LECTURE NOTES

on

DISCRETE MATHEMATICS

Eusebius Doedel

LOGIC

Introduction. First we introduce some basic concepts needed in our discussion of logic. These will be covered in more detail later.

A *set* is a collection of "objects" (or "elements").

EXAMPLES :

- the infinite set of *all integers* : $\mathbb{Z} \equiv \{\cdots, -2, -1, 0, 1, 2, 3, \cdots\}$.
- the infinite set of *all positive integers* : $\mathbb{Z}^+ \equiv \{1, 2, 3, \cdots\}$.
- the infinite set $\mathbb{R}$ of *all real numbers*.
- the finite set $\{T, F\}$, where T denotes "*True*" and F "*False*".
- the finite set of alphabetic characters : $\{a, b, c, \cdots, z\}$.

A *function* (or "*map*", or "*operator*") is a rule that associates to every element of a set one element in another set.

EXAMPLES :

- If $S_1 = \{a, b, c\}$ and $S_2 = \{1, 2\}$ then the associations

$$a \mapsto 2, \qquad b \mapsto 1, \qquad c \mapsto 2,$$

define a function f from S_1 to S_2 . We write

$$f \ : \ S_1 \longrightarrow S_2 \ .$$

- Similarly $f(n) = n^2$ defines a function $f \ : \ \mathbb{Z}^+ \longrightarrow \mathbb{Z}^+$.

- $f(n) = n^2$ can also be viewed as a function $f \ : \ \mathbb{Z} \longrightarrow \mathbb{Z}$.

EXAMPLE :

Let $\mathbb{P}_n$ denoet the infinite set of all polynomial functions $p(x)$ of degree n or less with integer coefficients.

- The derivative operator D restricted to elements of $\mathbb{P}_n$ can be viewed as a function from $\mathbb{P}_n$ to $\mathbb{P}_{n-1}$,

$$D \ : \ \mathbb{P}_n \ \longrightarrow \ \mathbb{P}_{n-1}, \qquad D \ : \ p \ \mapsto \ \frac{dp}{dx} \ .$$

For example, if $p(x) \ = \ x^3 + 2x + 1$, then

$$D \ : \ x^3 + 2x + 1 \ \mapsto \ 3x^2 + 2 \ ,$$

i.e.,

$$D(x^3 + 2x + 1) \ = \ 3x^2 + 2 \ .$$

EXAMPLE :

- We can also define functions of *several variables*, *e.g.*,

$$f(x, y) = x + y \ ,$$

can be viewed as a function "from $\mathbb{Z}^+$ cross $\mathbb{Z}^+$ into $\mathbb{Z}^+$".

We write

$$f \ : \ \mathbb{Z}^+ \times \mathbb{Z}^+ \ \longrightarrow \ \mathbb{Z}^+ \ .$$

Basic logical operators.

The basic logical operators

$$\wedge \quad (\text{“and”} \quad , \quad \text{“conjunction”})$$

$$\vee \quad (\text{“or”} \quad , \quad \text{“disjunction”})$$

$$\neg \quad (\text{“not”} \quad , \quad \text{“negation”})$$

are defined in the tables below :

p	$\neg p$
T	F
F	T

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

Let $\mathbb{B} \equiv \{\, T \;, F \,\}$. Then we can view $\neg$, $\vee$, and $\wedge$, as functions

$$\neg \;:\; \mathbb{B} \longrightarrow \mathbb{B}, \qquad \vee \;:\; \mathbb{B} \times \mathbb{B} \longrightarrow \mathbb{B}\;, \qquad \wedge \;:\; \mathbb{B} \times \mathbb{B} \longrightarrow \mathbb{B}\;.$$

We can also view the arithmetic operators $-$, $+$, and $\times$, as functions

$$- \;:\; \mathbb{Z} \longrightarrow \mathbb{Z}, \qquad + \;:\; \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}, \qquad * \;:\; \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z},$$

defined by value tables, for example,

x	$-x$
.	.
-2	2
-1	1
0	0
1	-1
2	-2
.	.

Logical expressions.

A *logical expression* (or "*proposition*") $P(p, q, \cdots)$ is a function

$$P \ : \ \mathbb{B} \times \mathbb{B} \times \cdots \times \mathbb{B} \ \longrightarrow \ \mathbb{B} \ .$$

For example,

$$P_1(p, q) \ \equiv \ p \vee \neg q \qquad \text{and} \qquad P_2(p, q, r) \ \equiv \ p \wedge (q \vee r)$$

are logical expressions.

Here

$$P_1 \ : \ \mathbb{B} \times \mathbb{B} \longrightarrow \mathbb{B} \ ,$$

and

$$P_2 \ : \ \mathbb{B} \times \mathbb{B} \times \mathbb{B} \longrightarrow \mathbb{B} \ .$$

The values of a logical expression can be listed in a *truth table* .

EXAMPLE :

p	q	$\neg q$	$p \vee (\neg q)$
T	T	F	T
T	F	T	T
F	T	F	F
F	F	T	T

Analogously, *arithmetic expressions* such as

$$A_1(x, y) \equiv x + (-y) \qquad \text{and} \qquad A_2(x, y, z) \equiv x \times (y + z)$$

can be considered as functions

$$A_1 \ : \ \mathbb{R} \times \mathbb{R} \ \longrightarrow \ \mathbb{R}, \qquad \text{and} \qquad A_2 \ : \ \mathbb{R} \times \mathbb{R} \times \mathbb{R} \ \longrightarrow \ \mathbb{R} \ ,$$

or, equivalently,

$$A_1 \ : \ \mathbb{R}^2 \ \longrightarrow \ \mathbb{R}, \qquad \text{and} \qquad A_2 \ : \ \mathbb{R}^3 \ \longrightarrow \ \mathbb{R} \ .$$

Two propositions are *equivalent* if they always have the same values.

EXAMPLE :

$$\neg(p \vee q) \quad \text{is equivalent to} \quad \neg p \wedge \neg q \ ,$$

(one of *de Morgan's laws*), as can be seen in the table below :

p	q	$p \vee q$	$\neg(p \vee q)$	$\neg p$	$\neg q$	$\neg p \wedge \neg q$
T	T	T	F	F	F	F
T	F	T	F	F	T	F
F	T	T	F	T	F	F
F	F	F	T	T	T	T

NOTE :

In arithmetic

$$-(x+y) \quad \text{is equivalent to} \quad (-x)+(-y)\ ,$$

i.e., we do *not* have that

$$-(x+y) \quad \text{is equivalent to} \quad (-x)\times(-y)\ .$$

Thus the analogy between logic and arithmetic is limited.

The three basic logical operators $\neg$, $\vee$, and $\wedge$, are all we need.

However, it is very convenient to introduce some *additional operators*, much like in arithmetic, where we write x^3 to denote $x \times (x \times x)$.

Three such additional operators are

$\oplus$	"*exclusive or*"
$\rightarrow$	"conditional" , "*if then*"
$\leftrightarrow$	"biconditional" , "*if and only if*" , "iff"

defined as :

p	q	$p \oplus q$	$p \rightarrow q$	$p \leftrightarrow q$
T	T	F	T	T
T	F	T	F	F
F	T	T	T	F
F	F	F	T	T

EXAMPLE :

Suppose two persons, P and Q, are suspected of committing a crime.

- Let P denote the statement by P that

  "Q did it, or we did it together".

- Let Q denote the statement by Q that

  "P did it, or if I did it then we did it together".

- Suppose we know P always tells the truth and Q always lies.

Who committed the crime ?

NOTE : By "did it" we mean "was involved".

Let p denote "P did it" and let q denote "Q did it".

Then p and q are logical variables.

We are given that the value of the logical expression

$$q \vee (p \wedge q) \quad \text{is} \quad \textit{True} \ ,$$

and that

$$p \vee \Big(q \rightarrow (p \wedge q)\Big) \quad \text{is} \quad \textit{False} \ .$$

Equivalently we have that the value of the logical expression

$$\neg\Big(p \vee \Big(q \rightarrow (p \wedge q)\Big)\Big) \ \wedge \ \Big(q \vee (p \wedge q)\Big)$$

is *True* .

Our problem is to find for what values of p and q this is the case.

As an analogy from arithmetic, consider the problem of finding the values of x and y in $\mathbb{Z}$ so that

$$\text{the value of the arithmetic expression } x^2 + y \text{ is } 5 \ ,$$

and such that

$$\text{the value of } x + y \text{ is } 3 \ ,$$

i.e., we want to find all solutions of the the simultaneous equations

$$x^2 + y = 5 \ , \qquad x + y = 3 \ .$$

(How many solutions are there ?)

For the "crime problem" we have the truth table

p	q	$\neg\Big(p \quad \vee\Big(q \quad \rightarrow \quad (p \wedge q)\Big)\Big)$				$\wedge\Big(q \quad \vee \quad (p \wedge q)\Big)$		
T	T	F	T	T	T	F	T	T
T	F	F	T	T	F	F	F	F
F	T	T	F	F	F	T	T	F
F	F	F	T	T	F	F	F	F
(1)	(2)	(6)	(5)	(4)	(3)	(9)	(8)	(7)

The order of evaluation has been indicated at the bottom of the table.

The values of the entire expression are in column (9).

We observe that the expression is *True* only if $p = F$ and $q = T$.

Therefore Q was involved in the crime, but P was not.

EXERCISE :

Consider the logical expression in the preceding "crime" example.

Find a much simpler, *equivalent* logical expression.

(It must have precisely the *same values* as listed in column "(9)".)

EXERCISE :

Suppose three persons, P, Q, and R, are suspects in a crime.

- P states that "Q or R, or both, were involved".
- Q states that "P or R, or both, were involved".
- R states that "P or Q, but not both, were involved".

- Suppose P and Q always tell the truth, while R always lies.

Who were involved in the crime ?

NOTE : there may be more than one solution $\cdots$

EXERCISE :

Construct a truth table for the logical expression

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

Based on the truth table find a simpler, *equivalent* logical expression.

A *contradiction* is a logical expression whose value is always *False* .

For example $p \wedge \neg p$ is a contradiction :

p	$\neg p$	$p \wedge \neg p$
T	F	F
F	T	F

A *tautology* is a logical expression that is always *True* .

For example $p \vee \neg p$ is a tautology :

p	$\neg p$	$p \vee \neg p$
T	F	T
F	T	T

A logical expression that is neither a tautology nor a contradiction is called a *contingency*.

EXERCISE :

Verify by truth table that the following expressions are *tautologies* :

$$\Big(\ (p \to q) \ \wedge \ p \ \Big) \quad \to \quad q \quad ,$$

$$\Big(\ (p \to q) \ \wedge \ \neg q \ \Big) \quad \to \quad \neg p \quad .$$

NOTATION :

We use the symbol "$\Rightarrow$" to indicate that a conditional statement is a tautology.

For example, from the preceding exercise we have

$$\Big((p \to q) \ \wedge \ p \Big) \ \Rightarrow \ q \quad , \qquad (\text{"modus ponens"}) \ ,$$

$$\Big((p \to q) \ \wedge \ \neg q \Big) \ \Rightarrow \ \neg p \quad , \qquad (\text{"modus tollens"}) \ .$$

As another example we show that

$$\Big((p \to q) \wedge (\neg p \to r) \wedge (q \to r)\Big) \;\to\; r$$

is a tautology.

p	q	r	$\Big((p \to q)$	$\wedge$	$(\neg p$	$\to r)$	$\wedge$	$(q \to r)\Big)$	$\to$	r
T	T	T	T	T	F	T	T	T	T	T
T	T	F	T	T	F	T	F	F	T	F
T	F	T	F	F	F	T	F	T	T	T
T	F	F	F	F	F	T	F	T	T	F
F	T	T	T	T	T	T	T	T	T	T
F	T	F	T	F	T	F	F	F	T	F
F	F	T	T	T	T	T	T	T	T	T
F	F	F	T	F	T	F	F	T	T	F
(1)	(2)	(3)	(5)	(9)	(6)	(7)	(10)	(8)	(11)	(4)

The last column (11) consist of *True* values only. Therefore we can write

$$\Big((p \to q) \wedge (\neg p \to r) \wedge (q \to r)\Big) \Rightarrow r$$

QUESTION : Does it matter which of the two $\wedge$'s is evaluated first?

EXAMPLE :

Here we illustrate another technique that can sometimes be used to show that a conditional statement is a tautology.

Consider again the logical expression

$$P(p, q, r) \Longleftrightarrow (p \rightarrow q) \wedge (\neg p \rightarrow r) \wedge (q \rightarrow r) \ .$$

We want to show that

$$P(p, q, r) \Rightarrow r \ ,$$

i.e., that

$$P(p, q, r) \rightarrow r \quad \text{always has value } \textit{True} \ .$$

NOTE : We need only show that:

We *can't have* that $P(p, q, r)$ is *True* , while r is *False* .

So suppose that $P(p, q, r)$ is *True* , while r is *False* .

(*We must show that this cannot happen !*)

Thus all three of

$$(a) \quad p \to q \qquad (b) \quad \neg p \to F \qquad \text{and} \qquad (c) \quad q \to F$$

have value *True* .

(c) can only have value *True* if $q = F$.

(b) can only have value *True* if $\neg p = F$, *i.e.*, if $p = T$.

But then (a) becomes $T \to F$ which has value F .

So indeed, not all three, (a), (b), and (c) can have value *True* .

QED ! ("*quod erat demonstrandum*": "which was to be shown")

NOTE :

This was an example of a *proof by contradiction*.

(We will give more examples later $\cdots$)

EXERCISE :

Use a proof "by contradiction" to prove the following:

$$\Big(\ (p \to q) \ \wedge \ p \ \Big) \ \Rightarrow \ q \quad ,$$

$$\Big(\ (p \to q) \ \wedge \ \neg q \ \Big) \ \Rightarrow \ \neg p \quad .$$

(Already done by truth table.)

EXERCISE :

Also use a "*direct proof*" to prove that

$$\Big(\ (p \to q) \ \wedge \ p \ \Big) \ \Rightarrow \ q \quad ,$$

$$\Big(\ (p \to q) \ \wedge \ \neg q \ \Big) \ \Rightarrow \ \neg p \quad .$$

(In a *direct proof* one assumes that the LHS is *True* and then one shows that the RHS must be *True* also.)

NOTATION :

From the definition of the $\leftrightarrow$ operator we see that logical expressions

$$P_1(p, q, \cdots) \qquad \text{and} \qquad P_2(p, q, \cdots) \ ,$$

are equivalent if and only if

$$P_1(p, q, \cdots) \ \leftrightarrow \ P_2(p, q, \cdots)$$

is a tautology.

In this case we write

$$P_1(p, q, \cdots) \iff P_2(p, q, \cdots) \ .$$

EXAMPLE :

$$\neg(p \wedge q) \quad \text{is equivalent to} \quad \neg p \vee \neg q \ ,$$

i.e.,

$$\neg(p \wedge q) \iff (\neg p \vee \neg q) \ ,$$

as seen in the truth table

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

The operators

$$\oplus \quad , \quad \rightarrow \quad , \quad \text{and} \quad \leftrightarrow \quad ,$$

can be expressed in terms of the basic operators

$$\neg \quad , \quad \wedge \quad , \quad \text{and} \quad \vee \quad ,$$

as verified below :

p	q	$(p \oplus q)$	$\leftrightarrow$	$\Big($	$(p \vee q)$	$\wedge$	$\neg$	$(p \wedge q)\Big)$
T	T	F	T		T	F	F	T
T	F	T	T		T	T	T	F
F	T	T	T		T	T	T	F
F	F	F	T		F	F	T	F

p	q	$(p \rightarrow q)$	$\leftrightarrow$	$(q$	$\vee$	$\neg p)$
T	T	T	T	T	F	
T	F	F	T	F	F	
F	T	T	T	T	T	
F	F	T	T	T	T	

p	q	$(p \leftrightarrow q)$	$\leftrightarrow$	$\Big((q \vee \neg p)$	$\wedge(p$	$\vee$	$\neg q)\Big)$
T	T	T	T	T	T	T	F
T	F	F	T	F	F	T	T
F	T	F	T	T	F	F	F
F	F	T	T	T	T	T	T

Thus we can write

$$p \oplus q \iff (p \vee q) \wedge \neg(p \wedge q) \ ,$$

$$p \rightarrow q \iff q \vee \neg p \ ,$$

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

It also follows that

$$p \leftrightarrow q \iff (p \rightarrow q) \wedge (q \rightarrow p) \ .$$

Basic logical equivalences.

The fundamental logical equivalences ("laws") are :

$p \vee q \iff q \vee p$	$p \wedge q \iff q \wedge p$	*commutative law*
$p \vee (q \wedge r) \iff (p \vee q) \wedge (p \vee r)$	$p \wedge (q \vee r) \iff (p \wedge q) \vee (p \wedge r)$	*distributive law*
$p \vee F \iff p$	$p \wedge T \iff p$	*identity law*
$p \vee \neg p \iff T$	$p \wedge \neg p \iff F$	*complement law*

Some useful additional laws are :

$\neg T \iff F$	$\neg F \iff T$	*negation law*
$p \vee p \iff p$	$p \wedge p \iff p$	*idempotent law*
$p \vee T \iff T$	$p \wedge F \iff F$	*domination law*
$p \vee (p \wedge q) \iff p$	$p \wedge (p \vee q) \iff p$	*absorption law*

NOTE : Remember the *absorption laws* : they can be very useful !

Some more laws are :

$(p \vee q) \vee r \iff p \vee (q \vee r)$	$(p \wedge q) \wedge r \iff p \wedge (q \wedge r)$	*associative law*
$\neg(p \vee q) \iff \neg p \wedge \neg q$	$\neg(p \wedge q) \iff \neg p \vee \neg q$	*de Morgan*
$\neg(\neg p) \iff p$		*double negation*
$p \to q \iff \neg q \to \neg p$		*contrapositive*

- All laws of logic can in principle be proved using truth tables.

- To illustrate the *axiomatic nature* of the fundamental laws, we prove an additional law using only the fundamental laws.

- At every step the fundamental law used will be indicated.

- Once proved, additional laws may be used in further proofs.

EXAMPLE : *Proof of the idempotent law*

$$p \vee p \iff p$$

p	$\iff$	$p \vee F$	identity law
	$\iff$	$p \vee (p \wedge \neg p)$	complement law
	$\iff$	$(p \vee p) \wedge (p \vee \neg p)$	distributive law
	$\iff$	$(p \vee p) \wedge T$	complement law
	$\iff$	$p \vee p$	identity law

NOTE :

- Proving additional laws, using only the fundamental laws, is not as easy as one might expect, because we have very few tools available.

- However after proving some of these additional equivalences we have a more powerful set of laws.

Simplification of logical expressions.

It is useful to simplify logical expressions as much as possible.

This is much like in arithmetic where, for example, the expression

$$x^3 + 3x^2y + 3xy^2 + y^3$$

is equivalent to

$$(x + y)^3 \ .$$

EXAMPLE : Reconsider the logical expression

$$\neg\Big(p \vee \Big(q \rightarrow (p \wedge q)\Big)\Big) \ \wedge \ \Big(q \vee (p \wedge q)\Big)$$

from the "crime example".

It is equivalent to the much simpler logical expression

$$\neg p \wedge q \ ,$$

because it has the same truth table values :

p	q	$\neg p$	$\neg p \wedge q$
T	T	F	F
T	F	F	F
F	T	T	T
F	F	T	F

One way to simplify a logical expression is by using

- the fundamental laws of logic,
- known additional laws,
- the definitions of the additional logical operators.

For the "crime example" this can be done as follows :

	$\neg\Big(p \vee \Big(q \to (p \wedge q)\Big)\Big) \;\wedge\; \Big(q \vee (p \wedge q)\Big)$	
$\Longleftrightarrow$	$\neg\Big(p \vee \Big(q \to (p \wedge q)\Big)\Big) \;\wedge\; \Big(q \vee (q \wedge p)\Big)$	commutative law
$\Longleftrightarrow$	$\neg\Big(p \vee \Big(q \to (p \wedge q)\Big)\Big) \;\wedge\; q$	absorption law
$\Longleftrightarrow$	$\neg\Big(p \vee \Big((p \wedge q) \vee \neg q\Big)\Big) \;\wedge\; q$	equivalence of $\to$
$\Longleftrightarrow$	$\neg\Big(\Big(p \vee (p \wedge q)\Big) \vee \neg q\Big) \;\wedge\; q$	associative law
$\Longleftrightarrow$	$\neg\Big(p \vee \neg q\Big) \;\wedge\; q$	absorption law
$\Longleftrightarrow$	$\ldots$	

	$\neg\Big(p \vee \neg q\Big) \ \wedge \ q$	
$\Longleftrightarrow$	$\Big(\neg p \wedge \neg\neg q\Big) \ \wedge \ q$	de Morgan
$\Longleftrightarrow$	$\Big(\neg p \wedge q\Big) \ \wedge \ q$	double negation
$\Longleftrightarrow$	$\neg p \wedge \Big(q \wedge q\Big)$	associative law
$\Longleftrightarrow$	$\neg p \wedge q$	idempotent law

EXERCISE :

Use logical equivalences to simplify the logical expression

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

(This example was already considered before, using a truth table.)

EXERCISE :

Use logical equivalences to verify the following equivalence:

$$(\neg p \wedge q) \vee (\neg q \wedge p) \iff (p \vee q) \wedge \neg(p \wedge q) \ .$$

(This was considered before in connection with the $\oplus$ operator.)

EXERCISE :

Use logical equivalences to show that the logical expression

$$\Big((p \to q) \wedge (\neg p \to r) \wedge (q \to r)\Big) \;\to\; r \;,$$

is a tautology, *i.e.*, show that

$$\Big((p \to q) \wedge (\neg p \to r) \wedge (q \to r)\Big) \Rightarrow r \;.$$

NOTE : Earlier we proved this by truth table and by contradiction.

Predicate Calculus.

Let S be a set.

A *predicate* P is a function from S to $\{T, F\}$:

$$P : S \longrightarrow \{T, F\},$$

or

$$P : S \times S \times \cdots \times S \longrightarrow \{T, F\}.$$

or

$$P : S_1 \times S_2 \times \cdots \times S_n \longrightarrow \{T, F\}.$$

EXAMPLE : Let $\mathbb{Z}^+$ denote the set of all positive integers.

Define

$$P \ : \ \mathbb{Z}^+ \longrightarrow \{ T \ , F \ \}$$

by

$$P(x) = T \quad \text{if} \ \ x \in \mathbb{Z}^+ \text{ is even} \ ,$$

$$P(x) = F \quad \text{if} \ \ x \in \mathbb{Z}^+ \text{ is odd} \ .$$

We can think of $P(x)$ as the statement

"x is an even integer",

which can be either *True* or *False* .

- What are the values of $P(12)$, P(37), P(-3) ?

EXAMPLE :

Let U be a set and S a subset of U.

Let $P(x)$ denote the statement "$x \in S$", *i.e.*,

$$P(x) \Longleftrightarrow x \in S \ .$$

Then

$$P \ : \ U \longrightarrow \{ T \ , F \ \} \ .$$

EXAMPLE :

Let $P(x, y)$ denote the statement "$x + y = 5$", *i.e.*,

$$P(x, y) \iff x + y = 5 \ .$$

Then we can think of P as a function

$$P \ : \ \mathbb{Z}^+ \times \mathbb{Z}^+ \longrightarrow \{ T \ , F \ \} \ .$$

Quantifiers.

For a more compact notation we introduce the *quantifiers*

$$\forall\,, \qquad \exists\,, \qquad \text{and} \qquad \exists!$$

DEFINITIONS : Let S be a set and P a predicate, $P\ :\ S\ \longrightarrow\ \{\,T\ ,F\ \}\,.$

Then we define :

$\forall x \in S\ P(x)$	means	" $P(x) = T$ for all $x \in S$ ".
$\exists x \in S\ P(x)$	means	" there exists an $x \in S$ for which $P(x) = T$ ".
$\exists! x \in S\ P(x)$	means	" there is a unique $x \in S$ for which $P(x) = T$ ".

If it is clear from the context what S is, then one often simply writes

$$\forall x\ P(x)\ , \qquad \exists x\ P(x)\ , \qquad \exists! x\ P(x)\ .$$

If S has a *finite number of elements* then

$$\forall x\ P(x) \iff P(x_1) \wedge P(x_2) \wedge \cdots \wedge P(x_n)$$

$$\exists x\ P(x) \iff P(x_1) \vee P(x_2) \vee \cdots \vee P(x_n)$$

and

$$\begin{aligned} \exists! x\ P(x) \iff & \Big(P(x_1) \wedge \neg P(x_2) \wedge \neg P(x_3) \wedge \neg \cdots \wedge \neg P(x_n)\Big) \\ & \vee \Big(\neg P(x_1) \wedge P(x_2) \wedge \neg P(x_3) \wedge \neg \cdots \wedge \neg P(x_n)\Big) \\ & \vee \cdots \\ & \vee \Big(\neg P(x_1) \wedge \neg P(x_2) \wedge \neg P(x_3) \wedge \neg \cdots \wedge P(x_n)\Big) \end{aligned}$$

Let S be a set and

$$P \ : \ S \ \times \ S \ \longrightarrow \ \{ T \ , F \ \} \ .$$

Then

$$\forall x, y \ P(x, y) \qquad \text{and} \qquad \forall x \forall y \ P(x, y)$$

both mean

$$\forall x \Big(\forall y P(x, y) \Big) \ .$$

Thus $\forall x, y \ P(x, y)$ means

"*$P(x, y)$ is True for any choice of x and y*".

Similarly,

$$\exists x, y \; P(x, y) \qquad \text{and} \qquad \exists x \exists y \; P(x, y)$$

both mean

$$\exists x \Big(\exists y P(x, y) \Big) \; .$$

Thus $\exists x, y \; P(x, y)$ means

"*There exist an* x *and* y *for which* $P(x, y)$ *is True* ".

EXAMPLE :

Let

$$P \quad : \quad S \times S \longrightarrow \{ T , F \} ,$$

where

$$S = \{1, 2\} .$$

Then

$$\forall x, y \; P(x, y) \iff P(1, 1) \; \wedge \; P(1, 2) \; \wedge \; P(2, 1) \; \wedge \; P(2, 2) ,$$

while

$$\exists x, y \; P(x, y) \iff P(1, 1) \; \vee \; P(1, 2) \; \vee \; P(2, 1) \; \vee \; P(2, 2) .$$

EXERCISE : Let

$$P \ : \ \mathbb{Z} \times \mathbb{Z} \longrightarrow \{ T \ , F \ \} \ ,$$

where $P(x, y)$ denotes

$$\text{“ } x \ + \ y \ = \ 5 \text{ ”}.$$

What are the values of the following propositions ?

$$\forall x, y \ P(x, y)$$

$$\exists x, y \ P(x, y)$$

$$\forall x \ \exists ! y \ P(x, y)$$

$$\exists x \ \forall y \ P(x, y)$$

EXERCISE : Let

$$P \ : \ \mathbb{Z}^+ \times \mathbb{Z}^+ \times \mathbb{Z}^+ \longrightarrow \{ T \ , F \ \} \ ,$$

where $P(x, y, z)$ denotes the statement

$$\text{“ } x^2 \ + \ y^2 \ = \ z \text{ ”}.$$

What are the values of the following propositions?

$$\exists x, y, z \ P(x, y, z)$$

$$\forall x, y, z \ P(x, y, z)$$

$$\forall x, y \ \exists z \ P(x, y, z)$$

$$\forall x, z \ \exists y \ P(x, y, z)$$

$$\forall z \ \exists x, y \ P(x, y, z)$$

EXAMPLE :

Let

$$P,\ Q \quad : \quad S \longrightarrow \{\, T \ , F \ \} \ ,$$

where

$$S = \{1, 2\} \ .$$

Then

$$\forall x \Big(P(x) \vee Q(x) \Big) \iff \Big(P(1) \vee Q(1) \Big) \ \wedge \ \Big(P(2) \vee Q(2) \Big) \ ,$$

while

$$\forall x, y \Big(P(x) \vee Q(y) \Big) \iff$$

$$\Big(P(1) \vee Q(1) \Big) \wedge \Big(P(1) \vee Q(2) \Big) \wedge \Big(P(2) \vee Q(1) \Big) \wedge \Big(P(2) \vee Q(2) \Big) \ .$$

EXERCISE : (see preceding example $\cdots$):

Show that

$$\forall x \Big(P(x) \vee Q(x) \Big)$$

is *not equivalent* to

$$\forall x, y \Big(P(x) \vee Q(y) \Big)$$

Hint: Take $S = \{1, 2\}$, and find predicates P and Q so that one of the propositions is *True* and the other one *False* .

EXAMPLE : If

$$P,\ Q \ : \ S \longrightarrow \{\, T \ , F \,\} \ ,$$

where

$$S = \{1, 2\} \ ,$$

then

$$\exists x \Big(P(x) \wedge Q(x) \Big) \iff \Big(P(1) \wedge Q(1) \Big) \ \vee \ \Big(P(2) \wedge Q(2) \Big) \ .$$

EXAMPLE : If again

$$P,\ Q \ : \ S \longrightarrow \{\, T \ , F \,\} \ ,$$

and

$$S = \{1, 2\} \ ,$$

then

$$\forall x \Big(P(x) \to Q(x) \Big) \iff \Big(P(1) \to Q(1) \Big) \ \wedge \ \Big(P(2) \to Q(2) \Big)$$

$$\iff \Big(\neg P(1) \vee Q(1) \Big) \ \wedge \ \Big(\neg P(2) \vee Q(2) \Big) \ .$$

EXAMPLE :

$$\boxed{\Big(\forall x P(x)\Big) \vee \Big(\forall x Q(x)\Big) \quad \not\Longleftrightarrow \quad \forall x \Big(P(x) \vee Q(x)\Big)}$$

i.e., there are predicates P and Q for which the equivalence not valid.

As a *counterexample* take

$$P,\ Q \quad : \quad \mathbb{Z}^+ \longrightarrow \{\, T \,, F \,\} \,,$$

where

$$P(x) \Longleftrightarrow \text{“}x \text{ is even”} \,, \quad \text{and} \quad Q(x) \Longleftrightarrow \text{“}x \text{ is odd”} \,.$$

Then the RHS is *True* but the LHS is *False* .

EXERCISE :

Show that

$$\boxed{\Big(\exists x P(x)\Big) \wedge \Big(\exists x Q(x)\Big) \quad \not\Longleftrightarrow \quad \exists x \Big(P(x) \wedge Q(x)\Big)}$$

by giving an example where LHS and RHS have a different logical value.

Some equivalences (Valid for *any* propositions P and Q) :

(1)	$\neg\Big(\exists x P(x)\Big)$	$\Longleftrightarrow$	$\forall x\Big(\neg P(x)\Big)$
(2)	$\Big(\forall x P(x)\Big) \wedge \Big(\forall x Q(x)\Big)$	$\Longleftrightarrow$	$\forall x\Big(P(x) \wedge Q(x)\Big)$
(3)	$\Big(\forall x P(x)\Big) \wedge \Big(\forall x Q(x)\Big)$	$\Longleftrightarrow$	$\forall x \forall y\Big(P(x) \wedge Q(y)\Big)$
(4)	$\Big(\forall x P(x)\Big) \vee \Big(\forall x Q(x)\Big)$	$\Longleftrightarrow$	$\forall x \forall y\Big(P(x) \vee Q(y)\Big)$

EXAMPLE : Proof of Equivalence (1) when the set S is *finite* .

$$
\begin{aligned}
\neg\Big(\exists x P(x)\Big) &\iff \neg\Big(P(x_1) \vee P(x_2) \vee \cdots \vee P(x_n)\Big) \\
&\iff \neg\Big(P(x_1) \vee \Big(P(x_2) \vee \cdots \vee P(x_n)\Big)\Big) \\
&\iff \neg P(x_1) \wedge \neg\Big(P(x_2) \vee \cdots \vee P(x_n)\Big) \\
&\iff \cdots \\
&\iff \neg P(x_1) \wedge \neg P(x_2) \wedge \neg \cdots \wedge \neg P(x_n) \\
&\iff \forall x \neg P(x)
\end{aligned}
$$

EXERCISES :

These equivalences are easily seen to be valid:

- Prove Equivalence 2 :

$$\Big(\forall x P(x)\Big) \wedge \Big(\forall x Q(x)\Big) \iff \forall x \Big(P(x) \wedge Q(x)\Big)$$

- Prove Equivalence 3 :

$$\Big(\forall x P(x)\Big) \wedge \Big(\forall x Q(x)\Big) \iff \forall x \forall y \Big(P(x) \wedge Q(y)\Big)$$

EXAMPLE : Proof of Equivalence (4) .

$$\Big(\forall x P(x)\Big) \vee \Big(\forall x Q(x)\Big) \iff \forall x \forall y \Big(P(x) \vee Q(y)\Big)$$

NOTE : A correct proof consist of verifying that

$$\text{LHS} \Rightarrow \text{RHS} \quad \text{and} \quad \text{RHS} \Rightarrow \text{LHS}$$

or equivalently

$$\text{LHS} \Rightarrow \text{RHS} \quad \text{and} \quad \neg\, \text{LHS} \Rightarrow \neg\, \text{RHS}$$

PROOF :

(i) $\Big(\forall x P(x)\Big) \vee \Big(\forall x Q(x)\Big) \;\Rightarrow\; \forall x \forall y \Big(P(x) \vee Q(y)\Big)$

is easily seen to be *True* by a direct proof (with 2 *cases*).

(ii) $\neg\Big[\Big(\forall x P(x)\Big) \vee \Big(\forall x Q(x)\Big)\Big] \;\Rightarrow\; \neg\forall x \forall y \Big(P(x) \vee Q(y)\Big)$

can be rewritten as

$$\Big(\exists x \neg P(x)\Big) \wedge \Big(\exists x \neg Q(x)\Big) \;\Rightarrow\; \exists x \exists y \Big(\neg P(x) \wedge \neg Q(y)\Big)$$

P and Q being arbitrary, we may replace them by $\neg P$ and $\neg Q$:

$$\Big(\exists x P(x)\Big) \wedge \Big(\exists x Q(x)\Big) \;\Rightarrow\; \exists x \exists y \Big(P(x) \wedge Q(y)\Big)$$

which is easily seen to be *True* by a direct proof.

QED !

EXERCISE :

Prove that the equivalence

$$\boxed{\Big(\forall x P(x)\Big) \wedge \Big(\exists x Q(x)\Big) \iff \forall x \exists y \Big(P(x) \wedge Q(y)\Big)}$$

is valid for *all* propositions P and Q.

Hint : This proof can be done along the lines of the preceding proof.

More equivalences (Valid for *any* propositions P and Q) :

(5)	$\neg\Big(\forall x P(x)\Big)$	$\Longleftrightarrow$	$\exists x \neg P(x)$
(6)	$\Big(\exists x P(x)\Big) \vee \Big(\exists x Q(x)\Big)$	$\Longleftrightarrow$	$\exists x \Big(P(x) \vee Q(x)\Big)$
(7)	$\Big(\exists x P(x)\Big) \vee \Big(\exists x Q(x)\Big)$	$\Longleftrightarrow$	$\exists x \exists y \Big(P(x) \vee Q(y)\Big)$
(8)	$\Big(\exists x P(x)\Big) \wedge \Big(\exists x Q(x)\Big)$	$\Longleftrightarrow$	$\exists x \exists y \Big(P(x) \wedge Q(y)\Big)$

Equivalences (5)-(8) follow from

- negating equivalences (1)-(4), and
- replacing P by $\neg P$ and Q by $\neg Q$ ..

EXAMPLE : Proof of Equivalence (6), using Equivalence (2)

(2)	$\Big(\forall x P(x)\Big) \wedge \Big(\forall x Q(x)\Big) \iff \forall x \Big(P(x) \wedge Q(x)\Big)$
	$\neg\Big(\Big(\forall x P(x)\Big) \wedge \Big(\forall x Q(x)\Big)\Big) \iff \neg\forall x \Big(P(x) \wedge Q(x)\Big)$
	$\Big(\exists x \neg P(x)\Big) \vee \Big(\exists x \neg Q(x)\Big)\Big) \iff \exists x \Big(\neg P(x) \vee \neg Q(x)\Big)$
(6)	$\Big(\exists x P(x)\Big) \vee \Big(\exists x Q(x)\Big) \iff \exists x \Big(P(x) \vee Q(x)\Big)$

EXERCISE :

- Prove Equivalence 7 using Equivalence 3.

- Prove Equivalence 8 using Equivalence 4.

EXAMPLE (of *negating* a logical expression) :

$$\neg\exists x\forall y\forall z P(x,y,z) \iff \forall x\neg\Big(\forall y\Big(\forall z P(x,y,z)\Big)\Big)$$

$$\iff \forall x\exists y\neg\Big(\forall z P(x,y,z)\Big)$$

$$\iff \forall x\exists y\exists z\neg P(x,y,z)$$

EXAMPLE (of *transforming* a logical expression) :

$$
\begin{aligned}
\exists x\Big(P(x) \to Q(x)\Big) \quad &\Longleftrightarrow \quad \exists x\Big(\neg P(x) \vee Q(x)\Big) \\
&\Longleftrightarrow \quad \Big(\exists x \neg P(x)\Big) \vee \Big(\exists x Q(x)\Big) \qquad \star \\
&\Longleftrightarrow \quad \Big(\neg \forall x P(x)\Big) \vee \Big(\exists x Q(x)\Big) \\
&\Longleftrightarrow \quad \Big(\forall x P(x)\Big) \to \Big(\exists x Q(x)\Big)
\end{aligned}
$$

$\star$ This step follows from the earlier Equivalence 6.

EXAMPLE : (from Rosen's book: in detail)

Let

$D(x)$	denote the statement	"x is a duck"
$P(x)$	,,	"x is one of my poultry"
$O(x)$	,,	"x is an officer"
$W(x)$	,,	"x is willing to waltz"

Statement	logic	equivalent
Ducks never waltz	$\neg\exists x\Big(D(x)\wedge W(x)\Big)$	$\forall x\Big((D(x)\rightarrow\neg W(x)\Big)$
Officers always waltz	$\neg\exists x\Big((O(x)\wedge\neg W(x)\Big)$	$\forall x\Big((O(x)\rightarrow W(x)\Big)$
All my poultry are ducks	$\forall x\Big((D(x)\vee\neg P(x)\Big)$	$\forall x\Big((P(x)\rightarrow D(x)\Big)$
My poultry are not officers	$\forall x\neg\Big(O(x)\wedge P(x)\Big)$	$\forall x\Big((P(x)\rightarrow\neg O(x)\Big)$

QUESTION : Do the first three statements imply the last one?

Do the first three statements imply the last one, *i.e.*, is

$$\Big[\Big(\forall x(D(x) \to \neg W(x))\Big) \ \wedge \ \Big(\forall x(O(x) \to W(x))\Big) \ \wedge \ \Big(\forall x(P(x) \to D(x))\Big)\Big]$$
$$\to \quad \Big(\forall x(P(x) \to \neg O(x))\Big)$$

a tautology, *i.e.*, do we have

$$\Big[\Big(\forall x(D(x) \to \neg W(x))\Big) \ \wedge \ \Big(\forall x(O(x) \to W(x))\Big) \ \wedge \ \Big(\forall x(P(x) \to D(x))\Big)\Big]$$
$$\Rightarrow \quad \Big(\forall x(P(x) \to \neg O(x))\Big)$$

The answer is *YES* .

In fact, it is a tautology for *any* predicates D, O, P, W.

$$\Big[\underbrace{\Big(\forall x(D(x) \to \neg W(x))\Big)}_{(1)} \wedge \underbrace{\Big(\forall x(O(x) \to W(x))\Big)}_{(2)} \wedge \underbrace{\Big(\forall x(P(x) \to D(x))\Big)}_{(3)}\Big]$$

$$\Rightarrow \underbrace{\Big(\forall x(P(x) \to \neg O(x))\Big)}_{(4)}$$

To prove this, we must show that :

if (1) , (2) , and (3) are *True* then (4) is *True* .

To show (4) is *True* , we must show:

If, for arbitrary z, $P(z)$ is *True* then, using (1,2,3), $\neg O(z)$ is *True* .

$$\Big[\underbrace{\Big(\forall x(D(x) \to \neg W(x))\Big)}_{(1)} \wedge \underbrace{\Big(\forall x(O(x) \to W(x))\Big)}_{(2)} \wedge \underbrace{\Big(\forall x(P(x) \to D(x))\Big)}_{(3)}\Big]$$

$$\Rightarrow \underbrace{\Big(\forall x(P(x) \to \neg O(x))\Big)}_{(4)}$$

PROOF : Let z be an arbitrary element from our set of objects.

Assume $P(z)$ is *True* .

We must show that $\neg O(z)$ is *True* , *i.e.*, $O(z)$ is *False* .

From (3) it follows $D(z)$ is *True* .

From (1) follows $\neg W(z)$ is *True* . *i.e.*, $W(z)$ is *False* .

From (2), since $W(z)$ is *False* , it follows $O(z)$ is *False* . **QED !**

EXERCISE (from Rosen):

Express each of the following using predicates and quantifiers:

(1) All clear explanations are satisfactory.

(2) Some excuses are unsatisfactory.

(3) Some excuses are not clear explanations.

Question : Does (3) follow from (1) and (2) ?

Hint : See preceding example.

REVIEW EXERCISES.

Problem 1. By truth table check if the $\oplus$ operator is associative:

$$(p \oplus q) \oplus r \iff p \oplus (q \oplus r) \ .$$

Problem 2. Use logical equivalences to prove that

$$p \to (q \to r) \iff (p \wedge q) \to r \ .$$

Problem 3. By contradiction show that the following is a tautology:

$$[(p \vee t) \wedge (p \to q) \wedge (q \to r) \wedge (r \to s) \wedge (s \to t)] \ \to \ t \ .$$

Problem 4. Use logical equivalences to simplify

$$([(p \wedge q) \leftrightarrow p] \to p) \ \to \ (p \to q) \ .$$

Problem 5. Verify the following basic tautologies, which are known as "*laws of inference*", and which are useful in proofs:

Tautology	Name
$(p \wedge (p \to q)) \Rightarrow q$	modus ponens
$(\neg q \wedge (p \to q)) \Rightarrow \neg p$	modus tollens
$((p \to q) \wedge (q \to r)) \Rightarrow (p \to r)$	hypothetical syllogism
$((p \vee q) \wedge \neg p) \Rightarrow q$	disjunctive syllogism
$((p \vee q) \wedge (\neg p \vee r)) \Rightarrow (q \vee r)$	resolution

Problem 6. Express the following statements in predicate logic:

(a) "*There is a unique x for which $P(x)$ is True* ."

(b) "*There is no greatest integer*."

(c) "*x_0 is the smallest integer for which $P(x)$ is True* ."

(d) "*Every person has exactly two parents*."

NOTE :

- Let $P(x, y)$ denote "*y is a parent of x* " .
- You may use the predicates $x \leq y$, $x > y$, and $x \neq y$.

Problem 7.

Let $P(x, y, z)$ denote the statement

$$x^2\ y\ =\ z\ ,$$

where the universe of discourse of all three variables is the set $\mathbb{Z}$.

What is the truth value of each of the following?

$P(1, 1, 1)$ $\qquad$ $\forall y, z \exists x P(x, y, z)$

$P(0, 7, 0)$ $\qquad$ $\exists! y, z \forall x P(x, y, z)$

$\forall x, y, z P(x, y, z)$ $\qquad$ $\forall x, y \exists z P(x, y, z)$

$\exists x, y, z P(x, y, z)$ $\qquad$ $\forall x \exists y, z P(x, y, z)$

Problem 8.

Let $P(x, y, z, n)$ denote the statement

$$x^n + y^n = z^n ,$$

where $x, y, z, n \in \mathbb{Z}^+$.

What is the truth value of each of the following:

$P(1, 1, 2, 1)$	$\forall x, y \exists! z P(x, y, z, 1)$
$P(3, 4, 5, 2)$	$\forall z \exists x, y P(x, y, z, 1)$
$P(7, 24, 25, 2)$	$\exists x, y \forall z P(x, y, z, 2)$
$\exists! x, y, z P(x, y, z, 2)$	$\exists x, y, z P(x, y, z, 3)$

NOTE : One of the above is very difficult!

Problem 9.

Give an example that shows that

$$\forall x \exists y P(x,y) \iff \exists y \forall x P(x,y) \ .$$

Problem 10.

Prove that

$$\forall x [P(x) \to Q(x)] \Rightarrow [\forall x P(x) \to \forall x Q(x)].$$

Problem 11.

Prove that

$$\forall x \exists y (P(x) \vee Q(y)) \iff \forall x P(x) \vee \exists x Q(x) \ .$$

MATHEMATICAL PROOFS.

- We will illustrate some often used *basic proof techniques* .

  (Some of these techniques we have already seen $\cdots$)

- Several examples will be taken from elementary Number Theory.

DEFINITIONS : Let $n, m \in \mathbb{Z}^+$.

- We call n *odd* if $\exists k \in \mathbb{Z} \ : \ k \geq 0, \ n = 2k + 1$.
- We call n *even* if n is not odd. (Then $n = 2k$ for some $k \in \mathbb{Z}^+$.)

- We say "m *divides* n", and write $m|n$, if $n = qm$ for some $q \in \mathbb{Z}^+$.
- In this case we call m a *divisor* of n.
- If $m|n$ then we also say that "n *is divisible by* m".

- n $(n \geq 2)$ is a *prime number* if its only positive divisors are 1 and n.
- n $(n \geq 2)$ *composite* if it is not prime.
- n and m are *relatively prime* if 1 is their only common divisor.

Direct proofs.

Many mathematical statements have the form

$$\text{“ if } \; P \; \text{ then } \; Q \text{ ”}$$

i.e.,

$$P \;\Rightarrow\; Q \;,$$

or, more often,

$$\forall x \Big(P(x) \rightarrow Q(x) \Big) \;,$$

where P and Q represent *specific predicates* .

RECALL : a *direct proof* consists of

- assuming that, for arbitrary x, $P(x)$ is *True*
- demonstrating that $Q(x)$ is then necessarily *True* also,

PROPOSITION : If $n \in \mathbb{Z}^+$ is odd then n^2 is odd.

REMARK :

This proposition is of the form $P \Rightarrow Q$ or, more specifically,

$$\forall n \in \mathbb{Z}^+ \ : \ P(n) \ \rightarrow \ Q(n) \ ,$$

where P and Q are predicates (functions)

$$P, \ Q \ : \ \mathbb{Z}^+ \ \longrightarrow \ \{ T \ , F \ \} \ ,$$

namely,

$$P(n) \Longleftrightarrow \text{"}n \ is \ odd \text{"} \quad , \quad Q(n) \Longleftrightarrow \text{"}n^2 \ is \ odd \text{"} \ .$$

NOTE : Actually $Q(n) \Longleftrightarrow P(n^2)$ here !

If $n \in \mathbb{Z}^+$ is odd then n^2 is odd.

PROOF :

Assume $n \in \mathbb{Z}^+$ is odd (*i.e.*, assume $P(n) = T$).

Then, by definition, $n = 2k + 1$ for some $k \in \mathbb{Z}$, $k \geq 0$.

By computation we find

$$n^2 \;=\; (2k+1)^2 \;=\; 2(2k^2+2k)+1 \;=\; 2m+1 \;,$$

where we have defined $m \equiv 2k^2 + 2k$.

Thus, by definition, n^2 is odd, *i.e.*, $Q(n) = T$. **QED !**

PROPOSITION : If $n \in \mathbb{Z}^+$ is odd then $8 \mid (n-1)(n+1)$.

PROOF : If $n \in \mathbb{Z}^+$ is odd then we can write

$$n \;=\; 2k+1 \quad \text{for some integer } k, \quad k \geq 0 \; .$$

By computation we find

$$(n-1)(n+1) \;=\; n^2-1 \;=\; 4k^2+4k \;=\; 4k(k+1) \; .$$

Clearly

$$4 \mid 4k(k+1) \; .$$

Note, however, that either k is even or $k+1$ is even, *i.e.*,

$$2 \mid k \qquad \text{or} \qquad 2 \mid (k+1) \; .$$

Thus

$$8 \mid 4k(k+1) \; . \qquad\qquad \textbf{QED !}$$

LEMMA (Needed in the following example $\cdots$) For $x \in \mathbb{R}$, $x \neq 0, 1$:

$$\sum_{k=0}^{n} x^k \quad = \quad \frac{1 - x^{n+1}}{1 - x} \ , \qquad \forall n \geq 0 \ , \qquad (\ \textit{Geometric sum} \ ) \ .$$

PROOF (a *"constructive proof"*) :

Let

$$S_n \quad = \quad \sum_{k=0}^{n} x^k \ .$$

Then

$$S_n \quad = \quad 1 \ + \ x \ + \ x^2 \ + \ \cdots \ + \ x^{n-1} \ + \ x^n \ ,$$

$$x \cdot S_n \quad = \quad x \ + \ x^2 \ + \ \cdots \ + \ x^{n-1} \ + \ x^n \ + \ x^{n+1} \ ,$$

so that

$$S_n \ - \ x \cdot S_n \quad = \quad (1 - x) \cdot S_n \quad = \quad 1 - x^{n+1} \ ,$$

from which the formula follows. **QED !**

DEFINITION :

A *perfect number* is a number that equals the sum of all of its divisors, except the number itself.

EXAMPLES :

6 is perfect :

$$6 \;=\; 3 \;+\; 2 \;+\; 1\;,$$

and 28 is perfect :

$$28 \;=\; 14 \;+\; 7 \;+\; 4 \;+\; 2 \;+1\;,$$

and so is 496 :

$$496 \;=\; 248 \;+\; 124 \;+\; 62 \;+\; 31 \;+\; 16 \;+\; 8 \;+\; 4 \;+\; 2 \;+\; 1\;.$$

PROPOSITION : Let $m \in \mathbb{Z}^+$, $m > 1$.

$$\text{If } 2^m - 1 \text{ is prime, then } n \equiv 2^{m-1}(2^m - 1) \text{ is perfect,}$$

or, using quantifiers,

$$\forall m \in \mathbb{Z}^+ \ : \ 2^m - 1 \text{ is prime} \ \rightarrow \ 2^{m-1}(2^m - 1) \text{ is perfect .}$$

PROOF : Assume $2^m - 1$ is prime.

Then the divisors of $n \ = \ 2^{m-1}(2^m - 1)$ are

$$1, \ 2, \ 2^2, \ 2^3, \ \cdots, \ 2^{m-1} \ ,$$

and

$$(2^m - 1), \ 2(2^m - 1), \ 2^2(2^m - 1), \ \cdots, \ 2^{m-2}(2^m - 1), \ 2^{m-1}(2^m - 1) \ .$$

The last divisor is equal to n , so we do not include it in the sum.

The sum is then

$$\begin{aligned}
\sum_{k=0}^{m-1} 2^k \;+\; (2^m-1)\sum_{k=0}^{m-2} 2^k \;&=\; \frac{1-2^m}{1-2} \;+\; (2^m-1)\frac{1-2^{m-1}}{1-2} \\
&=\; (2^m-1) \;+\; (2^m-1)(2^{m-1}-1) \\
&=\; (2^m-1)\,(1+2^{m-1}-1) \\
&=\; (2^m-1)\,2^{m-1} \;=\; n. \qquad\qquad \textbf{QED !}
\end{aligned}$$

NOTE : We used the formula

$$\sum_{k=0}^{m} x^k \;=\; \frac{1-x^{m+1}}{1-x}\;, \qquad (\text{the } \textit{geometric sum})\;,$$

(valid for $x \neq 0, 1$).

Proving the contrapositive.

It is easy to see (by Truth Table) that

$$p \to q \iff \neg q \to \neg p \ .$$

EXAMPLE :

The statement

$$\text{“}n^2 \text{ even} \Rightarrow n \text{ even”},$$

proved earlier is equivalent to

$$\text{“}\neg(n \text{ even}) \Rightarrow \neg(n^2 \text{ even})\text{”},$$

i.e., it is equivalent to

$$n \text{ odd} \Rightarrow n^2 \text{ odd} \ .$$

This equivalence justifies the following :

If we must prove

$$P \Rightarrow Q \ ,$$

then we may equivalently prove the *contrapositive*

$$\neg Q \Rightarrow \neg P \ .$$

(Proving the contrapositive is *sometimes easier* .)

PROPOSITION : Let $n \in \mathbb{Z}^+$, with $n \geq 2$.

If the sum of the divisors of n is equal to $n + 1$ then n is prime.

PROOF : We prove the contrapositive :

If n is *not* prime then the sum of the divisors can *not* equal $n + 1$.

So suppose that n is not prime.

Then n has divisors

$$1,\ n,\ \text{and } m,\quad \text{for some } m \in \mathbb{Z}^+,\ m \neq 1,\ m \neq n\ ,$$

and possibly more.

Thus the sum of the divisors is greater than $n + 1$. **QED !**

Some specific contrapositives.

$(p \wedge q) \rightarrow r$	$\Longleftrightarrow$	$\neg r \rightarrow (\neg p \vee \neg q)$
$(p \vee q) \rightarrow r$	$\Longleftrightarrow$	$\neg r \rightarrow (\neg p \wedge \neg q)$
$\Big(\forall x P(x)\Big) \rightarrow q$	$\Longleftrightarrow$	$\neg q \rightarrow \Big(\exists x \neg P(x)\Big)$
$\Big(\exists x P(x)\Big) \rightarrow q$	$\Longleftrightarrow$	$\neg q \rightarrow \Big(\forall x \neg P(x)\Big)$
$p \rightarrow \forall x Q(x)$	$\Longleftrightarrow$	$\Big(\exists x \neg Q(x)\Big) \rightarrow \neg p$
$p \rightarrow \exists x Q(x)$	$\Longleftrightarrow$	$\Big(\forall x \neg Q(x)\Big) \rightarrow \neg p$

PROPOSITION : Let $n \in \mathbb{Z}^+$, with $n \geq 2$.

$$\forall a, b \in \mathbb{Z}^+ \; (\; n|a \; \vee \; n|b \; \vee \; n \not| ab \;) \qquad \Rightarrow \qquad n \text{ is prime .}$$

PROOF : The contrapositive is

$$\text{If} \quad n \quad \text{is not prime} \quad \text{then} \quad \exists a, b \; (\; n \not| a \; \wedge \; n \not| b \; \wedge \; n|ab \;) \; .$$

Here the contrapositive is *easier to understand* and quite *easy to prove* :

Note that if n is not prime then

$$n \; = \; a \; b \; ,$$

for certain integers a and b, both greater than 1 and less than n.

Clearly $n \not| a$, $n \not| b$, and $n|ab$. **QED !**

PROPOSITION : Let $n \in \mathbb{Z}^+$. Then

$$5|n^2 \quad \Rightarrow \quad 5|n \ ,$$

PROOF : We prove the *contrapositive* , *i.e.*,

$$5 \not| n \quad \Rightarrow \quad 5 \not| n^2 \ .$$

So suppose $5 \not| n$.

Then we have the following *cases* :

$$\begin{array}{lcl}
n = 5k+1 & \Rightarrow & n^2 = 25k^2 + 10k + 1 \ = \ 5(5k^2 + 2k) + 1 \ , \\
n = 5k+2 & \Rightarrow & n^2 = 25k^2 + 20k + 4 \ = \ 5(5k^2 + 4k) + 4 \ , \\
n = 5k+3 & \Rightarrow & n^2 = 25k^2 + 30k + 9 \ = \ 5(5k^2 + 6k + 1) + 4 \ , \\
n = 5k+4 & \Rightarrow & n^2 = 25k^2 + 40k + 16 = \ 5(5k^2 + 8k + 3) + 1 \ ,
\end{array}$$

for $k \in \mathbb{Z}$, $k \geq 0$.

This shows that $5 \not| n^2$. **QED !**

Proof by contradiction.

To prove a statement $P \Rightarrow Q$ *by contradiction* :

- assume $P = T$ and $Q = F$,

- show that these assumptions lead to an impossible conclusion (a "contradiction").

(We have already seen some proofs by contradiction.)

PROPOSITION :

If a prime number is the sum of two prime numbers

then one of these equals 2.

PROOF :

Let p_1, p_2, and p be prime numbers, with $p_1 + p_2 = p$.

Suppose that neither p_1 nor p_2 is equal to 2.

Then both p_1 and p_2 must be odd (and greater than 2) .

Hence $p = p_1 + p_2$ is even, and greater than 2.

This contradicts that p is prime. **QED !**

PROPOSITION : $\sqrt{2}$ is irrational, *i.e.*, if $m, n \in \mathbb{Z}^+$ then $\frac{m}{n} \neq \sqrt{2}$.

PROOF : Suppose $m, n \in \mathbb{Z}^+$ and $\frac{m}{n} = \sqrt{2}$.

We may assume m and n are *relatively prime* (cancel common factors).

Then $m = \sqrt{2}\, n$	$\Rightarrow$	$m^2 = 2n^2$	*
	$\Rightarrow$	m^2 even	
	$\Rightarrow$	m even	(proved earlier)
	$\Rightarrow$	$\exists k \in \mathbb{Z}^+ (m = 2k)$	
	$\Rightarrow$	$2n^2 = m^2 = (2k)^2 = 4k^2$	(using * above)
	$\Rightarrow$	$n^2 = 2k^2$	
	$\Rightarrow$	n^2 even	
	$\Rightarrow$	n even	

Thus both n and m are even and therefore both are divisible by two.

This contradicts that they are relatively prime. **QED !**

NOTATION : The "$\Rightarrow$" means that the immediately following statement is implied by the preceding statement(s).

EXERCISE :

Use a proof by contradiction to show the following:

$$(p \vee q) \ \wedge \ (p \rightarrow r) \ \wedge \ (q \rightarrow r) \quad \Rightarrow \quad r \ .$$

$$(p \rightarrow q) \ \wedge \ (q \rightarrow r) \quad \Rightarrow \quad p \rightarrow r \ .$$

Hint : See a similar example earlier in the Lecture Notes.

PROPOSITION :

If the integers

$$1,\ 2,\ 3,\ \cdots,\ 10,$$

are placed around a circle, in any order, then there exist three integers in consecutive locations around the circle that have a sum greater than or equal to 18.

PROOF : (by contradiction)

Suppose any three integers in consecutive locations around the circle have sum less than 18, that is, less then or equal to 17.

Excluding the number 1, which must be placed somewhere, there remain exactly three groups of three integers in consecutive locations.

The total sum is then less than or equal to $1 + 17 + 17 + 17 = 52$.

However, we know that this sum must equal

$$1 + 2 + 3 + \cdots + 10 = 55 .$$

Hence we have a contradiction. **QED !**

Proof by cases (another example) :

PROPOSITION : Let $n \in \mathbb{Z}^+$. Then

$$6 \mid n(n+1)(n+2) \ .$$

PROOF : We always have that $2|n$ or $2|(n+1)$. (Why ?)

There remain *three cases* to be considered :

For some $k \in \mathbb{Z}^+$, $k \geq 0$:

$$n = 3k \quad : \quad \text{Then } 3|n \ ,$$

$$n = 3k+1 \quad : \quad \text{Then } 3|(n+2) \ ,$$

$$n = 3k+2 \quad : \quad \text{Then } 3|(n+1) \ .$$

QED !

FACT : Any real number x can be uniquely written as

$$x \;=\; n \;+\; r \;,$$

where

$$n \in \mathbb{Z} \quad \text{and} \quad r \in \mathbb{R} \;, \quad \text{with} \quad 0 \leq r < 1 \;.$$

DEFINITION : We then define the *floor* of x as

$$\lfloor x \rfloor \;\equiv\; n \;.$$

EXAMPLES : $\lfloor 7 \rfloor = 7$, $\lfloor -7 \rfloor = -7$, $\lfloor \pi \rfloor = 3$, $\lfloor -\pi \rfloor = -4$.

EXAMPLE : Use a proof by cases to show that

$$\lfloor 2x \rfloor \;=\; \lfloor x \rfloor \;+\; \lfloor x + \frac{1}{2} \rfloor \;.$$

$$\lfloor 2x \rfloor \;=\; \lfloor x \rfloor \;+\; \lfloor x + \tfrac{1}{2} \rfloor \qquad , \qquad x \;=\; n \;+\; r \qquad , \quad 0 \;\leq\; r \;<\; 1$$

PROOF :

Case 1 : $0 \;\leq\; r \;<\; \frac{1}{2}$: Then

$$0 \;\leq\; 2r \;<\; 1 \qquad \text{and} \qquad \frac{1}{2} \;\leq\; r + \frac{1}{2} \;<\; 1 \,.$$

LHS :
$$\lfloor 2x \rfloor \;=\; \lfloor 2n + 2r \rfloor \;=\; 2n$$

RHS :
$$\lfloor x \rfloor \;=\; \lfloor n + r \rfloor \;=\; n$$

$$\lfloor x + \frac{1}{2} \rfloor \;=\; \lfloor n + r + \frac{1}{2} \rfloor \;=\; n$$

so that the identity is satisfied.

$$\lfloor 2x \rfloor \;=\; \lfloor x \rfloor \;+\; \lfloor x + \tfrac{1}{2} \rfloor \qquad , \qquad x \;=\; n \;+\; r \qquad , \quad 0 \;\leq\; r \;<\; 1$$

PROOF : (continued $\cdots$)

Case 2 : $\frac{1}{2} \leq r < 1$: Then

$$1 \;\leq\; 2r < 2 \qquad \text{and} \qquad 1 \;\leq\; r + \frac{1}{2} \;<\; 1 \;+\; \frac{1}{2} \,.$$

LHS :
$$\lfloor 2x \rfloor \;=\; \lfloor 2n + 2r \rfloor \;=\; 2n + 1$$

RHS :
$$\lfloor x \rfloor \;=\; \lfloor n + r \rfloor \;=\; n$$

$$\lfloor x + \frac{1}{2} \rfloor \;=\; \lfloor n + r + \frac{1}{2} \rfloor \;=\; n + 1$$

so that the identity is satisfied. **QED !**

Existence proofs.

- Mathematical problems often concern the *existence*, or *non-existence*, of certain objects.

- Such problems may arise from the mathematical formulation of problems that arise in many scientific areas.

- A proof that establishes the existence of a certain object is called an *existence proof*.

EXAMPLE : For any positive integer n there exists a sequence of n *consecutive composite integers* , *i.e.*,

$$\forall n \in \mathbb{Z}^+ \exists m \in \mathbb{Z}^+ \ : \ m+i \ \text{ is composite } , \ i = 1, \cdots, n \ .$$

For example,

$n = 2$: (8,9) are 2 consecutive composite integers ($m = 7$),

$n = 3$: (8,9,10) are 3 three consecutive composite integers ($m = 7$),

$n = 4$: (24,25,26,27) are 4 consecutive composite integers ($m = 23$),

$n = 5$: (32,33,34,35,36) are 5 consecutive composite integers ($m = 31$).

$$\forall n \in \mathbb{Z}^+ \exists m \in \mathbb{Z}^+ \ : \ m+i \ \text{ is composite }, \ i = 1, \cdots, n \ .$$

PROOF :

Let $m = (n+1)! + 1$.

Then, clearly, the n consecutive integers

$$(n+1)! + 1 + 1, \quad (n+1)! + 1 + 2, \quad \cdots, \quad (n+1)! + 1 + n \ ,$$

are composite. (Why ?) **QED !**

NOTE : This is a *constructive* existence proof : We demonstrated the existence of m by showing its value (as a function of n).

PROPOSITION : There are infinitely many prime numbers.

The idea of the proof (*by contradiction*) :

- Assume there is only a *finite* number of prime numbers.
- Then we'll show $\exists N > 1 \in \mathbb{Z}^+$ that is *neither prime nor composite* .
- But this is *impossible* !
- Thus there must be *infinitely* many prime numbers !

PROOF :

Suppose the total number of primes is *finite* , say,

$$p_1,\ p_2,\ \cdots,\ p_n\ .$$

Let

$$\boxed{N\ =\ p_1 p_2 \cdots p_n\ +\ 1}$$

- Then N cannot be prime. (Why not ?)

- Also, none of the $p_1, p_2, \cdots, p_n$ divide N,

  since N divided by p_i gives a remainder of 1 , $(i = 1, \cdots, n)$.

- Thus N cannot be composite either ! **QED !**

NOTE :

- This proof is a *non-constructive* existence proof.

- We proved the existence of an infinite number of primes without actually showing them !

NOTE :

- There is no general recipe for proving a mathematical statement and often there is more than one correct proof.

- One generally tries to make a proof as simple as possible, so that others may understand it more easily.

- Nevertheless, proofs can be very difficult, even for relatively simple statements such as Fermat's Last Theorem :

$$\neg\exists x, y, z, n \in \mathbb{Z}^+, n \geq 3 \ : \ x^n + y^n = z^n \ .$$

NOTE :

- There are many mathematical statements that are thought to be correct, but that have not yet been proved ("*open problems* "), *e.g.*, the "*Goldbach Conjecture* " :

"Every even integer greater than 2 is the sum of two prime numbers".

- Indeed, proving mathematical results is as much an art as it is a science, requiring creativity as much as clarity of thought.

- An essential first step is always to fully understand the problem.

- Where possible, experimentation with simple examples may help build intuition and perhaps suggest a possible method of proof.

REVIEW EXERCISES.

Problem 1. Use a *direct proof* to show the following:

$$(p \vee q) \ \wedge \ (q \to r) \ \wedge \ \Big((p \wedge s) \to t \Big) \ \wedge \ \Big(\neg q \to (u \wedge s) \Big) \ \wedge \ \neg r \ \Rightarrow \ t \ .$$

(Assuming the left-hand-side is *True* , you must show that t is *True* .)

Problem 2. Let n be a positive integer.

Prove the following statement by proving its contrapositive:

$$\text{"}\textit{If} \ \ n^3 + 2n + 1 \ \ \textit{is odd then} \ \ n \ \ \textit{is even}\text{"}.$$

Problem 3. Let n be an integer. Show that

$$3|n^2 \quad \Rightarrow \quad 3|n \ ,$$

by proving its contrapositive.

Hint : There are two cases to consider.

Problem 4. Give a direct proof to show the following:

The sum of the squares of any two rational numbers is a rational number.

Problem 5.

Show that for all positive real x

$$\text{if } x \text{ is irrational then } \sqrt{x} \text{ is irrational .}$$

by proving the *contrapositive* .

Problem 6. Use a proof *by contradiction* to prove the following:

If the integers $1,\ 2,\ 3,\ \cdots,\ 7,$ are placed around a circle, in any order, then there exist two adjacent integers that have a sum greater than or equal to 9 .

(Can you also give a *direct Proof* ?)

FACT : Any real number x can be uniquely written as

$$x \;=\; n \;-\; r \;,$$

where

$$n \in \mathbb{Z} \quad \text{and} \quad r \in \mathbb{R} \;, \quad \text{with} \quad 0 \leq r < 1 \;.$$

DEFINITION : We then define the *ceiling* of x as

$$\lceil x \rceil \;\equiv\; n \;.$$

EXAMPLES : $\lceil 7 \rceil = 7$, $\lceil -7 \rceil = -7$, $\lceil \pi \rceil = 4$, $\lceil -\pi \rceil = -3$.

Problem 7.

Is the following equality valid for all positive integers n and m ?

$$\lfloor \frac{n+m}{2} \rfloor \;=\; \lceil \frac{n}{2} \rceil \;+\; \lfloor \frac{m}{2} \rfloor \;.$$

If *Yes* then give a proof. If *No* then give a counterexample.

SET THEORY

Basic definitions.

- Let U be the collection of all objects under consideration.

  (U is also called the "*universe*" of objects under consideration.)

- A *set* is a collection of objects from U.

Let A , B , and C be sets.

$x \in A \iff$ "x is an element (a member) of A".	
$x \notin A \iff \neg(x \in A)$	
$A \subseteq B \iff \forall x \in U : x \in A \Rightarrow x \in B$	subset
$A = B \iff (A \subseteq B) \wedge (B \subseteq A)$	equality

The above take values in $\{ T , F \}$.

The following are *set-valued* :

$A \cup B \equiv \{ x \in U : (x \in A) \vee (x \in B) \}$		union
$A \cap B \equiv \{ x \in U : (x \in A) \wedge (x \in B) \}$		intersection
$\bar{A} \equiv \{ x \in U : x \notin A \}$		complement
$A - B \equiv \{ x \in U : (x \in A) \wedge (x \notin B) \}$		difference

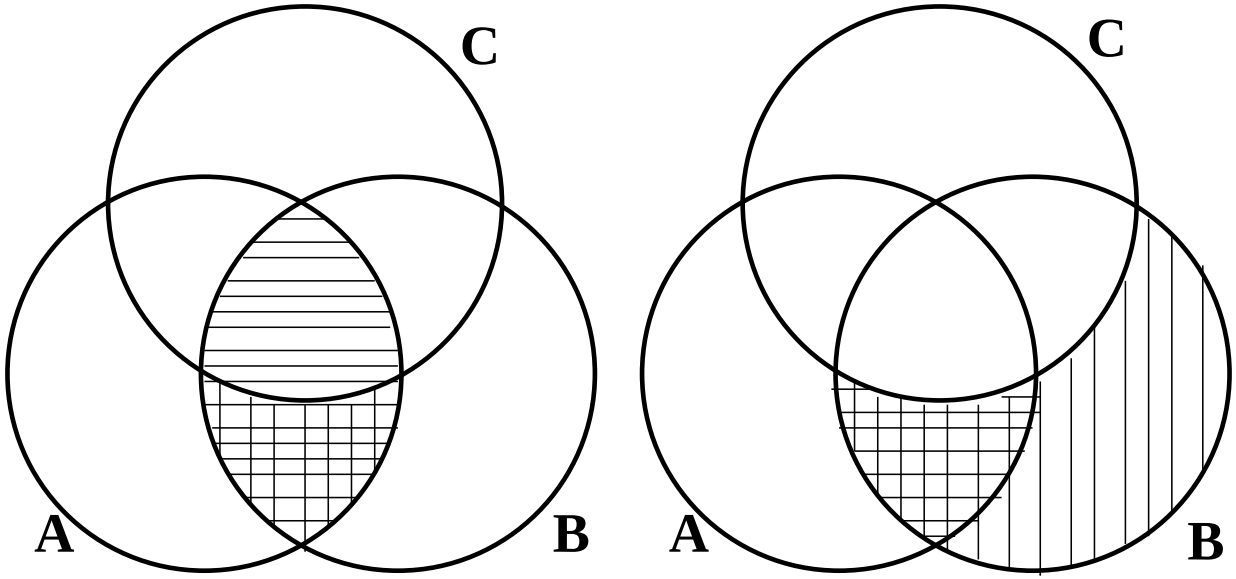
Venn diagram.

This is a useful visual aid for proving set theoretic identities.

EXAMPLE : For the two sides of the identity

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

we have the following Venn diagrams :



The *actual proof* of the identity, using the above definitions and the laws of logic, is as follows :

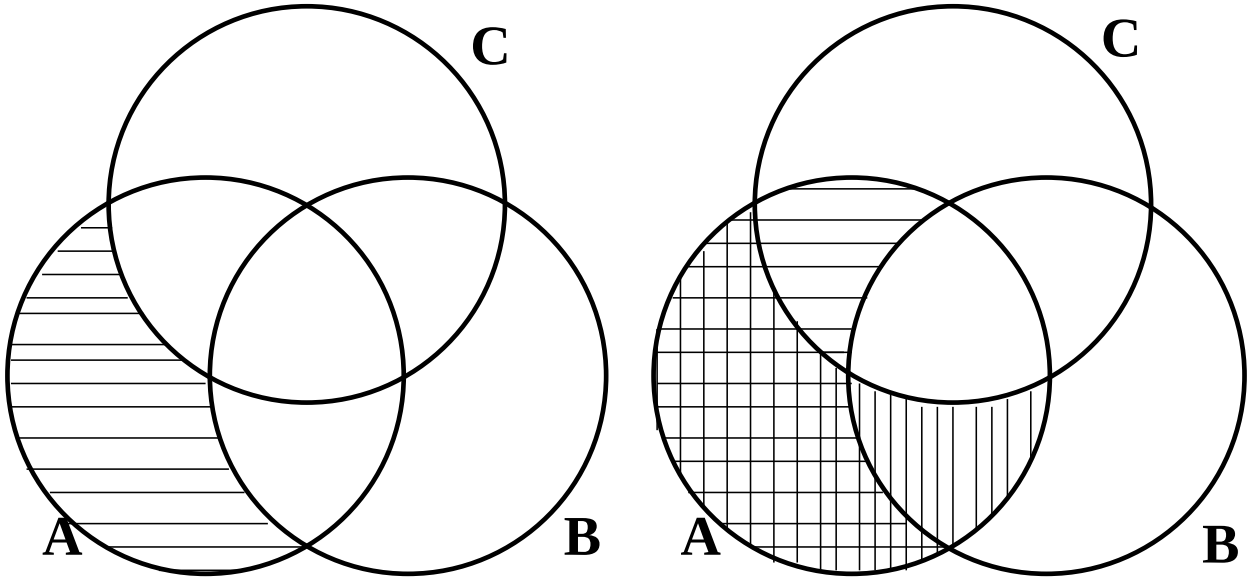
$x \in \Big((A \cap B) - C\Big)$	
$\iff x \in (A \cap B) \ \wedge \ x \notin C$	
$\iff (x \in A \wedge x \in B) \ \wedge \ x \notin C$	
$\iff x \in A \ \wedge \ (x \in B \ \wedge \ x \notin C)$	associative law
$\iff x \in A \ \wedge \ x \in (B - C)$	
$\iff x \in A \cap (B - C)$	

EXAMPLE :

For the two sides of the identity

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

we have the following Venn diagrams :



The *actual proof* of the identity is as follows :

$x \in \Big(A - (B \cup C)\Big)$	
$\iff \quad x \in A \ \wedge \ x \notin (B \cup C)$	
$\iff \ x \in A \ \wedge \ \neg(x \in (B \cup C))$	
$\iff \ x \in A \ \wedge \ \neg(x \in B \vee x \in C)$	
$\iff \ x \in A \ \wedge \ x \notin B \ \wedge \ x \notin C$	de Morgan
$\iff \ x \in A \ \wedge \ x \in A \ \wedge \ x \notin B \ \wedge x \ \notin C$	idempotent law
$\iff \ x \in A \ \wedge \ x \notin B \ \wedge \ x \in A \ \wedge \ x \notin C$	commut.+assoc.
$\iff \ x \in (A - B) \ \wedge \ x \in (A - C)$	
$\iff \ x \in (A - B) \cap (A - C)$	

EXAMPLE : $A \cap B = A \cup B \quad \Rightarrow \quad A = B$

PROOF : (a *direct* proof $\cdots$)

Assume $(A \cap B) = (A \cup B)$. We must show that $A = B$.

This is done in *two stages* :

(i) show $A \subseteq B$ and (ii) show $B \subseteq A$.

To show (i) :

Let $x \in A$. We must show that $x \in B$.

Since $x \in A$ it follows that $x \in A \cup B$.

Since $(A \cap B) = (A \cup B)$ it follows that $x \in (A \cap B)$.

Thus $x \in B$ also.

The proof of (ii) proceeds along the same steps.

Subsets.

$S \subseteq U$ means S is a *subset* of a universal set U .

The *set of all subsets* of U is denoted by 2^U or $P(U)$, the *power set* .

This name is suggested by the following fact :

If U *has* n *elements then* $P(U)$ *has* 2^n *elements (sets)* .

EXAMPLE :

Let

$$U \;=\; \{1\;,\;2\;,\;3\}\;.$$

Then

$$P(U) \;=\; \Big\{\;\{\},\;\{1\},\;\{2\},\;\{3\},\;\{1,2\},\;\{1,3\},\;\{2,3\},\;\{1,2,3\}\;\Big\}\;.$$

We see that $P(U)$ has $2^3 = 8$ elements .

NOTE : The empty set $\emptyset = \{\}$ and U itself are included in $P(U)$.

Basic set theoretic identities :

$A \cup B = B \cup A$	$A \cap B = B \cap A$	*commutative laws*
$A \cup (B \cap C) =$ $(A \cup B) \cap (A \cup C)$	$A \cap (B \cup C) =$ $(A \cap B) \cup (A \cap C)$	*distributive laws*
$A \cup \emptyset = A$	$A \cap U = A$	*identity laws*
$A \cup \bar{A} = U$	$A \cap \bar{A} = \emptyset$	*complement laws*

Some additional identities :

$\bar{U} = \emptyset$	$\bar{\emptyset} = U$	
$A \cup A = A$	$A \cap A = A$	*idempotent laws*
$A \cup U = U$	$A \cap \emptyset = \emptyset$	*domination laws*
$A \cup (A \cap B) = A$	$A \cap (A \cup B) = A$	*absorption laws*

Some more identities :

$(A \cup B) \cup C = A \cup (B \cup C)$	$(A \cap B) \cap C = A \cap (B \cap C)$	*associative law*
$\overline{A \cup B} = \bar{A} \cap \bar{B}$	$\overline{A \cap B} = \bar{A} \cup \bar{B}$	*de Morgan's laws*
$\bar{\bar{A}} = A$		*involution law*

All the preceding identities can be proved using the definitions of set theory and the laws of logic.

Note the close correspondence of these identities to the laws of logic.

NOTE : One can also proceed *axiomatically* by only assuming :

- the existence of a power set $P(U)$, where U is a universal set ,
- special elements U and $\emptyset$,
- a unary operator $^-$, and two binary operators $\cup$ and $\cap$,
- the basic set theoretic identities .

Given this setup one can derive all other set theoretic identities.

Note the close correspondence between the above axiomatic setup and the axiomatic setup of logic !

EXAMPLE :

Prove the idempotent law

$$A \cup A = A$$

using only the basic set theoretic identities :

A	$A \cup \emptyset$	identity law
	$A \cup (A \cap \bar{A})$	complement law
	$(A \cup A) \cap (A \cup \bar{A})$	distributive law
	$(A \cup A) \cap U$	complement law
	$A \cup A$	identity law

EXAMPLE :

(to illustrate the close relation between Set Theory and Logic $\cdots$)

Using another approach we prove the absorption law :

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

Thus we must prove

$$\forall x \in U \;:\; x \in A \cup (A \cap B) \iff x \in A$$

$$\forall x \in U \;:\; x \in A \;\vee\; x \in A \cap B \iff x \in A$$

$$\forall x \in U \;:\; x \in A \;\vee\; (x \in A \;\wedge\; x \in B) \iff x \in A$$

$$\boxed{\forall x \in U \ : \ x \in A \ \vee \ (x \in A \ \wedge \ x \in B) \iff x \in A}$$

Define logical predicates $a(x)$ and $b(x)$:

$$a(x) \iff x \in A \qquad , \qquad b(x) \iff x \in B \ .$$

Then we must prove

$$\forall x \in U \ : \ a(x) \ \vee \ (a(x) \wedge b(x)) \iff a(x) \ .$$

It suffices to prove that, for arbitrary logical variables a and b ,

$$a \vee (a \wedge b) \iff a \quad .$$

But this is the *absorption law* from logic !

REVIEW EXERCISES.

For each of the following, determine whether it is valid or invalid.
If valid then give a proof. If invalid then give a counterexample.

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

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

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

(4) $(A \cap B) \cup (A \cap \bar{B}) = A$

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

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

(7) $B \cap C \subseteq A \Rightarrow (B - A) \cap (C - A) = \emptyset$

(8) $(A \cup B) - (A \cap B) = A \Rightarrow B = \emptyset$

FUNCTIONS

DEFINITIONS : Let A and B be sets.

Then f is called

a function from A *to* B

if to *each element* of A it associates exactly one element of B .

We write

$$f \ : \ A \longrightarrow B$$

and we call A the *domain of* f and B the *codomain of* f .

We also define the *range of* f to be

$$f(A) \ \equiv \ \{b \in B \ : \ b = f(a) \ \text{ for some } a \in A\} \ .$$

We say that f is :

one-to-one (or *injective*) iff $\forall a_1, a_2 \in A : a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$

iff $\forall a_1, a_2 \in A : f(a_1) = f(a_2) \Rightarrow a_1 = a_2$

onto (or *surjective*) iff $\forall b \in B \; \exists a \in A : f(a) = b$

iff $f(A) = B$

bijective iff f is one-to-one and onto

EXAMPLE :

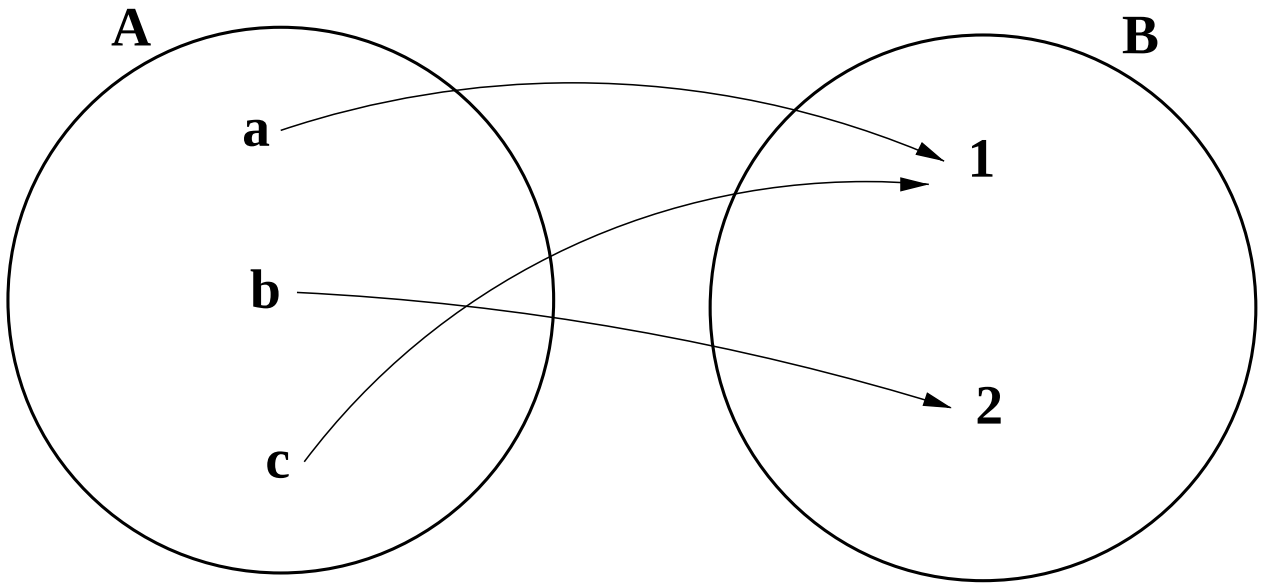
Let

$$A = \{a, b, c\} \qquad , \qquad B = \{1, 2\} \ ,$$

and let $f : A \longrightarrow B$ be defined by

$$f : a \mapsto 1 \quad , \quad f : b \mapsto 2 \quad , \quad f : c \mapsto 1 \ .$$

Then f not one-to-one, but f is onto.



EXAMPLE :

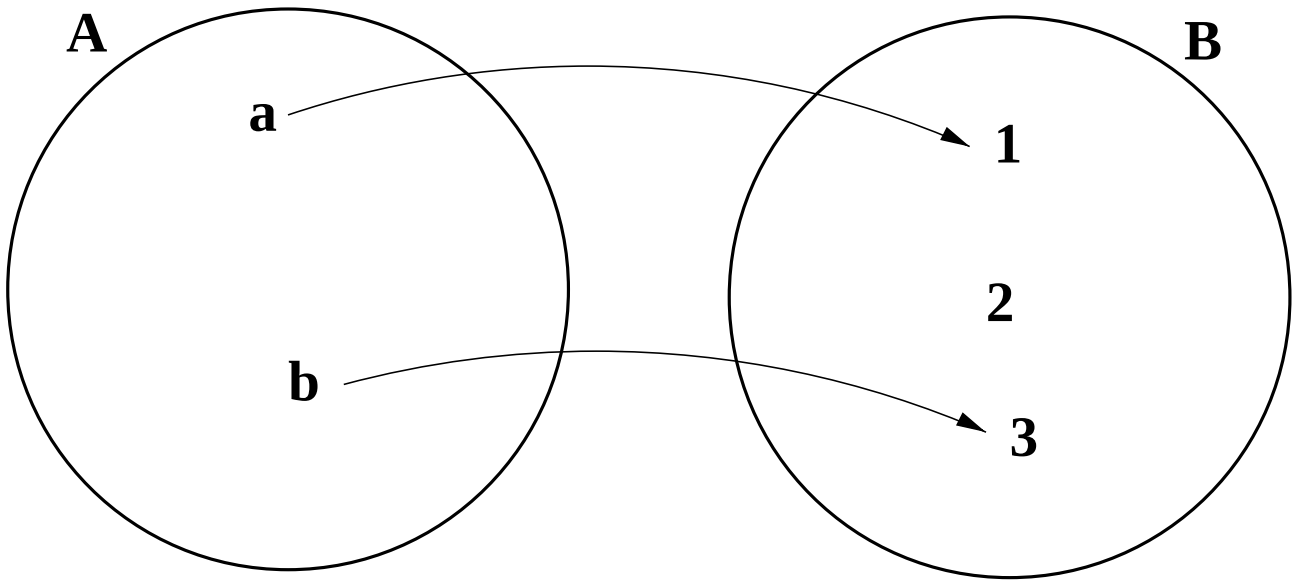
Let

$$A = \{a, b\} \ , \qquad B = \{1, 2, 3\} \ ,$$

and let $f \ : \ A \longrightarrow B$ be defined by

$$f \ : \ a \mapsto 1 \quad , \quad f \ : \ b \mapsto 3 \ .$$

Then f is one-to-one but not onto.



EXAMPLE :

Let $A = B = \mathbb{Z}^+$, and let

$$f : \mathbb{Z}^+ \longrightarrow \mathbb{Z}^+$$

be defined by

$$f : n \mapsto \frac{n(n+1)}{2} ,$$

i.e.,

$$f(n) = \frac{n(n+1)}{2} .$$

Then f is one-to-one but not onto.

$$\boxed{f(n) \;\equiv\; n(n+1)/2}$$

PROOF : **(1)** f is *not onto* :

Here

$$f(\mathbb{Z}^+) \;=\; \{\; 1\;,\; 3\;,\; 6\;,\; 10\;,\; 15\;,\; 21\;,\; \cdots\;\}\;,$$

so it seems that f is not onto.

To be precise, we show that $f(n)$ can never be equal to 2 :

$$f(n) = 2 \quad \Longleftrightarrow \quad n(n+1)/2 = 2 \quad \Longleftrightarrow \quad n^2 + n - 4 = 0\;.$$

But this quadratic equation has no integer roots.

(2) f is *one-to-one* : Assume that $f(n_1) = f(n_2)$.

We must show that $n_1 = n_2$:

$$
\begin{aligned}
f(n_1) \;=\; f(n_2) \quad &\Longleftrightarrow \quad n_1(n_1+1)/2 \;=\; n_2(n_2+1)/2 \\
&\Longleftrightarrow \quad n_1^2 + n_1 \;=\; n_2^2 + n_2 \\
&\Longleftrightarrow \quad n_1^2 - n_2^2 \;=\; -\,(n_1 - n_2) \\
&\Longleftrightarrow \quad (n_1+n_2)(n_1-n_2) \;=\; -\,(n_1-n_2) \\
&\Longleftrightarrow \quad n_1 \;=\; n_2 \quad \text{or} \quad n_1 + n_2 \;=\; -\,1
\end{aligned}
$$

However $n_1, n_2 \in \mathbb{Z}^+$. Thus $n_1 + n_2$ cannot be negative.

It follows that $n_1 = n_2$. **QED !**

EXAMPLE :

Define

$$f \;:\; \mathbb{Z}\times\mathbb{Z} \longrightarrow \mathbb{Z}\times\mathbb{Z}$$

or equivalently

$$f \;:\; \mathbb{Z}^2 \longrightarrow \mathbb{Z}^2$$

by

$$f(m,n) \;=\; (m+n\;,\; m-n)\;,$$

or equivalently, in matrix multiplication notation

$$f \;:\; \begin{pmatrix} m \\ n \end{pmatrix} \;\mapsto\; \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} m \\ n \end{pmatrix} \;.$$

Then f is one-to-one, but not onto.

PROOF :

(i) *One-to-one* :

Suppose

$$f(m_1, n_1) \;=\; f(m_2, n_2) \;.$$

Then

$$(m_1 + n_1 \;,\; m_1 - n_1) \;=\; (m_2 + n_2 \;,\; m_2 - n_2) \;,$$

i.e.,

$$m_1 + n_1 \;=\; m_2 + n_2 \;,$$

and

$$m_1 - n_1 \;=\; m_2 - n_2 \;.$$

Add and subtract the equations, and divide by 2 to find

$$m_1 = m_2 \quad \text{and} \quad n_1 = n_2 \;,$$

that is,

$$(m_1, n_1) \;=\; (m_2, n_2) \;.$$

Thus f is one-to-one.

(ii) *Not onto* :

Let $(s,d) \in \mathbb{Z}^2$ be arbitrary. Can we solve

$$f(m,n) \;=\; (s,d)\;,$$

i.e., can we solve

$$\begin{aligned} m+n &= s\;, \\ m-n &= d\;, \end{aligned}$$

for $m,n \in \mathbb{Z}$?

Add and subtract the two equations, and divide by 2 to get

$$m \;=\; \frac{s+d}{2} \qquad \text{and} \qquad n \;=\; \frac{s-d}{2}\;.$$

However, m and n need not be integers, *e.g.*, take $s=1$, $d=2$.

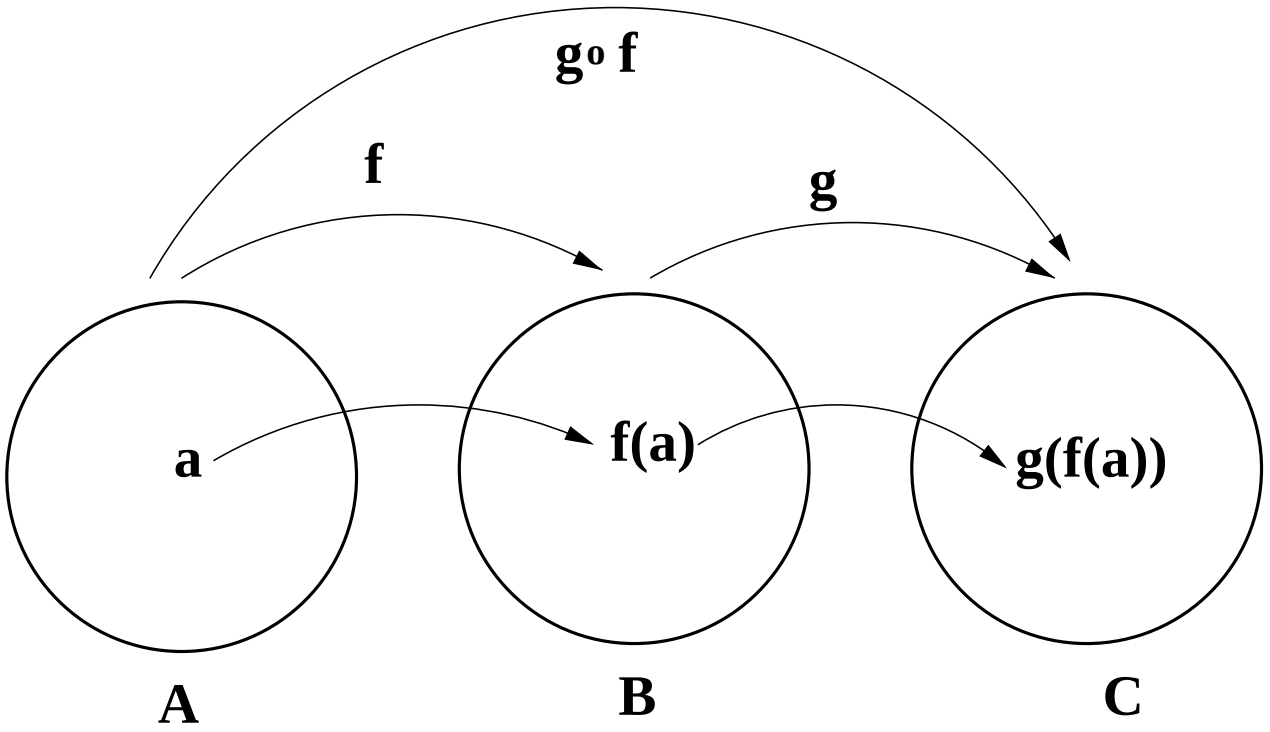
Thus f is *not* onto. **QED !**

Given two functions

$$f \ : \ A \longrightarrow B \quad \text{and} \quad g \ : \ B \longrightarrow C \ ,$$

we can *compose* them :

$$(g \circ f)(a) \ \equiv \ g\Big(f(a)\Big) \ .$$



EXAMPLE :

Let $A = B = C = \mathbb{Z}$ (all integers), and define $f, g \ : \ \mathbb{Z} \longrightarrow \mathbb{Z}$ by

$$f(n) \ \equiv \ n^2 + 2n - 1 \qquad , \quad g(n) \ \equiv \ 2n - 1 \ .$$

- Let $h_1(n) \ \equiv \ f\Big(g(n)\Big)$. Then

$$h_1(n) \ = \ f(2n-1) \ = \ (2n-1)^2 + 2(2n-1) - 1 \ = \ 4n^2 - 2 \ .$$

- Let $h_2(n) \ \equiv \ g\Big(f(n)\Big)$. Then

$$h_2(n) \ = \ g(n^2 + 2n - 1) \ = \ 2(n^2 + 2n - 1) - 1 \ = \ 2n^2 + 4n - 3 \ .$$

- Let $h_3(n) \ \equiv \ g\Big(g(n)\Big)$. Then

$$h_3(n) \ = \ g(2n-1) \ = \ 2(2n-1) - 1 \ = \ 4n - 3 \ .$$

Inverses. Let

$$f \ : \ A \longrightarrow B \ ,$$

and

$$g \ : \ B \longrightarrow A \ .$$

Then g is called the *inverse of* f if

$$\forall a \in A \quad : \quad g\Big(f(a)\Big) = a \ ,$$

and

$$\forall b \in B \quad : \quad f\Big(g(b)\Big) = b \ .$$

If f has an inverse g then we say

f is invertible ,

and we write f^{-1} for g .

EXAMPLE :

Let $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ be defined by $f : n \mapsto n-1$, *i.e.*,

$$f(n) = n-1 \quad (\text{"shift operator"}) .$$

- f is one-to-one :

If $f(n_1) = f(n_2)$ then $n_1 - 1 = n_2 - 1$, *i.e.*, $n_1 = n_2$.

- f is onto :

Given any $m \in \mathbb{Z}$, can we find n such that $f(n) = m$?

That is, can we find n such that $n - 1 = m$?

Easy: $n = m + 1$!

$$\boxed{f(n) \;=\; n-1\;, \qquad f \;:\; \mathbb{Z} \longrightarrow \mathbb{Z}}$$

It follows that f is invertible, with inverse

$$f^{-1}(m) \;=\; m+1\;.$$

Check :

$$f\Big(f^{-1}(m)\Big) \;=\; f(m+1) \;=\; (m+1)-1 \;=\; m\;,$$

$$f^{-1}\Big(f(n)\Big) \;=\; f^{-1}(n-1) \;=\; (n-1)+1 \;=\; n\;.$$

EXAMPLE :

Let $f : \mathbb{R} \longrightarrow \mathbb{R}$ be defined by $f : x \mapsto 1 - 2x$, *i.e.*,

$$f(x) = 1 - 2x \ .$$

- f is one-to-one :

If $f(x_1) = f(x_2)$ then $1 - 2x_1 = 1 - 2x_2$, *i.e.*, $x_1 = x_2$.

- f is onto :

Given any $y \in \mathbb{R}$, can we find x such that $f(x) = y$?

That is, can we find x such that $1 - 2x = y$?

Easy: $x = (1 - y)/2$!

(We actually *constructed* the inverse in this step : $f^{-1}(y) = \frac{1-y}{2}$.)

$$\boxed{f(x) \;=\; 1-2x\;, \qquad f \;:\; \mathbb{R} \longrightarrow \mathbb{R}}$$

We found that f is invertible, with inverse

$$f^{-1}(y) \;=\; \frac{1-y}{2}\;.$$

Check (not really necessary $\cdots$) :

$$f\Big(f^{-1}(y)\Big) \;=\; f((1-y)/2) \;=\; 1-2\Big((1-y)/2\Big) \;=\; y\;,$$

$$f^{-1}\Big(f(x)\Big) \;=\; f^{-1}(1-2x) \;=\; \frac{1-(1-2x)}{2} \;=\; x\;.$$

NOTE : We *constructed* $f^{-1}(y)$ by solving $f(x)=y$ for x .

THEOREM :

$f : A \longrightarrow B$ is invertible if and only if f is $1-1$ and onto .

REMARK :

- It is not difficult to see that this theorem holds for finite sets.

- However, the proof also applies to infinite sets.

PROOF :

(1a) First we show that if f is invertible then f is $1-1$.

By contradiction: Suppose f is invertible but not $1-1$.

Since f is not $1-1$ there exist $a_1, a_2 \in A$, $a_1 \neq a_2$, such that

$$f(a_1) = f(a_2) \equiv b_0 \ .$$

Since f is invertible there is a function $g \ : \ B \longrightarrow A$ such that

$$g\Big((f(a)\Big)) = a, \quad \forall a \in A \ .$$

In particular

$$g\Big(f(a_1)\Big) = a_1 \ , \quad \text{and} \quad g\Big(f(a_2)\Big) = a_2 \ ,$$

i.e.,

$$g(b_0) = a_1 \ , \quad \text{and} \quad g(b_0) = a_2 \ .$$

Thus g is not single-valued (not a function). **Contradiction !**

(1b) Now we show that if f is invertible then f is onto.

By contradiction: Suppose f is invertible but not onto.

Since f is not onto there exists $b_0 \in B$ such that

$$f(a) \neq b_0, \quad \forall a \in A \ .$$

Since f is invertible there is a function $g \ : \ B \longrightarrow A$ such that

$$f\Big(g(b)\Big) = b, \quad \forall b \in B \ .$$

In particular

$$f\Big(g(b_0)\Big) \ = \ b_0 \ , \quad \text{where} \quad g(b_0) \in A \ .$$

But this contradicts that $f(a) \neq b_0$, $\forall a \in A$.

(2a) Next we show that if f is $1-1$ and onto then f is invertible.

Define a function $g \ : \ B \longrightarrow A$ as follows :

Since f is $1-1$ and onto we have that for any $b \in B$

$$b = f(a) \ \text{ for some unique } a \in A \ .$$

For each such $a \in A$ set

$$g(b) \ = \ a \ .$$

Then $g \ : \ B \longrightarrow A$, and by construction

$$f\Big(g(b)\Big) \ = \ f(a) \ = \ b \ .$$

(2b) We still must show that $\forall a \in A : g\Big(f(a)\Big) = a$.

By contradiction : Suppose $g\Big(f(a_0)\Big) \neq a_0$ for some $a_0 \in A$.

Define $b_0 = f(a_0)$. Then $b_0 \in B$ and

$$g(b_0) \neq a_0 ,$$

where both $g(b_0)$ and a_0 lie in A .

Since f is one-to-one it follows that

$$f\Big(g(b_0)\Big) \neq f(a_0) ,$$

i.e.,

$$f\Big(g(b_0)\Big) \neq b_0 .$$

But this contradicts the result of (2a) ! **QED !**

EXAMPLE :

- Define $f \ : \ \mathbb{Z}^+ \longrightarrow \mathbb{Z}^+$ by

$$f(n) \ = \ n(n-2)(n-4)+4 \ .$$

Then f is *not one-to-one* ; for example, $f(2) = f(4) = 4$:

n	1	2	3	4	5	6	7	$\cdots$
$f(n)$	7	4	1	4	19	52	109	$\cdots$

Using calculus one can show that $f(n)$ is increasing for $n \geq 3$.

Thus f is *not onto* ; for example,

$$\forall n \in \mathbb{Z}^+ \ : \ f(n) \neq 2 \ .$$

- Now let

$$S \;=\; f(\mathbb{Z}^+) \;=\; \{1, 4, 7, 19, 52, 109, \cdots\} \;,$$

and consider f as a function

$$f \;:\; \mathbb{Z}^+ \longrightarrow S \;.$$

Then f is onto, but still not one-to-one, since $f(2) = f(4) = 4$.

- Finally let

$$D \;=\; \mathbb{Z}^+ - \{2\} \;,$$

and consider f as a function

$$f \;:\; D \longrightarrow S \;.$$

Now f is one-to-one and onto, and hence invertible.

EXAMPLE : The *floor* and *ceiling* functions.

FACT :

$\forall x \in \mathbb{R} \quad \exists\,!\, n \in \mathbb{Z} \quad$ and $\quad \exists\,!\, r \in \mathbb{R}$ with $0 \leq r < 1$ such that

$$x \;=\; n \;+\; r \;.$$

We already defined the *floor function*, $\lfloor \cdot \rfloor$, as

$$\lfloor x \rfloor \;=\; n \;.$$

EXAMPLES :

$$\lfloor \pi \rfloor \;=\; 3 \;, \qquad \lfloor e \rfloor \;=\; 2 \;, \qquad \lfloor 3 \rfloor \;=\; 3 \;, \qquad \lfloor -7/2 \rfloor \;=\; -\,4 \;,$$

where $e \;=\; 2.71828 \cdots$.

FACT :

$\forall x \in \mathbb{R} \quad \exists\,!\, n \in \mathbb{Z} \quad$ and $\quad \exists\,!\, r \in \mathbb{R}$ with $0 \leq r < 1$ such that

$$x \;=\; n \;-\; r \;.$$

We already defined the *ceiling function*, $\lceil \cdot \rceil$, as

$$\lceil x \rceil \;=\; n \;.$$

EXAMPLES :

$$\lceil \pi \rceil \;=\; 4 \;, \qquad \lceil e \rceil \;=\; 3 \;, \qquad \lceil 3 \rceil \;=\; 3 \;, \qquad \lceil -7/2 \rceil \;=\; -\,3 \;.$$

We see that

$$\lfloor \cdot \rfloor \quad : \quad \mathbb{R} \longrightarrow \mathbb{Z} \ ,$$

and

$$\lceil \cdot \rceil \quad : \quad \mathbb{R} \longrightarrow \mathbb{Z} \ .$$

EXERCISE :

- Is $\lfloor \cdot \rfloor$ one-to-one? onto? invertible?
- Is $\lceil \cdot \rceil$ one-to-one? onto? invertible?
- Draw the graphs of $\lfloor \cdot \rfloor$ and $\lceil \cdot \rceil$.

EXAMPLE : Let $p\ ,\ k \in \mathbb{Z}^+\ .$

Then

$$\lceil\ \frac{p}{k}\ \rceil\ <\ \frac{p+k}{k}\ .$$

PROOF :

By definition of the ceiling function we can write

$$\frac{p}{k}\ =\ \lceil\ \frac{p}{k}\ \rceil\ -\ r\ ,$$

where $0\ \leq\ r\ <\ 1\ .$

Hence

$$\lceil\ \frac{p}{k}\ \rceil\ =\ \frac{p}{k}\ +\ r\ <\ \frac{p}{k}\ +\ 1\ =\ \frac{p+k}{k}\ .$$ **QED !**

EXAMPLE : Show that the *linear function*

$$f \ : \ \mathbb{R}^2 \ \longrightarrow \ \mathbb{R}^2$$

defined by

$$f(x,y) \ = \ (x+y \ , \ x-y) \ ,$$

or, in matrix form,

$$f \ : \ \begin{pmatrix} x \\ y \end{pmatrix} \ \mapsto \ \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \ ,$$

is one-to-one and onto.

- One-to-one : Exercise!

Hint : See the earlier example where this function was considered as

$$f \ : \ \mathbb{Z}^2 \ \longrightarrow \ \mathbb{Z}^2 \ .$$

- Onto :

$$f(x,y) \;=\; (x+y\;,\;x-y) \qquad \text{or} \qquad f \;:\; \begin{pmatrix} x \\ y \end{pmatrix} \;\mapsto\; \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

We can *construct the inverse* by solving

$$f(x,y) \;=\; (s,d)\;,$$

that is, by solving

$$x+y \;=\; s \qquad , \qquad x-y \;=\; d\;,$$

for $x, y \in \mathbb{R}$:

$$x \;=\; \frac{s+d}{2} \qquad , \qquad y \;=\; \frac{s-d}{2}\;.$$

Thus the inverse is

$$g(s,d) \;=\; (\frac{s+d}{2}\;,\;\frac{s-d}{2}) \qquad \text{or} \qquad g \;:\; \begin{pmatrix} s \\ d \end{pmatrix} \;\mapsto\; \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} \end{pmatrix} \begin{pmatrix} s \\ d \end{pmatrix}\;.$$

$$f(x,y) \;=\; (x+y\ ,\ x-y) \qquad , \qquad g(s,d) \;=\; (\tfrac{s+d}{2}\ ,\ \tfrac{s-d}{2})$$

Check (not really necessary $\cdots$) :

$$f(g(s,d)) \;=\; f(\frac{s+d}{2}\ ,\ \frac{s-d}{2})$$

$$=\; (\frac{s+d}{2}+\frac{s-d}{2}\ ,\ \frac{s+d}{2}-\frac{s-d}{2}) \;=\; (s,d)\ ,$$

and

$$g(f(x,y)) \;=\; g(x+y\ ,\ x-y)$$

$$=\; (\frac{(x+y)+(x-y)}{2}\ ,\ \frac{(x+y)-(x-y)}{2}) \;=\; (x,y)\ .$$

EXAMPLE :

More generally, a function

$$f \;\; : \;\; \mathbb{R}^2 \;\longrightarrow\; \mathbb{R}^2$$

is *linear* if it can be written as

$$f(x,y) \;=\; (\; a_{11}\; x + a_{12}\; y \;,\; a_{21}\; x + a_{22}\; y \;)\;,$$

or equivalently, as *matrix-vector multiplication* ,

$$f \;\; : \;\; \begin{pmatrix} x \\ y \end{pmatrix} \;\mapsto\; \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \;,$$

where $a_{ij} \in \mathbb{R}$, $(i,j = 1,2)$.

$$f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2 \quad , \quad f : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

This function is invertible if the *determinant*

$$D \equiv a_{11}a_{22} - a_{12}a_{21} \neq 0 \, .$$

In this case the inverse is given by

$$f^{-1} : \begin{pmatrix} s \\ d \end{pmatrix} \mapsto \frac{1}{D} \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix} \begin{pmatrix} s \\ d \end{pmatrix} \, .$$

EXERCISE : Check that

$$f^{-1}(f(x,y)) = (x,y) \quad \text{and} \quad f(f^{-1}(s,d)) = (s,d) \, .$$

Now consider the same linear function

$$f \ : \ \begin{pmatrix} n \\ m \end{pmatrix} \ \mapsto \ \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} n \\ m \end{pmatrix} ,$$

but with $a_{ij} \in \mathbb{Z}$, $(i, j = 1, 2)$, and as a function

$$f \ : \ \mathbb{Z}^2 \longrightarrow \mathbb{Z}^2 \ .$$

Is

$$f^{-1} \ : \ \begin{pmatrix} s \\ d \end{pmatrix} \ \mapsto \ \frac{1}{D} \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix} \begin{pmatrix} s \\ d \end{pmatrix} \ .$$

still the inverse?

ANSWER : Not in general !

f is now invertible only if the *determinant*

- $D \;=\; a_{11}a_{22} - a_{12}a_{21} \;\neq\; 0,$

  and

- $\forall i, j \;:\quad D \mid a_{ij}$.

In this case f^{-1} is still given by

$$f^{-1} \;:\; \begin{pmatrix} s \\ d \end{pmatrix} \;\mapsto\; \frac{1}{\mathrm{D}} \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix} \begin{pmatrix} s \\ d \end{pmatrix} \;.$$

EXERCISE : Show that

$$f \ : \ \begin{pmatrix} n \\ m \end{pmatrix} \ \mapsto \ \begin{pmatrix} 3 & 2 \\ 4 & 3 \end{pmatrix} \begin{pmatrix} n \\ m \end{pmatrix} \ ,$$

is invertible as a function $f \ : \ \mathbb{Z}^2 \longrightarrow \mathbb{Z}^2$.

What is the inverse?

EXERCISE : Show that

$$f \ : \ \begin{pmatrix} n \\ m \end{pmatrix} \ \mapsto \ \begin{pmatrix} 3 & 1 \\ 4 & 3 \end{pmatrix} \begin{pmatrix} n \\ m \end{pmatrix} \ ,$$

is *not* invertible as a function $f \ : \ \mathbb{Z}^2 \longrightarrow \mathbb{Z}^2$.

REVIEW EXERCISES.

Problem 1.

Define

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

by

$$f(x) \equiv \begin{cases} 1/x & \text{if} \quad x \neq 0 \ , \\ \\ 0 & \text{if} \quad x = 0 \ . \end{cases}$$

- Draw the graph of f .
- Is f one-to-one?
- Is f onto?
- What is f^{-1} ?

Problem 2. Consider a function

$$f \ : \ A \ \longrightarrow \ B \ .$$

For each of the following, can you find a function f that is

(i) one-to-one (ii) onto (iii) one-to-one and onto ?

- $A \ = \ \{1, 2, 3\}$, $B \ = \ \{1, 2\}$
- $A \ = \ \{1, 2\}$, $B \ = \ \{1, 2, 3\}$
- $A \ = \ \{\text{all even positive integers}\}$, $B \ = \ \{\text{all odd positive integers}\}$

Problem 3.

Can you find a function $f : \mathbb{Z} \longrightarrow \mathbb{Z}^+$ that is one-to-one and onto ?

Can you find a function $g : \mathbb{Z}^+ \longrightarrow \mathbb{Z}$ that is one-to-one and onto ?

Problem 4. Let S_n be a finite set of n elements.

Show that a function

$$f : S_n \longrightarrow S_n$$

is one-to-one if and only if it is onto.

Problem 5. Let $f : A \longrightarrow B$ and $g : B \longrightarrow C$ be functions.

- Suppose f and g are one-to-one.

  Is the composition $g \circ f$ necessarily one-to-one?

- Suppose the composition $g \circ f$ is one-to-one.

  Are f and g necessarily one-to-one?

- Suppose f and g are onto.

  Is the composition $g \circ f$ necessarily onto?

- Suppose the composition $g \circ f$ is onto.

  Are f and g necessarily onto?

Justify your answers.

Problem 6.

Let $\mathbb{P}_2$ denote the set of *all polynomials of degree* 2 *or less* ,

i.e., polynomials of the form

$$p(x) \;=\; a\,x^2 \;+\; b\,x \;\;+\; c\;, \qquad a,b,c \in \mathbb{R} \;\;,\;\; x \in \mathbb{R}\;.$$

Let $\mathbb{P}_1$ denote the set of *all polynomials of degree* 1 *or less* ,

i.e., polynomials of the form

$$p(x) \;=\; d\,x \;+\; e\;, \qquad d,e \in \mathbb{R} \;\;,\;\; x \in \mathbb{R}\;.$$

Consider the *derivative function* (or *derivative operator*)

$$D \;\;:\;\; \mathbb{P}_2 \;\;\longrightarrow\;\; \mathbb{P}_1\;.$$

For example,

$$D \quad : \quad 3x^2 + 7x - 4 \quad \mapsto \quad 6x + 7 \ ,$$

and

$$D \quad : \quad 5x - 2\pi \quad \mapsto \quad 5 \ .$$

QUESTIONS :

- Is D indeed a *function* from $\mathcal{P}_2$ to $\mathcal{P}_1$?
- Is D one-to-one ?
- Is D onto ?
- Does D have an inverse ?

Problem 7. If A and B are sets, and if

$$f \;:\; A \longrightarrow B\,,$$

then for any subset S of A we define *the image of S* as

$$f(S) \;\equiv\; \{b \in B \;:\; b = f(a) \text{ for some } a \in S\}\,.$$

Let S and T be subsets of A. Prove that

- $f(S \cup T) \;=\; f(S) \cup f(T)\,,$
- $f(S \cap T) \;\subseteq\; f(S) \cap f(T)\,.$
- Also give an example that shows that in general

$$f(S \cap T) \;\neq\; f(S) \cap f(T)\,.$$

Problem 8. If A and B are sets, and if

$$f \;:\; A \;\longrightarrow\; B\;,$$

then for any subset S of B we define *the pre-image of S* as

$$f^{-1}(S) \;\equiv\; \{a \in A \;:\; f(a) \in S\}\;.$$

NOTE : $f^{-1}(S)$ is defined even if f does not have an inverse!

Let S and T be subsets of B . Prove that

- $f^{-1}(S \cup T) \;=\; f^{-1}(S) \cup f^{-1}(T)\;,$
- $f^{-1}(S \cap T) \;=\; f^{-1}(S) \cap f^{-1}(T)\;.$

THE DIVISION THEOREM :

$$\forall n \in \mathbb{Z},\ \forall d \in \mathbb{Z}^+,\ \exists!\ q, r \in \mathbb{Z}\ :\ (\ 0 \leq r < d\ ,\quad n = qd + r\ )\ .$$

EXAMPLE : If $n = 21$ and $d = 8$ then

$$n \ = \ 2 \cdot d \ + \ 5\ .$$

Thus, here $q = 2$ and $r = 5$.

- d is called the *divisor*,
- q is called the *quotient*; we write $q = n \text{ div } d$,
- r is called the *remainder*; we write $r = n \bmod d$.

EXAMPLES :

$n = 14\ ,\ d = 5\ :\qquad 14\ =\ 2 \cdot d\ +\ 4\ ,\quad$ so

$$14 \text{ div } 5\ =\ 2 \qquad \text{and} \qquad 14 \bmod 5\ =\ 4\ .$$

$n = -14\ ,\ d = 5\ :\qquad -14\ =\ (-3) \cdot d\ +\ 1\ ,\quad$ so

$$-14 \text{ div } 5\ =\ -3 \qquad \text{and} \qquad -14 \bmod 5\ =\ 1\ .$$

Let $d \in \mathbb{Z}^+$ and $n, q, r \in \mathbb{Z}$.

From the definitions of "div" and "mod" it follows that :

PROPERTY 1 : $n = (n \text{ div } d)\, d + n \bmod d$

Example : $23 = (23 \text{ div } 7) \cdot 7 + 23 \bmod 7$

PROPERTY 2 : If $0 \leq r < d$ then $(qd + r) \bmod d = r$

Example : $(5 \cdot 7 + 3) \bmod 7 = 3$

PROPERTY 3 : $(qd + n \bmod d) \bmod d = n \bmod d$

Example : $(5 \cdot 7 + 23 \bmod 7) \bmod 7 = 23 \bmod 7$

PROPERTY 4 : Let $a, b \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$. Then

$$(ad + b) \bmod d \;=\; b \bmod d \;.$$

PROOF :

By the Division Theorem

$$b = qd + r, \quad \text{where} \quad r = b \bmod d \;, \quad \text{with} \quad 0 \leq r < d \;.$$

Thus, using Property 2

$$(ad + b) \bmod d \;=\; \Big((a + q)d + r\Big) \bmod d \;=\; r \;=\; b \bmod d \;.$$

QED !

EXAMPLE : $(57 \cdot 7 + 13) \bmod 7 \;=\; 13 \bmod 7 \;.$

PROPERTY 5 : Let $a \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$. Then

$$(a \bmod d) \bmod d \;=\; a \bmod d \;.$$

PROOF : Using Property 3,

$$(a \bmod d) \bmod d \;=\; (0 \cdot d + a \bmod d) \bmod d \;=\; a \bmod d \;.$$

EXAMPLE :

$$(59 \bmod 7) \bmod 7 \;=\; 59 \bmod 7 \;.$$

PROPERTY 6 :

Let $a, b \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$. Then

$$(a+b) \bmod d \;=\; (a \bmod d + b \bmod d) \bmod d \;.$$

EXAMPLE :

$$(5+8) \bmod 3 \;=\; 1 \quad = \quad (5 \bmod 3 + 8 \bmod 3) \bmod 3 \;.$$

PROOF :

By the Division Theorem

$$a = q_a d + r_a \ , \quad \text{where} \quad r_a = a \bmod d \ , \quad \text{with} \quad 0 \leq r_a < d \ ,$$

$$b = q_b d + r_b \ , \quad \text{where} \quad r_b = b \bmod d \ , \quad \text{with} \quad 0 \leq r_b < d \ .$$

Thus

$$\begin{aligned}
(a+b) \bmod d &= (q_a d + r_a + q_b d + r_b) \bmod d \\
&= \Big((q_a + q_b) d + r_a + r_b \Big) \bmod d \\
&= (r_a + r_b) \bmod d \quad \text{(using Property 4)} \\
&= (a \bmod d + b \bmod d) \bmod d \ . \quad \textbf{QED !}
\end{aligned}$$

DEFINITION :

If $a, b \in \mathbb{Z}$, $d \in \mathbb{Z}^+$, and if

$$a \bmod d \;=\; b \bmod d \;,$$

then we also write

$$a \equiv b \pmod{d} \;,$$

and we say

"a is *congruent* to b *modulo* d".

EXAMPLE :

$$83 \;\equiv\; 31 \pmod{26} \;.$$

Note that $83 - 31 \;=\; 52$, which is divisible by 26 , *i.e.*,

$$26 \mid (83 - 31) \;.$$

PROPOSITION : Let $a, b \in \mathbb{Z}$, and $d \in \mathbb{Z}^+$. Then

$$a \equiv b \pmod{d} \quad \text{if and only if} \quad d \mid (a - b) \ .$$

PROOF :

(⇒) First, if $a \equiv b \pmod{d}$ then, by definition,

$$a \bmod d \ = \ b \bmod d \ .$$

Hence there exist $q_a, q_b, r \in \mathbb{Z}$, with $0 \leq r < d$, such that

$$a \ = \ q_a d + r \qquad \text{and} \quad b \ = \ q_b d + r \qquad \text{(same remainder)}.$$

It follows that

$$a - b \ = \ (q_a - q_b)\, d \ ,$$

so that $d \mid (a - b)$.

$$\boxed{a \equiv b \pmod{d} \quad \text{if and only if} \quad d \mid (a-b)}$$

($\Leftarrow$) Conversely, if $d \mid (a-b)$ then

$$a - b \;=\; qd \;,$$

i.e. ,

$$a \;=\; b \;+\; qd \;,$$

for some $q \in \mathbb{Z}$.

It follows that

$$a \bmod d \;=\; (b + qd) \bmod d \;=\; b \bmod d \;.$$

PROPOSITION : If $a, b \in \mathbb{Z}$, and $c, d \in \mathbb{Z}^+$, then

$$a \equiv b \pmod{d} \quad \Rightarrow \quad ac \equiv bc \pmod{dc} \ .$$

PROOF :

$a \equiv b \pmod{d}$ if and only if $d \mid (a - b)$,

i.e.,

$$a - b = qd \ , \quad \text{for some } q \in \mathbb{Z} \ .$$

Then $ac - bc = qdc$, so that $(dc) \mid (ac - bc)$,

i.e.,

$$ac \equiv bc \pmod{dc} \ .$$

NOTE : We also have that $ac \equiv bc \pmod{d}$.

PROPOSITION : Let $a, b \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$. Then

$$a \equiv b \pmod{2d} \quad \Rightarrow \quad a^2 \equiv b^2 \pmod{4d} .$$

EXAMPLE : Let $a = 13$, $b = 7$ $d = 3$. Then

$$13 \equiv 7 \pmod{2 \cdot 3} ,$$

i.e.,

$$13 \pmod 6 = 7 \pmod 6 ,$$

and

$$13^2 \equiv 7^2 \pmod{4 \cdot 3} ,$$

i.e.,

$$169 \pmod{12} = 49 \pmod{12} \qquad (\textbf{Check}!) .$$

$$a \equiv b \pmod{2d} \quad \Rightarrow \quad a^2 \equiv b^2 \pmod{4d}$$

PROOF : Suppose $a \equiv b \pmod{2d}$.

Then $2d|(a-b)$, *i.e.*, $a - b = q2d$, for some $q \in \mathbb{Z}$.

Thus a and b differ by an even number.

It follows that a and b must be both even or both odd.

Hence $a+b$ must be even, *i.e.*, $a + b = 2c$ for some $c \in \mathbb{Z}$.

Then $a^2 - b^2 = (a+b)(a-b) = (2c)(q2d) = cq\ 4d$.

It follows that $4d|(a^2 - b^2)$, *i.e.*, $a^2 \equiv b^2 \pmod{4d}$. **QED !**

NOTE : Also $a^2 \equiv b^2 \pmod{2d}$ and $a^2 \equiv b^2 \pmod{d}$.

PROPOSITION : If $n > 3$ then not all of

$$n \quad , \quad n+2 \quad , \quad n+4 \ ,$$

can be primes.

Idea of the proof : Always one of these three numbers is divisible by 3 .

PROOF. By contradiction : Assume that $n > 3$ and that

$$n \ , \ n+2 \ \text{ and } \ n+4 \ \text{ are primes .}$$

Since n is prime and $n > 3$ we have

$$n \bmod 3 \ = \ 1 \quad \text{or} \quad n \bmod 3 \ = \ 2 \ . \qquad \text{(Why ?)}$$

Case 1 : If $n \bmod 3 \ = \ 1$ then $n \ = \ 3k+1$ and

$$n+2 \ = \ 3k+3 \ , \quad i.e., \quad 3 | (n+2) \ .$$

Case 2 : If $n \bmod 3 \ = \ 2$ then $n \ = \ 3k+2$ and

$$n+4 \ = \ 3k+6 \ , \quad i.e., \quad 3 | (n+4) \ .$$

Contradiction !

THE FACTORIZATION THEOREM :

$$\forall n \in (\mathbb{Z}^+ - \{1\}) \ , \ \exists! \left(m, \ \{p_i\}_{i=1}^m, \ \{n_i\}_{i=1}^m \right) \ :$$

$$m \in \mathbb{Z}^+ ,$$

$$\forall i \ (i = 1, \cdots, m) \ : \ p_i, n_i \in \mathbb{Z}^+ \ ,$$

$$1 < p_1 < p_2 < \cdots < p_m \ ,$$

$$\forall i \ (i = 1, \cdots, m) \ : \ \ p_i \ \text{ is a prime number } \ ,$$

$$n \ = \ p_1^{n_1} \ p_2^{n_2} \ \cdots \ p_m^{n_m} \ .$$

EXAMPLE : $\qquad 252 \ = \ 2^2 \ 3^2 \ 7^1 \ .$

PROPOSITION : $\log_2 3$ is irrational.

PROOF : By contradiction:

Suppose $\log_2 3$ is rational, *i.e.*, $\exists p, q \in \mathbb{Z}^+$, such that

$$\log_2 3 \;=\; p/q \;.$$

By definition of the log function it follows that

$$2^{p/q} \;=\; 3 \;,$$

from which

$$2^p \;=\; 3^q \;.$$

Let $n \;=\; 2^p$. Then $n \in \mathbb{Z}^+$, with $n \geq 2$.

Then n has two different prime factorizations, namely

$$n \;=\; 2^p \qquad \text{and} \qquad n \;=\; 3^q \;.$$

This contradicts the Factorization Theorem. **QED !**

REMARK :

The fact that

$$2^p \neq 3^q ,$$

also follows from the facts that 2^p is even and 3^q is odd.

DEFINITION :

We call $n \in \mathbb{Z}^+$ a *perfect square* if

$$\exists k \in \mathbb{Z}^+ \quad : \quad n \; = \; k^2 \; .$$

FACT :

The factorization of a perfect square has only even powers :

If

$$k \quad = \quad p_1^{n_1} \; p_2^{n_2} \; \cdots \; p_m^{n_m} \; ,$$

then

$$n \quad = \quad k^2 \quad = \quad p_1^{2n_1} \; p_2^{2n_2} \; \cdots \; p_m^{2n_m} \; .$$

PROPOSITION :

If $n \in \mathbb{Z}^+$ is not a perfect square then $\sqrt{n}$ is irrational.

PROOF :

By contradiction :

Suppose n is not a perfect square, but $\sqrt{n}$ is rational.

Thus

$$\sqrt{n} \;=\; \frac{p}{q} \;,$$

i.e.,

$$p^2 \;=\; n\, q^2 \;,$$

for some $p, q \in \mathbb{Z}^+$.

$$p^2 = n\, q^2$$

- The prime factorization of p^2 has even powers only.
- The prime factorization of q^2 has even powers only.
- The prime factorization of n must have an odd power,

  (otherwise n would be a perfect square).
- Thus the factorization of nq^2 must have an odd power.
- Thus p^2 has two distinct factorizations:

  one with even powers and one with at least one odd power.

This contradicts the uniqueness in the Factorization Theorem.

QED !

DEFINITION :

$k \in \mathbb{Z}^+$ is the *greatest common divisor* of $n, m \in \mathbb{Z}^+$,

$$k \;=\; \gcd(n, m) \;,$$

if

- $k|n$ and $k|m$,
- no positive integer greater than k divides both n and m .

REMARK :

One can determine

$$\gcd(\ n\ ,\ m\ )$$

from the minimum exponents in the prime factorizations of n and m.

EXAMPLE : If

$$n\ =\ 168\ , \qquad m\ =\ 900\ ,$$

then

$$n\ =\ 2^3\ 3^1\ 7^1\ , \qquad m\ =\ 2^2\ 3^2\ 5^2\ ,$$

and

$$\gcd(168, 900)\ \ =\ \ 2^2\ 3^1\ \ =\ \ 12\ .$$

THE EUCLIDEAN THEOREM :

Let $n\ ,\ d\ \in\ \mathbb{Z}^{+}$, and let

$$r\ =\ n \bmod d\ , \qquad \text{(the remainder)}$$

Then

$$\gcd(n,d)\ =\ \begin{cases} \gcd(d\ ,\ r) & \text{if} \quad r\ >\ 0\ , \\ \\ d & \text{if} \quad r\ =\ 0\ . \end{cases}$$

EXAMPLE :

$$\begin{aligned}
\gcd(93\ ,\ 36) &= \gcd(36\ ,\ 93 \bmod 36) &&= \gcd(36\ ,\ 21) \\
&= \gcd(21\ ,\ 36 \bmod 21) &&= \gcd(21\ ,\ 15) \\
&= \gcd(15\ ,\ 21 \bmod 15) &&= \gcd(15\ ,\ 6) \\
&= \gcd(6\ ,\ 15 \bmod 6) &&= \gcd(6\ ,\ 3) \\
&= 3\ .
\end{aligned}$$

EXAMPLE :

$$\begin{aligned}
\gcd(2008\ ,\ 1947) &= \gcd(1947\ ,\ 2008 \bmod 1947) &&= \gcd(1947\ ,\ 61) \\
&= \gcd(61\ ,\ 1947 \bmod 61) &&= \gcd(61\ ,\ 56) \\
&= \gcd(56\ ,\ 61 \bmod 56) &&= \gcd(56\ ,\ 5) \\
&= \gcd(5\ ,\ 56 \bmod 5) &&= \gcd(5\ ,\ 1) \\
&= 1\ .
\end{aligned}$$

Thus 2008 and 1947 are *relatively prime* .

LEMMA :

Let $a, b, c \in \mathbb{Z}$, and $d \in \mathbb{Z}^+$.

Then

$$(1) \quad (a = b + c \ , \ d|a \ , \ d|b) \quad \Rightarrow \quad d|c \ ,$$

$$(2) \quad (a = b + c \ , \ d|b \ , \ d|c) \quad \Rightarrow \quad d|a \ ,$$

$$(3) \quad (a = bc \ , \ d|c) \quad \Rightarrow \quad d|a \ .$$

$$\boxed{(1) \qquad (\ a = b + c\ ,\quad d|a\ ,\quad d|b\ ) \quad \Rightarrow \quad d|c}$$

PROOF of (1) :

$$d|a \quad \Longleftrightarrow \quad \exists q_a \in \mathbb{Z} \ : \ a = d\ q_a\ ,$$

and

$$d|b \quad \Longleftrightarrow \quad \exists q_b \in \mathbb{Z} \ : \ b = d\ q_b\ .$$

Thus

$$c \ = \ a - b \ = \ d\ q_a - d\ q_b \ = \ d\ (q_a - q_b)\ .$$

Hence $d|c$.

EXERCISE : Prove (2) and (3) in a similar way.

$$\gcd(n,d) \;=\; \begin{cases} \gcd(d,r) & \text{if} \quad r > 0 \\ d & \text{if} \quad r = 0 \end{cases}$$

PROOF OF THE EUCLIDEAN THEOREM :

By the Division Theorem

$$n \;=\; q \cdot d \;+\; r \;,$$

where

$$q \;=\; n \text{ div } d \quad \text{and} \quad r \;=\; n \bmod d \;.$$

Case 1 : $r = 0$.

Then clearly $d|n$.

Also $d|d$ and no greater number than d divides d .

Hence $d = \gcd(n,d)$.

$$\gcd(n,d) \;=\; \begin{cases} \gcd(d,r) & \text{if} \quad r > 0 \\ d & \text{if} \quad r = 0 \end{cases}$$

Case 2 : $r > 0$:

Let $k = \gcd(n,d)$.

Then $k|n$ and $k|d$.

By the Division Theorem

$$n \;=\; q \cdot d \;+\; r \;,$$

By Lemma (3) $k|qd$.

By Lemma (1) $k|r$.

Thus k divides both d and r .

$$\boxed{\gcd(n,d) \;=\; \begin{cases} \gcd(d,r) & \text{if} \quad r > 0 \\ d & \text{if} \quad r = 0 \end{cases}}$$

$$k \;=\; \gcd(n,d) \quad , \quad n \;=\; q \cdot d \;+\; r \;.$$

Show k is the *greatest* common divisor of d and r :

By contradiction :

Suppose $k_1 > k$ and $k_1 = \gcd(d,r)$.

Thus $k_1 | d$ and $k_1 | r$

By Lemma (3) $k_1 | qd$.

By Lemma (2) $k_1 | n$.

Thus k_1 divides both n and d .

Since $k_1 > k$ this contradicts that $k = \gcd(n,d)$. **QED !**

REVIEW EXERCISES.

Problem 1.

Prove that a composite number n has a factor $k \leq \sqrt{n}$.

Thus to check if a number n is prime one needs only check whether

$$n \bmod k \quad = \quad 0 \ , \qquad k = 2, 3, \ \cdots \ , \lfloor \sqrt{n} \rfloor \ .$$

Problem 2. Use the above fact to check whether 143 is prime.

Problem 3. Find all integer solutions of

$$2x \equiv 7 (\text{mod } 17) \ .$$

Problem 4. Find all integer solutions of

$$4x \equiv 5 (\text{mod } 9) \ .$$

Problem 5.

Does there exists an integer x that simultaneously satisfies

$$x \equiv 2 (\text{mod } 6) \qquad \text{and} \qquad x \equiv 3 (\text{mod } 9) \ ?$$

Problem 6. Let

$$S \;=\; \{\, 0,\; 1,\; 2,\; 3,\; 4,\; 5,\; 6,\; 7,\; 8,\; 9 \,\}\;,$$

and define

$$f \;:\; S \;\longrightarrow\; S\;,$$

by

$$f(k) \;=\; (5k+3) \bmod 10\;.$$

Is f invertible?

Problem 7. with S as above, also consider

$$f(k) \;=\; (6k+3) \bmod 10\;,$$

and

$$f(k) \;=\; (7k+3) \bmod 10\;.$$

Problem 8. Let $n \geq 2$,

$$S_n \;=\; \{\, 0\,,\; 1\,,\; 2\,,\; 3\,,\; \cdots\,,\; n-1\,\}\,,$$

and define

$$f \;:\; S_n \;\longrightarrow\; S_n\,,$$

by

$$f(k) \;=\; (pk \;+\; s) \bmod n\,,$$

where p is prime, with $p > n$, and $s \in S_n$.

Prove that f is *one-to-one* (and hence *onto* and *invertible*).

THE PRINCIPLE OF INDUCTION

Let

$$S \;=\; \{\, s_1 \,,\; s_2 \,,\; s_3 \,,\; \cdots \,\}$$

be a *countably infinite set* .

Suppose P is a predicate,

$$P \;:\; S \;\longrightarrow\; \{\, T \,,\; F \,\} \,,$$

such that :

(i) $\qquad P(s_1) = T \quad ,$

(ii) $\qquad P(s_n) = T \quad \Rightarrow \quad P(s_{n+1}) = T \quad .$

Then

$$P(s) \;=\; T \quad , \quad \text{for all} \;\; s \in S \;.$$

EXAMPLE :

$$\sum_{k=1}^{n} k \;=\; \frac{n(n+1)}{2} \;, \qquad \forall n \in \mathbb{Z}^{+} \;.$$

Here $S = \mathbb{Z}^{+}$ and

$$P(n) \;=\; T \qquad \text{if} \qquad \sum_{k=1}^{n} k \;=\; \frac{n(n+1)}{2} \;,$$

and

$$P(n) \;=\; F \qquad \text{if} \qquad \sum_{k=1}^{n} k \;\neq\; \frac{n(n+1)}{2} \;.$$

We must show that $P(n) = T$ for all n .

PROOF :

(i) "By inspection" the formula holds if $n = 1$, *i.e.*, $P(1) = T$.

(ii) Suppose $P(n) = T$ *for some arbitrary* $n \in \mathbb{Z}^+$, *i.e.*,

$$\sum_{k=1}^{n} k \;=\; \frac{n(n+1)}{2} \;.$$

We must show that $P(n+1) = T$, *i.e.*,

$$\sum_{k=1}^{n+1} k \;=\; \frac{(n+1)\,\Big((n+1)+1\Big)}{2} \;.$$

This is done as follows:

$$\sum_{k=1}^{n+1} k \;=\; \Big(\sum_{k=1}^{n} k\Big) + (n+1) \;=\; \frac{n(n+1)}{2} + (n+1)$$

$$=\; \frac{(n+1)\,\Big((n+1)+1\Big)}{2} \;. \qquad \textbf{QED !}$$

EXAMPLE :

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6} , \qquad \forall n \in \mathbb{Z}^+ .$$

PROOF :

(i) Again the formula is valid if $n = 1$.

(ii) Suppose

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6} ,$$

for some arbitrary $n \in \mathbb{Z}^+$.

We must show that

$$\sum_{k=1}^{n+1} k^2 = \frac{(n+1)\left((n+1)+1\right)\left(2(n+1)+1\right)}{6} .$$

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6} \quad \Rightarrow \quad \sum_{k=1}^{n+1} k^2 = \frac{(n+1)\ ((n+1)+1)\ (2(n+1)+1)}{6}$$

To do this :

$$\begin{aligned}
\sum_{k=1}^{n+1} k^2 &= \left(\sum_{k=1}^{n} k^2\right) + (n+1)^2 \\
&= n(n+1)(2n+1)/6 + (n+1)^2 \\
&= (n+1)\left(n(2n+1) + 6(n+1)\right)/6 \\
&= (n+1)\ (2n^2+7n+6)/6 \\
&= (n+1)\ (n+2)\ (2n+3)/6 \\
&= (n+1)\left((n+1)+1\right)\left(2(n+1)+1\right)/6\ . \quad \textbf{QED !}
\end{aligned}$$

EXAMPLE :

$$(n^3 - n) \bmod 3 \;=\; 0 \;, \quad \forall n \in \mathbb{Z}^+ \;.$$

PROOF :

(i) By inspection $P(1) = T$.

(ii) Suppose $P(n) = T$, *i.e.*,

$$(n^3 - n) \bmod 3 \;=\; 0 \;, \text{ for some arbitrary } n \in \mathbb{Z}^+ \;.$$

We must show that $P(n+1) = T$, *i.e.*,

$$\Big((n+1)^3 - (n+1)\Big) \bmod 3 \;=\; 0 \;.$$

$$(n^3 - n) \bmod 3 \;=\; 0 \qquad \Rightarrow \qquad (\;(n+1)^3 - (n+1)\;) \bmod 3 \;=\; 0$$

To do this :

$$\begin{aligned}
\Big((n+1)^3 - (n+1)\Big) \bmod 3 \;&=\; (n^3 + 3n^2 + 3n - n) \bmod 3 \\
&=\; \Big(3(n^2+n) + n^3 - n\Big) \bmod 3 \\
&=\; (n^3 - n) \bmod 3 \;=\; 0 \text{ . } \mathbf{QED} \text{ !}
\end{aligned}$$

EXAMPLE :

Let $P(n)$ denote the statement

"A set S_n of n elements has 2^n subsets".

CLAIM : $P(n) = T$ for all $n \geq 0$.

PROOF :

(i) $P(0) = T$ because the empty set has one subset, namely itself.

(ii) Suppose that $P(n) = T$ *for some arbitrary* n , ($n \geq 0$) ,

i.e., S_n has 2^n subsets.

We must show that $P(n+1) = T$, *i.e.*, S_{n+1} has 2^{n+1} subsets.

To do this write

$$S_{n+1} \;=\; \{\, s_1 \,,\; s_2 \,,\; \cdots \,,\; s_n \,,\; s_{n+1} \,\} \;\;=\;\; S_n \;\cup\; \{s_{n+1}\} \,.$$

Now count the subsets of S_{n+1} :

(a) By inductive hypothesis S_n has 2^n subsets.

These are also subsets of S_{n+1} .

(b) All other subsets of S_{n+1} have the form

$$T \;\cup\; \{s_{n+1}\} \,,$$

where T is any subset of S_n .

Thus there are 2^n such additional subsets.

The total number of subsets of S_{n+1} is therefore

$$2^n \;+\; 2^n \;=\; 2^{n+1} \,. \qquad \textbf{QED !}$$

EXAMPLE :

Let $P(n)$ denote the statement

$$3^n < n!$$

CLAIM :

$$P(n) = T \quad \text{for all integers } n \text{ with } n > 6 \ .$$

REMARK : $P(n)$ is *False* for $n \leq 6$. (**Check**!)

PROOF :

(i) $P(7) = T$, because

$$3^7 \;=\; 2187 \;<\; 5040 \;=\; 7!$$

(ii) Assume $P(n) = T$ *for some arbitrary* n , $(n \geq 7)$,

i.e.,

$$3^n \;<\; n! \qquad (n \geq 7) \; .$$

We must show that $P(n+1) = T$, *i.e.*,

$$3^{n+1} \;<\; (n+1)!$$

$$3^n < n! \quad \Rightarrow \quad 3^{n+1} < (n+1)!$$

To do this :

$$\begin{aligned}
3^{n+1} &= 3 \cdot 3^n \\
&< 3 \cdot n! && \text{(by inductive assumption)} \\
&< (n+1)\, n! && \text{(since } n \geq 7\text{)} \\
&= (n+1)!
\end{aligned}$$

EXERCISE : For which nonnegative integers is

$$n^2 \leq n! \ ?$$

Prove your answer by induction.

EXERCISE : For which positive integers n is

$$n^2 \leq 2^n \ ?$$

Prove your answer by induction.

EXAMPLE :

Let

$$H_m \equiv \sum_{k=1}^{m} \frac{1}{k} \, . \qquad (\text{"Harmonic numbers."})$$

Let $P(n)$ denote the statement

$$H_{2^n} \geq 1 + \frac{n}{2} \, .$$

CLAIM : $P(n) = T$ for all $n \in \mathbb{Z}^+$.

PROOF :

(i) It is clear that $P(1) = T$, because

$$H_{2^1} = \sum_{k=1}^{2} \frac{1}{k} = 1 + \frac{1}{2} \, .$$

(ii) Assume that

$$P(n) \;=\; T \quad \textit{for some arbitrary} \quad n \in \mathbb{Z}^+ \;,$$

i.e.,

$$H_{2^n} \;\geq\; 1 \;+\; \frac{n}{2} \;.$$

We must show that

$$P(n+1) = T \quad ,$$

i.e.,

$$H_{2^{n+1}} \;\geq\; 1 \;+\; \frac{n+1}{2} \;.$$

To do this :

$$
\begin{aligned}
H_{2^{n+1}} \;=\; \sum_{k=1}^{2^{n+1}} \frac{1}{k} \;&=\; \sum_{k=1}^{2^{n}} \frac{1}{k} \;+\; \sum_{k=2^n+1}^{2^{n+1}} \frac{1}{k} \\
&= \sum_{k=1}^{2^{n}} \frac{1}{k} \;+\; \sum_{k=2^n+1}^{2^n+2^n} \frac{1}{k} \\
&\geq \; (1+\frac{n}{2}) \;+\; 2^n \; \frac{1}{2^n+2^n} \\
&= \; (1+\frac{n}{2}) \;+\; \frac{1}{2} \\
&= \; 1+\frac{n+1}{2} \; . \qquad \textbf{QED !}
\end{aligned}
$$

REMARK :

It follows that

$$\sum_{k=1}^{\infty} \frac{1}{k} \quad \textit{diverges} \ ,$$

i.e.,

$$\sum_{k=1}^{n} \frac{1}{k} \quad \longrightarrow \quad \infty \qquad \text{as} \qquad n \longrightarrow \infty \ .$$

EXAMPLE : (The Binomial Formula.)

For $n \geq 0$, a, b nonzero,

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k,$$

where

$$\binom{n}{k} \equiv \frac{n!}{k!\,(n-k)!} .$$

REMARK : Thus we can write

$$(a+b)^n = a^n + \binom{n}{1} a^{n-1}b + \binom{n}{2} a^{n-2}b^2 + \cdots + \binom{n}{n-1} ab^{n-1} + b^n .$$

PROOF :

The formula holds if $n = 0$. (**Check**!)

Assume that *for some arbitrary* n, ($n \geq 0$)

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k .$$

We must show that the formula is also valid for $n+1$, *i.e.*, that

$$(a+b)^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} a^{n+1-k} b^k .$$

This can be done as follows :

$$
\begin{aligned}
(a+b)^{n+1} &= (a+b)(a+b)^n = (a+b)\sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k \\
&= a^{n+1}+\sum_{k=1}^{n}\binom{n}{k}a^{n-k+1}b^k+\sum_{k=0}^{n-1}\binom{n}{k}a^{n-k}b^{k+1}+b^{n+1} \\
&= a^{n+1}+\sum_{k=1}^{n}\binom{n}{k}a^{n-k+1}b^k+\sum_{k=1}^{n}\binom{n}{k-1}a^{n-k+1}b^k+b^{n+1} \\
&= a^{n+1}+\sum_{k=1}^{n}\left\{\binom{n}{k}+\binom{n}{k-1}\right\}a^{n-k+1}b^k+b^{n+1} \\
&= a^{n+1}+\sum_{k=1}^{n}\binom{n+1}{k}a^{n-k+1}b^k+b^{n+1} \\
&= \sum_{k=0}^{n+1}\binom{n+1}{k}a^{n+1-k}b^k\ . \qquad \textbf{QED !}
\end{aligned}
$$

REMARK :

In the proof we used the fact that

$$\begin{pmatrix} n \\ k \end{pmatrix} + \begin{pmatrix} n \\ k-1 \end{pmatrix} = \frac{n!}{k!\,(n-k)!} + \frac{n!}{(k-1)!\,(n-k+1)!}$$

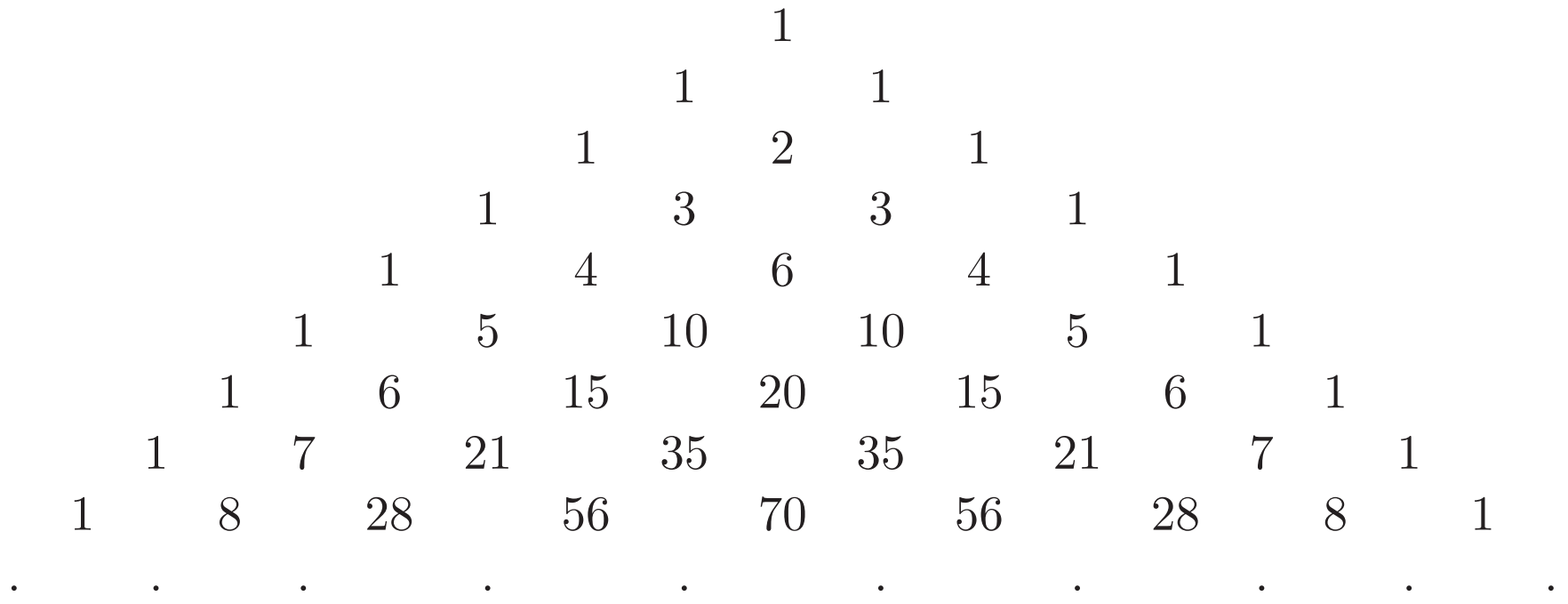
$$= \frac{n!\,(n-k+1) \;+\; n!\,k}{k!\,(n-k+1)!}$$

$$= \frac{(n+1)!}{k!\,(n-k+1)!}$$

$$= \begin{pmatrix} n+1 \\ k \end{pmatrix} .$$

REMARK :

One can order the binomial coefficients in *Pascal's triangle* as follows :



Observe that every entry can be obtained by summing the closest entries in the preceding row.

This is so because the $(n+1)$st and $(n+2)$nd rows look like :

$$\begin{array}{ccccccccc} & 1 & \cdots\cdots\cdots & \binom{n}{k-1} & & \binom{n}{k} & \cdots\cdots\cdots & 1 & \\ 1 & & \cdots\cdots\cdots & & \binom{n+1}{k} & & \cdots\cdots\cdots & & 1 \end{array}$$

and we have shown above that

$$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k} .$$

REMARKS :

- The advantage of a proof by induction is that it is systematic.

- A disadvantage is that the result (*e.g.*, a formula) must be known in advance from a heuristic argument or by trial and error.

- In contrast, a *constructive proof* actually derives the result.

EXAMPLE : For $x \in \mathbb{R}$, $x \neq 0, 1$:

$$\sum_{k=0}^{n} x^k \quad = \quad \frac{1 - x^{n+1}}{1 - x} \ , \qquad \forall n \geq 0 \ , \qquad (\ \textit{Geometric sum} \ ) \ .$$

PROOF (a *constructive proof* : already done earlier) :

Let

$$S_n \quad = \quad \sum_{k=0}^{n} x^k \ .$$

Then

$$S_n \quad = \quad 1 \ + \ x \ + \ x^2 \ + \ \cdots \ + \ x^{n-1} \ + \ x^n \ ,$$

$$x \cdot S_n \quad = \quad x \ + \ x^2 \ + \ \cdots \ + \ x^{n-1} \ + \ x^n \ + \ x^{n+1} \ ,$$

so that

$$S_n \ - \ x \cdot S_n \quad = \quad (1 - x) \cdot S_n \quad = \quad 1 - x^{n+1} \ ,$$

from which the formula follows. **QED !**

ALTERNATE PROOF (*by induction*) :

(i) "By inspection" we find that the formula holds if $n = 0$.

(ii) Suppose that $S_n = \frac{1-x^{n+1}}{1-x}$, *for some arbitary* n, ($n \geq 0$) .

Show $S_{n+1} = \frac{1-x^{(n+1)+1}}{1-x}$:

$$S_{n+1} = S_n + x^{n+1} = \frac{1-x^{n+1}}{1-x} + x^{n+1}$$

$$= \frac{(1-x^{n+1}) + x^{n+1}(1-x)}{1-x}$$

$$= \frac{1-x^{n+1}+x^{n+1}-x^{n+2}}{1-x}$$

$$= \frac{1-x^{(n+1)+1}}{1-x} \; . \qquad \textbf{QED !}$$

EXERCISE :

Use mathematical induction to prove that

$$21 \mid (4^{n+1} + 5^{2n-1}) ,$$

whenever n is a positive integer.

EXERCISE :

The Fibonacci numbers are defined as: $f_1 = 1$, $f_2 = 1$, and

$$f_n = f_{n-1} + f_{n-2} , \qquad \text{for } n \geq 3 .$$

Use a proof by induction to show that

$$3 \mid f_{4n} ,$$

for all $n \geq 1$.

Variations on the Principle of Induction.

Let $S = \{\ s_1,\ s_2,\ s_3,\ \cdots\ \}$ be a countably infinite set and P a predicate :

$$P \ : \ S \longrightarrow \{\ T\ ,\ F\ \}\ .$$

VARIATION 1 : (as used so far $\cdots$)

$$\Big(P(s_1)\ \wedge\ \Big[\forall n \geq 1 : P(s_n) \Rightarrow P(s_{n+1})\Big]\Big) \Rightarrow \forall n : P(s_n)\ .$$

VARIATION 2 :

$$\Big(P(s_1) \wedge P(s_2) \wedge \Big[\forall n \geq 2 : P(s_{n-1}) \wedge P(s_n) \Rightarrow P(s_{n+1})\Big]\Big) \Rightarrow \forall n : P(s_n)\ .$$

VARIATION $\cdots$

STRONG INDUCTION :

$$\Big(P(s_1) \wedge \forall n \geq 1 : \Big[P(s_1) \wedge P(s_2) \wedge \cdots \wedge P(s_n) \Rightarrow P(s_{n+1})\Big]\Big) \Rightarrow \forall n : P(s_n)\ .$$

EXAMPLE : The Fibonacci Numbers.

The *Fibonacci numbers* are defined recursively as

$$f_1 = 1 ,$$

$$f_2 = 1 ,$$

$$f_n = f_{n-1} + f_{n-2} , \qquad \text{for} \quad n \geq 3 .$$

$f_1 = 1$ $f_{11} = 89$ $f_{21} = 10946$

$f_2 = 1$ $f_{12} = 144$ $f_{22} = 17711$

$f_3 = 2$ $f_{13} = 233$ $f_{23} = 28657$

$f_4 = 3$ $f_{14} = 377$ $f_{24} = 46368$

$f_5 = 5$ $f_{15} = 610$ $f_{25} = 75025$

$f_6 = 8$ $f_{16} = 987$ $f_{26} = 121393$

$f_7 = 13$ $f_{17} = 1597$ $f_{27} = 196418$

$f_8 = 21$ $f_{18} = 2584$ $f_{28} = 317811$

$f_9 = 34$ $f_{19} = 4181$ $f_{29} = 514229$

$f_{10} = 55$ $f_{20} = 6765$ $f_{30} = 832040$

PROPERTY :

There is an explicit formula for f_n , namely

$$f_n \quad = \quad \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n \quad - \quad \left(\frac{1-\sqrt{5}}{2} \right)^n \right] \quad .$$

We can also write

$$
\begin{aligned}
f_n &= \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n \right] \\
&= \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2}\right)^n \left[1 - \left(\frac{1-\sqrt{5}}{1+\sqrt{5}}\right)^n \right] \\
&\approx \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2}\right)^n \left[1 - \left(\frac{1-2.236}{1+2.236}\right)^n \right] \\
&= \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2}\right)^n \left[1 + (-1)^{n+1} \Big(0.3819\Big)^n \right] \\
&\approx \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2}\right)^n .
\end{aligned}
$$

$$f_1 = 1 \approx 0.72361 \qquad f_{11} = 89 \approx 88.99775$$

$$f_2 = 1 \approx 1.17082 \qquad f_{12} = 144 \approx 144.00139$$

$$f_3 = 2 \approx 1.89443 \qquad f_{13} = 233 \approx 232.99914$$

$$f_4 = 3 \approx 3.06525 \qquad f_{14} = 377 \approx 377.00053$$

$$f_5 = 5 \approx 4.95967 \qquad f_{15} = 610 \approx 609.99967$$

$$f_6 = 8 \approx 8.02492 \qquad f_{16} = 987 \approx 987.00020$$

$$f_7 = 13 \approx 12.98460 \qquad f_{17} = 1597 \approx 1596.99987$$

$$f_8 = 21 \approx 21.00952 \qquad f_{18} = 2584 \approx 2584.00008$$

$$f_9 = 34 \approx 33.99412 \qquad f_{19} = 4181 \approx 4180.99995$$

$$f_{10} = 55 \approx 55.00364 \qquad f_{20} = 6765 \approx 6765.00003$$

$$\boxed{f_n \;=\; \tfrac{1}{\sqrt{5}}\left[\;\left(\tfrac{1+\sqrt{5}}{2}\right)^n \;-\; \left(\tfrac{1-\sqrt{5}}{2}\right)^n\;\right]}$$

PROOF (By Induction, using Variation 2) :

The formula is valid when $n = 1$:

$$f_1 \;=\; \frac{1}{\sqrt{5}}\left[\;\frac{1+\sqrt{5}}{2} \;-\; \frac{1-\sqrt{5}}{2}\;\right] \;=\; 1 \;.$$

The formula is also valid when $n = 2$:

$$f_2 \;=\; \frac{1}{\sqrt{5}}\left[\;\left(\frac{1+\sqrt{5}}{2}\right)^2 \;-\; \left(\frac{1-\sqrt{5}}{2}\right)^2\;\right] \;=\; \frac{1}{\sqrt{5}}\,\sqrt{5} \;=\; 1 \;.$$

(**Check**!)

Inductively, assume that we have

$$f_{n-1} \quad = \quad \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2}\right)^{n-1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n-1} \right] ,$$

and

$$f_n \quad = \quad \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2}\right)^{n} - \left(\frac{1-\sqrt{5}}{2}\right)^{n} \right] .$$

We must show that

$$f_{n+1} \quad = \quad \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1} \right] .$$

Using the inductive hypothesis for n and $n-1$ we have

$$f_{n+1} \quad = \quad f_{n-1} \quad + \quad f_n \qquad \text{(by definition)}$$

$$= \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2}\right)^{n-1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n-1} + \left(\frac{1+\sqrt{5}}{2}\right)^{n} - \left(\frac{1-\sqrt{5}}{2}\right)^{n} \right]$$

$$= \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2}\right)^{n-1} \left(1+\frac{1+\sqrt{5}}{2}\right) - \left(\frac{1-\sqrt{5}}{2}\right)^{n-1} \left(1+\frac{1-\sqrt{5}}{2}\right) \right]$$

$$= \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2}\right)^{n-1} \left(\frac{3+\sqrt{5}}{2}\right) - \left(\frac{1-\sqrt{5}}{2}\right)^{n-1} \left(\frac{3-\sqrt{5}}{2}\right) \right]$$

$$= \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2}\right)^{n-1} \left(\frac{1+\sqrt{5}}{2}\right)^{2} - \left(\frac{1-\sqrt{5}}{2}\right)^{n-1} \left(\frac{1-\sqrt{5}}{2}\right)^{2} \right]$$

$$= \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1} \right] . \qquad \textbf{QED !}$$

Direct solution of the Fibonacci recurrence relation.

$$f_1 \;=\; 1\,, \qquad f_2 \;=\; 1\,,$$

$$f_k \;=\; f_{k-1} \;+\; f_{k-2}\,, \qquad \text{for} \quad k \;\geq\; 3\,.$$

Try solutions of the form

$$f_n \;=\; c\; z^n\,,$$

This gives

$$c\; z^n \;=\; c\; z^{n-1} \;+\; c\; z^{n-2}\,, \qquad \text{or} \qquad z^n \;-\; z^{n-1} \;-\; z^{n-2} \;=\; 0\,,$$

from which we obtain the *characteristic equation*

$$z^2 \;-\; z \;-\; 1 \;=\; 0\,.$$

$$\boxed{z^2 \;-\; z \;-\; 1 \;=\; 0}$$

The characteristic equation has solutions ("*roots*"):

$$z \;=\; \frac{1 \;\pm\; \sqrt{1 \;+\; 4}}{2} \;,$$

that is,

$$z_1 \;=\; \frac{1 \;+\; \sqrt{5}}{2} \qquad , \qquad z_2 \;=\; \frac{1 \;-\; \sqrt{5}}{2} \;.$$

The *general solution* of the recurrence relation is then

$$f_n \;=\; c_1 \; z_1^n \;+\; c_2 \; z_2^n \;.$$

$$\boxed{f_n \;=\; c_1\, z_1^n \;+\; c_2\, z_2^n}$$

The constants c_1 and c_2 are determined by the *initial conditions* :

$$f_1 \;=\; 1 \quad \Rightarrow \quad c_1\, z_1 \;+\; c_2\, z_2 \;=\; 1\,,$$

and

$$f_2 \;=\; 1 \quad \Rightarrow \quad c_1\, z_1^2 \;+\; c_2\, z_2^2 \;=\; 1\,,$$

that is,

$$c_1\, \frac{1+\sqrt{5}}{2} \quad + \quad c_2\, \frac{1-\sqrt{5}}{2} \quad = \quad 1\,,$$

and

$$c_1 \left(\frac{1+\sqrt{5}}{2}\right)^2 \quad + \quad c_2 \left(\frac{1-\sqrt{5}}{2}\right)^2 \quad = \quad 1\,,$$

from which we find

$$c_1 \;=\; \frac{1}{\sqrt{5}} \qquad \text{and} \qquad c_2 \;=\; -\,\frac{1}{\sqrt{5}}\,. \qquad (\textbf{Check!})$$

$$\boxed{f_n \;=\; c_1\, z_1^n \;+\; c_2\, z_2^n}$$

We found that

$$z_1 \;=\; \frac{1 \;+\; \sqrt{5}}{2} \qquad , \qquad z_2 \;=\; \frac{1 \;-\; \sqrt{5}}{2}\,.$$

and

$$c_1 \;=\; \frac{1}{\sqrt{5}} \qquad \text{and} \qquad c_2 \;=\; -\,\frac{1}{\sqrt{5}}\,. \qquad (\textbf{Check!})$$

from which

$$f_n \;=\; \frac{1}{\sqrt{5}}\left(\frac{1 \;+\; \sqrt{5}}{2}\right)^n \;-\; \frac{1}{\sqrt{5}}\left(\frac{1 \;-\; \sqrt{5}}{2}\right)^n\,.$$

REVIEW EXERCISES.

Problem 1.

Prove that the Fibonacci numbers satisfy the following relations:

- $\sum_{k=1}^{n} f_{2k-1} = f_{2n}$, for $n \in \mathbb{Z}^+$.
- $f_{n-1}\, f_{n+1} - f_n^2 = (-1)^n$, for $n \in \mathbb{Z}^+$, $(n \geq 2)$.
- $-f_1 + f_2 - f_3 + \cdots - f_{2n-1} + f_{2n} = f_{2n-1} - 1$, for $n \in \mathbb{Z}^+$.

Problem 2. The recurrence relation

$$x_{n+1} \;=\; c\, x_n\, (1 - x_n)\;, \qquad n = 1, 2, 3, \;\cdots\;,$$

known as the *logistic equation*, models population growth when there are limited resources.

Write a small computer program (using *real* arithmetic) to see what happens to the sequence x_n, $n = 1, 2, 3, \;\cdots$, with $0 < x_1 < 1$, for each of the following values of c :

(a) 0.5 , (b) 1.5 , (c) 3.2 , (d) 3.5 , (e) 3.9

Problem 3. Find an explicit solution to the recurrence relation

$$x_{n+1} \;=\; 3\, x_n - 2\, x_{n-1}\;, \qquad n = 1, 2, 3, \;\cdots\;,$$

with $x_1 = 1$ and $x_2 = 3$.

RELATIONS

A *binary relation* relates elements of a set to elements of another set.

EXAMPLE :

The operator "$\leq$" relates elements of $\mathbb{Z}$ to elements of $\mathbb{Z}$. *e.g.*,

$$2 \leq 5 \,, \quad \text{and} \quad 3 \leq 3 \,, \quad \text{but} \quad 7 \not\leq 2 \,.$$

We can also view this relation as a function

$$\leq \quad : \quad \mathbb{Z} \times \mathbb{Z} \longrightarrow \{ T \,, F \} \,.$$

RECALL :

Let

$$A \;=\; \{a_1, a_2, \cdots, a_{n_A}\} \quad \text{and} \quad B \;=\; \{b_1, b_2, \cdots, b_{n_B}\} \;.$$

The *product set* $A \times B$ is the set of all ordered pairs from A and B.

More precisely,

$$A \times B \;\equiv\; \{(a, b) \;:\; a \in A,\; b \in B\} \;.$$

NOTE :

- The product set $A \times B$ has $n_A \cdot n_B$ elements.

- If A and B are distinct and nonempty then $A \times B \neq B \times A$.

EXAMPLE :

If

$$A = \{ \, ! \, , \, ? \, \} \qquad \text{and} \qquad B = \{ \, \bullet \, , \, \circ \, , \, \square \, \} \, ,$$

then

$$A \times B = \{ \, (!, \bullet) \, , \, (!, \circ) \, , \, (!, \square) \, , \, (?, \bullet) \, , \, (?, \circ) \, , \, (?, \square) \, \} \, .$$

We can now equivalently define :

DEFINITION :

A *binary relation* R from A to B is a subset of $A \times B$.

NOTATION :

If $R \subseteq A \times B$, and

$$(a, b) \in R \ ,$$

then we say that

$$\text{“}a \text{ is } R\text{-related to } b\text{”} ,$$

and we also write

$$a \ R \ b \quad .$$

EXAMPLE :

Let $A = \{1, 3\}$ and $B = \{3, 5, 9\}$.

Let R denote the relation "*divides*" from A to B, *i.e.*,

$$aRb \qquad \text{if and only if} \qquad a|b \ .$$

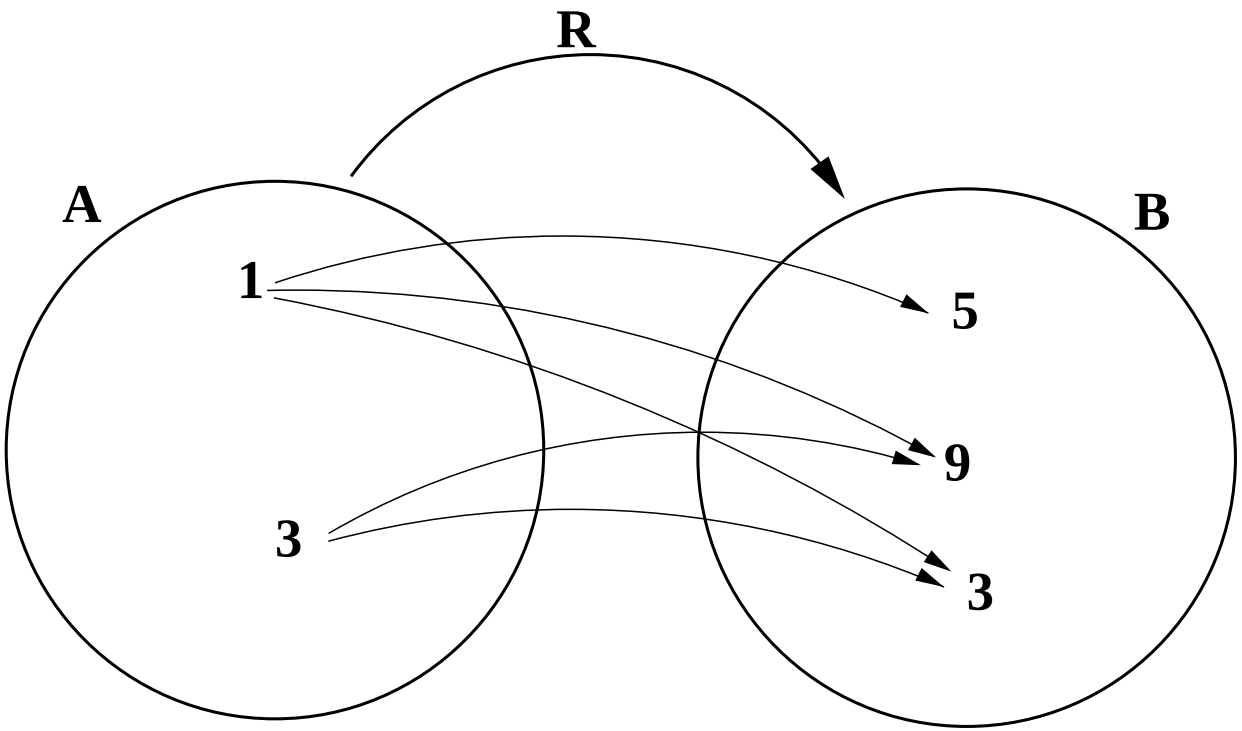
Then

$$1R3 \ , \ 1R5 \ , \ 1R9 \ , \ 3R3 \ , \ \text{and} \ 3R9 \ .$$

Thus

$$R = \{ \ (1,3) \ , \ (1,5) \ , \ (1,9) \ , \ (3,3) \ , \ (3,9) \ \} \ .$$

We can represent R by the following diagram



This representation is an example of a *directed bipartite graph*.

Note that R is not a function, since it is multi-valued.

REMARK :

We see that a *relation* generalizes the notion of a *function*.

Unlike functions from a set A to a set B :

- A relation does not have to be defined for all $a \in A$.

- A relation does not have to be single-valued.

A finite relation from a set A into itself can be represented by an ordinary *directed graph*.

EXAMPLE :

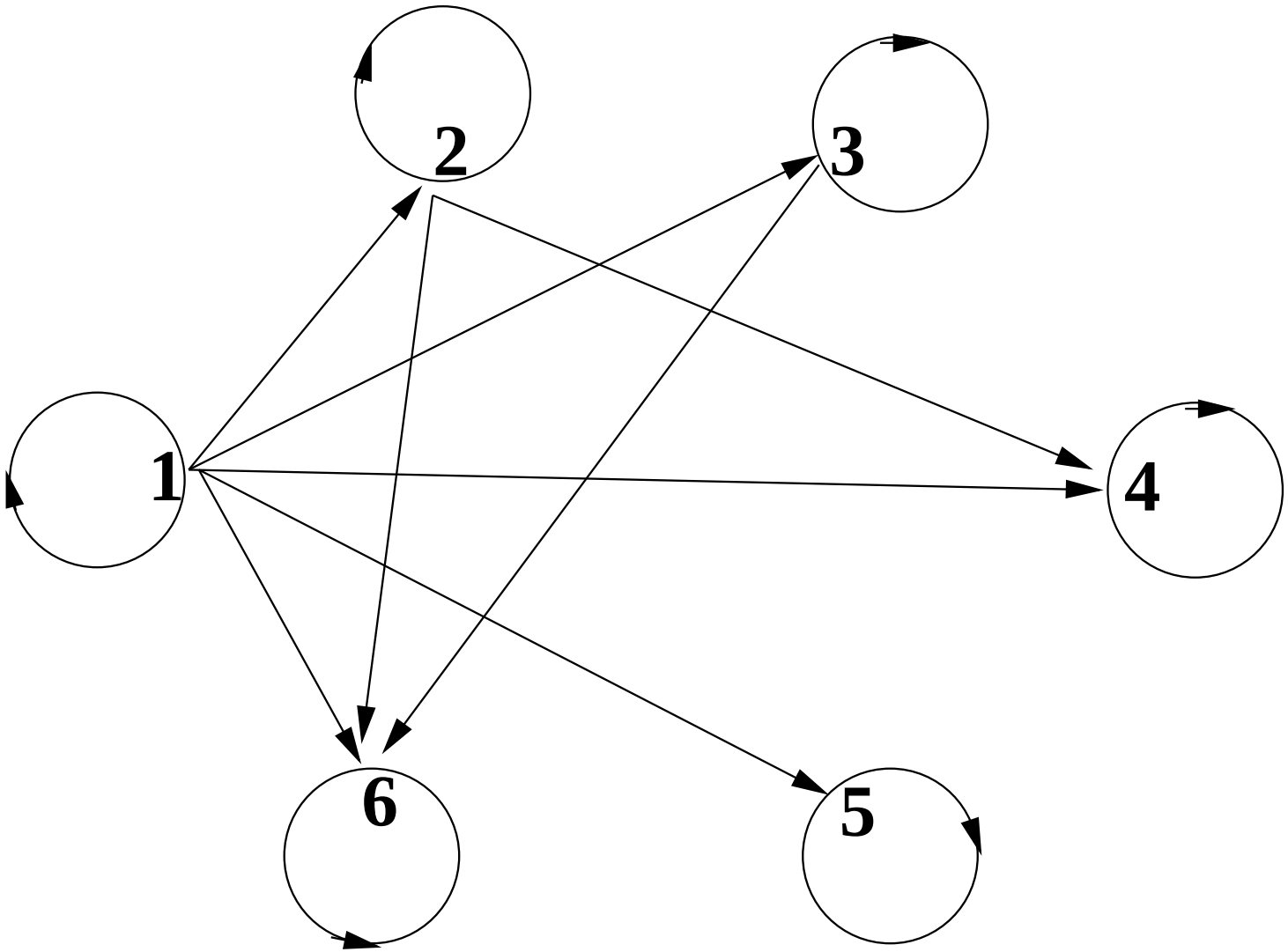
Let

$$A = \{1 , 2 , 3 , 4 , 5 , 6\} ,$$

and let R denote the relation "*divides*" from A to A .

We say that R *is a relation* "*on* A" .

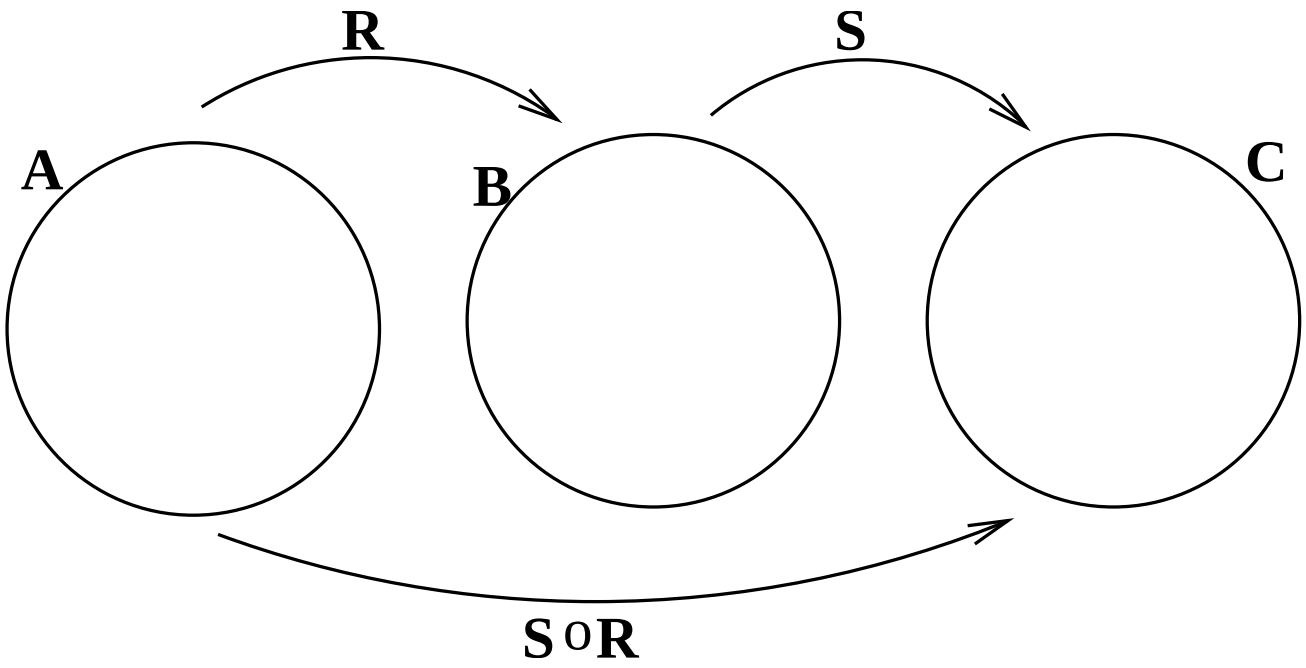
This relation has the following directed graph representation :



The “divides” relation on the set A .

We can *compose* relations as follows :

Let R be a relation from A to B , and S a relation from B to C.



Then $S \circ R$ is the relation from A to C defined by

$$a(S \circ R)c \qquad \text{if and only if} \qquad \exists b \in B \ : \ aRb \ \wedge \ bSc \ .$$

EXAMPLE :

Let

$$A = \{1, 2, 3\}, \qquad B = \{2, 6\}, \quad \text{and} \quad C = \{1, 9, 15\},$$

and define the relations R and S by

$$aRb \qquad \text{if and only if} \qquad a|b \ ,$$

and

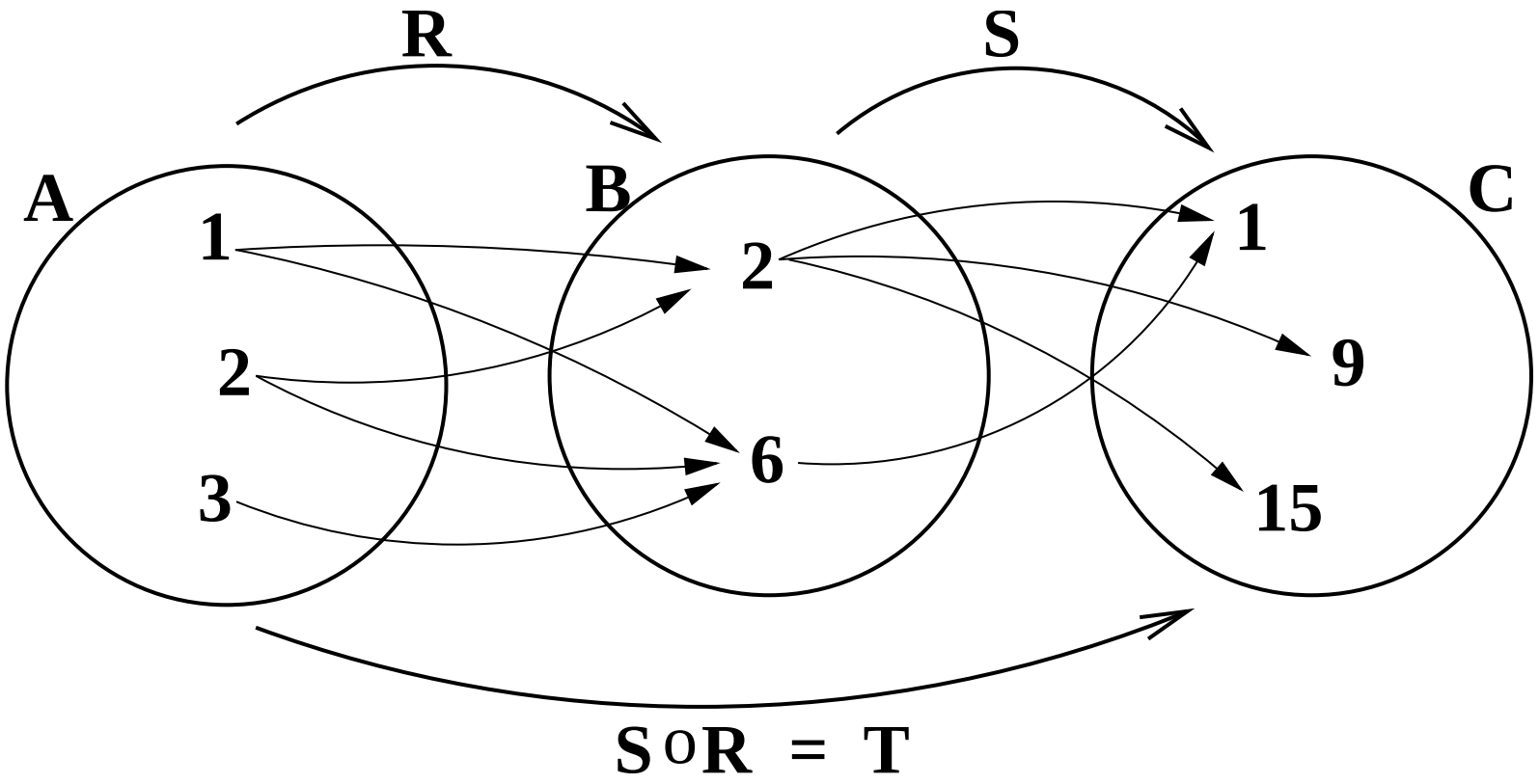
$$bSc \qquad \text{if and only if} \qquad b + c \ \text{ is prime} \ .$$

Define

$$T \ = \ S \circ R \ .$$

Then from the diagram below we see that

$$T = \{\ (1,1)\ ,\ (1,9)\ ,\ (1,15)\ ,\ (2,1)\ ,\ (2,9)\ ,\ (2,15)\ ,\ (3,1)\ \}\ .$$



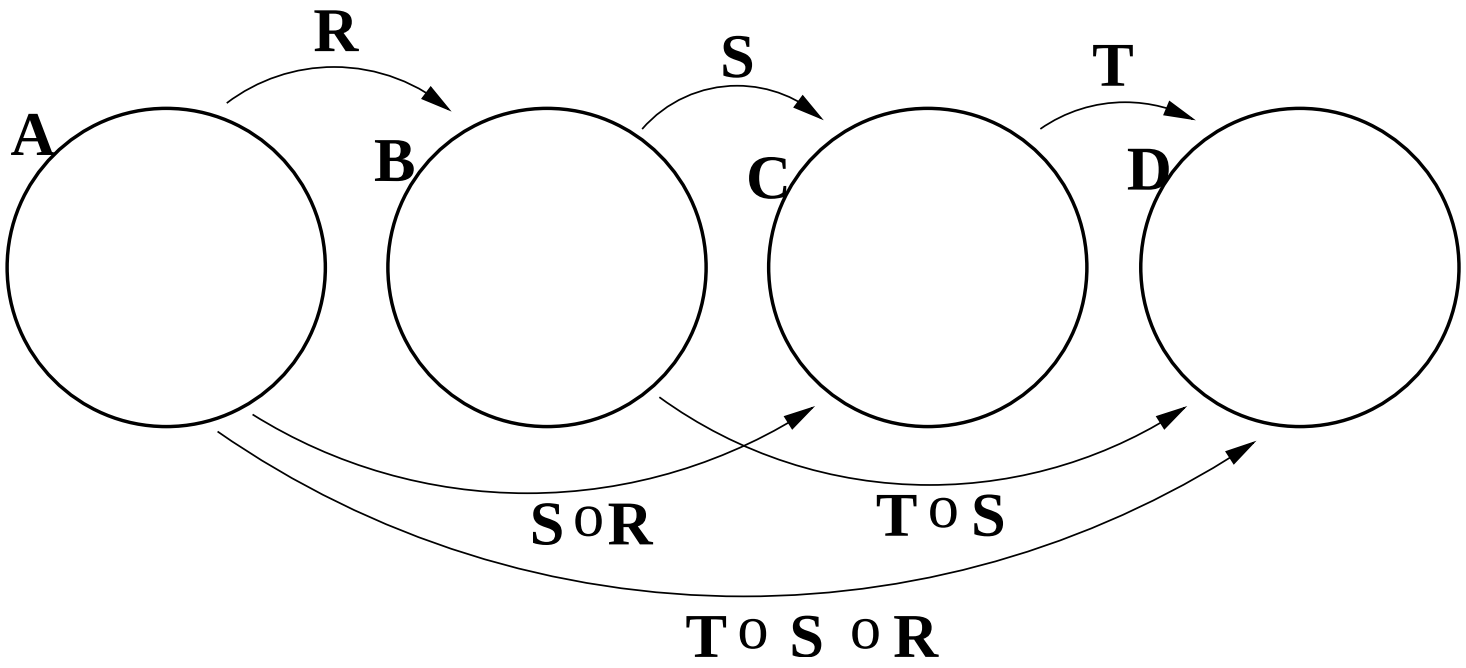
Let A, B, C, and D be sets, and let R S, and T be relations :

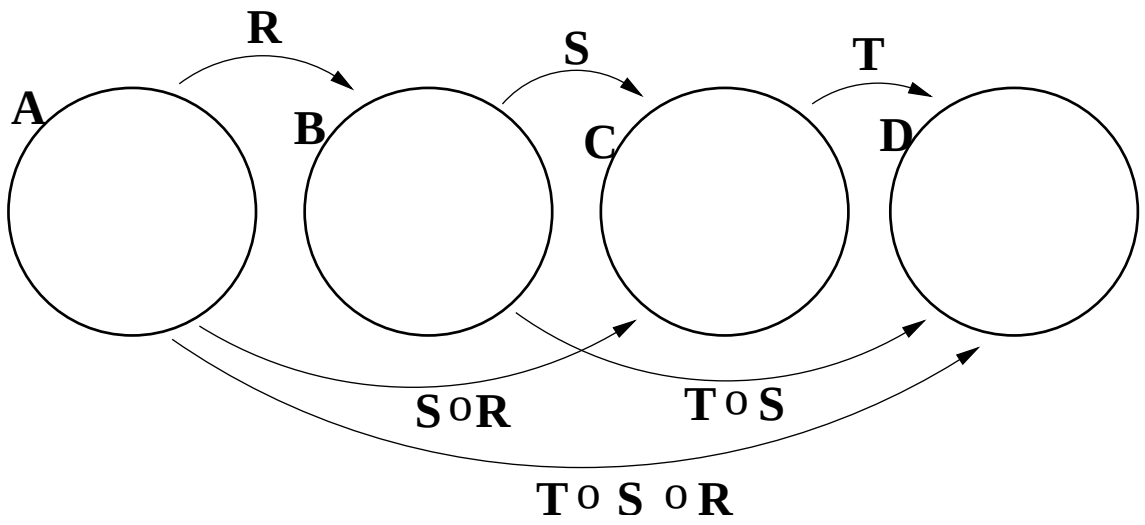
$$R \ : \ A \longrightarrow B \ , \qquad S \ : \ B \longrightarrow C \ , \qquad T \ : \ C \longrightarrow D \ .$$

PROPOSITION :

The composition of relations is associative, *i.e.*,

$$(T \circ S) \circ R \ = \ T \circ (S \circ R) \ .$$





$$\boxed{(T \circ S) \circ R \;=\; T \circ (S \circ R)\;.}$$

PROOF : Let $a \in A$ and $d \in D$. Then

$$a(T \circ S) \circ Rd \iff \exists b \in B \;:\; (aRb \;\wedge\; bT \circ Sd)$$

$$\iff \exists b \in B, \exists c \in C \;:\; (aRb \;\wedge\; bSc \;\wedge\; cTd)$$

$$\iff \exists c \in C, \exists b \in B \;:\; (aRb \;\wedge\; bSc \;\wedge\; cTd)$$

$$\iff \exists c \in C \;:\; (aS \circ Rc \;\wedge\; cTd) \iff aT \circ (S \circ R)d\;.$$

QED !

EXAMPLE : Let the relation R on

$$A \quad = \quad \{\ 2, 3, 4, 8, 9, 12\ \}\ ,$$

be defined by

$$(a, b) \in R \quad \text{if and only if} \quad (a|b\ \wedge\ a \neq b)\ .$$

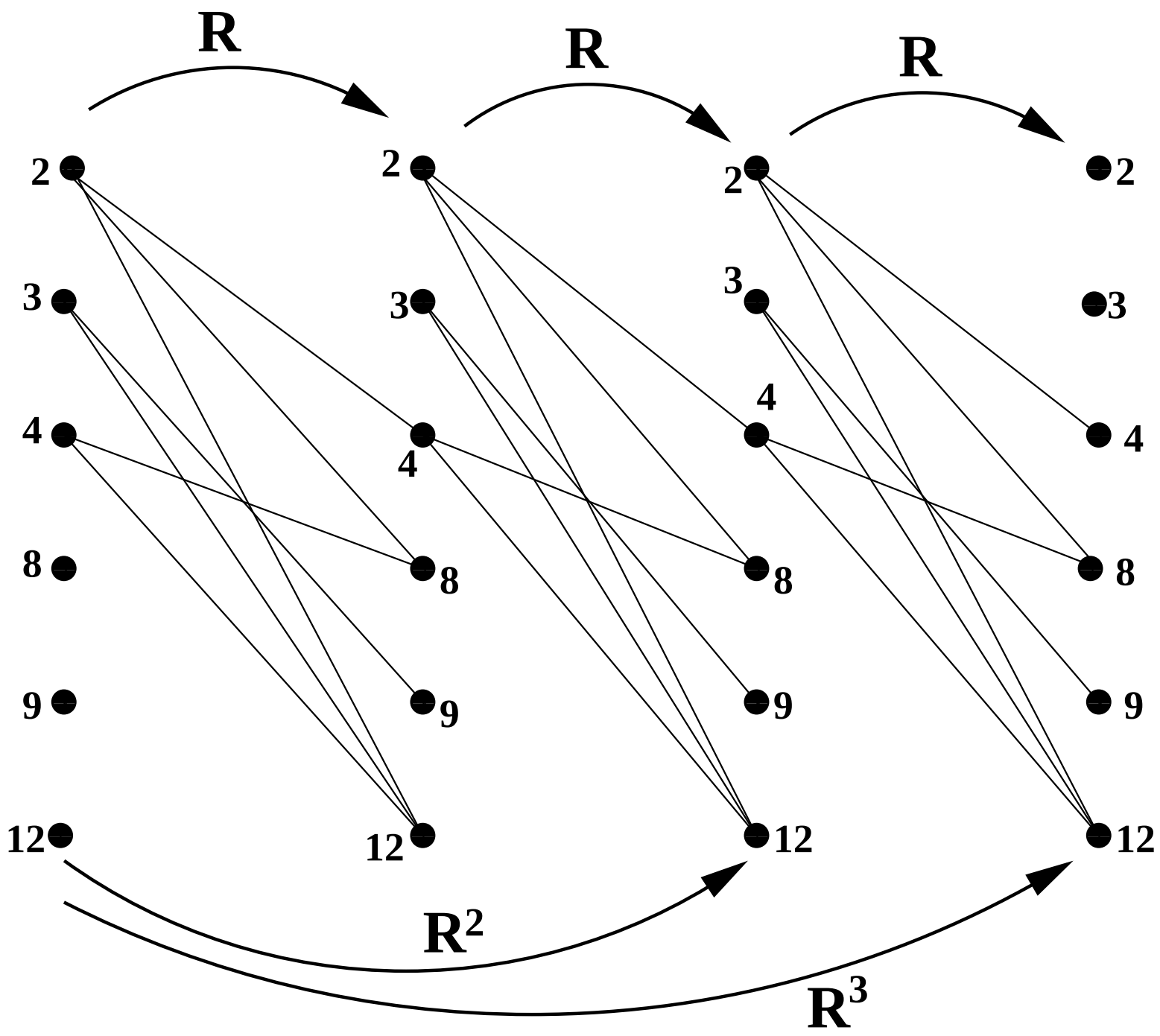
Then

$$R = \{\ (2, 4)\ ,\ (2, 8)\ ,\ (2, 12)\ ,\ (3, 9)\ ,\ (3, 12)\ ,\ (4, 8)\ ,\ (4, 12)\ \}\ ,$$

and

$$R^2 \quad \equiv \quad R \circ R \quad = \quad \{\ (2, 8)\ ,\ (2, 12)\ \}\ ,$$

$$R^3 \quad \equiv \quad R^2 \circ R \quad = \quad R \circ R \circ R \quad = \quad \{\ \}\ .$$


R
R
R
2
3
4
8
9
12
2
3
4
8
9
12
2
3
4
8
9
12
2
3
4
8
9
12
R²
R³

EXAMPLE :

Let R be the relation on the set of all real numbers defined by

$$xRy \quad \text{if and only if} \quad xy = 1$$

Then

$$xR^2z \iff \exists y : xRy \text{ and } yRz$$

$$\iff \exists y : xy = 1 \text{ and } yz = 1$$

$$\iff x = z \text{ and } x \neq 0 \,. \qquad \text{(Why ?)}$$

The last equivalence in detail:

$$\exists y : xy = 1 \text{ and } yz = 1 \quad \text{if and only if} \quad x = z \text{ and } x \neq 0 \ .$$

PROOF : $(\Rightarrow)$ Let x and z be real numbers, and assume that

$$\exists y : xy = 1 \text{ and } yz = 1 \ .$$

Then x and z cannot equal zero.

Thus we can write

$$y = \frac{1}{x} \quad \text{and} \quad y = \frac{1}{z} \ .$$

Hence $1/x = 1/z$, *i.e.*, $x = z$.

Thus $x = z$ and $x \neq 0$.

$$\exists y : xy = 1 \text{ and } yz = 1 \quad \text{if and only if} \quad x = z \text{ and } x \neq 0 \ .$$

(⇐)

Conversely, suppose x and z are real numbers with

$$x = z \quad \text{and} \quad x \neq 0 \ .$$

Let $y = 1/x$.

Then $xy = 1$ and $yz = 1$.

QED !

Similarly

$$\begin{aligned} xR^3z &\iff \exists y \ : \ xR^2y \ \text{ and } \ yRz \\ &\iff \exists y \ : \ x = y \ \text{ and } \ x \neq 0 \ \text{ and } \ yz = 1 \\ &\iff xz = 1 \qquad\qquad\qquad\qquad\qquad\qquad (\text{Why ?}) \end{aligned}$$

Thus

$$\begin{aligned} R^3 &= R \ , \\ R^4 &= R^3 \circ R = R \circ R = R^2 \ , \\ R^5 &= R^4 \circ R = R^2 \circ R = R^3 = R \ , \end{aligned}$$

and so on $\cdots$

Thus we see that

$$R^n = R^2 \qquad \text{if} \quad n \text{ is even} \ ,$$

and

$$R^n = R \qquad \text{if} \quad n \text{ is odd} \ .$$

EXAMPLE :

Let R be the relation on the real numbers defined by

$$xRy \quad \text{if and only if} \quad x^2 + y^2 \leq 1 \ .$$

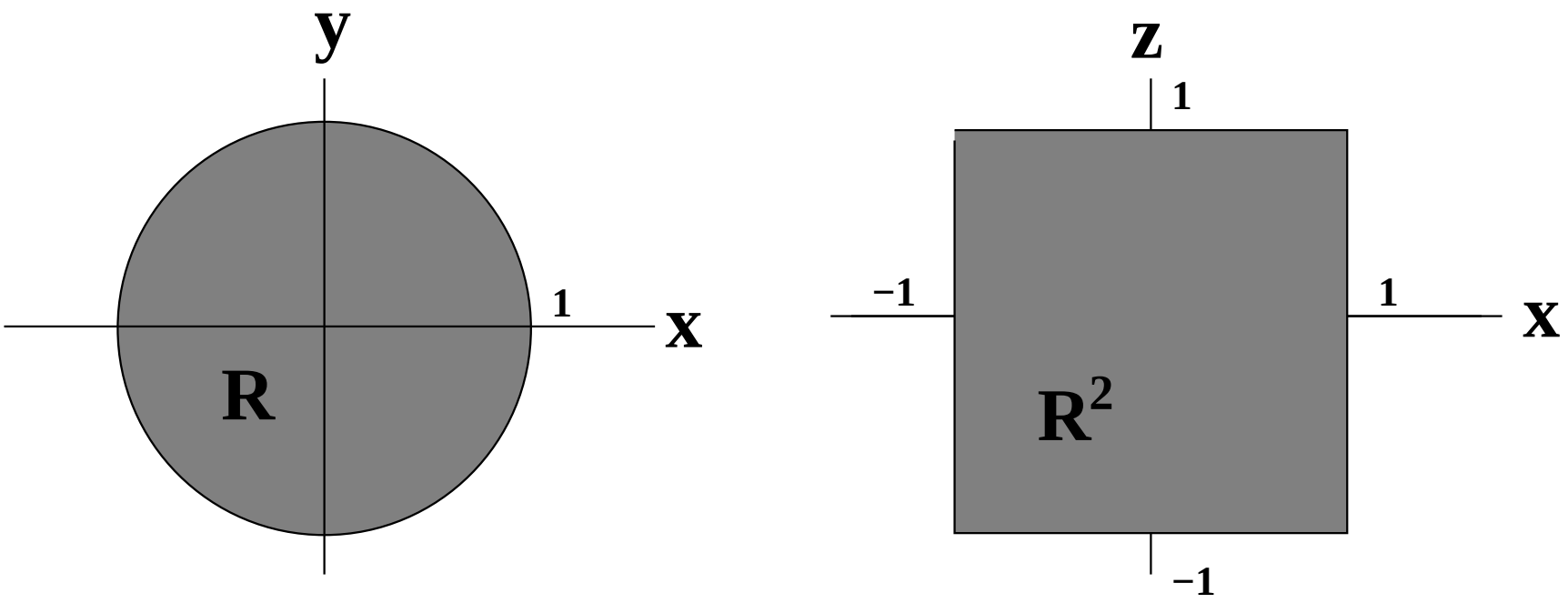
Then

$$xR^2z \iff \exists y \ : \ xRy \ \text{ and } \ yRz$$

$$\iff \exists y \ : \ x^2 + y^2 \leq 1 \ \text{ and } \ y^2 + z^2 \leq 1$$

$$\iff x^2 \leq 1 \ \text{ and } \ z^2 \leq 1 \qquad \text{(Why ?)}$$

$$\iff |\, x \,| \leq 1 \ \text{ and } \ |\, z \,| \leq 1 \ .$$



The relations R and R^2 as subsets of $\mathbb{R}^2$.

Similarly

$$
\begin{aligned}
x R^3 z \quad &\Longleftrightarrow \quad \exists y \ : \ x R^2 y \ \text{ and } \ y R z \\
&\Longleftrightarrow \quad \exists y \ : \ |\, x \,| \ \leq \ 1 \ \text{ and } \ |\, y \,| \ \leq \ 1 \ \text{ and } \ y^2 + z^2 \ \leq \ 1 \\
&\Longleftrightarrow \quad \exists y \ : \ |\, x \,| \ \leq \ 1 \ \text{ and } \ y^2 + z^2 \ \leq \ 1 \qquad \text{(Why ?)} \\
&\Longleftrightarrow \quad |\, x \,| \ \leq \ 1 \ \text{ and } \ |\, z \,| \ \leq \ 1 \qquad \text{(Why ?)}
\end{aligned}
$$

Thus $R^3 = R^2$.

Similarly

$$R^4 \quad = \quad R^3 \circ R \quad = \quad R^2 \circ R \quad = \quad R^3 \quad = \quad R^2 \ ,$$

$$R^5 \quad = \quad R^4 \circ R \quad = \quad R^2 \circ R \quad = \quad R^3 \quad = \quad R^2 \ ,$$

and so on $\cdots$

Thus we see that

$$R^n \ = \ R^2 \qquad \text{for all} \quad n \geq 2 \ .$$

The relation matrix.

A relation between finite sets can be represented by a *relation matrix*.

(Also known as the *transition matrix*).

For a relation R from A to B the relation matrix R has entries

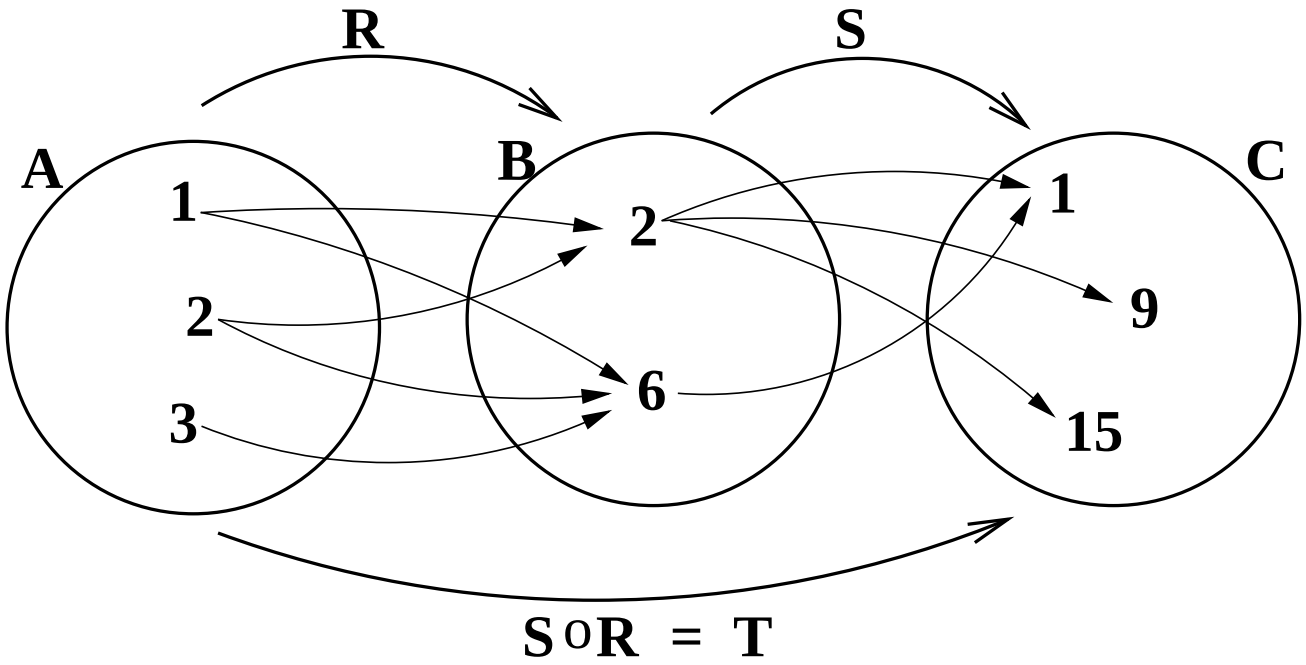
$$R_{ij} = \begin{cases} 0 & \text{if} \quad (a_i, b_j) \notin R \ , \\ \\ 1 & \text{if} \quad (a_i, b_j) \in R \ . \end{cases}$$

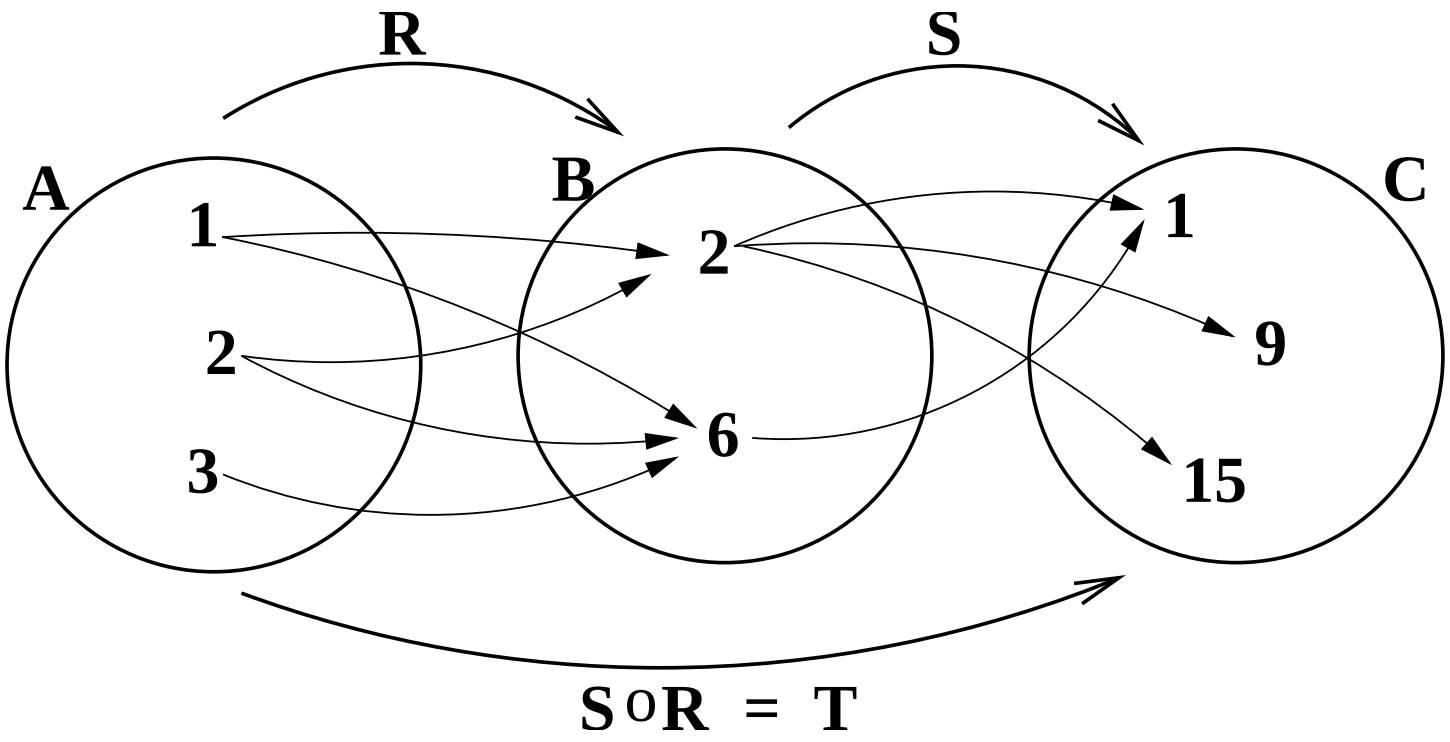
EXAMPLE :

Reconsider the example where

$$A = \{1, 2, 3\}, \quad B = \{2, 6\}, \quad \text{and} \quad C = \{1, 9, 15\} \ ,$$

aRb if and only if $a|b$, and bSc if and only if $b + c$ is prime .



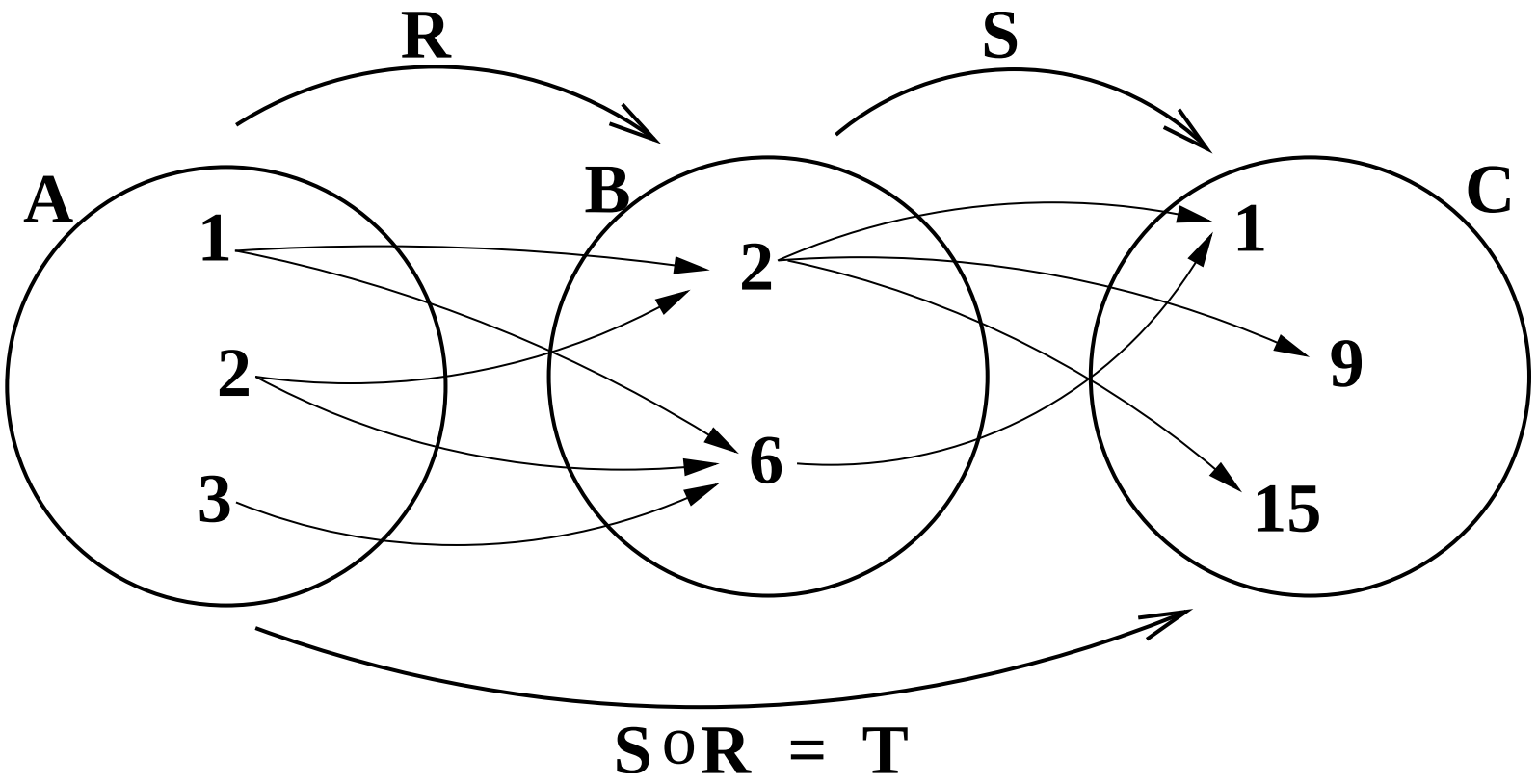


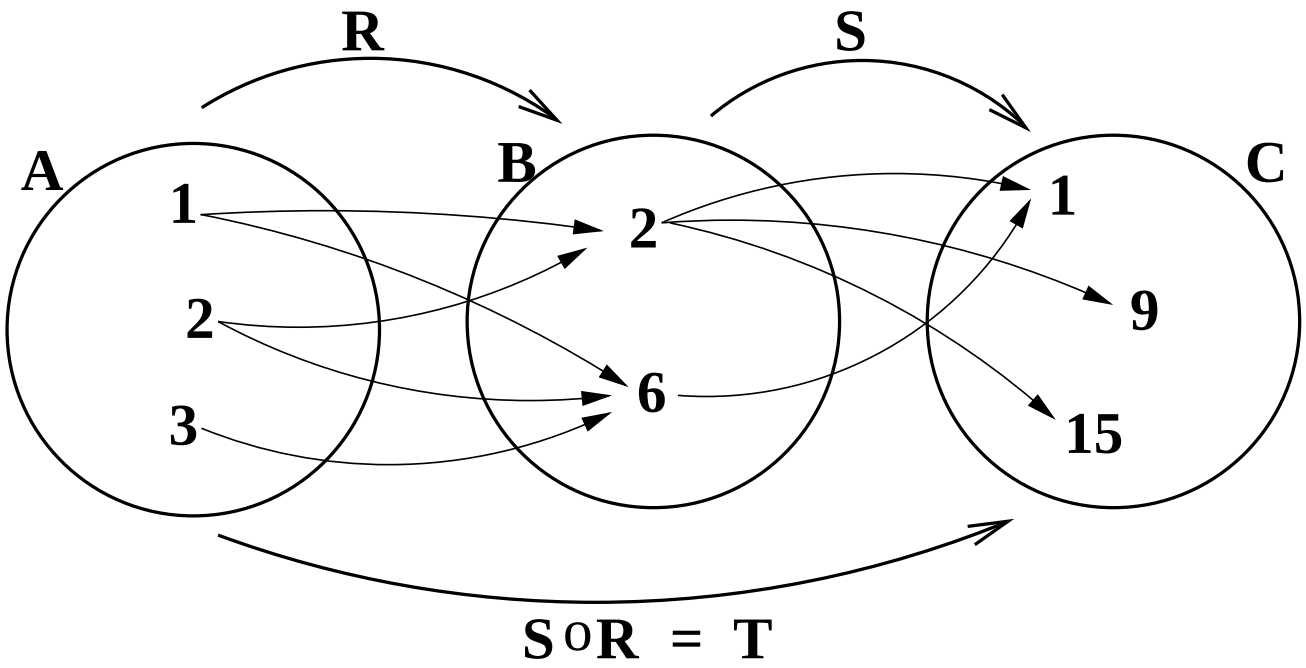
The relation matrices of R and S are

$$R = \begin{array}{c} \\ \mathbf{1} \\ \mathbf{2} \\ \mathbf{3} \end{array} \begin{array}{c} \begin{array}{cc} \mathbf{2} & \mathbf{6} \end{array} \\ \begin{pmatrix} 1 & 1 \\ 1 & 1 \\ 0 & 1 \end{pmatrix} \end{array} \qquad \text{and} \qquad S = \begin{array}{c} \\ \mathbf{2} \\ \mathbf{6} \end{array} \begin{array}{c} \begin{array}{ccc} \mathbf{1} & \mathbf{9} & \mathbf{15} \end{array} \\ \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix} \end{array}.$$

We found that

$$T \;=\; S \circ R \;=\; \{\, (1,1)\,,\; (1,9)\,,\; (1,15)\,,\; (2,1)\,,\; (2,9)\,,\; (2,15)\,,\; (3,1)\,\}\,.$$





The relation matrices of R and S were found to be

$$R = \begin{pmatrix} 1 & 1 \\ 1 & 1 \\ 0 & 1 \end{pmatrix} \quad , \quad S = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix} .$$

The relation matrix of $T = S \circ R$ is

$$T = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix} .$$

PROPOSITION :

Let A, B, and C be finite sets.

Let R be a relation from A to B.

Let S be a relation from B to C.

Let $T = S \circ R$.

Then the relation matrix of T has the same *zero-structure* as the *matrix product* RS.

PROOF :

$$T_{ij} = 1 \iff a_i T c_j$$

$$\iff a_i R b_k \text{ and } b_k S c_j, \text{ for some } b_k \in B$$

$$\iff R_{ik} = 1 \text{ and } S_{kj} = 1 \text{ for some } k$$

$$\iff \sum_{\ell=1}^{n_B} R_{i\ell}\ S_{\ell j} \neq 0$$

$$\iff [RS]_{ij} \neq 0\ . \qquad \textbf{QED !}$$

REMARK :

If we use *Boolean arithmetic*, then $T = RS$.

EXAMPLE :

The matrix product RS in the preceding example is

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 1 \\ 2 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix} .$$

Using Boolean arithmetic the matrix product is

$$T = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix} .$$

The inverse of a relation.

Let R be a relation from A to B.

Then the inverse relation R^{-1} is the relation from B to A defined by

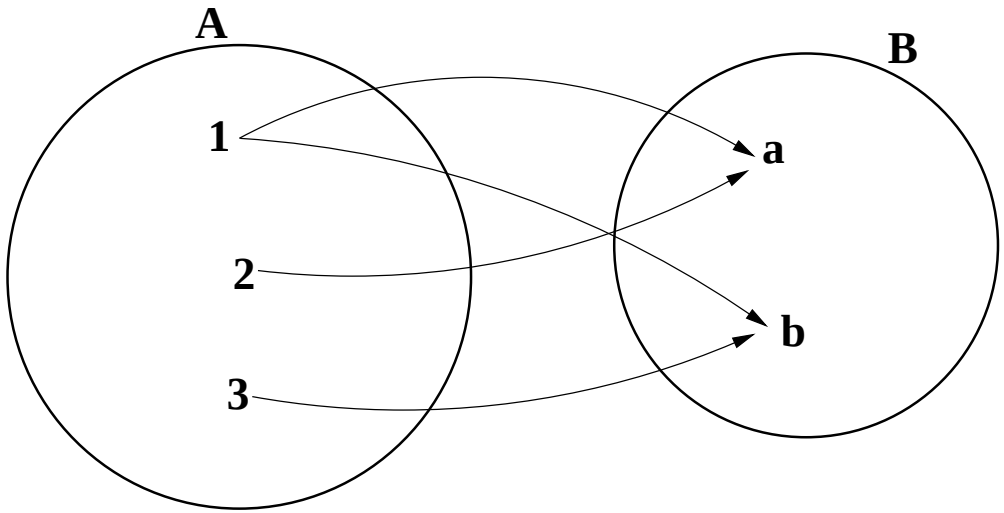
$$b \; R^{-1} \; a \quad \text{if and only if} \quad a \; R \; b \; ,$$

or, in equivalent notation,

$$(b, a) \in R^{-1} \quad \text{if and only if} \quad (a, b) \in R \; .$$

Thus, unlike functions, *relations are always invertible*.

EXAMPLE :



Here

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

and

$$R^{-1} = \{(a, 1), (a, 2), (b, 1), (b, 3)\} \ .$$

The relation matrices are

$$R = \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} , \qquad R^{-1} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \ .$$

Note that

$$R^{-1} \;=\; R^T \quad \text{(transpose)} \; .$$

This holds in general, because if

$$A = \{a_1, a_2, \cdots, a_{n_A}\} \; , \qquad B = \{b_1, b_2, \cdots, b_{n_B}\} \; ,$$

then, by definition of R^{-1} we have for any a_i, b_j that

$$b_j R^{-1} a_i \iff a_i R b_j \; .$$

Hence $[R^{-1}]_{ji} \;=\; R_{ij}$.

EXERCISE : Let R be the relation on the set

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

defined by

$$a_1 R a_2 \quad \text{if and only if} \quad a_1 < a_2 .$$

- Write down R as a subset of $A \times A$.
- Show the relation matrix of R .
- Do the same for R^2 , R^3 , $\cdots$

EXERCISE : Do the same for $a_1 R a_2$ if and only if $a_1 \leq a_2$.

EXERCISE : Do the same for $a_1 R a_2$ if and only if $a_1 + a_2 = 5$.

EXERCISE : Do the same for the set $\mathbb{Z}$ instead of A .

DEFINITION : Let R be a relation on A (*i.e.*, from A to A).

- R is called *reflexive* if

$$\forall a \in A \ : \ (a, a) \in R, \qquad i.e., \ \ \forall a \in A \ : \ aRa \ ,$$

i.e., if the relation matrix R (for finite A) satisfies

$$\forall i \ : \ R_{ii} = 1 \ .$$

EXAMPLES :

The "divides" relation on $\mathbb{Z}^+$ is reflexive.

The "$\leq$" relation on $\mathbb{Z}$ is reflexive.

The "$\subseteq$" relation on a power set 2^A is reflexive.

The "$<$" relation on $\mathbb{Z}$ is *not* reflexive.

- R is *symmetric* if

$$\forall a, b \in A \ : \ aRb \ \rightarrow \ bRa \ ,$$

or, equivalently,

$$aRb \Rightarrow bRa \ ,$$

i.e., if the relation matrix (for finite A) is symmetric :

$$\forall i, j \ : \ R_{ij} = R_{ji} \ .$$

EXAMPLES :

The relation on the real numbers defined by

$$xRy \quad \text{if and only if} \quad x^2 + y^2 \leq 1 \ ,$$

is symmetric.

The "divides" relation on $\mathbb{Z}^+$ is not symmetric.

- R is *antisymmetric* if for all $a, b \in A$ we have

$$aRb \ \wedge \ bRa \ \Rightarrow \ a = b \ ,$$

or equivalently,

$$a \neq b \ \Rightarrow \ \neg(aRb) \ \vee \ \neg(bRa) \ ,$$

i.e., if the relation matrix (for finite A) satisfies

$$\forall i, j \text{ with } i \neq j \ : \ R_{ij} R_{ji} \neq 1 \ .$$

EXAMPLES :

The "$\leq$" relation on $\mathbb{Z}$ is antisymmetric.

The "divides" relation on $\mathbb{Z}^+$ is antisymmetric.

The "$\subseteq$" relation on a power set 2^A is antisymmetric.

- R is *transitive* if

$$aRb \ \wedge \ bRc \Rightarrow aRc \ .$$

We'll show later that R is transitive if and only if

$$\sum_{k=1}^{n} R^k = R$$

in Boolean arithmetic

EXAMPLES :

The "divides" relation on $\mathbb{Z}^+$ is transitive.

The "$\leq$" relation on $\mathbb{Z}$ is transitive.

The "$\subseteq$" relation on a power set 2^S is transitive.

The relation $aRb \iff$ "$a + b$ is prime" on $\mathbb{Z}^+$ is *not* transitive.

EXERCISE : Let A be a set of n elements.

- How many relations are there on A ?

How many relations are there on A that are :

- symmetric ?
- antisymmetric ?
- symmetric and antisymmetric ?
- reflexive ?
- reflexive and symmetric ?
- transitive $^{(*)}$?

$^{(*)}$ **Hint** : Search the web for "*the number of transitive relations*" !

- An *equivalence relation* is a relation that is

  - reflexive

  - symmetric

  - transitive.

EXAMPLE :

The following relation on $\mathbb{Z}$ is an equivalence relation :

$$aRb \quad \text{if and only if} \quad a \bmod m \;=\; b \bmod m \;.$$

(Here $m \geq 2$ is fixed.)

- A *partial order* is a relation that is
  - reflexive
  - antisymmetric
  - transitive.

EXAMPLES :

The "divides" relation on $\mathbb{Z}^+$.

- The "$\leq$" relation on $\mathbb{Z}^+$.

- The "$\subseteq$" relation on the power set 2^S.

- The operator "$<$" on $\mathbb{Z}$ is *not* a partial order:
  (It is antisymmetric (!) and transitive, but not reflexive.)

- A relation R on a set A is called a *total order* if

  - R is a partial order, and

  - $\forall a, b \in A$ we have aRb or bRa .

EXAMPLES :

- The partial order "$\leq$" is also a total order on $\mathbb{Z}^+$.

- The partial order $m|n$ on $\mathbb{Z}^+$ is not a total order. (For example $5 \not| 7$ and $7 \not| 5$.)

- The partial order "$\subseteq$" on 2^S is not a total order.

Equivalence classes.

Let A be a set and let R be an equivalence relation on A .

Let $a_1 \in A$.

Define

$$[a_1] \quad = \quad \{a \in A \ : \ aRa_1\} \ ,$$

that is

$$[a_1] \quad = \quad \text{all elements of } A \text{ that "}\textit{are equivalent}\text{" to } a_1 \ .$$

Then $[a_1]$ is called the *equivalence class* generated by a_1 .

EXAMPLE :

Let R be the relation "congruence modulo 3" on $\mathbb{Z}^+$, *i.e.*,

$$aRb \qquad \text{if and only if} \qquad a \bmod 3 \;=\; b \bmod 3 \;.$$

For example

$$1R1 \;\;,\;\; 1R4 \;\;,\;\; 1R7 \;\;,\;\; 1R10 \;\;,\;\; \cdots \;\;,$$

$$2R2 \;\;,\;\; 2R5 \;\;,\;\; 2R8 \;\;,\;\; 2R11 \;\;,\;\; \cdots \;\;,$$

$$3R3 \;\;,\;\; 3R6 \;\;,\;\; 3R9 \;\;,\;\; 3R12 \;\;,\;\; \cdots \;\;.$$

Thus

$$[1] \;=\; \{\, 1\,,\; 4\,,\; 7\,,\; 10\,,\; 13\,, \cdots \,\}\,,$$

$$[2] \;=\; \{\, 2\,,\; 5\,,\; 8\,,\; 11\,,\; 14\,, \cdots \,\}\,,$$

$$[3] \;=\; \{\, 3\,,\; 6\,,\; 9\,,\; 12\,,\; 15\,, \cdots \,\}\,.$$

We see that

$$\mathbb{Z}^+ \;=\; [1] \,\cup\, [2] \,\cup\, [3]\,.$$

- The relation R has *partitioned* $\mathbb{Z}^+$ into the subsets $[1]$, $[2]$, $[3]$.
- Any member of a subset can represent the subset, *e.g.*,

$$[11] \;=\; [2]\,.$$

EXAMPLE :

Consider $\mathbb{Z} \times \mathbb{Z}$, the set of all ordered pairs of integers.

Define a relation R on $\mathbb{Z} \times \mathbb{Z}$ by

$$(a_1, b_1) R (a_2, b_2) \quad \text{if and only if} \quad a_1 - b_1 = a_2 - b_2 \ .$$

Note that R can be viewed as subset of

$$(\mathbb{Z} \times \mathbb{Z}) \times (\mathbb{Z} \times \mathbb{Z}) \ .$$

$$(a_1, b_1)R(a_2, b_2) \quad \text{if and only if} \quad a_1 - b_1 \;=\; a_2 - b_2$$

R is an equivalence relation :

- R is reflexive : $(a, b)R(a, b)$,
- R is symmetric : $(a_1, b_1)R(a_2, b_2) \;\Rightarrow\; (a_2, b_2)R(a_1, b_1)$,
- R is transitive:

$$(a_1, b_1)R(a_2, b_2) \;\wedge\; (a_2, b_2)R(a_3, b_3) \;\Rightarrow\; (a_1, b_1)R(a_3, b_3) \; .$$

.

$$(a_1, b_1) R (a_2, b_2) \quad \text{if and only if} \quad a_1 - b_1 \;=\; a_2 - b_2$$

The equivalence classes are

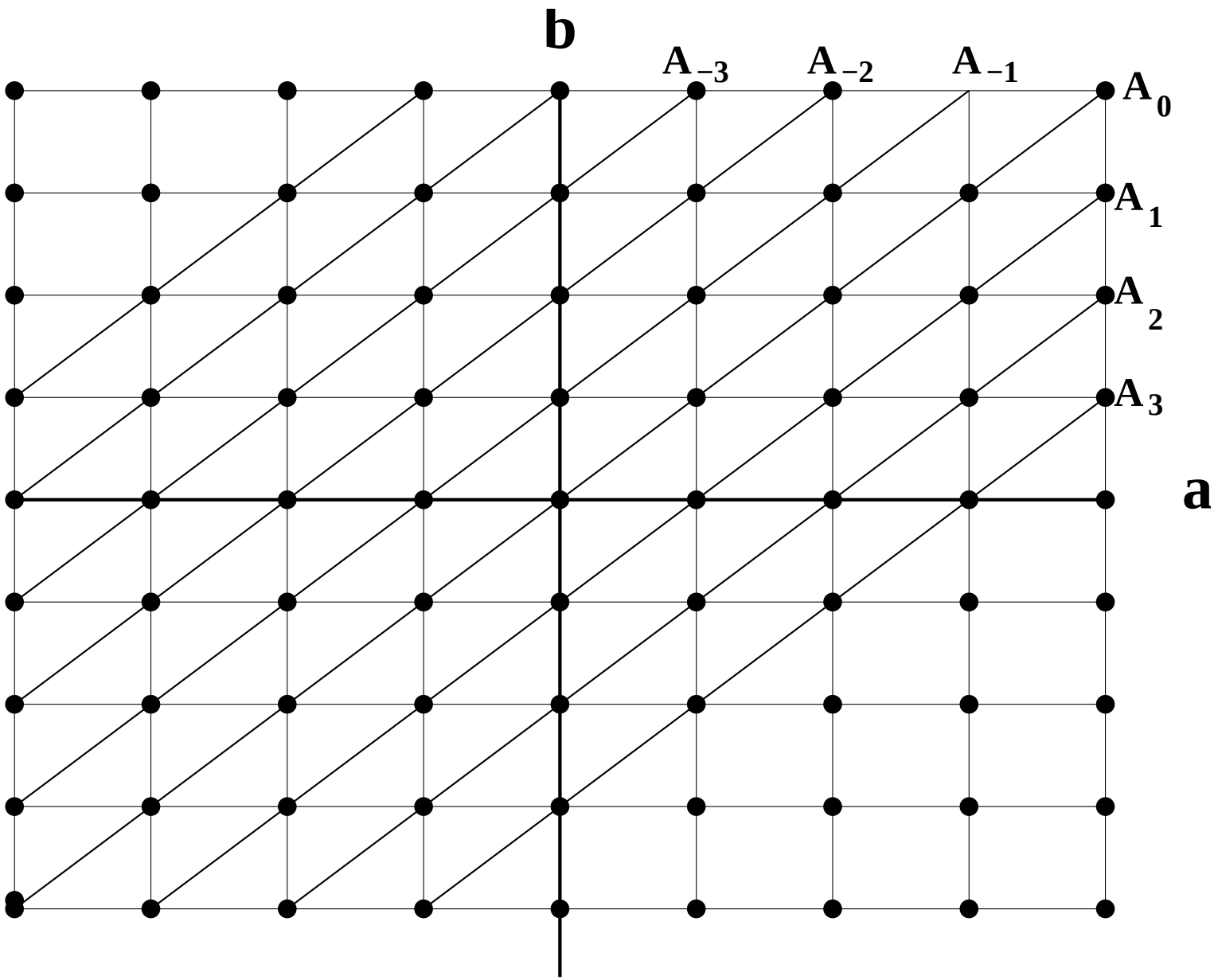
$$A_k \;=\; \{\; (a, b) \;:\; a - b = k \;\} \; .$$

For example,

$$A_1 \;=\; [(2, 1)] \;=\; \{ \cdots \;,\; (-1, -2) \;,\; (0, -1) \;,\; (1, 0) \;,\; (2, 1) \;, \cdots \} \; .$$

The sets A_k partition the set $\mathbb{Z} \times \mathbb{Z}$, namely,

$$\mathbb{Z} \times \mathbb{Z} \;\;=\;\; \cup_{k=-\infty}^{\infty} \; A_k \; .$$


b
A –3
A –2
A –1
A 0
A 1
A 2
A 3
a

DEFINITION :

- The *reflexive closure* of R is the smallest relation containing R that is reflexive.

- The *symmetric closure* of R is the smallest relation containing R that is symmetric.

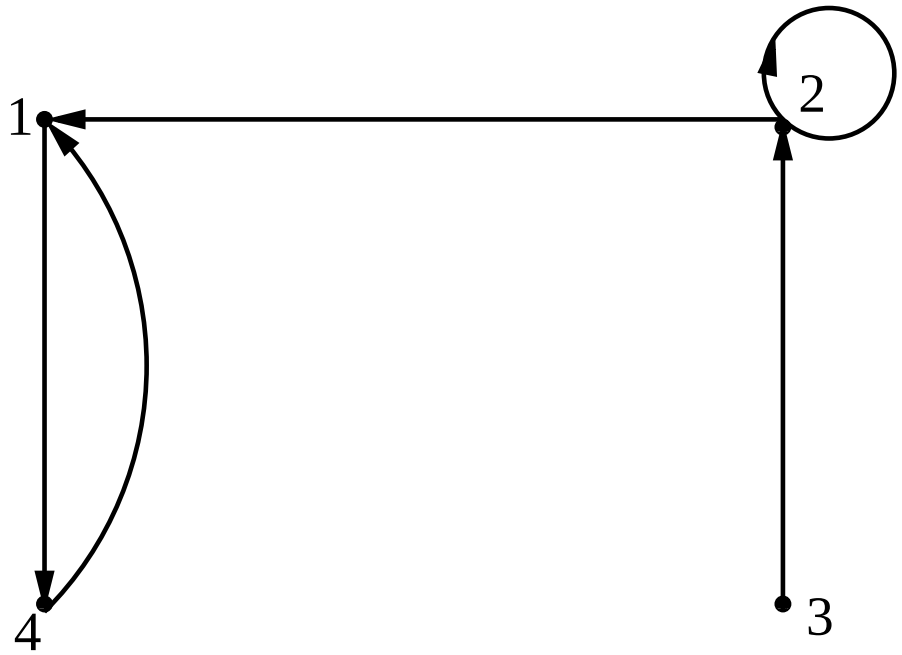
- The *transitive* closure of R is the smallest relation containing R that is transitive.

EXAMPLE :

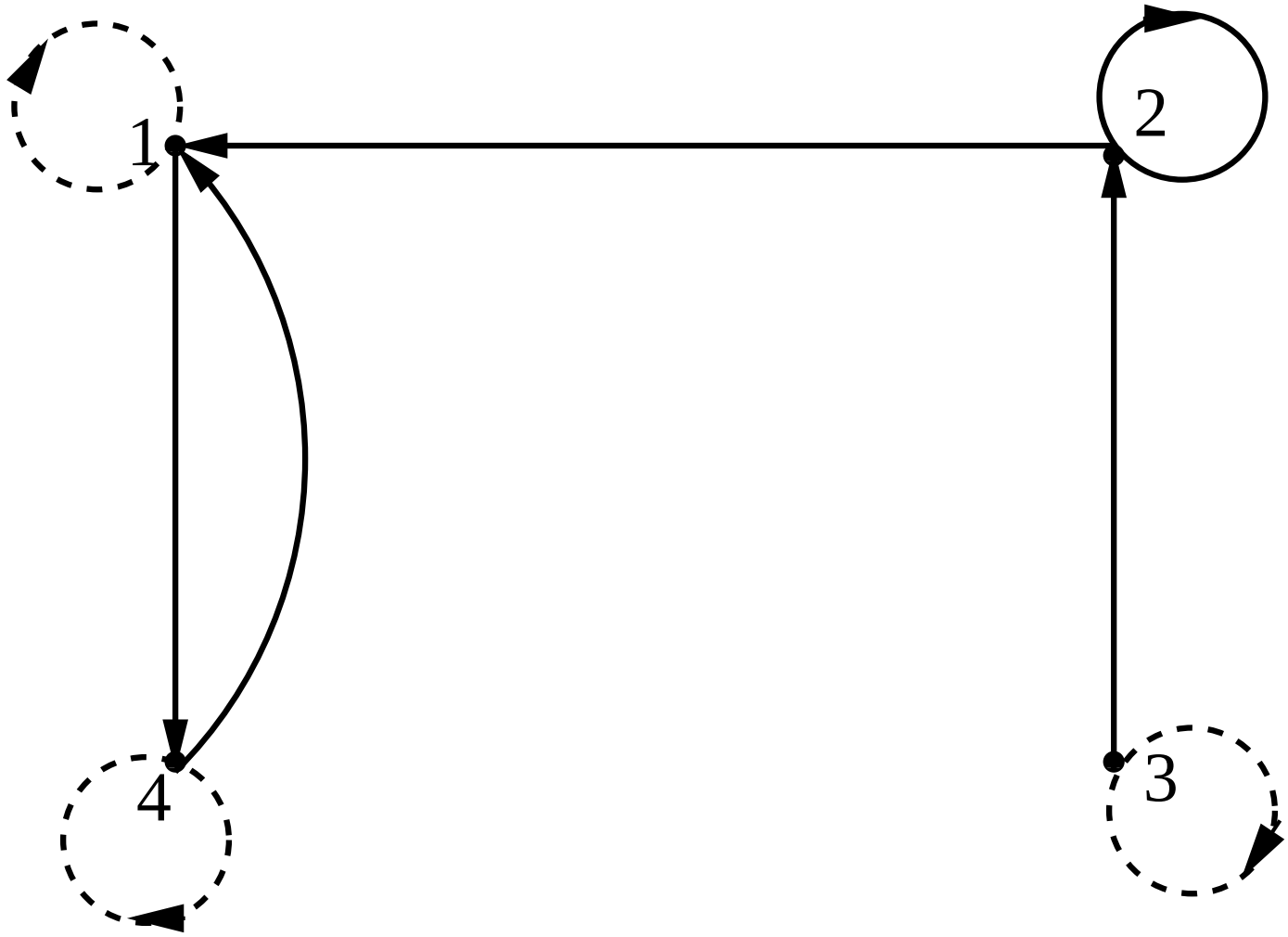
Let $A = \{1, 2, 3, 4\}$, and let R be the relation on A defined by

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

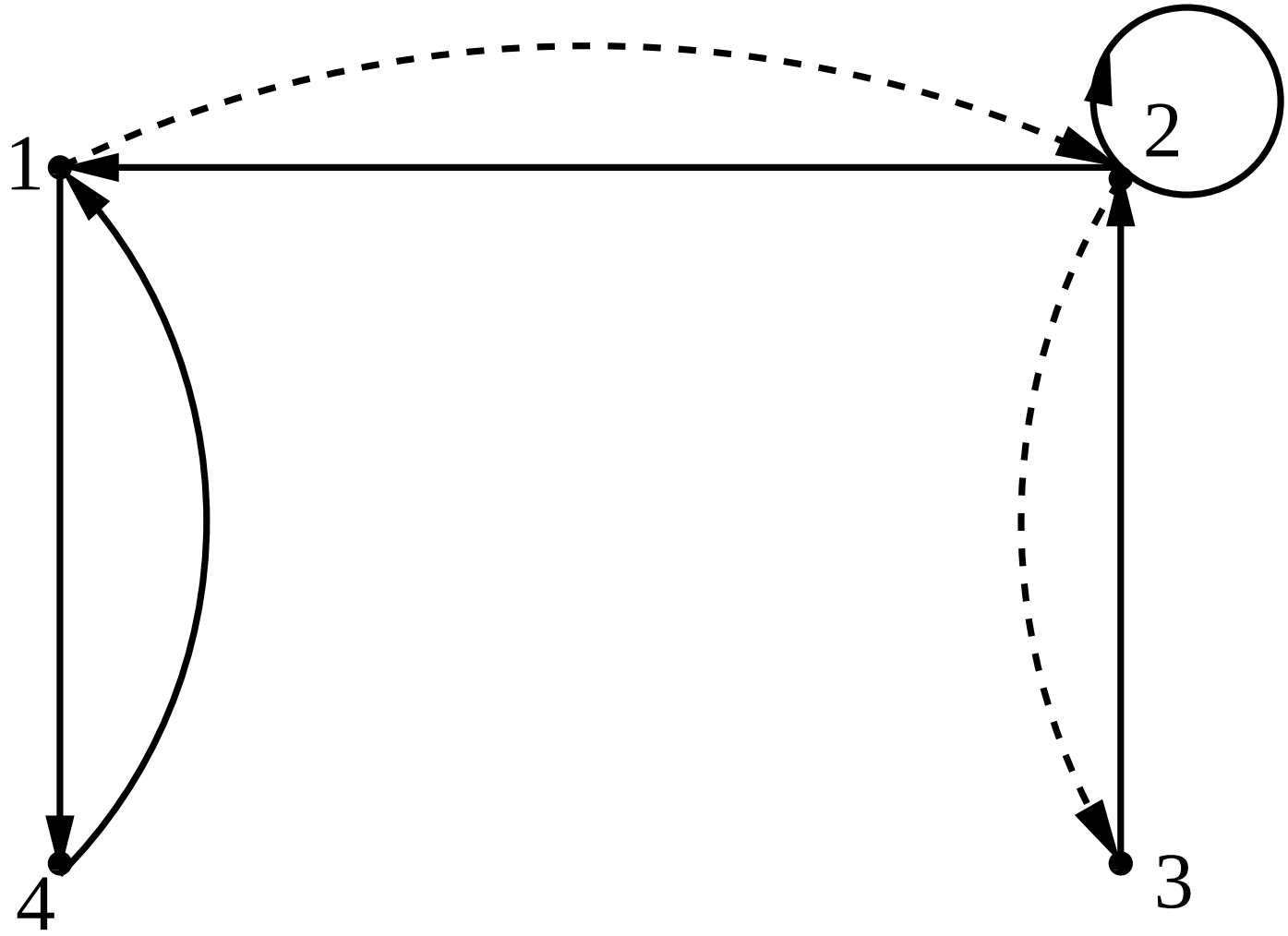
Then R is not reflexive, not symmetric, and not transitive :



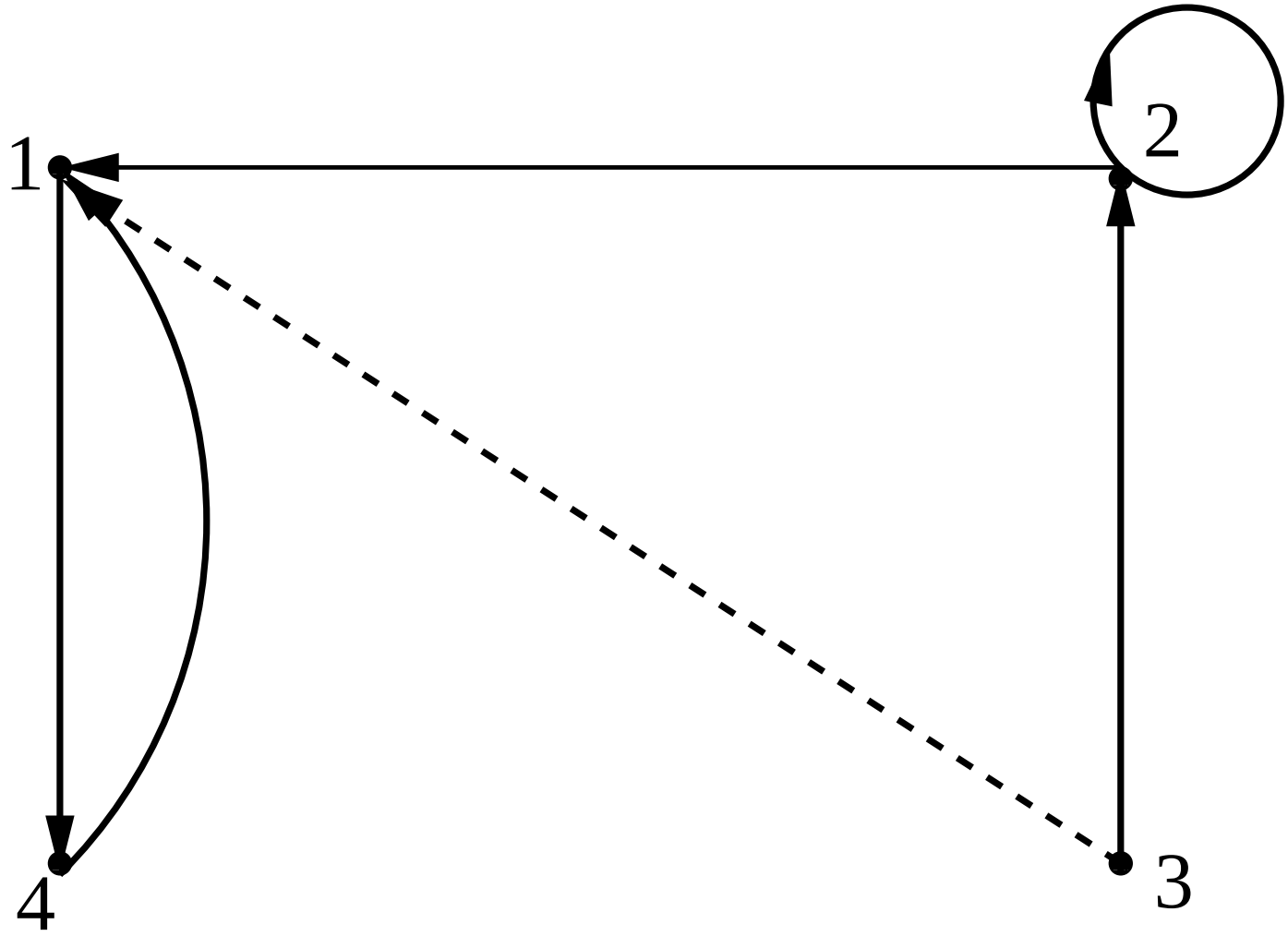
The *reflexive closure* of R is :



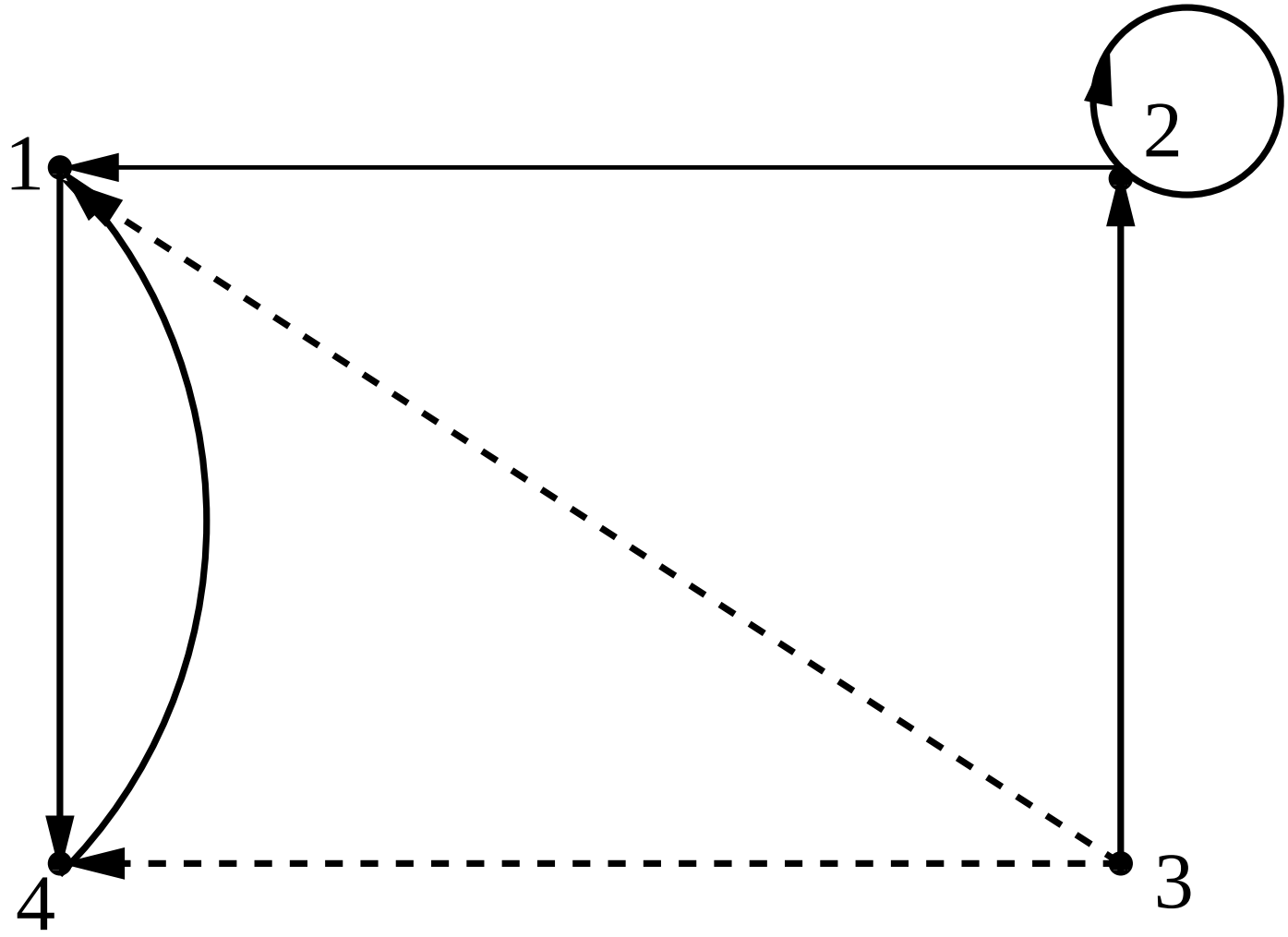
The *symmetric closure* of R is :



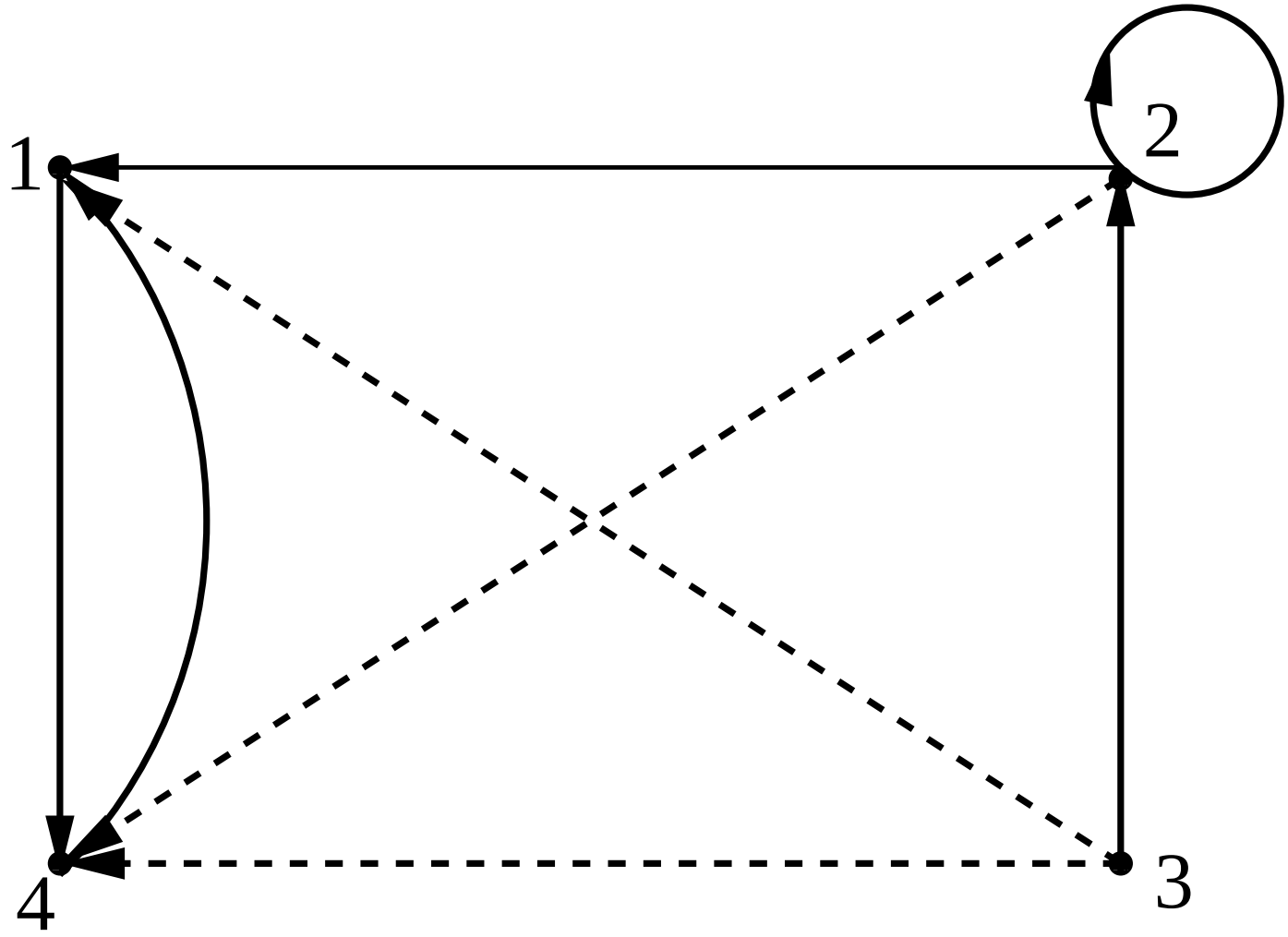
To get the *transitive closure* of R :



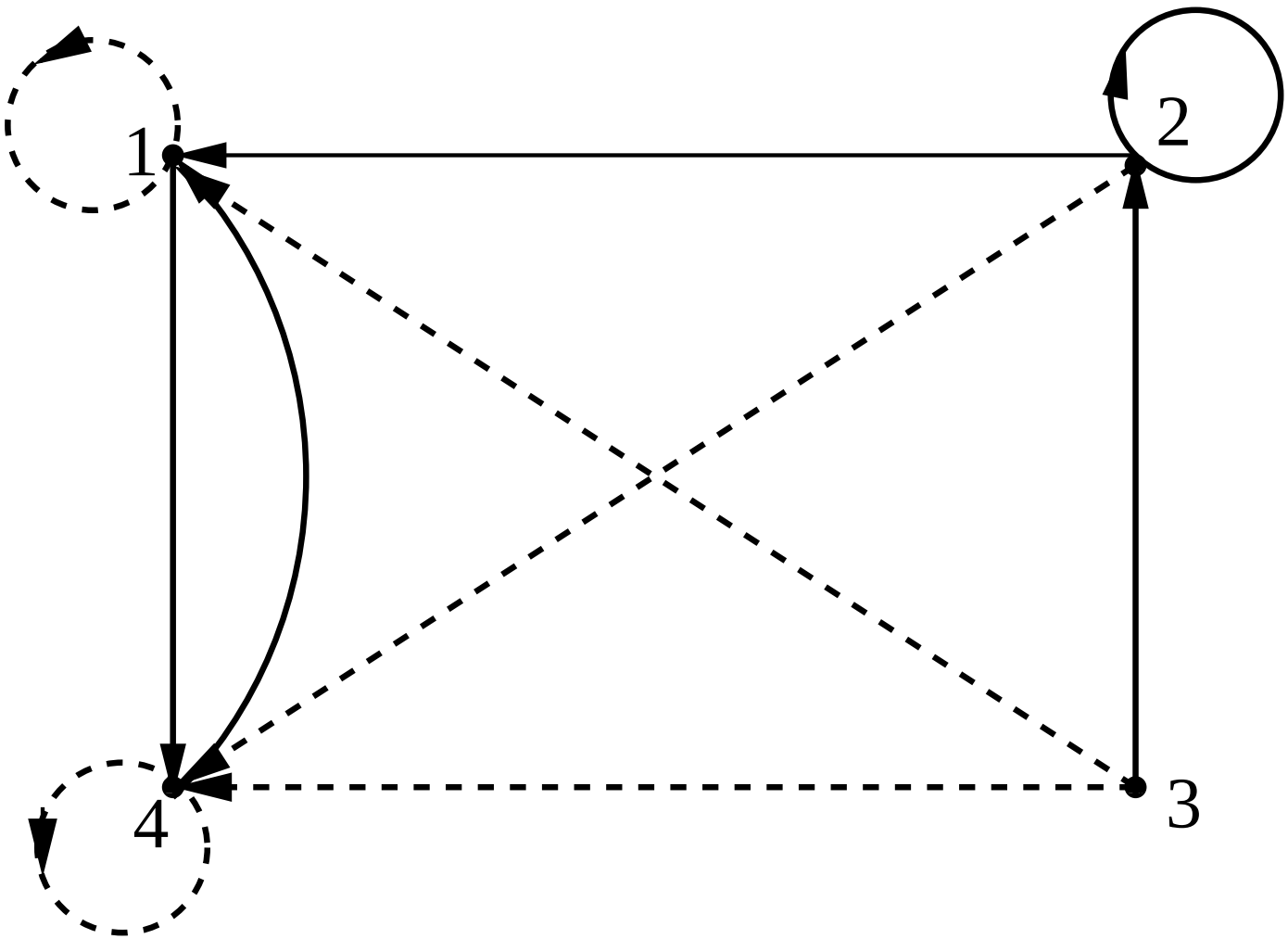
To get the *transitive closure* of R :



To get the *transitive closure* of R :



The *transitive closure* of R is :



PROPERTY : The transitive closure R^* of a relation R is given by

$$R^* \;=\; \cup_{k=1}^{\infty} R^k \;.$$

PROOF : Later $\cdots$

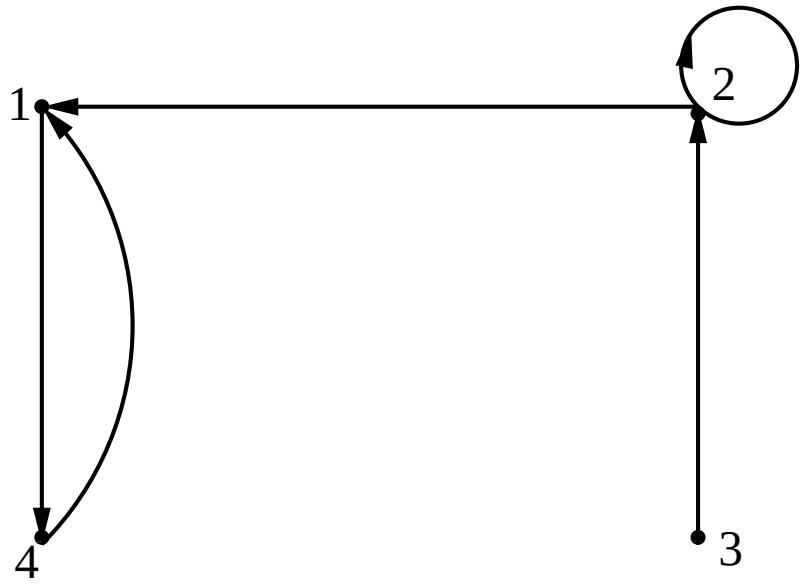
PROPERTY : For a *finite set* of n elements, the relation matrix of the transitive closure is

$$R^* \;=\; \sum_{k=1}^{n} R^k \qquad \text{(using Boolean arithmetic)} \;.$$

NOTE : It suffices to sum only the first n powers of the matrix R !

EXAMPLE : In the preceding example,

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



we have the relation matrix :

$$R \ = \ \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \ .$$

Thus, using Boolean arithmetic,

$$R^2 = R \cdot R = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$$R^3 = R \cdot R^2 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix},$$

$$R^4 = R \cdot R^3 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

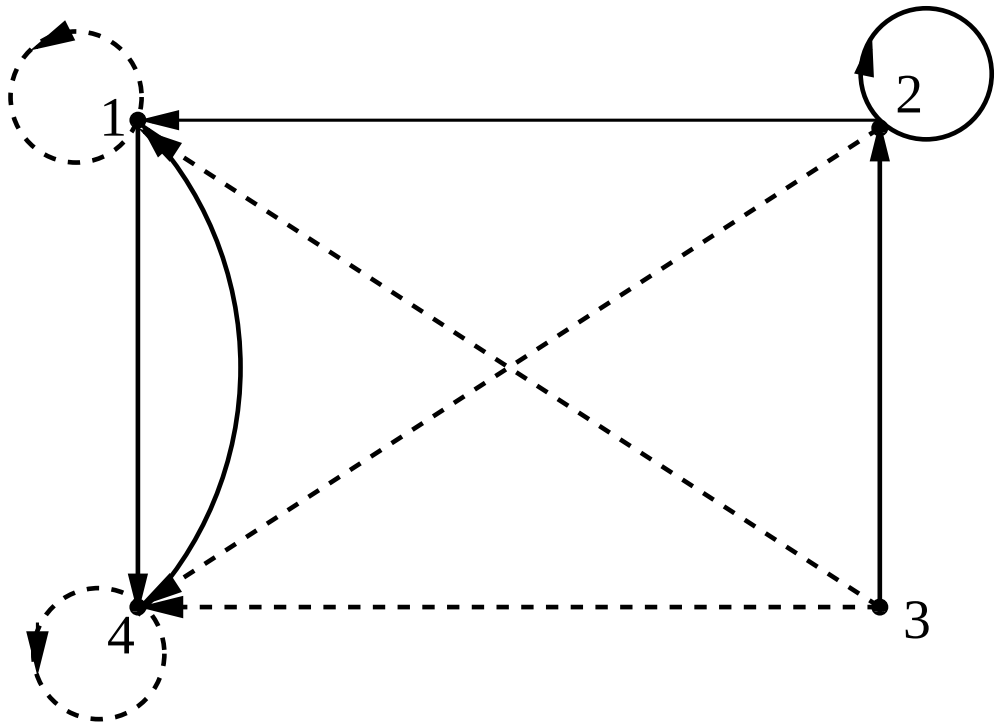
Therefore

$$R^* \quad = \quad \sum_{k=1}^{4} R^k \quad = \quad R \; + \; R^2 \; + \; R^3 \; + \; R^4 \quad =$$

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$= \quad \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix} .$$

The graph of R^* (shown before) is :



which indeed has the relation matrix

$$R^* = \sum_{k=1}^{4} R^k = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix} .$$

RECALL : The transitive closure R^* of a relation R is given by

$$\boxed{R^* \;=\; \cup_{k=1}^{\infty} R^k} \qquad \text{(to be proved later } \cdots \text{)}$$

EXAMPLE : Consider the relation R on the real numbers

$$xRy \quad \text{if and only if} \quad xy = 1 \; .$$

Earlier we found that

$$xR^2y \quad \text{if and only if} \quad x = y \;\; \wedge \;\; x \neq 0 \; ,$$

and

$$R \;=\; R^3 \;=\; R^5 \;=\; \cdots \;\; ,$$

$$R^2 \;=\; R^4 \;=\; R^6 \;=\; \cdots \;\; .$$

Thus the transitive closure is

$$xR^*y \quad \text{if and only if} \quad xy = 1 \;\vee\; (x = y \;\wedge\; x \neq 0) \; .$$

EXAMPLE : Again consider the relation R on the real numbers

$$xRy \quad \text{if and only if} \quad x^2 + y^2 \;\leq\; 1 \;.$$

Earlier we found that

$$xR^2y \quad \text{if and only if} \quad |\,x\,| \;\leq\; 1 \;\wedge\; |\,y\,| \;\leq\; 1 \;,$$

and

$$R^n \;=\; R^2 \;, \qquad \text{for } n \geq 2 \;.$$

Thus the transitive closure is

$$xR^*y \quad \text{if and only if} \quad x^2 + y^2 \;\leq\; 1 \;\vee\; (\;|\,x\,| \leq 1 \;\wedge\; |\,y\,| \leq 1\;) \;,$$

that is,

$$xR^*y \quad \text{if and only if} \quad |\,x\,| \;\leq\; 1 \;\wedge\; |\,y\,| \;\leq\; 1 \;. \qquad \text{(Why ?)}$$

EXERCISE : Let R be the relation on the real numbers given by

$$xRy \quad \text{if and only if} \quad x^2 + y^2 = 1 \ .$$

- Draw R as a subset of the real plane.
- Is R reflexive?
- Is R symmetric?
- Is R antisymmetric?
- Is R transitive?
- What is R^2 ? (Be careful!)
- What is R^3 ?
- What is the transitive closure of R ?

EXERCISE : Let R be the relation on the real numbers given by

$$xRy \quad \text{if and only if} \quad xy \leq 1 \ .$$

- Draw R as a subset of the real plane.
- Is R reflexive?
- Is R symmetric?
- Is R antisymmetric?
- Is R transitive?
- What is R^2 ?
- What is R^3 ?
- What is the transitive closure of R ?

EXERCISE : Let R be the relation on the real numbers given by

$$xRy \quad \text{if and only if} \quad x^2 \leq y \ .$$

- Draw R as a subset of the real plane.
- Is R reflexive?
- Is R symmetric?
- Is R antisymmetric?
- Is R transitive?
- What is R^2 ?
- What is R^3 ?
- What is R^n ? (Prove your formula for R^n by induction.)
- What is the transitive closure of R ?

$$\boxed{xRy \quad \text{if and only if} \quad x^2 \leq y}$$

Then

$$\begin{aligned} xR^2z &\iff \exists y \,:\, xRy \text{ and } yRz \\ &\iff \exists y \,:\, x^2 \leq y \text{ and } y^2 \leq z \\ &\iff x^4 \leq z\,. \end{aligned}$$

Similarly

$$\begin{aligned} xR^3z &\iff \exists y \,:\, xR^2y \text{ and } yRz \\ &\iff \exists y \,:\, x^4 \leq y \text{ and } y^2 \leq z \\ &\iff x^8 \leq z\,. \end{aligned}$$

By induction one can prove that

$$xR^nz \iff x^{2^n} \leq z\,.$$

We see that

- The relation R corresponds to the area of the x, y-plane that lies on or above the curve $y = x^2$.

- The relation R^2 corresponds to the area of the x, y-plane that lies on or above the curve $y = x^4$.

- The relation R^n corresponds to the area of the x, y-plane that lies on or above the curve $y = x^{2^n}$.

The transitive closure is

$$R^* \quad = \quad \cup_{k=1}^{\infty} R^k \ .$$

(to be proved later $\cdots$)

We find that R^* is the union of the following two regions:

- The area of the x, y-plane that lies on or above the curve $y = x^2$ (*i.e.*, the area that corresponds to the relation R).

- The area inside the rectangle whose corners are located at

$$(x, y) \ = \ (-1, 0) \ , \ (1, 0) \ , \ (1, 1) \ , \ (-1, 1) \ ,$$

(excluding the border of this rectangle).

(**Check**!)

Let R be a relation on a set A .

Recursively define

$$R^1 = R\ , \qquad R^{n+1} = R^n \circ R\ , \qquad n = 1, 2, 3, \ \cdots\ .$$

Then for all $n \in \mathbb{Z}^+$ we have:

PROPERTY 1 : $R^n \circ R \ = \ R \circ R^n$

PROPERTY 2 : R symmetric $\Rightarrow$ R^n is symmetric

EXERCISE : Use induction to prove these properties.

PROPERTY 1 : $R^n \circ R = R \circ R^n$, for all $n \in \mathbb{Z}^+$

PROOF : Clearly, the equality holds if $n = 1$.

Inductive assumption :

$$R^n \circ R = R \circ R^n \ , \quad \text{for some arbitrary } n \in \mathbb{Z}^+ \ .$$

We must show that

$$R^{n+1} \circ R = R \circ R^{n+1} \ .$$

To do this :

$$\begin{aligned}
R^{n+1} \circ R &= (R^n \circ R) \circ R && \text{(by definition)} \\
&= (R \circ R^n) \circ R && \text{(by inductive assumption)} \\
&= R \circ (R^n \circ R) && \text{(by associativity)} \\
&= R \circ R^{n+1} && \text{(by definition).}
\end{aligned}$$

QED !

PROPERTY 2 : R symmetric $\Rightarrow$ R^n is symmetric

PROOF : Clearly *True* if $n = 1$.

Inductively assume that R^n is symmetric.

We must show that R^{n+1} is symmetric:

$$aR^{n+1}b \iff aR^n \circ Rb \qquad \text{(by definition of power)}$$

$$\iff \exists p(aRp \ \wedge \ pR^n b) \qquad \text{(by definition of composition)}$$

$$\iff \exists p(pRa \ \wedge \ bR^n p) \qquad \text{(since } R \text{ and } R^n \text{ are symmetric)}$$

$$\iff \exists p(bR^n p \ \wedge \ pRa) \qquad \text{(commutative law of logic)}$$

$$\iff bR \circ R^n a \qquad \text{(by definition of composition)}$$

$$\iff bR^n \circ Ra \qquad \text{(by Property 1)}$$

$$\iff bR^{n+1}a \qquad \text{(by definition of power) .} \quad \textbf{QED !}$$

Let R be a relation on a set A and let $n \in \mathbb{Z}^+$.

PROPERTY 3 : R transitive $\Rightarrow$ R^n is transitive

PROOF :

Let R be transitive.

Obviously R^1 is transitive.

By induction assume that R^n is transitive for some $n \in \mathbb{Z}^+$.

We must show that R^{n+1} is transitive, *i.e.*, we must show that

$$aR^{n+1}b \ \wedge \ bR^{n+1}c \ \Rightarrow \ aR^{n+1}c \ .$$

Given R and R^n are transitive. Show R^{n+1} is transitive

$\cdots$ continuation of proof $\cdots$

$$aR^{n+1}b \ \wedge \ bR^{n+1}c$$

$$\Rightarrow \quad aR^n \circ Rb \ \wedge \ bR^n \circ Rc \qquad \text{(power)}$$

$$\Rightarrow \quad aR^n \circ Rb \ \wedge \ bR \circ R^n c \qquad \text{(by Property 1)}$$

$$\Rightarrow \quad aRp \wedge pR^n b \wedge bR^n q \wedge qRc \qquad (\exists p, q\text{: composition})$$

$$\Rightarrow \quad aRp \ \wedge \ pR^n q \ \wedge \ qRc \qquad \text{(inductive assumption)}$$

$$\Rightarrow \quad aR^n \circ Rq \ \wedge \ qRc \qquad \text{(composition)}$$

$$\Rightarrow \quad aR \circ R^n q \ \wedge \ qRc \qquad \text{(by Property 1)}$$

Given R and R^n are transitive. Show R^{n+1} is transitive.

$\cdots$ continuation of proof $\cdots$

$$aR \circ R^n q \ \wedge \ qRc$$

$$\Rightarrow \quad aR^n s \ \wedge \ sRq \ \wedge \ qRc \qquad (\exists s\text{: composition})$$

$$\Rightarrow \quad aR^n s \ \wedge \ sRc \qquad (\text{since } R \text{ is transitive})$$

$$\Rightarrow \quad aR \circ R^n c \qquad (\text{composition})$$

$$\Rightarrow \quad aR^n \circ Rc \qquad (\text{by Property 1})$$

$$\Rightarrow \quad aR^{n+1} c \qquad (\text{power}) \qquad \textbf{QED !}$$

Let R and S be relations on a set A .

Recall that we can also think of R as *a subset* of $A \times A$.

We have:

PROPERTY 4 : $\quad R \subseteq S \Rightarrow R^n \subseteq S^n$

PROOF : The statement clearly holds when $n = 1$.

Inductive step:

Given $R \subseteq S$ and $R^n \subseteq S^n$. Show $R^{n+1} \subseteq S^{n+1}$

To do this :

Suppose that $(x, z) \in R^{n+1}$.

Then $\exists y : (x, y) \in R$ and $(y, z) \in R^n$.

By the assumptions $(x, y) \in S$ and $(y, z) \in S^n$.

Hence $(x, z) \in S^{n+1}$. **QED !**

Let S be a relation on a set A .

PROPERTY 5 : S is transitive if and only if $\forall n \in \mathbb{Z}^+ \ : \ S^n \subseteq S$

PROOF :

$(\Leftarrow)$ $(\forall n \in \mathbb{Z}^+ \ : \ S^n \subseteq S) \quad \Rightarrow \quad S$ is transitive

Let $(x, y) \in S$ and $(y, z) \in S$.

Then, by definition of composition, $(x, z) \in S^2$.

Since, in particular, $S^2 \subseteq S$ it follows that $(x, z) \in S$.

Hence S is transitive.

$(\Rightarrow)$ $\boxed{S \text{ is transitive} \quad \Rightarrow \quad \forall n \in \mathbb{Z}^+ \ : \ S^n \subseteq S}$

By induction :

Clearly $S^n \subseteq S$ if $n = 1$.

Suppose that for some n we have $S^n \subseteq S$.

We must show that $S^{n+1} \subseteq S$.

Given (1): S is transitive, and (2): $S^n \subseteq S$. Show $S^{n+1} \subseteq S$

To do this, suppose that $(x, z) \in S^{n+1}$.

We must show that $(x, z) \in S$.

By definition of composition, $(x, z) \in S^n \circ S$, and hence

$$\exists y \ : \ (x, y) \in S \qquad \text{and} \qquad (y, z) \in S^n \ .$$

By inductive hypothesis (2) $(y, z) \in S$.

Thus $(x, y) \in S$ and $(y, z) \in S$.

By assumption (1) S is transitive, so that $(x, z) \in S$. **QED !**

THEOREM :

The transitive closure R^* of a relation R is given by

$$R^* \;=\; \cup_{k=1}^{\infty} R^k \;.$$

PROOF : Let $U \;=\; \cup_{k=1}^{\infty} R^k$.

We must show that

(1) U is transitive.

(2) U is the *smallest* transitive relation containing R .

If so, then $R^* \;=\; U$.

$$\boxed{U \quad = \quad \cup_{k=1}^{\infty} R^k} \qquad \star$$

(1) We first show that U is transitive :

Suppose $(x, y) \in U$ and $(y, z) \in U$.

We must show that $(x, z) \in U$.

From $\star$ it follows that

$$(x, y) \in R^m \quad \text{and} \quad (y, z) \in R^n \ , \quad \text{for some } m, n \in \mathbb{Z}^+ \ .$$

By definition of composition

$$(x, z) \in R^{n+m} \ .$$

Thus, using $\star$ again, it follows that

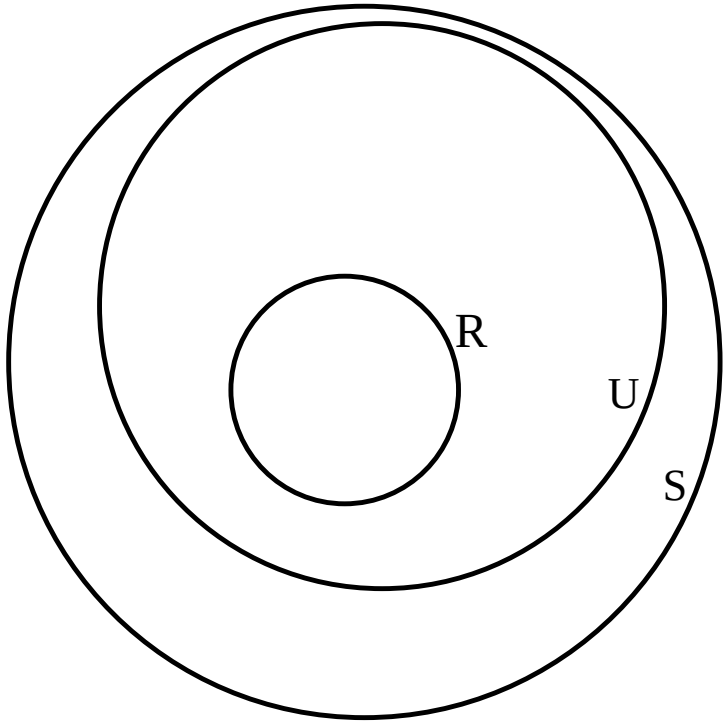
$$(x, z) \in U \ .$$

$$\boxed{U \quad = \quad \cup_{k=1}^{\infty} R^k} \quad \star$$

(2) Show U is the *smallest* transitive relation containing R :

To do this it suffices to show that :

$$(\ S \text{ transitive} \quad \text{and} \quad R \subseteq S\ ) \quad \Rightarrow \ U \subseteq S\ .$$



$U \quad = \quad \cup_{k=1}^{\infty} R^k$	$\star$
$R \subseteq S \;\Rightarrow\; R^n \subseteq S^n$	Property 4
S is transitive $\iff \forall n \in \mathbb{Z}^+ \;:\; S^n \subseteq S$	Property 5

To do: Given S transitive and $R \subseteq S$. Show $U \subseteq S$

Let $(x, y) \in U$. Then, by $\star$ we have

$$(x, y) \in R^n \quad \text{for some} \quad n \in \mathbb{Z}^+ \; .$$

By Property 4 : $(x, y) \in S^n$.

By Property 5 : $(x, y) \in S$. **QED !**

REVIEW PROBLEMS

and

REVIEW CLICKER QUESTIONS

Review Problem 1.

Prove that for every integer n we have

$$n^5 - n \equiv 0 \pmod{30}$$

Review Problem 2.

Suppose m and n are relatively prime integers; $m \geq 2$, $n \geq 2$.

Prove that $\log_m n$ is an irrational number.

Review Problem 3. If A and B are sets, and if

$$f \;:\; A \;\longrightarrow\; B\;,$$

then for any subset S of B we define *the pre-image of S* as

$$f^{-1}(S) \;\equiv\; \{a \in A \;:\; f(a) \in S\}\;.$$

NOTE : $f^{-1}(S)$ is defined even if f does not have an inverse!

Let S and T be subsets of B .

Prove that

$$f^{-1}(S \cap T) \;=\; f^{-1}(S) \cap f^{-1}(T)$$

Review Problem 4.

Prove that if a , b , and c are integers such that

$$m \geq 2 \qquad \text{and} \qquad a \equiv b (\text{mod } m)$$

then

$$\gcd(a, m) \;=\; \gcd(b, m) \;.$$

Review Problem 5.

Use mathematical induction to prove that

$$21 \mid (4^{n+1} + 5^{2n-1}) ,$$

whenever n is a positive integer.

Review Problem 6.

The Fibonacci numbers are defined as: $f_1 = 1$, $f_2 = 1$, and

$$f_n \;=\; f_{n-1} \;+\; f_{n-2} \;, \qquad \text{for } \; n \;\geq\; 3 \;.$$

Use a proof by induction to show that

$$f_{n-1}\, f_{n+1} \;\; - \;\; f_n^2 \;\; = \;\; (-1)^n$$

for all $n \geq 2$.

Review Problem 7.

Let A and B be non-empty sets.

Let f be a $1-1$ function from A to B.

Suppose S is an partial order on B.

Define a relation R on A as follows:

$$\forall a_1, a_2 \in R \quad : \qquad a_1 R a_2 \iff f(a_1) S f(a_2) \ .$$

Prove that R is an partial order on A.