3], [4]$

Notice that $[2] + [3] = [5] = [0]$

$$\text{since } (5k+2) + (5l+3) = 5(k+l+1) = 5n \in [0]$$

Similarly $[2] \cdot [3] = [6] = [1]$

$$\begin{aligned} \text{since } (5k+2) \cdot (5l+3) &= 25kl + 15k + 10l + 6 \\ &= 5(5kl + 3k + 2l + 1) + 1 \\ &= 5n + 1 \in [1] \end{aligned}$$

We can easily complete the following tables
which demonstrate addition (+) and multiplication (.)

on $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ ← forget the brackets $[,]$
for simplicity

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

•	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

(we just divide each result by 5 to find the remainder)

- (a) CLOSURE obvious
- (b) ASSOCIATIVITY: known
- (c) IDENTITY = 0
- (d) INVERSE: $0' = 0, 1' = 4, 2' = 3, 3' = 2, 4' = 1$

(\mathbb{Z}_5, \circ) is not a group.

But for $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$, (\mathbb{Z}_5^*, \circ) is a group

•	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

- (a) CLOSURE is obvious
- (b) ASSOCIATIVITY is known
- (c) IDENTITY = 1
- (d) INVERSE: $1' = 1, 2' = 3, 3' = 2, 4' = 4$

Both $(\mathbb{Z}_5, +)$ and (\mathbb{Z}_5^*, \circ) are abelian groups.

In general, for $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$

- $(\mathbb{Z}_n, +)$ is always a group
- (\mathbb{Z}_n^*, \circ) is not always a group
 (\mathbb{Z}_p^*, \circ) is a group $\Leftrightarrow p$ is prime

for example, for $\mathbb{Z}_4 = \{0, 1, 2, 3\}$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

is a group

	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

is not a group.

Indeed, if n is not a prime, say $n = u \cdot k$ $u, k \neq 1$

Then $[u] \cdot [k] = [n] = [0]$ which does not lie in \mathbb{Z}_n^*

► SOME THEORETICAL RESULTS

In a group $(G, *)$ [we denote a' by a^{-1}]

■ $(a^{-1})^{-1} = a$

Indeed, the definition $a * a^{-1} = e = a^{-1} * a$ implies that the inverse of a^{-1} is a

■ $(a * b)^{-1} = b^{-1} * a^{-1}$

It suffices to show that the inverse of $a * b$ is $b^{-1} * a^{-1}$. Indeed,

$$(a * b) * (b^{-1} * a^{-1}) = a * b * b^{-1} * a^{-1} = a * e * a^{-1} = a * a^{-1} = e.$$

Similarly $(b^{-1} * a^{-1}) * (a * b) = e$

■ $a * x = b \Rightarrow x = a^{-1} * b$

Indeed, $a * x = b \Rightarrow a^{-1} * (a * x) = a^{-1} * b$
 $\Rightarrow (a^{-1} * a) * x = a^{-1} * b$
 $\Rightarrow e * x = a^{-1} * b$
 $\Rightarrow x = a^{-1} * b$

■ $a^2 = e \Leftrightarrow a = a^{-1}$ (self-inverse)

We just "multiply" by a^{-1}

$$a^2 = e \Leftrightarrow a^2 * a^{-1} = e * a^{-1} \Leftrightarrow a * a * a^{-1} = a^{-1} \Leftrightarrow a = a^{-1}$$

NOTICE: a^n means $a * a * \dots * a$ (n times)

(But for + $a^n = a + a + \dots + a = n a$)

8. SUBGROUPS - LAGRANGE THEOREM

Let $(G, *)$ be a group and $H \subseteq G$ (subset)

H is a SUBGROUP of G , if $(H, *)$ is also a group

In fact, in order to show that H is a subgroup of G , we use

H is a SUBGROUP of G if

- (a) $e \in H$ (IDENTITY)
 - (b) $a, b \in H \Rightarrow a * b \in H$ (CLOSURE)
 - (c) $a \in H \Rightarrow a^{-1} \in H$ (INVERSE)
-

ASSOCIATIVITY obviously holds in any subset.

However, just for safety (!), let us mention it whenever we justify a subgroup!

EXAMPLE We know that $(\mathbb{Z}, +)$ is a group

Show that $A = \{2n | n \in \mathbb{Z}\}$ (set of even numbers)
is a subgroup of $(\mathbb{Z}, +)$

• Associativity clearly holds

(a) The identity $0 \in A$ (it is even)

(b) $a, b \in A$, say $a = 2m, b = 2n \Rightarrow a + b = 2m + 2n = 2(m+n) \in A$
∴ A is CLOSED under $+$.

(c) $a \in A$, say $a = 2n, a' = -a = 2(-n) \in A$

Therefore A is a subgroup

If H is a non-empty subset of G , in order to prove that H is a subgroup we can replace properties (a), (b), (c) above by one property only:

PROPOSITION

H is a subgroup of G if

$$(d) \quad a, b \in H \Rightarrow a * b^{-1} \in H.$$

PROOF

$$\bullet (a), (b), (c) \Rightarrow (d)$$

$$\begin{aligned} \text{if } a, b \in H, \text{ then } a, b^{-1} &\in H & [\text{by (c)}] \\ a * b^{-1} &\in H & [\text{by (b)}] \end{aligned}$$

$$\bullet (d) \Rightarrow (a), (b), (c)$$

If (d) is true then, if $a \in H$

$$a, a \in H \Rightarrow a * a^{-1} \in H \Rightarrow e \in H \text{ thus (a) is true}$$

$$e, a \in H \Rightarrow e * a^{-1} \in H \Rightarrow a^{-1} \in H \text{ thus (c) is true}$$

$$a, b \in H \Rightarrow a, b^{-1} \in H \Rightarrow a * b \in H \text{ thus (b) is true}$$

However, I suggest to use (a), (b), (c) instead of (d).

NOTICE: Every group G has at least two trivial subgroups:

$\{e\}$ (only the identity)
G itself

► FOR FINITE GROUPS

In Cayley tables it is easy to recognise the subgroups. We look for subsets where

- contain e
- CLOSURE occurs

Consider the example of page 40

$S_3 = \{e, \sigma_1, \sigma_2, \tau_1, \tau_2, \tau_3\}$. It is a group under \circ

\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

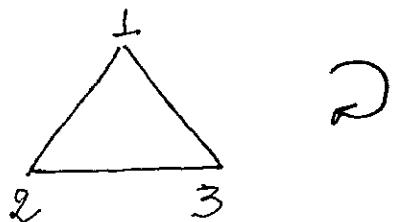
There are six subgroups!

- The trivial ones {e} and S_3 itself.
- $H_1 = \{e, \sigma_1, \sigma_2\}$ ← (observe that it is closed)
- $H_2 = \{e, \tau_1\}$ ← (look at the rows and columns of e and τ_1 only)
- $H_3 = \{e, \tau_2\}$
- $H_4 = \{e, \tau_3\}$

It is interesting to see a geometrical representation of S_3 . (known as symmetric group)

► GEOMETRICAL INTERPRETATION OF S_3

Consider the equilateral triangle

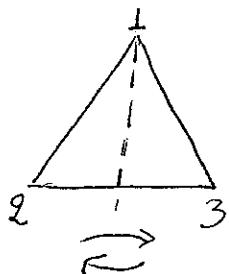


A clockwise rotation (2) by 60° maps
 $1 \mapsto 3, 3 \mapsto 2, 2 \mapsto 1$: This is $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

Two rotations give $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

Three rotations give e (the identity)

On the other hand



This reflection about the dotted line gives

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

Two reflections give e : $\tau_1 \circ \tau_1 = e$

Similarly we obtain τ_2 and τ_3

Hence S_3 describes the symmetries of an equilateral triangle.

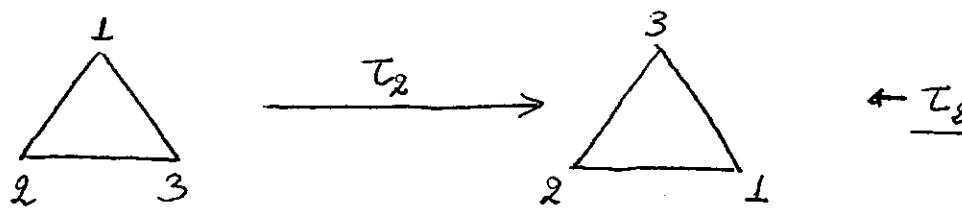
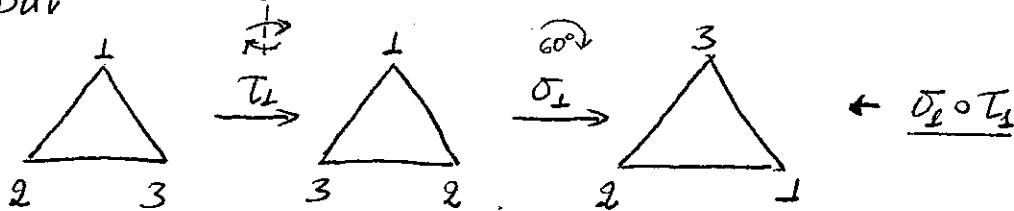
The subgroup $H_1 = \{e, \sigma_1, \sigma_2\}$ describes only the rotations. H_2, H_3, H_4 describe reflections.

The composition of permutations becomes combination of symmetries.

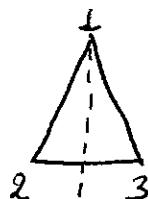
For example:

$$\boxed{\sigma_2 \circ \tau_1 = \tau_2} \quad (\leftarrow \text{look at the table})$$

But



• The symmetries of the isosceles:



There is only one reflection $\xrightarrow{\leftrightarrow} \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

The corresponding group is $H_2 = \{e, \tau_2\}$

• The symmetries of a scalene:



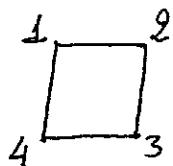
There is no symmetry except e
We obtain the trivial group {e}.

► THE SYMMETRIC GROUP S_4 [★]

It consists of all permutations on $\{1, 2, 3, 4\}$.

Clearly $|S_4| = 4! = 24$

Among those let us determine the symmetries of a square (in cycle form)



Rotations:

$$e = (1)(2)(3)(4); \quad \sigma = (1\ 2\ 3\ 4), \quad \sigma^2 = (1\ 3)(2\ 4), \quad \sigma^3 = (1\ 4\ 3\ 2)$$

Reflections in diagonals:

$$\tau_1 = (1)(3)(2\ 4) \quad \tau_2 = (1\ 3)(2)(4)$$

Vertical and Horizontal reflections:

$$\tau_3 = (1\ 2)(3\ 4) \quad \tau_4 = (1\ 4)(2\ 3)$$

The set of all these 8 permutations

$$\{e, \sigma, \sigma^2, \sigma^3, \tau_1, \tau_2, \tau_3, \tau_4\}$$

forms a subgroup of S_4 .

[★] REMARK In general S_n is called symmetric group. It consists of $n!$ elements

► LAGRANGE THEOREM

We start with a definition; the ORDER of a group G .

$$\boxed{\text{order}(G) = |G| = \text{no of elements of } G}$$

- For infinite groups, such as $(\mathbb{R}, +)$, $(\mathbb{Z}, +)$

$$|G| = \infty$$

- Look at $S_3 = \{e, \sigma_1, \sigma_2, \tau_1, \tau_2, \tau_3\}$

$$\text{order}(S_3) = |S_3| = 6$$

Look at also the orders of its subgroups:

$$H_0 = \{e\} \quad \rightarrow \text{order} = 1$$

$$H_1 = \{e, \sigma_1, \sigma_2\} \quad \rightarrow \text{order} = 3$$

$$H_2 = \{e, \tau_1\} \quad H_3 = \{e, \tau_2\} \quad H_4 = \{e, \tau_3\} \quad \rightarrow \text{order} = 2$$

$$S_3 \quad \rightarrow \text{order} = 6$$

This is not an accident!

LAGRANGE THEOREM

Let H be a subgroup of G .

The order of H divides the order of G :

$$\text{i.e. } \boxed{|H| \text{ divides } |G|}$$

► THE ORDER OF AN ELEMENT

Consider again $S_3 = \{e, \sigma_1, \sigma_2, \tau_1, \tau_2, \tau_3\}$

We have seen that $\sigma_1^3 = e$ (i.e. $\sigma_1 \circ \sigma_2 \circ \sigma_1 = e$)

It is clear that $\sigma_1^6 = e$, $\sigma_1^9 = e$ and so on.

The smallest exponent that gives e is said to be the order of σ_1 . Hence

$$\text{order}(\sigma_1) = 3$$

Similarly $\sigma_2^3 = e$, $\tau_1^2 = e$, $\tau_2^2 = e$, $\tau_3^2 = e$

thus $\text{order}(\sigma_2) = 3$ $\text{order}(\tau_1) = 2$ etc.

DEFINITION. Let G be a group and $a \in G$.

We say that

$$\underline{\text{order}(a) = n}$$

if n is the smallest positive integer such that

$$a^n = e$$

In an infinite group we may have

a, a^2, a^3, a^4, \dots all different

Then $\text{order}(a) = +\infty$

Notice that $e^k = e$, thus

$$\text{order}(e) = 1$$

The powers of an element a form a subset.
It is denoted by $\langle a \rangle$

- If $\text{order}(a) = n$

$$\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$$

- If $\text{order}(a) = +\infty$

$$\langle a \rangle = \{e, a, a^2, a^3, \dots\} \text{ (infinite)}$$

For example, in S_3

$$\langle e \rangle = \{e\}$$

$$\langle \sigma_1 \rangle = \{e, \sigma_1, \sigma_2\}$$

$$\langle \sigma_2 \rangle = \{e, \sigma_2, \sigma_1\}$$

$$\langle \tau_1 \rangle = \{e, \tau_1\}$$

$$\langle \tau_2 \rangle = \{e, \tau_2\}$$

$$\langle \tau_3 \rangle = \{e, \tau_3\}$$

} the same

PROPOSITION: Let G be a group and $a \in G$
 $\text{order}(a) = n$

Then

$\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$ is a subgroup of G

PROOF.

(a) $a^n = e \in \langle a \rangle$

(b) $\langle a \rangle$ is closed: if $a^i, a^j \in \langle a \rangle$

$$a^i * a^j = a^{i+j} \in \langle a \rangle$$

(c) For each $a^i \in \langle a \rangle$, there is an inverse a^{n-i}
since $a^i * a^{n-i} = a^n = e, a^{n-i} * a^i = e$

If $H = \langle a \rangle$, we say that a GENERATES H
or a is a GENERATOR of H .

EXAMPLE Consider $G = \{e, a, b, c\}$ with

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Clearly $e^1 = e \rightarrow \text{order}(e) = 1$
 $a^2 = e \rightarrow \text{order}(a) = 2$
 $b^2 = e \rightarrow \text{order}(b) = 2$
 $c^2 = e \rightarrow \text{order}(c) = 2$

a generates the subgroup $\langle a \rangle = \{e, a\}$

b generates the subgroup $\langle b \rangle = \{e, b\}$

c generates the subgroup $\langle c \rangle = \{e, c\}$

Notice that G cannot be generated by
any element.

COROLLARY OF LAGRANGE THEOREM

Let G be a finite group and $a \in G$

Then $\text{order}(a)$ divides $|G|$

PROOF.

Suppose $\text{order}(a) = n$. Then $\langle a \rangle = \{e, a, \dots, a^{n-1}\}$

Thus $\text{order}(\langle a \rangle) = |\langle a \rangle| = n$ which divides $|G|$.

► CYCLIC GROUPS

A group G is CYCLIC if $G = \langle a \rangle$

i.e. G can be generated by some element a .

e.g. $G = \{e, a, a^2, a^3\}$ where $a^4 = e$ is CYCLIC

$S_3 = \{e, \sigma_1, \sigma_2, \tau_1, \tau_2, \tau_3\}$ is NOT CYCLIC

(it cannot be generated by some a)

EXAMPLE Let $G = \{e, a, b, c\}$ with

*	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

(Notice that elements
rotate "cyclically")

If we find an element of order 4, G is cyclic.

Remember that each order divides 4, since $|G|=4$

$a^2 = b$ so $\text{order}(a) \neq 2$. It cannot be 3 either
so $\text{order}(a) = 4$

Indeed, $a^4 = a^2 * a^2 = b * b = e$

Hence, G is cyclic : $G = \langle a \rangle = \{e, a, a^2, a^3\}$

Also, $\text{order}(e) = 1$

$\text{order}(a) = 4$ ←

$\text{order}(b) = 2$

$\text{order}(c) = 4$ ←

Hence a, c are generators, i.e., $G = \langle a \rangle$ or $G = \langle c \rangle$

In fact, there are only two groups of order 4:

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

*	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	a	e	b

NOT CYCLIC

CYCLIC

(rewritten)



*	e	a	a^2	a^3
e	e	a	a^2	a^3
a	a	a^2	a^3	e
a^2	a^2	a^3	e	a
a^3	a^3	e	a	a^2

To decide if a group is CYCLIC or NOT we find the orders of the elements

If $|G|=n$ and $\text{order}(a)=n$ (for some $a \in G$)

then $G = \langle a \rangle$ CYCLIC.

For example, S_3 is not cyclic since there is no element of order 6.

EXAMPLE The cyclic group of order 3 is

$$G = \langle a \rangle = \{e, a, a^2\} \quad (a^3 = e)$$

GENERATORS: a, a^2 : since $\text{order}(a)=3$ $\text{order}(a^2)=3$.

EXAMPLE The cyclic group of order 6 is

$$G = \langle a \rangle = \{e, a, a^2, a^3, a^4, a^5\} \quad (a^6 = e)$$

[Compare with 6th root of 1 : $z^6 = 1$]

element order

e	1
a	6
a^2	3 \rightarrow since $(a^2)^3 = e$
a^3	2 \rightarrow since $(a^3)^2 = e$
a^4	3 \rightarrow since $(a^4)^3 = e$
a^5	6 \rightarrow Why?

• GENERATORS : a, a^5 (elements of order 6)

• SUBGROUPS : $\langle e \rangle = \{e\}$

$$\langle a \rangle = G$$

$$\langle a^2 \rangle = \{e, a^2, a^4\}$$

$$\langle a^3 \rangle = \{e, a^3\}$$

PROPOSITION Let G be a group of prime order p
i.e $|G|=p$. Then G is cyclic.

PROOF. Let $a \in G$, be any element except e .

By Lagrange, order(a) divides $p \Rightarrow$ order(a) = p .

Therefore, $\langle a \rangle = \{e, a, a^2, \dots, a^{p-1}\} = G$

i.e G is cyclic.

9. COSETS

Let G be a group and H be a subgroup

- If $a \in G$, we define the set

$$aH = \{ah \mid h \in H\}$$

That is, if we "multiply" a by all elements of H we obtain aH .

- We define the following relation on G :

$$\text{for } a, b \in G \quad a \sim b \Leftrightarrow a^{-1}b \in H$$

This is an equivalence relation:

REFLEXIVE: If $a \in G$, $a \sim a$ since $a^{-1}a = e \in H$.

SYMMETRIC: $a \sim b \Rightarrow a^{-1}b \in H$

$$\Rightarrow (a^{-1}b)^{-1} \in H$$

$$\Rightarrow b^{-1}a \in H$$

$$\Rightarrow b \sim a$$

TRANSITIVE: $a \sim b$ and $b \sim c \Rightarrow a^{-1}b \in H$ and $b^{-1}c \in H$

$$\Rightarrow (a^{-1}b)(b^{-1}c) \in H$$

$$\Rightarrow a^{-1}c \in H$$

$$\Rightarrow a \sim c$$

What is the equivalence class of $a \in G$?

$$x \in [a] \Leftrightarrow a \sim x \Leftrightarrow a^{-1}x \in H \Leftrightarrow a^{-1}x = h \text{ where } h \in H$$

$$\Leftrightarrow x = ah, h \in H \Leftrightarrow x \in aH$$

In other words, the equivalence classes of this relation are the sets of the form aH . These are called (left) cosets of H in G .

$$\boxed{\text{COSETS : } aH = \{ah \mid h \in H\}}$$

EXAMPLE Consider the finite group G

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$H = \{e, a\}$ is a subgroup. The cosets of H are

$$eH = H = \{e, a\} \quad (\text{a}H \text{ is the same coset})$$

$$bH = \{b, c\} \quad (cH \text{ is the same coset})$$

EXAMPLE Let $G = \langle a \rangle$ of order 6 (i.e. $a^6 = e$)

(a) The cosets of $H_1 = \langle a^2 \rangle = \{e, a^2, a^4\}$:

$$eH_1 = H_1 = \{e, a^2, a^4\} \quad aH_1 = \{a, a^3, a^5\}$$

(b) The cosets of $H_2 = \langle a^3 \rangle = \{e, a^3\}$:

$$eH_2 = \{e, a^3\}, \quad aH_2 = \{a, a^4\}, \quad a^2H_2 = \{a^2, a^5\}$$

NOTICE :

- $eH = H$ itself is always a coset
- The cosets give a partition of G
- If $|G| = n$ and $|H| = m$, we know by Lagrange that
 m divides n

Each coset has $\frac{n}{m}$ elements.

Let us see an infinite group:

EXAMPLE: Consider the additive group $(\mathbb{Z}, +)$

- The set A of even numbers is a subgroup.

There are two cosets

$$0+A = A = \{2n \mid n \in \mathbb{Z}\} \quad (\text{even numbers})$$

$$1+A = \{2n+1 \mid n \in \mathbb{Z}\} \quad (\text{odd numbers})$$

- The set B of multiples of 5 is a subgroup

$$B = 5\mathbb{Z} = \{5n \mid n \in \mathbb{Z}\}$$

There are 5 cosets:

$$B = \{5n \mid n \in \mathbb{Z}\}$$

$$1+B = \{5n+1 \mid n \in \mathbb{Z}\}$$

$$2+B = \{5n+2 \mid n \in \mathbb{Z}\}$$

$$3+B = \{5n+3 \mid n \in \mathbb{Z}\}$$

$$4+B = \{5n+4 \mid n \in \mathbb{Z}\}$$

► RIGHT COSETS

In a similar way the equivalence relation
 $a \sim b \Leftrightarrow ab^{-1} \in H$ (easy to check)

gives rise to the right cosets

$$Ha = \{ha \mid a \in H\}$$

EXAMPLE Consider the symmetric group

$$S_3 = \{e, \sigma_1, \sigma_2, \tau_1, \tau_2, \tau_3\} \quad (\text{see page 52})$$

and the subgroup $H = \{e, \tau_1\}$

LEFT COSETS

$$eH = H = \{e, \tau_1\}$$

$$\sigma_1 H = \{\sigma_1, \tau_2\}$$

$$\sigma_2 H = \{\sigma_2, \tau_3\}$$

RIGHT COSETS

$$He = H = \{e, \tau_1\}$$

$$H\sigma_1 = \{\sigma_1, \tau_3\}$$

$$H\sigma_2 = \{\sigma_2, \tau_2\}$$

(For $\sigma_i H$ we "multiply" σ_i by all elts of H on the left
For $H\sigma_i$ we "multiply" on the right).

NOTICE

If G is abelian, left cosets and right cosets coincide

10. HOMOMORPHISMS

Consider two groups

$$(G, *) \text{ and } (H, \Delta)$$

A function $f: G \rightarrow H$ is said to be a HOMOMORPHISM if

$$f(a * b) = f(a) \Delta f(b)$$

(as we say, f "respects" the operation)

EXAMPLE Group 1: (\mathbb{R}^+, \cdot) Group 2: $(\mathbb{R}, +)$

Show that the function

$$f: \mathbb{R}^+ \rightarrow \mathbb{R}, \quad f(x) = \ln x$$

is a HOMOMORPHISM.

Indeed,

$$f(a \cdot b) = \ln(a \cdot b) = \ln a + \ln b = f(a) + f(b)$$

If f is a bijection as well, we say that f is an ISOMORPHISM

$$\boxed{\text{HOMOMORPHISM} + \text{BIJECTION} = \text{ISOMORPHISM}}$$

If $f: G \rightarrow H$ is an isomorphism then we say that G and H are ISOLOGIC.

The function of the example above

$$f: \mathbb{R}^+ \rightarrow \mathbb{R} \quad f(x) = \ln x$$

is a bijection:

- f is "1-1": $f(x_1) = f(x_2) \Rightarrow \ln x_1 = \ln x_2 \Rightarrow x_1 = x_2$
- f is "ONTO": Range of $f = f(\mathbb{R}^+) = \mathbb{R}$.

Thus f is an ISOMORPHISM.

NOTICE If f is an isomorphism

f^{-1} is also an isomorphism

Indeed, if f is a bijection, f^{-1} is a bijection.

We know $f(a * b) = f(a) \circ f(b)$

Let $f(a) = x$, $f(b) = y$. Then

$$\begin{aligned} f^{-1}(x * y) &= f^{-1}(f(a) \circ f(b)) = \\ &= f^{-1}(f(a * b)) \\ &= a * b \\ &= f^{-1}(x) \circ f^{-1}(y) \end{aligned}$$

For the example above

$f(x) = \ln x$ is an isomorphism from (\mathbb{R}^+, \cdot) to $(\mathbb{R}, +)$

$f^{-1}(x) = e^x$ is an isomorphism from $(\mathbb{R}, +)$ to (\mathbb{R}^+, \cdot)

► FOR FINITE GROUPS

We usually observe CAYLEY tables.

In fact, ISOMORPHIC means they look similar.

e.g. G

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

H

*	1	c	c ²
1	1	c	c ²
c	c	c ²	1
c ²	c ²	1	c

In fact they are the same. (isomorphic)

The obvious isomorphism f maps

$$e \mapsto 1$$

$$a \mapsto c$$

$$b \mapsto c^2$$

(in this way f "respects" the operation)

Sometimes it is not obvious that the Cayley tables are similar

EXAMPLE. Consider two groups:

\mathbb{Z}_4 : +	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

G	*	e	a	b	c
e	e	a	b	c	
a	a	e	c	b	
b	b	c	a	e	
c	c	b	e	a	

They do not seem similar. However they are both cyclic.

$(\mathbb{Z}_4, +)$ is cyclic (known)

Let us see the orders in G

$$\text{order}(e)=1$$

$$\text{order}(a)=2$$

$$\text{order}(b)=4 \rightarrow \text{generator}$$

$$\text{order}(c)=4 \rightarrow \text{generator}$$

Hence $G = \{e, b, b^2, b^3\}$ (where $b^2=a$, $b^3=c$)

If we rearrange the elements of G , we obtain

*	e	b	a	c
e	e	b	a	c
b	b	a	c	e
a	a	c	e	b
c	c	e	b	a

isomorphic to

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

The isomorphism here is $f: \mathbb{Z}_4 \rightarrow G$, with

$$0 \mapsto e$$

$$1 \mapsto b$$

$$2 \mapsto a$$

$$3 \mapsto c$$

NOTICE. We have already said that there exist

- ONLY ONE group of order 3 } Any other group is
- ONLY TWO groups of order 4 } ISOMORPHIC to one of them

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a
(cyclic)			

*	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b
(cyclic)				

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a
(non-cyclic)				

► THEORETICAL RESULTS

Let $(G, *)$ and (H, Δ) be two groups and

$$f: G \rightarrow H \quad \text{a. homomorphism}$$

We denote the identities by e_G, e_H respectively.

■ PROPOSITION 1 $f(e_G) = e_H$

(f maps identity to identity)

PROOF

$$e_G * e_G = e_G \quad [\text{since } e_G \text{ identity in } G]$$

$$\Rightarrow f(e_G * e_G) = f(e_G)$$

$$\Rightarrow f(e_G) * f(e_G) = f(e_G) \quad [\text{since } f \text{ is a homom.}]$$

$\Rightarrow f(e_G)$ is the identity in H , i.e. $f(e_G) = e_H$

[Notice: $a * a^{-1} = a \Rightarrow a^{-1} * a * a = a^{-1} * a \Rightarrow a = e$]

■ PROPOSITION 2 $f(a^{-1}) = f(a)^{-1}$

(f maps inverse to inverse)

PROOF For any $a \in G$

$$a * a^{-1} = e_G$$

$$\Rightarrow f(a * a^{-1}) = f(e_G)$$

$$\Rightarrow f(a) * f(a^{-1}) = f(e_G) \quad [\text{since } f \text{ is a homom.}]$$

$$\Rightarrow f(a) * f(a^{-1}) = e_H \quad [\text{by PROPOSITION 1}]$$

$\Rightarrow f(a^{-1})$ is the inverse of $f(a)$

$$\text{i.e. } f(a)^{-1} = f(a^{-1})$$

■ PROPOSITION 3 Let f be an isomorphism
and $f(a) = b$
 $\text{order}(a) = n \Rightarrow \text{order}(b) = n$

PROOF Let $\text{order}(a) = n$, $\text{order}(b) = m$

$$\begin{aligned}\text{order}(a) = n &\Rightarrow a^n = e_G \\ &\Rightarrow f(a^n) = f(e_G) \\ &\Rightarrow f(a)^n = f(e_G) \quad [\text{since } f \text{ homom}] \\ &\Rightarrow b^n = e_H \quad [\text{by PROPOSITION 1}]\end{aligned}$$

But m is the smallest integer s.t. $b^m = e_H$

Hence $m \leq n$

However, f^{-1} is also an isomorphism, $f^{-1}(b) = a$

This implies $n \leq m$ (similarly)

Therefore $m = n$

■ PROPOSITION 4 Let f be an isomorphism
 G cyclic $\Rightarrow H$ cyclic.

PROOF: G is cyclic of order n

$\Rightarrow G = \langle a \rangle$, a = generator of order n

$\Rightarrow f(a)$ has also order n [by PROPOSITION 3]

$\Rightarrow H$ is cyclic with generator $f(a)$ i.e. $H = \langle f(a) \rangle$

NOTICE For finite groups we check the orders of their elements.

- different orders \Rightarrow non-isomorphic groups

EXAMPLE (Remember again that in fact there are exactly two groups of order 4)

Consider

G_1	*	e a b c
e	e	a b c
a	a	e c b
b	b	c e a
c	c	b a e

G_2	*	E A B C
E	E	A B C
A	A	B C E
B	B	C E A
C	C	E A B

G_3	*	I P Q R
I	I	P Q R
P	P	I R Q
Q	Q	R P I
R	R	Q I P

$$\text{ord}(e) = 1$$

$$\text{ord}(E) = 1$$

$$\text{ord}(I) = 1$$

$$\text{ord}(a) = 2$$

$$\text{ord}(A) = 4$$

$$\text{ord}(P) = 2$$

$$\text{ord}(b) = 2$$

$$\text{ord}(B) = 2$$

$$\text{ord}(Q) = 4$$

$$\text{ord}(c) = 2$$

$$\text{ord}(C) = 4$$

$$\text{ord}(R) = 4$$

- State some reasons to explain why G_1, G_2 are not isomorphic:
 - 3 elements of order 2 in G_1 } look at the 1 element of order 2 in G_2 } main diagonal.
 - different orders appear
 - there is an element of order 4 in G_2 , not in G_1
 - G_1 is not cyclic, G_2 is cyclic
- What about G_2 and G_3 ?
 - There is an element of order 4 in both groups
Hence they are both cyclic
Hence G_2, G_3 are isomorphic.

Let us see an example of a homomorphism which is not isomorphism

EXAMPLE

G	*	e a b c
e		e a b c
a		a b c e
b		b c e a
c		c e a b

H	A E A B C
E	E A B C
A	A E C B
B	B C E A
C	C B A E

Notice that G is cyclic $G = \langle a \rangle$

Consider the homomorphism f with

$$f(a) = A$$

Then $a^2 = b$, so $f(b) = f(a^2) = f(a)^2 = A^2 = E$

$a^3 = c$, so $f(c) = f(a^3) = f(a)^3 = A^3 = A$

To summarise

$$\begin{aligned} f: \quad & e \mapsto E \\ & a \mapsto A \\ & b \mapsto E \\ & c \mapsto A \end{aligned}$$

Notice that

f is not "1-1" (since $f(e) = f(b)$)

f is not "onto" (Range: $f(G) = \{E, A\} \neq H\}$)

► KERNEL AND RANGE

Let $f: G \rightarrow H$ be a homomorphism

We define

The KERNEL $\ker f = \{a \in G \mid f(a) = e_H\}$

i.e. $\ker f$ consists of all elements that map to e_H

In the previous example (page 74)

$$\ker f = \{e, b\}$$

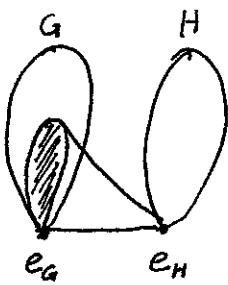
Notice that $\ker f = \{e, b\}$ is a subgroup of G

$f(G) = \{E, A\}$ is a subgroup of H

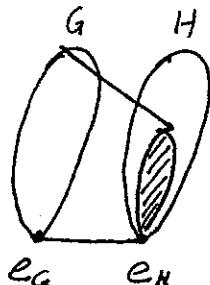
REMARK: The range of f is denoted by $f(G)$
but it also called image of f and
denoted by $\text{Im } f$

PROPOSITION Let $f: G \rightarrow H$ homomorphism

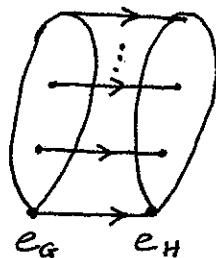
- (a) $\ker f = \{a \in G \mid f(a) = e_H\}$ is a subgroup of G
- (b) $f(G) = \{f(a) \mid a \in G\}$ is a subgroup of H
- (c) f isomorphism $\Leftrightarrow \ker f = \{e\}$ and $f(G) = H$.



(a)

Kernel $\ker f$ 

(b)

Range $f(G)$ 

(c)

 f is isomorphism $\ker f = \{e_G\}, f(G) = H$ PROOF(a) IDENTITY $e_G \in \ker f$ since $f(e_G) = e_H$ CLOSURE $a, b \in \ker f \Rightarrow a * b \in \ker f$ since $f(a * b) = f(a) \circ f(b) = e_H * e_H = e_H$ INVERSE $a \in \ker f \Rightarrow a^{-1} \in \ker f$ since $f(a^{-1}) = f(a)^{-1} = e_H^{-1} = e_H$ (b) IDENTITY $e_H \in f(G)$ since $e_H = f(e_G)$ CLOSURE $x, y \in f(G) \Rightarrow x * y \in f(G)$ since $x = f(a), y = f(b)$ for some $a, b \in G$ and $x * y = f(a) \circ f(b) = f(a * b)$ with $a * b \in G$ INVERSE $x \in f(G) \Rightarrow x^{-1} \in f(G)$ since $x = f(a)$ for some $a \in G$ and $x^{-1} = f(a)^{-1} = f(a^{-1})$ with $a^{-1} \in G$.(c) f is onto $\Leftrightarrow f(G) = H$

It suffices to show that

 f is "1-1" $\Leftrightarrow \ker f = \{e_G\}$

(\Rightarrow) If f is "1-1" then $\text{ker } f = \{e_G\}$

Indeed, if $a \in \text{ker } f$

then $f(a) = e_H = f(e_G) \Rightarrow a = e_G$. (since f "1-1")

Therefore $\text{ker } f = \{e_G\}$

(\Leftarrow) If $\text{ker } f = \{e_G\}$ then f is "1-1"

Indeed,

$$f(a) = f(b) \Rightarrow f(a) \circ f(b)^{-1} = e_H$$

$$\Rightarrow f(a) \circ f(b^{-1}) = e_H$$

$$\Rightarrow f(a * b^{-1}) = e_H$$

$$\Rightarrow a * b^{-1} \in \text{ker } f$$

$$\Rightarrow a * b^{-1} = e_G$$

$$\Rightarrow a = b$$

EXAMPLE Consider the following groups

$$G = \langle \alpha \rangle = \{\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5\} \quad \alpha^6 = 1 \quad (\text{cyclic})$$

$$S_3 = \{e, \sigma_1, \sigma_2, T_1, T_2, T_3\} \quad (\text{of page 52})$$

(a) What is the homomorphism $f: G \rightarrow S_3$

defined by $f: a \mapsto \sigma_1$?

We can easily derive that

$$1 \mapsto e \quad \alpha^3 \mapsto e \quad (\sigma_1^3)$$

$$\alpha \mapsto \sigma_1 \quad \alpha^4 \mapsto \sigma_1 \quad (\sigma_1^4)$$

$$\alpha^2 \mapsto \sigma_2 \quad (\sigma_1^2) \quad \alpha^5 \mapsto \sigma_2 \quad (\sigma_1^5)$$

- What is the kernel?

$$\ker f = \{1, a^3\} \quad (\text{it is a subgroup of } G)$$

- What is the range?

$$f(G) = \{e, \sigma_1, \sigma_2\} \quad (\text{it is a subgroup of } S_3)$$

(b) Consider now the subgroup $H = \{e, \sigma_1, \sigma_2\}$ of S_3

What is the homomorphism $g: H \rightarrow G$

defined by $\sigma_1 \mapsto a^2$?

We can easily derive that

$$e \mapsto 1$$

$$\sigma_1 \mapsto a^2$$

$$\sigma_2 \mapsto a^4 \quad (\text{since } \sigma_2 = \sigma_1^2)$$

- What is the kernel?

$$\ker g = \{e\} \quad (\text{Indeed, } g \text{ is "1-1"})$$

- What is the range?

$$g(H) = \{1, a^2, a^4\} \quad (\text{subgroup of } G)$$
