Slides

for Part IA CST 2025/26

Discrete Mathematics

<www.cl.cam.ac.uk/teaching/2526/DiscMath>

Prof Marcelo Fiore

Marcelo.Fiore@cl.cam.ac.uk

Dr Jon Sterling

js2878@cl.cam.ac.uk

What are we up to?

- Learn to read and write, and also work with, mathematical arguments.
- Doing some basic discrete mathematics.
- Getting a taste of computer science applications.

What is Discrete Mathematics?

from *Discrete Mathematics (second edition)* by N. Biggs

Discrete Mathematics is the branch of Mathematics in which we deal with questions involving finite or countably infinite sets. In particular this means that the numbers involved are either integers, or numbers closely related to them, such as fractions or 'modular' numbers.

What is it that we do?

In general:

Build mathematical models and apply methods to analyse problems that arise in computer science.

In particular:

Make and study mathematical constructions by means of definitions and theorems. We aim at understanding their properties and limitations.

Lecture plan

I. Proofs.

II. Numbers.

III. Sets.

IV. Regular languages and finite automata.

Proofs

Objectives

- To develop techniques for analysing and understanding mathematical statements.
- To be able to present logical arguments that establish mathematical statements in the form of clear proofs.
- To prove Fermat's Little Theorem, a basic result in the theory of numbers that has many applications in computer science.

Proofs in practice

We are interested in examining the following statement:

> The product of two odd integers is odd.

This seems innocuous enough, but it is in fact full of baggage.

Proofs in practice

We are interested in examining the following statement:

> The product of two odd integers is odd.

This seems innocuous enough, but it is in fact full of baggage.
For instance, it presupposes that you know:

- what a statement is;
- what the integers $(\ldots, -1, 0, 1, \ldots)$ are, and that amongst them there is a class of odd ones $(\ldots, -3, -1, 1, 3, \ldots)$;
- what the product of two integers is, and that this is in turn an integer.

More precisely put, we may write:

If $\mathfrak{m}$ and $\mathfrak{n}$ are odd integers then so is $\mathfrak{m} \cdot \mathfrak{n}$.

More precisely put, we may write:

If $\mathfrak{m}$ and $\mathfrak{n}$ are odd integers then so is $\mathfrak{m} \cdot \mathfrak{n}$.

which further presupposes that you know:

- what variables are;
- what

  if . . . then . . .

  statements are, and how one goes about proving them;
- that the symbol "$\cdot$" is commonly used to denote the product operation.

Even more precisely, we should write

> For all integers m and n, if m and n are odd then so is $\mathrm{m} \cdot \mathrm{n}$.

which now additionally presupposes that you know:

- what

  for all ...

  statements are, and how one goes about proving them.

Thus, in trying to understand and then prove the above statement, we are assuming quite a lot of *mathematical jargon* that one needs to learn and practice with to make it a useful, and in fact very powerful, tool.

Some mathematical jargon

Statement

A sentence that is either true or false — but not both.

Example 1

‘$e^{i\pi} + 1 = 0$’

Non-example

‘This statement is false’

Predicate

A statement whose truth depends on the value of one or more variables.

Example 2

1. *'* $e^{ix} = \cos x + i \sin x$ *'*

2. *'the function* f *is differentiable'*

Theorem

A very important true statement.

Proposition

A less important but nonetheless interesting true statement.

Lemma

A true statement used in proving other true statements.

Corollary

A true statement that is a simple deduction from a theorem or proposition.

Example 3

1. *Fermat's Last Theorem*
2. *The Pumping Lemma*

Conjecture

A statement believed to be true, but for which we have no proof.

Example 4

1. *Goldbach's Conjecture*
2. *The Riemann Hypothesis*

Proof

Logical explanation of why a statement is true; a method for establishing truth.

Proof

Logical explanation of why a statement is true; a method for establishing truth.

Logic

The study of methods and principles used to distinguish good (correct) from bad (incorrect) reasoning.

Example 5

1. *Classical predicate logic*
2. *Hoare logic*
3. *Temporal logic*

Axiom

A basic assumption about a mathematical situation.

Axioms can be considered facts that do not need to be proved (just to get us going in a subject) or they can be used in definitions.

Example 6

1. *Euclidean Geometry*
2. *Riemannian Geometry*
3. *Hyperbolic Geometry*

Definition

An explanation of the mathematical meaning of a word (or phrase).

The word (or phrase) is generally defined in terms of properties.

Warning: It is vitally important that you can recall definitions precisely. A common problem is not to be able to advance in some problem because the definition of a word is unknown.

Definition, theorem, intuition, proof in practice

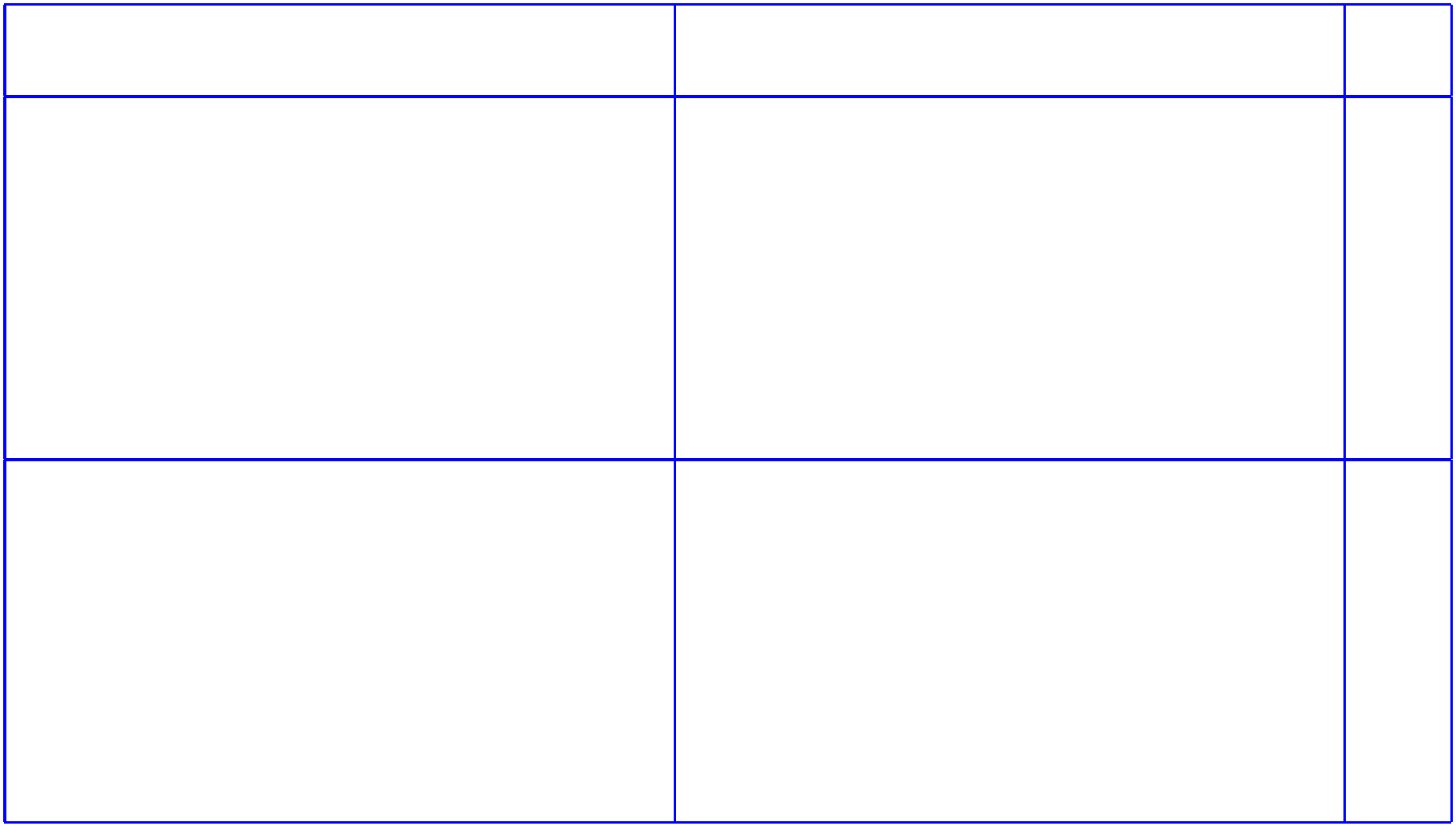
Proposition 8 *For all integers* $\mathfrak{m}$ *and* $\mathfrak{n}$*, if* $\mathfrak{m}$ *and* $\mathfrak{n}$ *are odd then so is* $\mathfrak{m} \cdot \mathfrak{n}$*.*

Definition, theorem, intuition, proof in practice

Definition 7 *An integer is said to be* odd *whenever it is of the form* $2 \cdot i + 1$ *for some (necessarily unique) integer* i*.*

Proposition 8 *For all integers* m *and* n*, if* m *and* n *are odd then so is* $m \cdot n$*.*

Intuition:



PROOF OF Proposition 8:

Simple and composite statements

A statement is *simple* (or *atomic*) when it cannot be broken into other statements, and it is *composite* when it is built by using several (simple or composite statements) connected by *logical* expressions (e.g., if. . . then. . . ; . . . implies . . . ; . . . if and only if . . . ; . . . and. . . ; either . . . or . . . ; it is not the case that . . . ; for all . . . ; there exists . . . ; etc.)

Examples:

‘2 is a prime number’

‘for all integers m and n, if $m \cdot n$ is even then either n or m are even’

Proof Structure

Assumptions	Goals
statements that may be used for deduction	statements to be established

Implication

Theorems can usually be written in the form

if a collection of *assumptions* holds, **then** so does some *conclusion*

or, in other words,

a collection of *assumptions* **implies** some *conclusion*

or, in symbols,

a collection of *hypotheses* $\Longrightarrow$ some *conclusion*

NB Identifying precisely what the assumptions and conclusions are is the first goal in dealing with a theorem.

Implications

- How to *prove* them as goals.
- How to *use* them as assumptions.

How to prove implication goals

The main proof strategy for implication:

To prove a goal of the form

$$P \implies Q$$

assume that P is true and prove Q.

NB *Assuming* is not *asserting*! Assuming a statement amounts to the same thing as adding it to your list of hypotheses.

Proof pattern:

In order to prove that

$$P \implies Q$$

1. Write: Assume P.
2. Show that Q logically follows.

Scratch work:

Before using the strategy

Assumptions	Goal
	$P \implies Q$
$\vdots$	

After using the strategy

Assumptions	Goal
	Q
$\vdots$	
P	

Proposition 8 *If* $\mathfrak{m}$ *and* $\mathfrak{n}$ *are odd integers, then so is* $\mathfrak{m} \cdot \mathfrak{n}$*.*

PROOF:

Definition 9 *A real number is:*

- rational *if it is of the form* $\mathtt{m}/\mathtt{n}$ *for a pair of integers* $\mathtt{m}$ *and* $\mathtt{n}$*; otherwise it is* irrational*.*
- positive *if it is greater than* 0*, and* negative *if it is smaller than* 0*.*
- nonnegative *if it is greater than or equal* 0*, and* nonpositive *if it is smaller than or equal* 0*.*
- natural *if it is a nonnegative integer.*

Proposition 10 *Let* x *be a positive real number. If* $\sqrt{x}$ *is rational then so is* x*.*

PROOF:

How to use implication assumptions

Logical Deduction by Modus Ponens

A main rule of *logical deduction* is that of *Modus Ponens*:

> From the statements P and $P \implies Q$,
> the statement Q follows.

or, in other words,

> If P and $P \implies Q$ hold then so does Q.

or, in symbols,

$$\frac{P \qquad P \implies Q}{Q}$$

The use of implications:

To use an assumption of the form $P \implies Q$,
aim at establishing P.
Once this is done, by Modus Ponens, one can
conclude Q and so further assume it.

Theorem 11 *Let* P_1, P_2, *and* P_3 *be statements. If* $P_1 \implies P_2$ *and* $P_2 \implies P_3$ *then* $P_1 \implies P_3$.

PROOF:

Bi-implication

Some theorems can be written in the form

P is equivalent to Q

or, in other words,

P implies Q, and vice versa

or

Q implies P, and vice versa

or

P if, and only if, Q $\qquad$ P iff Q

or, in symbols,

$$P \iff Q$$

Proof pattern:

In order to prove that

$$P \iff Q$$

1. Write: $(\Longrightarrow)$ and give a proof of $P \implies Q$.
2. Write: $(\Longleftarrow)$ and give a proof of $Q \implies P$.

Divisibility and congruence

Definition 12 *Let* d *and* n *be integers. We say that* d divides n, *and write* $d \mid n$, *whenever there is an integer* k *such that* $n = k \cdot d$.

Example 13 *The statement* $2 \mid 4$ *is true, while* $4 \mid 2$ *is not.*

Divisibility and congruence

Definition 12 *Let d and n be integers. We say that d divides n, and write $d \mid n$, whenever there is an integer k such that $n = k \cdot d$.*

Example 13 *The statement $2 \mid 4$ is true, while $4 \mid 2$ is not.*

Definition 14 *Fix a positive integer m. For integers a and b, we say that a is congruent to b modulo m, and write $a \equiv b \pmod{m}$, whenever $m \mid (a - b)$.*

Example 15

1. $18 \equiv 2 \pmod{4}$
2. $2 \equiv -2 \pmod{4}$
3. $18 \equiv -2 \pmod{4}$

Proposition 16 *For every integer* $\mathfrak{n}$,

1. $\mathfrak{n}$ *is even if, and only if,* $\mathfrak{n} \equiv 0 \pmod 2$, *and*

2. $\mathfrak{n}$ *is odd if, and only if,* $\mathfrak{n} \equiv 1 \pmod 2$.

PROOF:

The use of bi-implications:

To use an assumption of the form $P \iff Q$, use it as two separate assumptions $P \implies Q$ and $Q \implies P$.

Universal quantifications

- How to *prove* them as goals.
- How to *use* them as assumptions.

Universal quantification

Universal statements are of the form

> **for all** individuals x of the universe of discourse,
> the property $P(x)$ holds

or, in other words,

> no matter what individual x in the universe of discourse
> one considers, the property $P(x)$ for it holds

or, in symbols,

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

Example 17

2. *For every positive real number* x*, if* $\sqrt{x}$ *is rational then so is* x*.*

3. *For every integer* n*, we have that* n *is even iff so is* n^2*.*

The main proof strategy for universal statements:

To prove a goal of the form

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

let x stand for an arbitrary individual and prove $P(x)$.

Proof pattern:

In order to prove that

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

1. Write: Let x be an arbitrary individual.

2. Show that $P(x)$ holds.

Proof pattern:

In order to prove that

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

1. Write: Let x be an arbitrary individual.

   Warning: Make sure that the variable x is new (also referred to as fresh) in the proof! If for some reason the variable x is already being used in the proof to stand for something else, then you must use an unused variable, say y, to stand for the arbitrary individual, and prove $P(y)$.

2. Show that $P(x)$ holds.

Scratch work:

Before using the strategy

Assumptions	Goal
	$\forall x.\, P(x)$
⋮	

After using the strategy

Assumptions	Goal
	$P(x)$ (for a new (or fresh) x)
⋮	

Example:

Assumptions	unprovable Goal
$\vdots$	for all integers n, $n \geq 1$
$n > 0$	
$\vdots$	

How to use universal statements

Assumptions

$\vdots$

$\forall x.\, x^2 \geq 0$

$\vdots$

$\pi^2 \geq 0$

$e^2 \geq 0$

$0^2 \geq 0$

$\vdots$

The use of universal statements:

To use an assumption of the form $\forall x.\, P(x)$, you can plug in any value, say a, for x to conclude that $P(a)$ is true and so further assume it.

This rule is called *universal instantiation*.

Proposition 18 *Fix a positive integer* $\mathfrak{m}$*. For integers* $\mathfrak{a}$ *and* $\mathfrak{b}$*, we have that* $\mathfrak{a} \equiv \mathfrak{b} \pmod{\mathfrak{m}}$ *if, and only if, for all positive integers* $\mathfrak{n}$*, we have that* $\mathfrak{n} \cdot \mathfrak{a} \equiv \mathfrak{n} \cdot \mathfrak{b} \pmod{\mathfrak{n} \cdot \mathfrak{m}}$*.*

PROOF:

Equality in proofs

Examples:

- If $a = b$ and $b = c$ then $a = c$.
- If $a = b$ and $x = y$ then $a + x = b + x = b + y$.

Equality axioms

Just for the record, here are the axioms for *equality*.

- Every individual is equal to itself.

$$\forall x.\ x = x$$

- For any pair of equal individuals, if a property holds for one of them then it also holds for the other one.

$$\forall x. \forall y.\ x = y \implies \big(P(x) \implies P(y)\big)$$

NB From these axioms one may deduce the usual intuitive properties of equality, such as

$$\forall x. \forall y.\ x = y \implies y = x$$

and

$$\forall x. \forall y. \forall z.\ x = y \implies (y = z \implies x = z) \quad .$$

However, in practice, you will not be required to formally do so; rather you may just use the properties of equality that you are already familiar with.

Conjunctions

- How to *prove* them as goals.
- How to *use* them as assumptions.

Conjunction

Conjunctive statements are of the form

P **and** Q

or, in other words,

both P and also Q hold

or, in symbols,

$P \wedge Q$ or $P \ \& \ Q$

The proof strategy for conjunction:

To prove a goal of the form

$$P \wedge Q$$

first prove P and subsequently prove Q (or vice versa).

Proof pattern:

In order to prove

$$P \wedge Q$$

1. Write: Firstly, we prove P. and provide a proof of P.
2. Write: Secondly, we prove Q. and provide a proof of Q.

Scratch work:

Before using the strategy

Assumptions	Goal
	$P \wedge Q$
⋮	

After using the strategy

Assumptions	Goal	Assumptions	Goal
	P		Q
⋮		⋮	

The use of conjunctions:

To use an assumption of the form $P \wedge Q$,
treat it as two separate assumptions: P and Q.

Theorem 19 *For every integer* n*, we have that* $6 \mid n$ *iff* $2 \mid n$ *and* $3 \mid n$*.*

PROOF:

Existential quantifications

- How to *prove* them as goals.
- How to *use* them as assumptions.

Existential quantification

Existential statements are of the form

> **there exists** an individual x in the universe of discourse for which the property $P(x)$ holds

or, in other words,

> **for some** individual x in the universe of discourse, the property $P(x)$ holds

or, in symbols,

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

Example: The Pigeonhole Principle.

Let n be a positive integer. If $n + 1$ letters are put in n pigeonholes then there will be a pigeonhole with more than one letter.

Theorem 20 (Intermediate value theorem) *Let f be a real-valued continuous function on an interval $[a, b]$. For every y in between $f(a)$ and $f(b)$, there exists v in between a and b such that $f(v) = y$.*

Intuition:

The main proof strategy for existential statements:

To prove a goal of the form

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

find a *witness* for the existential statement; that is, a value of x, say w, for which you think $P(x)$ will be true, and show that indeed $P(w)$, i.e. the predicate $P(x)$ instantiated with the value w, holds.

Proof pattern:

In order to prove

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

1. Write: $\mathrm{Let}\ w = \ldots$ (the witness you decided on).
2. Provide a proof of $P(w)$.

Scratch work:

Before using the strategy

Assumptions	Goal
	$\exists x.\, P(x)$

$\vdots$

After using the strategy

Assumptions	Goals
	$P(w)$

$\vdots$

$w = \ldots$ (the witness you decided on)

Proposition 21 *For every positive integer* k*, there exist natural numbers* i *and* j *such that* $4 \cdot k = i^2 - j^2$*.*

PROOF:

The use of existential statements:

To use an assumption of the form $\exists x.\, P(x)$, introduce a new variable x_0 into the proof to stand for some individual for which the property $P(x)$ holds. This means that you can now assume $P(x_0)$ true.

Theorem 23 *For all integers* $\mathfrak{l}$, $\mathfrak{m}$, $\mathfrak{n}$, *if* $\mathfrak{l} \mid \mathfrak{m}$ *and* $\mathfrak{m} \mid \mathfrak{n}$ *then* $\mathfrak{l} \mid \mathfrak{n}$.

PROOF:

Unique existence

The notation

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

stands for

the *unique existence* of an x for which the property $P(x)$ holds .

That is,

$$\exists x.\, P(x) \;\wedge\; \Big(\forall y.\, \forall z.\, \big(P(y) \wedge P(z)\big) \implies y = z\Big)$$

Example: The congruence property modulo $\mathfrak{m}$ uniquely characterises the natural numbers from 0 to $\mathfrak{m}-1$.

Proposition 24 *Let $\mathfrak{m}$ be a positive integer and let $\mathfrak{n}$ be an integer.*

Define

$$P(z) = [0 \leq z < \mathfrak{m} \wedge z \equiv \mathfrak{n} \pmod{\mathfrak{m}}] \ .$$

Then

$$\forall x, y. P(x) \wedge P(y) \implies x = y \ .$$

PROOF:

A proof strategy

To prove

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

for an arbitrary x construct the unique witness and name it, say as $f(x)$, showing that

$$P\big(x, f(x)\big)$$

and

$$\forall y.\, P(x, y) \implies y = f(x)$$

hold.

Disjunctions

- How to *prove* them as goals.
- How to *use* them as assumptions.

Disjunction

Disjunctive statements are of the form

$$\boxed{P \text{ or } Q}$$

or, in other words,

$$\boxed{\text{either } P, Q, \text{ or both hold}}$$

or, in symbols,

$$\boxed{P \vee Q}$$

The main proof strategy for disjunction:

To prove a goal of the form

$$P \vee Q$$

you may

1. try to prove P (if you succeed, then you are done); or
2. try to prove Q (if you succeed, then you are done); otherwise
3. break your proof into cases; proving, in each case, either P or Q.

Proposition 25 *For all integers* $\mathfrak{n}$*, either* $\mathfrak{n}^2 \equiv 0 \pmod 4$ *or* $\mathfrak{n}^2 \equiv 1 \pmod 4$*.*

PROOF:

The use of disjunction:

To use a disjunctive assumption

$$P_1 \vee P_2$$

to establish a goal Q, consider the following two cases in turn: (i) assume P_1 to establish Q, and (ii) assume P_2 to establish Q.

Scratch work:

Before using the strategy

Assumptions	Goal
	Q
$\vdots$	
$P_1 \vee P_2$	

After using the strategy

Assumptions	Goal	Assumptions	Goal
	Q		Q
$\vdots$		$\vdots$	
P_1		P_2	

Proof pattern:

In order to prove Q from some assumptions amongst which there is

$$P_1 \vee P_2$$

write: We prove the following two cases in turn: (i) that assuming P_1, we have Q; and (ii) that assuming P_2, we have Q. Case (i): Assume P_1. and provide a proof of Q from it and the other assumptions. Case (ii): Assume P_2. and provide a proof of Q from it and the other assumptions.

A little arithmetic

Lemma 27 *For all positive integers* p *and natural numbers* m*, if* $m = 0$ *or* $m = p$ *then* $\binom{p}{m} \equiv 1 \pmod{p}$*.*

PROOF:

Lemma 28 *For all integers* p *and* m*, if* p *is prime and* $0 < \mathrm{m} < \mathrm{p}$ *then* $\binom{\mathrm{p}}{\mathrm{m}} \equiv 0 \pmod{\mathrm{p}}$*.*

PROOF:

Proposition 29 *For all prime numbers* p *and integers* $0 \leq m \leq p$, *either* $\binom{p}{m} \equiv 0 \pmod{p}$ *or* $\binom{p}{m} \equiv 1 \pmod{p}$.

PROOF:

Binomial Theorem

$$(m+n)^p = \sum_{k=0}^{p} \binom{p}{k} \cdot m^{p-k} \cdot n^k$$

A little more arithmetic

Corollary 33 (The Freshman's Dream) *For all natural numbers* m, n *and primes* p,

$$(m+n)^p \equiv m^p + n^p \pmod{p} \ .$$

PROOF:

Corollary 34 (The Dropout Lemma) *For all natural numbers* $\mathfrak{m}$ *and primes* $\mathfrak{p}$*,*

$$(\mathfrak{m}+1)^{\mathfrak{p}} \equiv \mathfrak{m}^{\mathfrak{p}}+1 \pmod{\mathfrak{p}} \ .$$

Proposition 35 (The Many Dropout Lemma) *For all natural numbers* $\mathfrak{m}$ *and* $\mathfrak{i}$*, and primes* $\mathfrak{p}$*,*

$$(\mathfrak{m}+\mathfrak{i})^{\mathfrak{p}} \equiv \mathfrak{m}^{\mathfrak{p}}+\mathfrak{i} \pmod{\mathfrak{p}} \ .$$

PROOF:

Fermat's Little Theorem

The Many Dropout Lemma (Proposition 35) gives the first part of the following very important theorem as a corollary.

Theorem 36 (Fermat's Little Theorem) *For all natural numbers* i *and primes* p*,*

1. $\mathrm{i}^{\mathrm{p}} \equiv \mathrm{i} \pmod{\mathrm{p}}$*, and*
2. $\mathrm{i}^{\mathrm{p}-1} \equiv 1 \pmod{\mathrm{p}}$ *whenever* i *is not a multiple of* p*.*

The fact that the first part of Fermat's Little Theorem implies the second one will be proved later on .

Every natural number i not a multiple of a prime number p has a *reciprocal* modulo p, namely $\mathrm{i}^{\mathrm{p}-2}$, as $\mathrm{i} \cdot (\mathrm{i}^{\mathrm{p}-2}) \equiv 1 \pmod{\mathrm{p}}$.

Btw

1. Fermat's Little Theorem has applications to:
   (a) primality testing[a],
   (b) the verification of floating-point algorithms, and
   (c) cryptographic security.

[a] For instance, to establish that a positive integer $\mathtt{m}$ is not prime one may proceed to find an integer $\mathtt{i}$ such that $\mathtt{i}^{\mathtt{m}} \not\equiv \mathtt{i} \pmod{\mathtt{m}}$.

Negation

Negations are statements of the form

$$\boxed{\text{not } P}$$

or, in other words,

$$\boxed{P \text{ is not the case}}$$

or

$$\boxed{P \text{ is absurd}}$$

or

$$\boxed{P \text{ leads to contradiction}}$$

or, in symbols,

$$\boxed{\neg P}$$

A first proof strategy for negated goals and assumptions:

If possible, reexpress the negation in an *equivalent* form and use instead this other statement.

Logical equivalences

$$
\begin{aligned}
\neg(P \Longrightarrow Q) &\iff P \wedge \neg Q \\
\neg(P \Longleftrightarrow Q) &\iff P \Longleftrightarrow \neg Q \\
\neg(\forall x.\, P(x)) &\iff \exists x.\, \neg P(x) \\
\neg(P \wedge Q) &\iff (\neg P) \vee (\neg Q) \\
\neg(\exists x.\, P(x)) &\iff \forall x.\, \neg P(x) \\
\neg(P \vee Q) &\iff (\neg P) \wedge (\neg Q) \\
\neg(\neg P) &\iff P \\
\neg P &\iff (P \Rightarrow \mathbf{false})
\end{aligned}
$$

Theorem 37 *For all statements* P *and* Q*,*

$$(P \implies Q) \implies (\neg Q \implies \neg P) \quad .$$

PROOF:

Proof by contradiction

Amongst the equivalences for negation, we have postulated the somewhat controversial:

$$\neg\neg P \iff P$$

which is *classically* accepted.

Proof by contradiction

Amongst the equivalences for negation, we have postulated the somewhat controversial:

$$\neg\neg P \iff P$$

which is *classically* accepted.

In this light,

to prove P

one may equivalently

prove $\neg P \implies \mathbf{false}$;

that is,

assuming $\neg P$ leads to contradiction.

This technique is known as *proof by contradiction*.

The strategy for proof by contradiction:

To prove a goal P by contradiction is to prove the equivalent statement $\neg \mathrm{P} \implies \mathbf{false}$

The strategy for proof by contradiction:

To prove a goal P by contradiction is to prove the equivalent statement $\neg P \implies \mathbf{false}$

Proof pattern:

In order to prove

$$P$$

1. Write: We use proof by contradiction. So, suppose P is false.
2. Deduce a logical contradiction.
3. Write: This is a contradiction. Therefore, P must be true.

Scratch work:

Before using the strategy

Assumptions	Goal
	P
$\vdots$	

After using the strategy

Assumptions	Goal
	contradiction
$\vdots$	
$\neg P$	

Theorem 39 *For all statements* P *and* Q*,*

$$(\neg Q \implies \neg P) \implies (P \implies Q) \quad .$$

PROOF:

Proof by contrapositive

Corollary 40 *For all statements* P *and* Q*,*

$$(P \implies Q) \iff (\neg Q \implies \neg P) \quad .$$

Btw Using the above equivalence to prove an implication is known as *proof by contrapositive*.

Corollary 41 *For every positive irrational number* x*, the real number* $\sqrt{x}$ *is irrational.*

Lemma 42 *A positive real number* x *is rational iff*

$$\exists \textit{ positive integers } \mathrm{m}, \mathrm{n}: \quad \mathrm{x} = \mathrm{m}/\mathrm{n} \ \wedge \ \neg\big(\exists \textit{ prime } \mathrm{p}: \ \mathrm{p} \mid \mathrm{m} \ \wedge \ \mathrm{p} \mid \mathrm{n}\big) \tag{$\dagger$}$$

PROOF:

Numbers

Objectives

- Get an appreciation for the abstract notion of number system, considering four examples: natural numbers, integers, rationals, and modular integers.
- Prove the correctness of three basic algorithms in the theory of numbers: the division algorithm, Euclid's algorithm, and the Extended Euclid's algorithm.
- Exemplify the use of the mathematical theory surrounding Euclid's Theorem and Fermat's Little Theorem in the context of public-key cryptography.
- To understand and be able to proficiently use the Principle of Mathematical Induction in its various forms.

Natural numbers

In the beginning there were the *natural numbers*

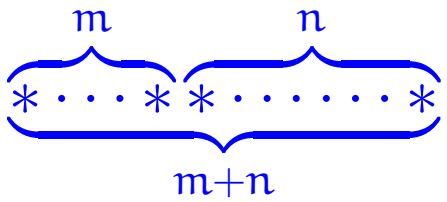
$$\mathbb{N} : \quad 0 , \quad 1 , \quad \ldots , \quad n , \quad n+1 , \quad \ldots$$

generated from *zero* by successive increment; that is, put in ML:

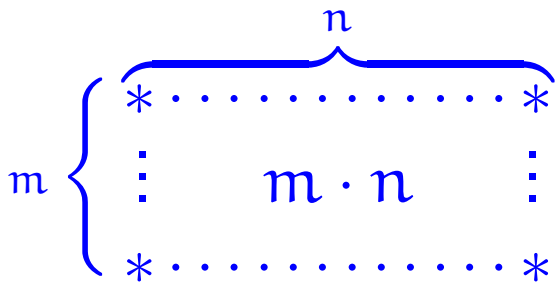
```
datatype
  N = zero | succ of N
```

The basic operations of this number system are:

- Addition



- Multiplication



The *additive structure* $(\mathbb{N}, 0, +)$ of natural numbers with zero and addition satisfies the following:

- Monoid laws

$$0 + n = n = n + 0 \quad , \quad (l + m) + n = l + (m + n)$$

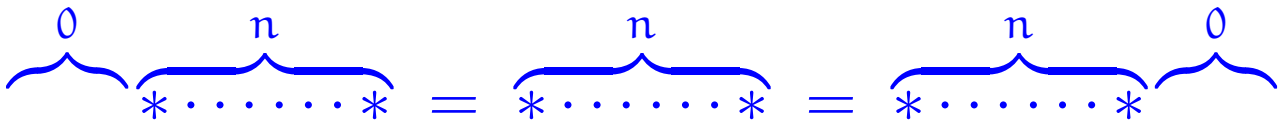
- Commutativity law

$$m + n = n + m$$

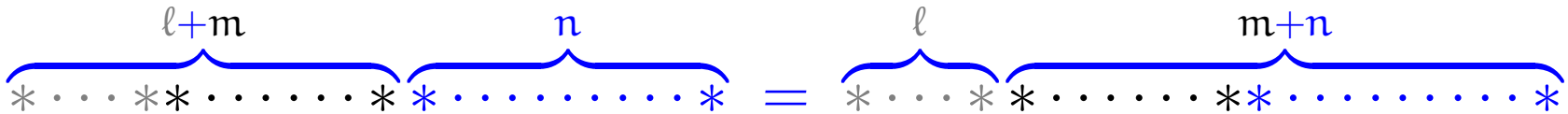
and as such is what in the mathematical jargon is referred to as a *commutative monoid*.

Commutative monoid laws

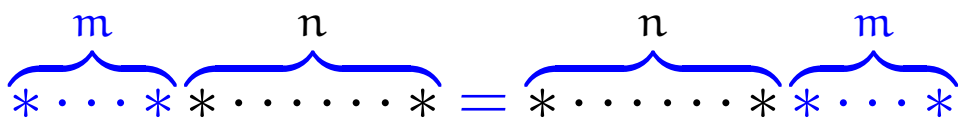
- Neutral element laws



- Associativity law



- Commutativity law



Monoids

Definition 43 *A* monoid *is an algebraic structure*

Monoids

Definition 43 *A* monoid *is an algebraic structure with*

- *a* neutral element*, say* e*,*
- *a* binary operation*, say* $\bullet$*,*

Monoids

Definition 43 *A* monoid *is an algebraic structure with*

- *a* neutral element*, say* e*,*
- *a* binary operation*, say* $\bullet$*,*

satisfying

- neutral element laws*:* $e \bullet x = x = x \bullet e$
- associativity law*:* $(x \bullet y) \bullet z = x \bullet (y \bullet z)$

Monoids

Definition 43 *A* monoid *is an algebraic structure with*

- *a* neutral element*, say* e*,*
- *a* binary operation*, say* $\bullet$*,*

satisfying

- neutral element laws*:* $e \bullet x = x = x \bullet e$
- associativity law*:* $(x \bullet y) \bullet z = x \bullet (y \bullet z)$

A monoid is commutative *if:*

- commutativity*:* $x \bullet y = y \bullet x$

is satisfied.

Also the *multiplicative structure* $(\mathbb{N}, 1, \cdot)$ of natural numbers with one and multiplication is a commutative monoid:

- Monoid laws

$$1 \cdot n = n = n \cdot 1 \quad , \quad (l \cdot m) \cdot n = l \cdot (m \cdot n)$$

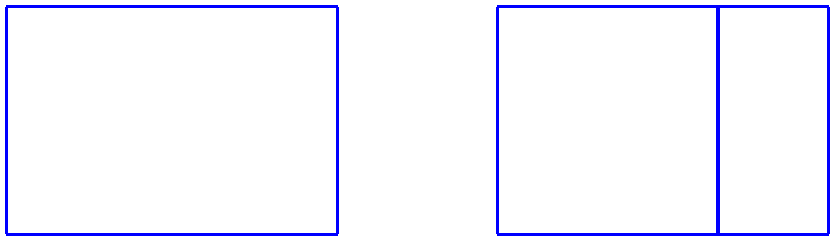
- Commutativity law

$$m \cdot n = n \cdot m$$

The additive and multiplicative structures interact nicely in that they satisfy the

- Distributive laws

$$\begin{aligned} l \cdot 0 &= 0 \\ l \cdot (m + n) &= l \cdot m + l \cdot n \end{aligned}$$



and make the overall structure $(\mathbb{N}, 0, +, 1, \cdot)$ into what in the mathematical jargon is referred to as a *commutative semiring*.

Semirings

Definition 44 *A* semiring *(or* rig*) is an algebraic structure*

Semirings

Definition 44 *A* semiring *(or* rig*) is an algebraic structure with*

- *a* commutative monoid *structure, say* $(0, \oplus)$,
- *a* monoid structure*, say* $(1, \otimes)$,

Semirings

Definition 44 *A* semiring *(or* rig*) is an algebraic structure with*

- *a* commutative monoid *structure, say* $(0, \oplus)$,
- *a* monoid structure*, say* $(1, \otimes)$,

satifying the distributivity laws*:*

- $0 \otimes x = 0 = x \otimes 0$
- $x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z)$, $(y \oplus z) \otimes x = (y \otimes x) \oplus (z \otimes x)$

Semirings

Definition 44 *A* semiring *(or* rig*) is an algebraic structure with*

- *a* commutative monoid *structure, say* $(0, \oplus)$,
- *a* monoid structure*, say* $(1, \otimes)$,

satifying the distributivity laws*:*

- $0 \otimes x = 0 = x \otimes 0$
- $x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z)$, $(y \oplus z) \otimes x = (y \otimes x) \oplus (z \otimes x)$

A semiring is commutative *whenever* $\otimes$ *is.*

Cancellation

The additive and multiplicative structures of natural numbers further satisfy the following laws.

- Additive cancellation

  For all natural numbers k, m, n,

  $$k + m = k + n \implies m = n \quad .$$

- Multiplicative cancellation

  For all natural numbers k, m, n,

  if $k \neq 0$ then $k \cdot m = k \cdot n \implies m = n \quad .$

Definition 45 *A binary operation* $\bullet$ *allows* cancellation *by an element* c

- on the left*: if* $c \bullet x = c \bullet y$ *implies* $x = y$
- on the right*: if* $x \bullet c = y \bullet c$ *implies* $x = y$

Example: The append operation on lists allows cancellation by any list on both the left and the right.

Inverses

Definition 46 *For a monoid with a neutral element e and a binary operation $\bullet$, and element x is said to admit an*

- inverse on the left *if there exists an element ℓ such that $\ell \bullet x = e$*
- inverse on the right *if there exists an element r such that $x \bullet r = e$*
- inverse *if it admits both left and right inverses*

Inverses

Definition 46 *For a monoid with a neutral element e and a binary operation $\bullet$, and element x is said to admit an*

- inverse on the left *if there exists an element ℓ such that $\ell \bullet x = e$*
- inverse on the right *if there exists an element r such that $x \bullet r = e$*
- inverse *if it admits both left and right inverses*

Proposition 47 *For a monoid $(e, \bullet)$ if an element admits an inverse then its left and right inverses are equal.*

PROOF:

Groups

Definition 49 *A* group *is a monoid in which every element has an inverse.*

An Abelian group *is a group for which the monoid is commutative.*

Inverses

Definition 50

1. *A number* x *is said to admit an* additive inverse *whenever there exists a number* y *such that* $x + y = 0$.

2. *A number* x *is said to admit a* multiplicative inverse *whenever there exists a number* y *such that* $x \cdot y = 1$.

Extending the system of natural numbers to: (i) admit all additive inverses and then (ii) also admit all multiplicative inverses for non-zero numbers yields two very interesting results:

Extending the system of natural numbers to: (i) admit all additive inverses and then (ii) also admit all multiplicative inverses for non-zero numbers yields two very interesting results:

(i) the *integers*

$$\mathbb{Z} \ : \quad \ldots -n\,,\ \ldots\,,\ -1\,,\ 0\,,\ 1\,,\ \ldots\,,\ n\,,\ \ldots$$

which then form what in the mathematical jargon is referred to as a *commutative ring*, and

(ii) the *rationals* $\mathbb{Q}$ which then form what in the mathematical jargon is referred to as a *field*.

Rings

Definition 51 *A* ring *is a semiring* $(0, \oplus, 1, \otimes)$ *in which the commutative monoid* $(0, \oplus)$ *is a group.*

A ring is commutative *if so is the monoid* $(1, \otimes)$*.*

Fields

Definition 52 *A* field *is a commutative ring in which every element besides* 0 *has a reciprocal (that is, and inverse with respect to* $\otimes$*).*

The division theorem and algorithm

Theorem 53 (Division Theorem) *For every natural number* m *and positive natural number* n*, there exists a unique pair of integers* q *and* r *such that* $q \geq 0$*,* $0 \leq r < n$*, and* $m = q \cdot n + r$*.*

The division theorem and algorithm

Theorem 53 (Division Theorem) *For every natural number* $\mathfrak{m}$ *and positive natural number* $\mathfrak{n}$*, there exists a unique pair of integers* $\mathfrak{q}$ *and* $\mathfrak{r}$ *such that* $\mathfrak{q} \geq 0$*,* $0 \leq \mathfrak{r} < \mathfrak{n}$*, and* $\mathfrak{m} = \mathfrak{q} \cdot \mathfrak{n} + \mathfrak{r}$*.*

Definition 54 *The natural numbers* $\mathfrak{q}$ *and* $\mathfrak{r}$ *associated to a given pair of a natural number* $\mathfrak{m}$ *and a positive integer* $\mathfrak{n}$ *determined by the Division Theorem are respectively denoted* $\mathrm{quo}(\mathfrak{m}, \mathfrak{n})$ *and* $\mathrm{rem}(\mathfrak{m}, \mathfrak{n})$*.*

PROOF OF Theorem 53:

The Division Algorithm in ML:

```
fun divalg( m , n )
  = let
      fun diviter( q , r )
        = if r < n then ( q , r )
          else diviter( q+1 , r-n )
    in
      diviter( 0 , m )
    end

fun quo( m , n ) = #1( divalg( m , n ) )

fun rem( m , n ) = #2( divalg( m , n ) )
```

Theorem 56 *For every natural number* m *and positive natural number* n*, the evaluation of* $\mathtt{divalg}(\mathrm{m}, \mathrm{n})$ *terminates, outputing a pair of natural numbers* $(\mathrm{q}_0, \mathrm{r}_0)$ *such that* $\mathrm{r}_0 < \mathrm{n}$ *and* $\mathrm{m} = \mathrm{q}_0 \cdot \mathrm{n} + \mathrm{r}_0$*.*

PROOF:

Proposition 57 *Let* m *be a positive integer. For all natural numbers* k *and* l*,*

$$\mathrm{k} \equiv \mathrm{l} \pmod{\mathrm{m}} \iff \mathrm{rem}(\mathrm{k}, \mathrm{m}) = \mathrm{rem}(\mathrm{l}, \mathrm{m}) \quad .$$

PROOF:

Corollary 58 *Let $\mathfrak{m}$ be a positive integer.*

1. *For every natural number $\mathfrak{n}$,*

$$\mathfrak{n} \equiv \mathrm{rem}(\mathfrak{n}, \mathfrak{m}) \pmod{\mathfrak{m}} \quad .$$

PROOF:

Corollary 58 *Let* m *be a positive integer.*

1. *For every natural number* n*,*

$$\mathrm{n} \equiv \mathrm{rem}(\mathrm{n}, \mathrm{m}) \pmod{\mathrm{m}} \quad .$$

2. *For every integer* k *there exists a unique integer* $[\mathrm{k}]_{\mathrm{m}}$ *such that*

$$0 \leq [\mathrm{k}]_{\mathrm{m}} < \mathrm{m} \quad \textit{and} \quad \mathrm{k} \equiv [\mathrm{k}]_{\mathrm{m}} \pmod{\mathrm{m}} \quad .$$

PROOF:

Modular arithmetic

For every positive integer m, the *integers modulo* m are:

$$\mathbb{Z}_m \ : \quad 0 \ , \quad 1 \ , \quad \ldots \ , \quad m-1 \ .$$

with arithmetic operations of addition $+_m$ and multiplication $\cdot_m$ defined as follows

$$\begin{aligned} k +_m l &= [k+l]_m &&= \mathrm{rem}(k+l, m) \ , \\ k \cdot_m l &= [k \cdot l]_m &&= \mathrm{rem}(k \cdot l, m) \end{aligned}$$

for all $0 \leq k, l < m$.

For k and l in $\mathbb{Z}_m$,

$$k +_m l \text{ and } k \cdot_m l$$

are the unique modular integers in $\mathbb{Z}_m$ such that

$$k +_m l \equiv k + l \pmod{m}$$

$$k \cdot_m l \equiv k \cdot l \pmod{m}$$

Example 60 *The addition and multiplication tables for* $\mathbb{Z}_4$ *are:*

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Note that the addition table has a cyclic pattern, while there is no obvious pattern in the multiplication table.

From the addition and multiplication tables, we can readily read tables for additive and multiplicative inverses:

	additive inverse
0	0
1	3
2	2
3	1

	multiplicative inverse
0	–
1	1
2	–
3	3

Interestingly, we have a non-trivial multiplicative inverse; namely, 3.

Example 61 *The addition and multiplication tables for* $\mathbb{Z}_5$ *are:*

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Again, the addition table has a cyclic pattern, while this time the multiplication table restricted to non-zero elements has a permutation pattern.

From the addition and multiplication tables, we can readily read tables for additive and multiplicative inverses:

	additive inverse
0	0
1	4
2	3
3	2
4	1

	multiplicative inverse
0	—
1	1
2	3
3	2
4	4

Surprisingly, every non-zero element has a multiplicative inverse.

Proposition 62 *For all natural numbers* $\mathfrak{m} > 1$*, the modular-arithmetic structure*

$$(\mathbb{Z}_{\mathfrak{m}}, 0, +_{\mathfrak{m}}, 1, \cdot_{\mathfrak{m}})$$

is a commutative ring.

NB Quite surprisingly, modular-arithmetic number systems have further mathematical structure in the form of multiplicative inverses

.

Proposition 63 *Let m be a positive integer. A modular integer k in $\mathbb{Z}_{\mathrm{m}}$ has a reciprocal if, and only if, there exist integers i and j such that $\mathrm{k} \cdot \mathrm{i} + \mathrm{m} \cdot \mathrm{j} = 1$.*

PROOF:

Integer linear combinations

Definition 64 *An integer r is said to be a linear combination of a pair of integers m and n whenever there are integers s and t such that $s \cdot m + t \cdot n = r$.*

Proposition 65 *Let m be a positive integer. A modular integer k in $\mathbb{Z}_m$ has a reciprocal if, and only if, 1 is an integer linear combination of m and k.*

Important mathematical jargon: Sets

Very roughly, sets are the mathematicians' data structures. Informally, we will consider a *set* as a (well-defined, unordered) collection of mathematical objects, called the *elements* (or *members*) of the set.

Set membership

The symbol '$\in$' known as the *set membership* predicate is central to the theory of sets, and its purpose is to build statements of the form

$$x \in A$$

that are true whenever it is the case that the object x is an element of the set A, and false otherwise.

Defining sets

The set	of even primes	is	$\{2\}$
	of booleans		$\{\mathbf{true}, \mathbf{false}\}$
	$[-2..3]$		$\{-2, -1, 0, 1, 2, 3\}$

Set comprehension

The basic idea behind set comprehension is to define a set by means of a property that precisely characterises all the elements of the set.

Notations:

$$\{x \in A \mid P(x)\} \quad , \quad \{x \in A : P(x)\}$$

Set equality

Two sets are equal precisely when they have the same elements

Examples:

- $\{x \in \mathbb{N} : 2 \mid x \wedge x \text{ is prime}\} = \{2\}$
- For a positive integer m,

$$\{x \in \mathbb{Z} : m \mid x\} = \{x \in \mathbb{Z} : x \equiv 0 \pmod{m}\}$$

- $\{d \in \mathbb{N} : d \mid 0\} = \mathbb{N}$

Equivalent predicates specify equal sets:

$$\{ x \in A \mid P(x) \} = \{ x \in A \mid Q(x) \}$$

iff

$$\forall x \in A.\ P(x) \iff Q(x)$$

Equivalent predicates specify equal sets:

$$\{x \in A \mid P(x)\} = \{x \in A \mid Q(x)\}$$

iff

$$\forall x \in A.\ P(x) \iff Q(x)$$

Example: For a positive integer m,

$$\{\, x \in \mathbb{Z}_m \mid x \text{ has a reciprocal in } \mathbb{Z}_m \,\}$$

$=$

$$\{\, x \in \mathbb{Z}_m \mid 1 \text{ is an integer linear combination of } m \text{ and } x \,\}$$

Greatest common divisor

Given a natural number n, the set of its *divisors* is defined by set comprehension as follows

$$D(n) = \{\, d \in \mathbb{N} : d \mid n \,\} \quad .$$

Greatest common divisor

Given a natural number n, the set of its *divisors* is defined by set comprehension as follows

$$D(n) = \{\, d \in \mathbb{N} : d \mid n \,\} \quad .$$

Example 67

1. $D(0) = \mathbb{N}$
2. $D(1224) = \left\{ \begin{array}{c} 1, 2, 3, 4, 6, 8, 9, 12, 17, 18, 24, 34, 36, 51, 68, \\ 72, 102, 136, 153, 204, 306, 408, 612, 1224 \end{array} \right\}$

Remark Sets of divisors are hard to compute. However, the computation of the greatest divisor is straightforward. :)

Going a step further, what about the *common divisors* of pairs of natural numbers? That is, the set

$$\mathrm{CD}(\mathrm{m}, \mathrm{n}) = \left\{ \mathrm{d} \in \mathbb{N} : \mathrm{d} \mid \mathrm{m} \wedge \mathrm{d} \mid \mathrm{n} \right\}$$

for $\mathrm{m}, \mathrm{n} \in \mathbb{N}$.

Going a step further, what about the *common divisors* of pairs of natural numbers? That is, the set

$$\mathrm{CD}(\mathrm{m},\mathrm{n}) = \left\{\, \mathrm{d} \in \mathbb{N} \,:\, \mathrm{d} \mid \mathrm{m} \,\wedge\, \mathrm{d} \mid \mathrm{n} \,\right\}$$

for $\mathrm{m}, \mathrm{n} \in \mathbb{N}$.

Example 68

$$\mathrm{CD}(1224, 660) = \{1, 2, 3, 4, 6, 12\}$$

Since $\mathrm{CD}(\mathrm{n},\mathrm{n}) = \mathrm{D}(\mathrm{n})$, the computation of common divisors is as hard as that of divisors. But, what about the computation of the *greatest common divisor*?

Lemma 71 (Key Lemma) *Let* m *and* m' *be natural numbers and let* n *be a positive integer such that* $\mathrm{m} \equiv \mathrm{m}' \pmod{\mathrm{n}}$*. Then,*

$$\mathrm{CD}(\mathrm{m}, \mathrm{n}) = \mathrm{CD}(\mathrm{m}', \mathrm{n}) \ .$$

PROOF:

Lemma 73 *For all positive integers* m *and* n*,*

$$\mathrm{CD}(\mathrm{m},\mathrm{n}) = \begin{cases} \mathrm{D}(\mathrm{n}) & \text{, if } \mathrm{n} \mid \mathrm{m} \\ \mathrm{CD}\big(\mathrm{n}, \mathrm{rem}(\mathrm{m},\mathrm{n})\big) & \text{, otherwise} \end{cases}$$

Lemma 73 *For all positive integers* m *and* n,

$$\mathrm{CD}(\mathrm{m},\mathrm{n}) = \begin{cases} \mathrm{D}(\mathrm{n}) & \text{, if } \mathrm{n} \mid \mathrm{m} \\ \mathrm{CD}\big(\mathrm{n}, \mathrm{rem}(\mathrm{m},\mathrm{n})\big) & \text{, otherwise} \end{cases}$$

Since a positive integer n is the greatest divisor in $\mathrm{D}(\mathrm{n})$, the lemma suggests a recursive procedure:

$$\gcd(\mathrm{m},\mathrm{n}) = \begin{cases} \mathrm{n} & \text{, if } \mathrm{n} \mid \mathrm{m} \\ \gcd\big(\mathrm{n}, \mathrm{rem}(\mathrm{m},\mathrm{n})\big) & \text{, otherwise} \end{cases}$$

for computing the *greatest common divisor*, of two positive integers m and n. This is

Euclid's Algorithm

gcd

```
fun gcd( m , n )
  =  let
       val ( q , r ) = divalg( m , n )
     in
       if r = 0 then n
       else gcd( n , r )
     end
```

Example 74 ($\gcd(13,34)=1$)

$$\begin{aligned}\gcd(13,34) &= \gcd(34,13)\\ &= \gcd(13,8)\\ &= \gcd(8,5)\\ &= \gcd(5,3)\\ &= \gcd(3,2)\\ &= \gcd(2,1)\\ &= 1\end{aligned}$$

NB If $\mathtt{gcd}$ terminates on input (m,n) with output $\gcd(m,n)$ then $\mathrm{CD}(m,n)=\mathrm{D}\big(\gcd(m,n)\big)$.

Proposition 75 *For all natural numbers* $\mathfrak{m}, \mathfrak{n}$ *and* $\mathfrak{a}, \mathfrak{b}$*,*
if $\mathrm{CD}(\mathfrak{m}, \mathfrak{n}) = \mathrm{D}(\mathfrak{a})$ *and* $\mathrm{CD}(\mathfrak{m}, \mathfrak{n}) = \mathrm{D}(\mathfrak{b})$ *then* $\mathfrak{a} = \mathfrak{b}$*.*

Proposition 75 *For all natural numbers* m, n *and* a, b*, if* $\mathrm{CD}(\mathrm{m}, \mathrm{n}) = \mathrm{D}(\mathrm{a})$ *and* $\mathrm{CD}(\mathrm{m}, \mathrm{n}) = \mathrm{D}(\mathrm{b})$ *then* $\mathrm{a} = \mathrm{b}$*.*

Proposition 76 *For all natural numbers* m, n *and* k*, the following statements are equivalent:*

1. $\mathrm{CD}(\mathrm{m}, \mathrm{n}) = \mathrm{D}(\mathrm{k})$*.*
2. - $\mathrm{k} \mid \mathrm{m} \ \wedge \ \mathrm{k} \mid \mathrm{n}$*, and*
   - *for all natural numbers* d*,* $\mathrm{d} \mid \mathrm{m} \ \wedge \ \mathrm{d} \mid \mathrm{n} \implies \mathrm{d} \mid \mathrm{k}$*.*

Definition 77 *For natural numbers* m, n *the unique natural number* k *such that*

- $\mathrm{k} \mid \mathrm{m} \ \wedge \ \mathrm{k} \mid \mathrm{n}$, *and*
- *for all natural numbers* d, $\mathrm{d} \mid \mathrm{m} \ \wedge \ \mathrm{d} \mid \mathrm{n} \implies \mathrm{d} \mid \mathrm{k}$.

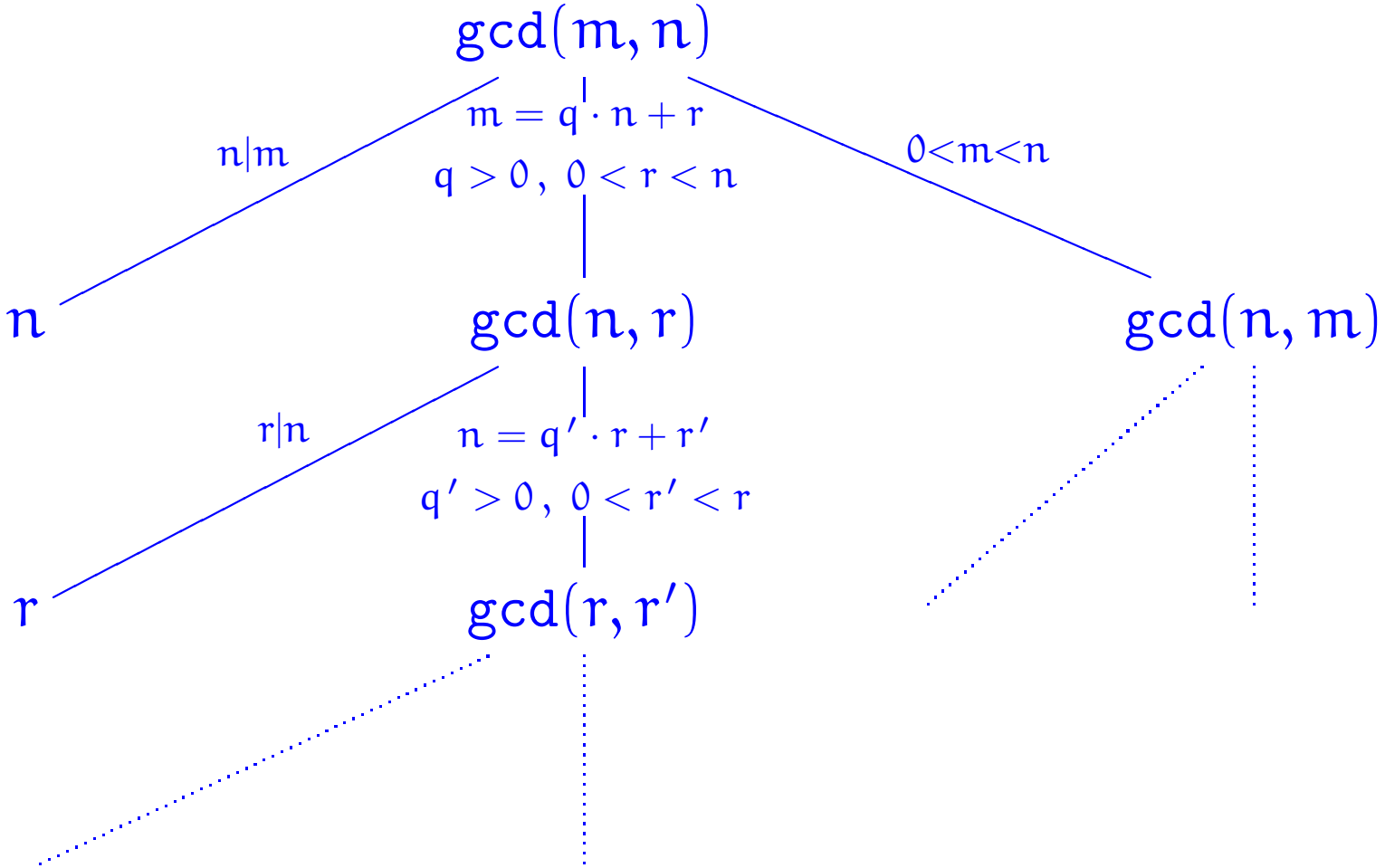
is called the greatest common divisor *of* m *and* n, *and denoted* $\mathrm{gcd}(\mathrm{m}, \mathrm{n})$.

Theorem 78 *Euclid's Algorithm* $\mathtt{gcd}$ *terminates on all pairs of positive integers and, for such* $\mathtt{m}$ *and* $\mathtt{n}$*, the positive integer* $\mathtt{gcd}(\mathtt{m}, \mathtt{n})$ *is the greatest common divisor of* $\mathtt{m}$ *and* $\mathtt{n}$ *in the sense that the following two properties hold:*

(i) *both* $\mathtt{gcd}(\mathtt{m}, \mathtt{n}) \mid \mathtt{m}$ *and* $\mathtt{gcd}(\mathtt{m}, \mathtt{n}) \mid \mathtt{n}$*, and*

(ii) *for all positive integers* $\mathtt{d}$ *such that* $\mathtt{d} \mid \mathtt{m}$ *and* $\mathtt{d} \mid \mathtt{n}$ *it necessarily follows that* $\mathtt{d} \mid \mathtt{gcd}(\mathtt{m}, \mathtt{n})$*.*

PROOF:


gcd(m, n)
m = q · n + r
q > 0, 0 < r < n
n|m
0<m<n
n
gcd(n, r)
gcd(n, m)
r|n
n = q′ · r + r′
q′ > 0, 0 < r′ < r
r
gcd(r, r′)

Fractions in lowest terms

```
fun lowterms( m , n )
  = let
      val gcdval = gcd( m , n )
    in
      ( m div gcdval , n div gcdval )
    end
```

Some fundamental properties of gcds

Lemma 80 *For all positive integers* l, m, *and* n,

1. ***(Commutativity)*** $\gcd(\mathrm{m},\mathrm{n}) = \gcd(\mathrm{n},\mathrm{m})$,
2. ***(Associativity)*** $\gcd\big(\mathrm{l},\gcd(\mathrm{m},\mathrm{n})\big) = \gcd(\gcd(\mathrm{l},\mathrm{m}),\mathrm{n})$,
3. ***(Linearity)***[a] $\gcd(\mathrm{l}\cdot\mathrm{m},\mathrm{l}\cdot\mathrm{n}) = \mathrm{l}\cdot\gcd(\mathrm{m},\mathrm{n})$.

PROOF:

[a] Aka (Distributivity).

Coprimality

Definition 81 *Two natural numbers are said to be* coprime *whenever their greatest common divisor is* 1.

Euclid's Theorem

Theorem 82 *For positive integers* k, m, *and* n, *if* $k \mid (m \cdot n)$ *and* $\gcd(k, m) = 1$ *then* $k \mid n$.

PROOF:

Corollary 83 (Euclid's Theorem) *For positive integers* $\mathfrak{m}$ *and* $\mathfrak{n}$*, and prime* $\mathfrak{p}$*, if* $\mathfrak{p} \mid (\mathfrak{m} \cdot \mathfrak{n})$ *then* $\mathfrak{p} \mid \mathfrak{m}$ *or* $\mathfrak{p} \mid \mathfrak{n}$*.*

Now, the second part of Fermat's Little Theorem follows as a corollary of the first part and Euclid's Theorem.

PROOF:

Fields of modular arithmetic

Corollary 85 *For prime p, every non-zero element i of $\mathbb{Z}_p$ has $[i^{p-2}]_p$ as multiplicative inverse. Hence, $\mathbb{Z}_p$ is what in the mathematical jargon is referred to as a field.*

Extended Euclid's Algorithm

Example 86

$$
\begin{array}{rl||rcrcr||}
 & \gcd(34,13) & 34 & = & 2\cdot & 13 & + & 8 \\
= & \gcd(13,8) & 13 & = & 1\cdot & 8 & + & 5 \\
= & \gcd(8,5) & 8 & = & 1\cdot & 5 & + & 3 \\
= & \gcd(5,3) & 5 & = & 1\cdot & 3 & + & 2 \\
= & \gcd(3,2) & 3 & = & 1\cdot & 2 & + & 1 \\
= & \gcd(2,1) & 2 & = & 2\cdot & 1 & + & 0 \\
= & 1 & & & & & & \\
\end{array}
$$

Extended Euclid's Algorithm

Example 86

$$
\begin{array}{rl||rcrcr||rcrcr}
 & \gcd(34,13) & 34 & = & 2\cdot & 13 & + & 8 & 8 & = & 34 & -2\cdot & 13 \\
= & \gcd(13,8) & 13 & = & 1\cdot & 8 & + & 5 & 5 & = & 13 & -1\cdot & 8 \\
= & \gcd(8,5) & 8 & = & 1\cdot & 5 & + & 3 & 3 & = & 8 & -1\cdot & 5 \\
= & \gcd(5,3) & 5 & = & 1\cdot & 3 & + & 2 & 2 & = & 5 & -1\cdot & 3 \\
= & \gcd(3,2) & 3 & = & 1\cdot & 2 & + & 1 & 1 & = & 3 & -1\cdot & 2 \\
= & \gcd(2,1) & 2 & = & 2\cdot & 1 & + & 0 & & & & & \\
= & 1 & & & & & & & & & & &
\end{array}
$$

$$
\begin{array}{lll||rrr}
 & \gcd(34,13) & 8 = & 34 & -2\cdot & 13 \\
= & \gcd(13,8) & 5 = & 13 & -1\cdot & 8 \\
 & & & & & \\
= & \gcd(8,5) & 3 = & 8 & -1\cdot & 5 \\
 & & & & & \\
= & \gcd(5,3) & 2 = & 5 & -1\cdot & 3 \\
 & & & & & \\
= & \gcd(3,2) & 1 = & 3 & -1\cdot & 2
\end{array}
$$

$$
\begin{array}{lll||rrcc}
 & \gcd(34,13) & & 8 = & 34 & -2\cdot & 13 \\
= & \gcd(13,8) & & 5 = & 13 & -1\cdot & 8 \\
 & & & = & 13 & -1\cdot & \overbrace{(34-2\cdot 13)} \\
 & & & = & -1\cdot 34+3\cdot 13 & & \\
= & \gcd(8,5) & & 3 = & 8 & -1\cdot & 5 \\
 & & & & & & \\
= & \gcd(5,3) & & 2 = & 5 & -1\cdot & 3 \\
 & & & & & & \\
= & \gcd(3,2) & & 1 = & 3 & -1\cdot & 2
\end{array}
$$

$$
\begin{array}{lll||lrcl}
 & \gcd(34,13) & & 8 = & 34 & -2\cdot & 13 \\
= & \gcd(13,8) & & 5 = & 13 & -1\cdot & \overbrace{8}^{(34-2\cdot 13)} \\
 & & & = & 13 & -1\cdot & (34-2\cdot 13) \\
 & & & = & -1\cdot 34+3\cdot 13 & & \\
= & \gcd(8,5) & & 3 = & 8 & -1\cdot & 5 \\
 & & & = & \overbrace{(34-2\cdot 13)}^{8} & -1\cdot & \overbrace{(-1\cdot 34+3\cdot 13)}^{5} \\
 & & & = & 2\cdot 34+(-5)\cdot 13 & & \\
= & \gcd(5,3) & & 2 = & 5 & -1\cdot & 3 \\
 & & & & & & \\
 & & & & & & \\
= & \gcd(3,2) & & 1 = & 3 & -1\cdot & 2 \\
 & & & & & &
\end{array}
$$

$$
\begin{array}{rl||rrcl}
 & \gcd(34,13) & 8 = & 34 & -2\cdot & 13 \\
= & \gcd(13,8) & 5 = & 13 & -1\cdot & 8 \\
 & & = & 13 & -1\cdot & \overbrace{(34-2\cdot 13)} \\
 & & = & -1\cdot 34+3\cdot 13 & & \\
= & \gcd(8,5) & 3 = & 8 & -1\cdot & 5 \\
 & & = & \overbrace{(34-2\cdot 13)} & -1\cdot & \overbrace{(-1\cdot 34+3\cdot 13)} \\
 & & = & 2\cdot 34+(-5)\cdot 13 & & \\
= & \gcd(5,3) & 2 = & 5 & -1\cdot & 3 \\
 & & = & \overbrace{-1\cdot 34+3\cdot 13} & -1\cdot & \overbrace{(2\cdot 34+(-5)\cdot 13)} \\
 & & = & -3\cdot 34+8\cdot 13 & & \\
= & \gcd(3,2) & 1 = & 3 & -1\cdot & 2
\end{array}
$$

$$
\begin{array}{rl||rcrcl}
 & \gcd(34,13) & 8 = & 34 & -2\cdot & 13 \\
= & \gcd(13,8) & 5 = & 13 & -1\cdot & 8 \\
 & & = & 13 & -1\cdot & \overbrace{(34-2\cdot 13)} \\
 & & = & -1\cdot 34+3\cdot 13 & & \\
= & \gcd(8,5) & 3 = & 8 & -1\cdot & 5 \\
 & & = & \overbrace{(34-2\cdot 13)} & -1\cdot & \overbrace{(-1\cdot 34+3\cdot 13)} \\
 & & = & 2\cdot 34+(-5)\cdot 13 & & \\
= & \gcd(5,3) & 2 = & 5 & -1\cdot & 3 \\
 & & = & \overbrace{-1\cdot 34+3\cdot 13} & -1\cdot & \overbrace{(2\cdot 34+(-5)\cdot 13)} \\
 & & = & -3\cdot 34+8\cdot 13 & & \\
= & \gcd(3,2) & 1 = & 3 & -1\cdot & 2 \\
 & & = & \overbrace{(2\cdot 34+(-5)\cdot 13)} & -1\cdot & \overbrace{(-3\cdot 34+8\cdot 13))} \\
 & & = & 5\cdot 34+(-13)\cdot 13 & &
\end{array}
$$

Integer linear combinations

Definition 64[a] An integer r is said to be a *linear combination* of a pair of integers m and n whenever

> there exist a pair of integers s and t, referred to as the *coefficients* of the linear combination, such that
>
> $$\begin{bmatrix} s & t \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r \ ;$$
>
> that is
>
> $$s \cdot m + t \cdot n = r \ .$$

[a] See page 195.

Theorem 87 *For all positive integers* m *and* n*,*

1. $\gcd(\mathrm{m},\mathrm{n})$ *is a linear combination of* m *and* n*, and*
2. *a pair* $\mathrm{lc}_1(\mathrm{m},\mathrm{n})$, $\mathrm{lc}_2(\mathrm{m},\mathrm{n})$ *of integer coefficients for it, i.e. such that*

$$\left[\begin{array}{cc} \mathrm{lc}_1(\mathrm{m},\mathrm{n}) & \mathrm{lc}_2(\mathrm{m},\mathrm{n}) \end{array}\right] \cdot \left[\begin{array}{c} \mathrm{m} \\ \mathrm{n} \end{array}\right] = \gcd(\mathrm{m},\mathrm{n}) \quad ,$$

can be efficiently computed.

Proposition 88 *For all integers* $\mathfrak{m}$ *and* $\mathfrak{n}$*,*

1. $\begin{bmatrix} ?_1 & ?_2 \end{bmatrix} \cdot \begin{bmatrix} \mathfrak{m} \\ \mathfrak{n} \end{bmatrix} = \mathfrak{m} \quad \wedge \quad \begin{bmatrix} ?_1 & ?_2 \end{bmatrix} \cdot \begin{bmatrix} \mathfrak{m} \\ \mathfrak{n} \end{bmatrix} = \mathfrak{n}$ *;*

Proposition 88 *For all integers* m *and* n,

1. $\begin{bmatrix} ?_1 & ?_2 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = m \ \wedge \ \begin{bmatrix} ?_1 & ?_2 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = n$;

2. *for all integers* s_1, t_1, r_1 *and* s_2, t_2, r_2,

$$\begin{bmatrix} s_1 & t_1 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r_1 \ \wedge \ \begin{bmatrix} s_2 & t_2 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r_2$$

implies

$$\begin{bmatrix} ?_1 & ?_2 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r_1 + r_2 \ ;$$

Proposition 88 *For all integers* m *and* n,

1. $\begin{bmatrix} ?_1 & ?_2 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = m \ \wedge \ \begin{bmatrix} ?_1 & ?_2 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = n$;

2. *for all integers* s_1, t_1, r_1 *and* s_2, t_2, r_2,

   $$\begin{bmatrix} s_1 & t_1 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r_1 \ \wedge \ \begin{bmatrix} s_2 & t_2 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r_2$$

   implies

   $$\begin{bmatrix} ?_1 & ?_2 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r_1 + r_2 \ ;$$

3. *for all integers* k *and* s, t, r,

   $$\begin{bmatrix} s & t \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r \ \textit{implies} \ \begin{bmatrix} ?_1 & ?_2 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = k \cdot r \ .$$

We extend Euclid's Algorithm $\mathtt{gcd}(\mathrm{m}, \mathrm{n})$ from computing on pairs of positive integers to computing on pairs of triples $((\mathrm{s}, \mathrm{t}), \mathrm{r})$ with s, t integers and r a positive integer satisfying the invariant that s, t are coefficientes expressing r as an integer linear combination of m and n.

gcd

```
fun  gcd( m , n )
= let
    fun  gcditer(          r1   ,  c as          r2  )
    = let
        val (q,r) = divalg(r1,r2)   (* r = r1-q*r2 *)
      in
        if r = 0
        then  c
        else  gcditer(  c ,                   r  )
      end
  in
     gcditer(         m  ,        n  )
  end
```

egcd

```
fun egcd( m , n )
= let
    fun egcditer( ((s1,t1),r1) , lc as ((s2,t2),r2) )
    = let
        val (q,r) = divalg(r1,r2)   (* r = r1-q*r2 *)
      in
        if r = 0
        then lc
        else egcditer( lc , ((s1-q*s2,t1-q*t2),r) )
      end
  in
    egcditer( ((1,0),m) , ((0,1),n) )
  end
```

```
fun gcd( m , n ) = #2( egcd( m , n ) )

fun lc1( m , n ) = #1( #1( egcd( m , n ) ) )

fun lc2( m , n ) = #2( #1( egcd( m , n ) ) )
```

Multiplicative inverses in modular arithmetic

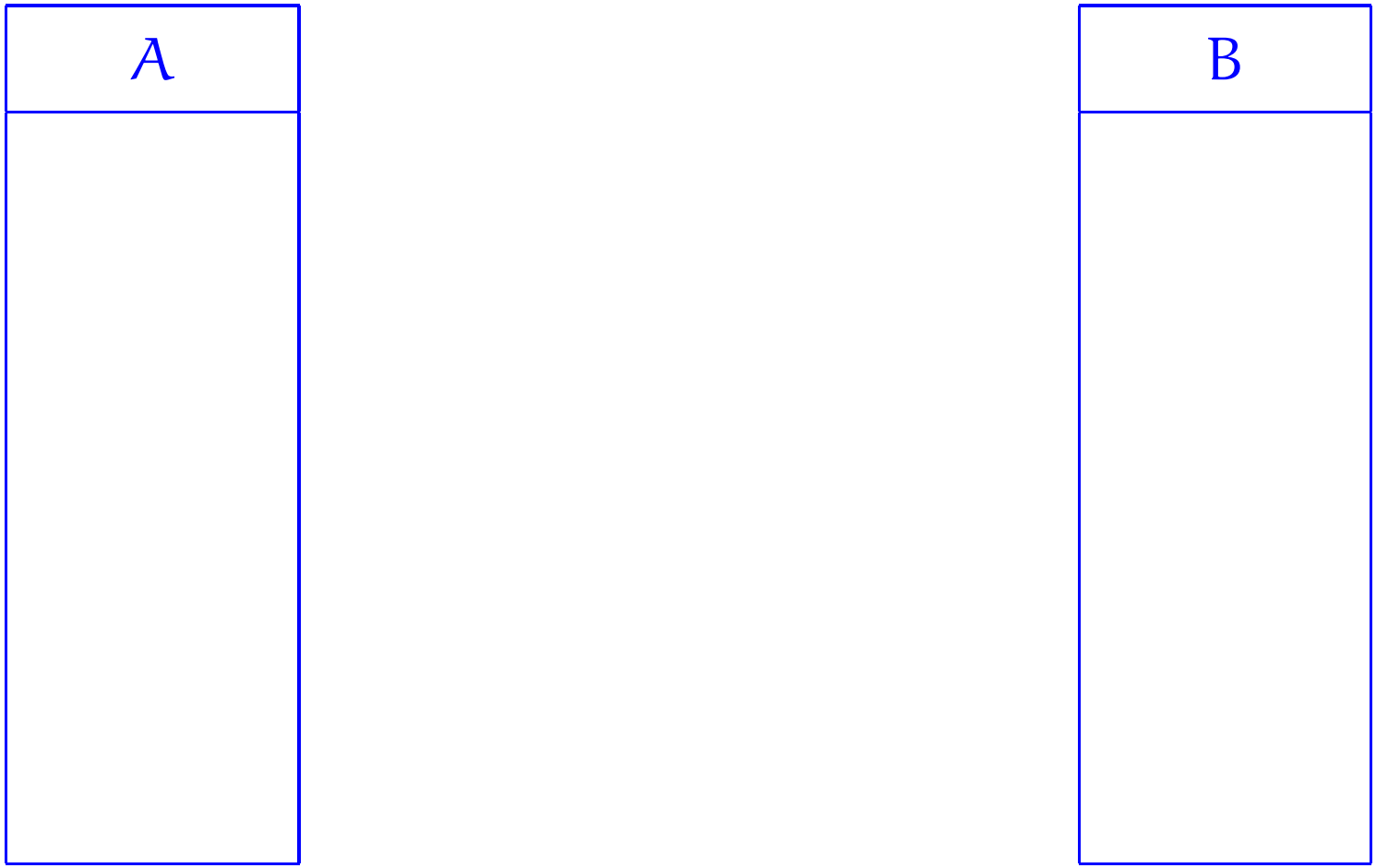
Corollary 92 *For all positive integers* m *and* n*,*

1. $\mathrm{n} \cdot \mathrm{lc}_2(\mathrm{m}, \mathrm{n}) \equiv \gcd(\mathrm{m}, \mathrm{n}) \pmod{\mathrm{m}}$*, and*
2. *whenever* $\gcd(\mathrm{m}, \mathrm{n}) = 1$*,*

   $\left[\mathrm{lc}_2(\mathrm{m}, \mathrm{n})\right]_{\mathrm{m}}$ *is the multiplicative inverse of* $[\mathrm{n}]_{\mathrm{m}}$ *in* $\mathbb{Z}_{\mathrm{m}}$.

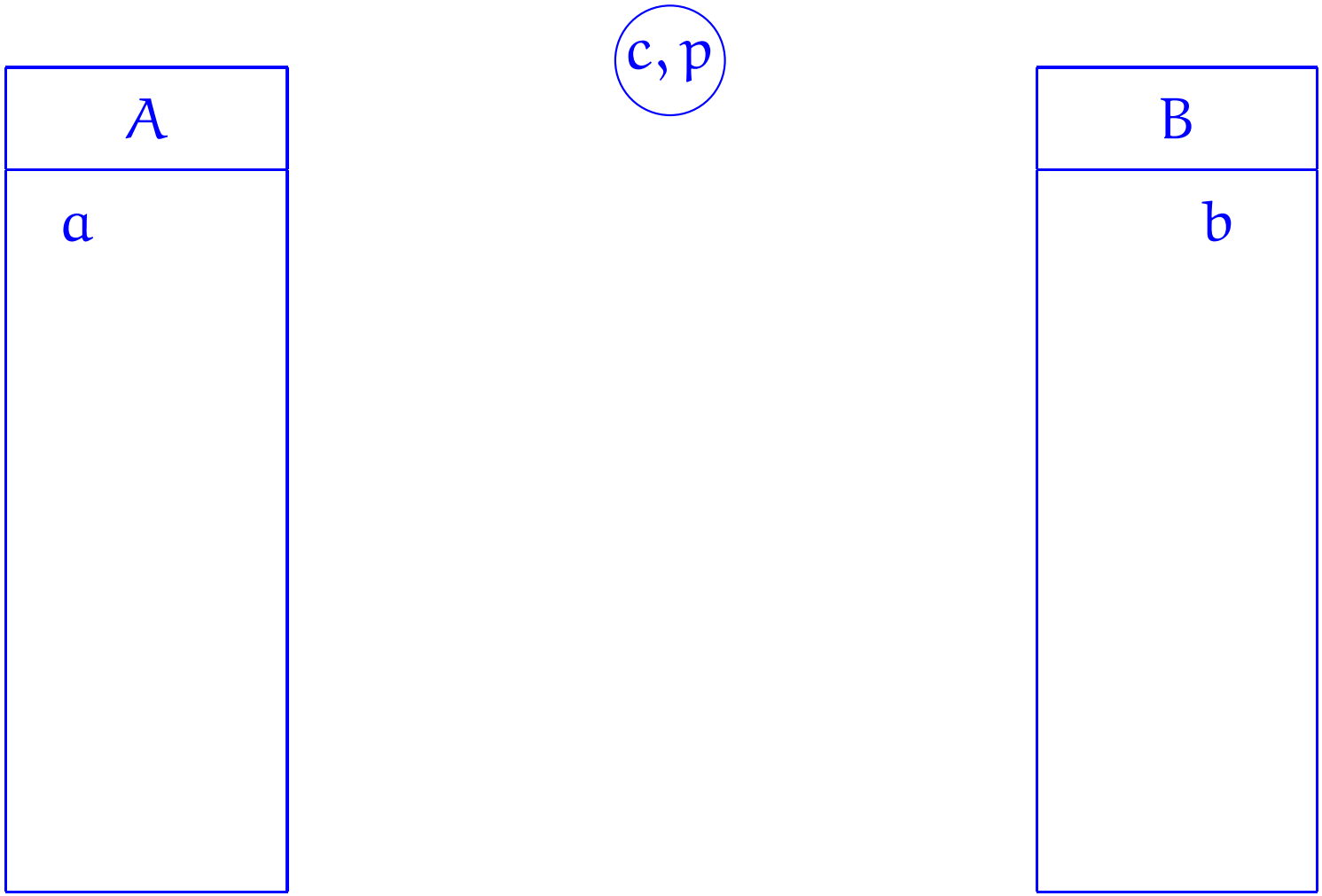
Diffie-Hellman cryptographic method

Shared secret key



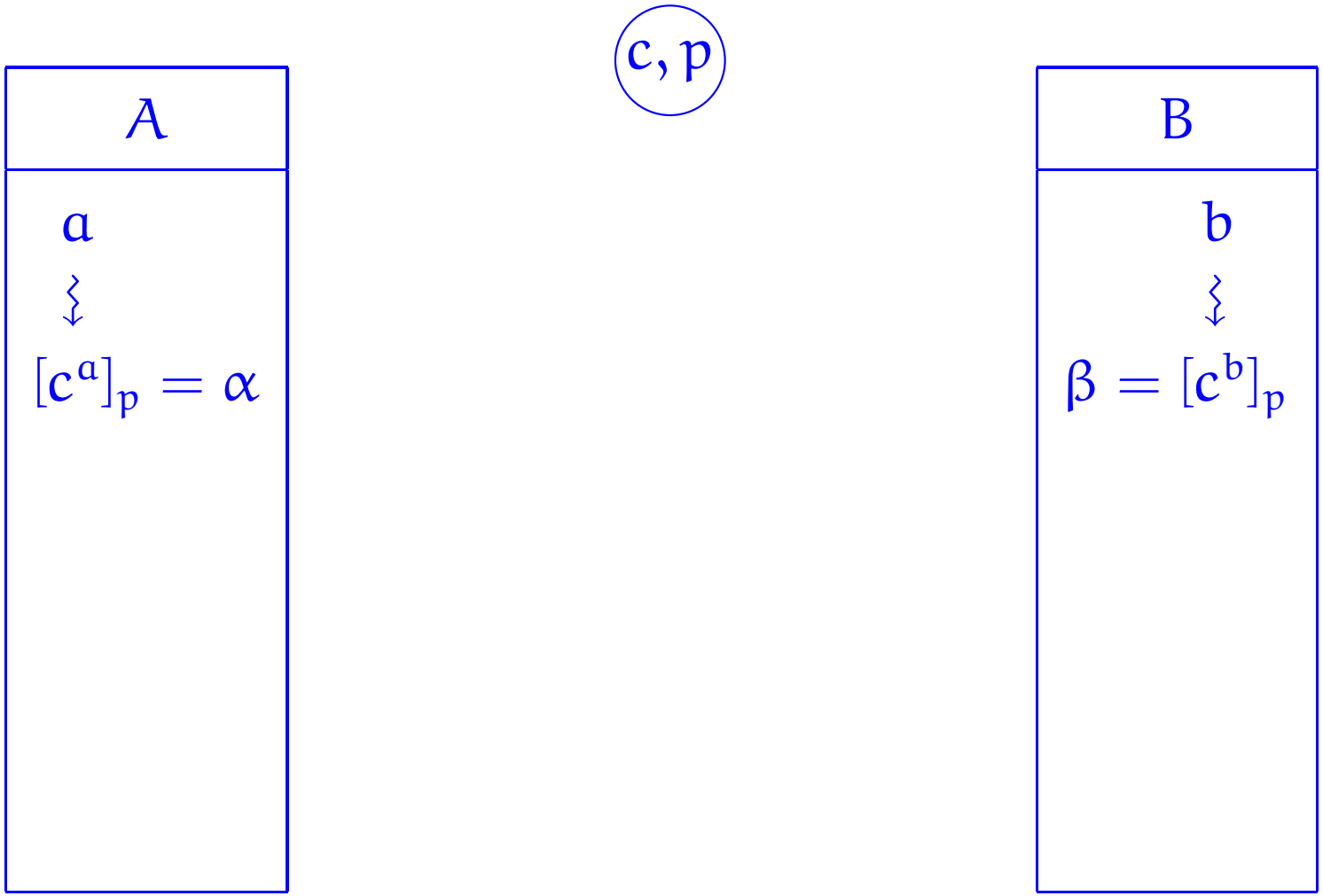
Diffie-Hellman cryptographic method

Shared secret key



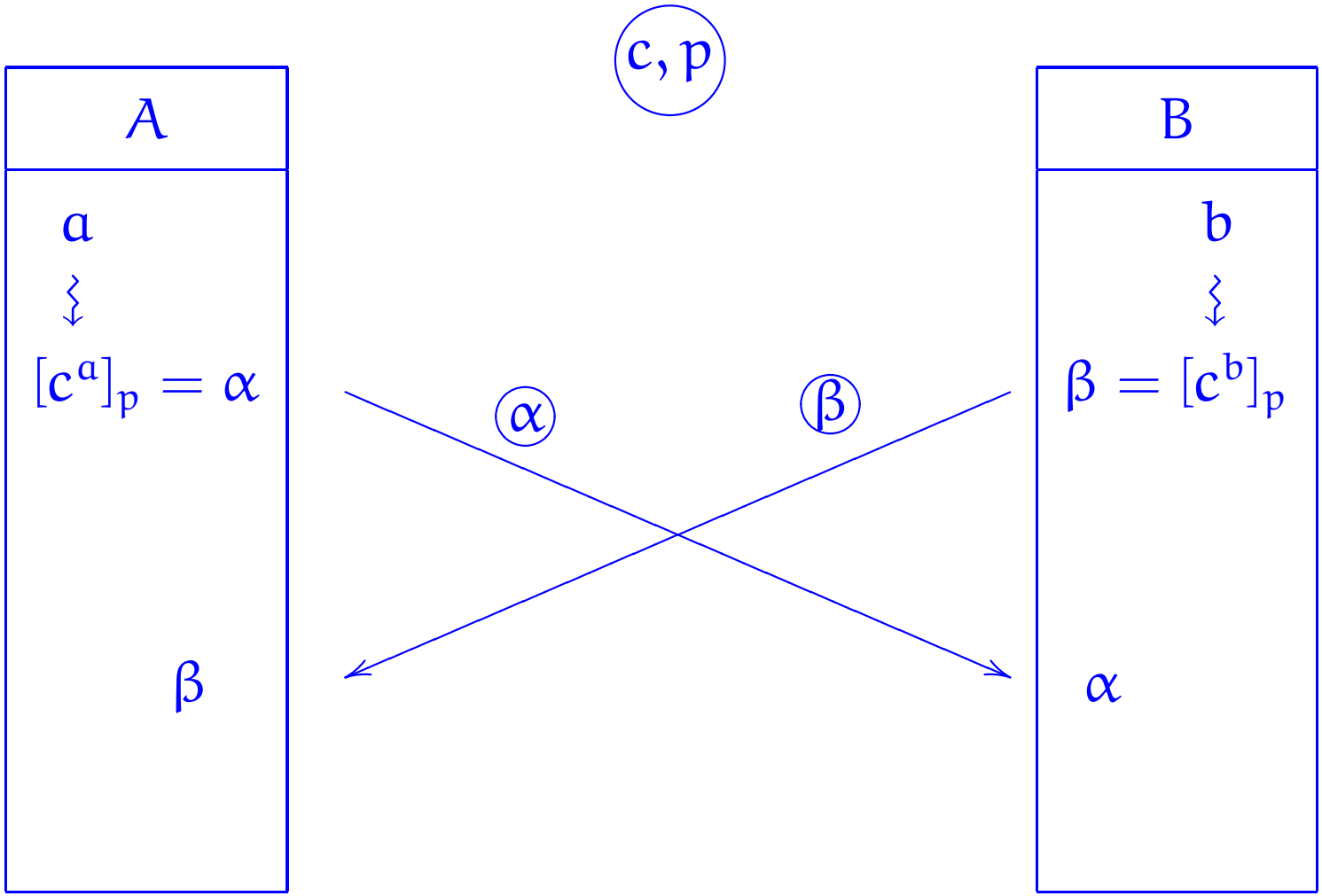
Diffie-Hellman cryptographic method

Shared secret key



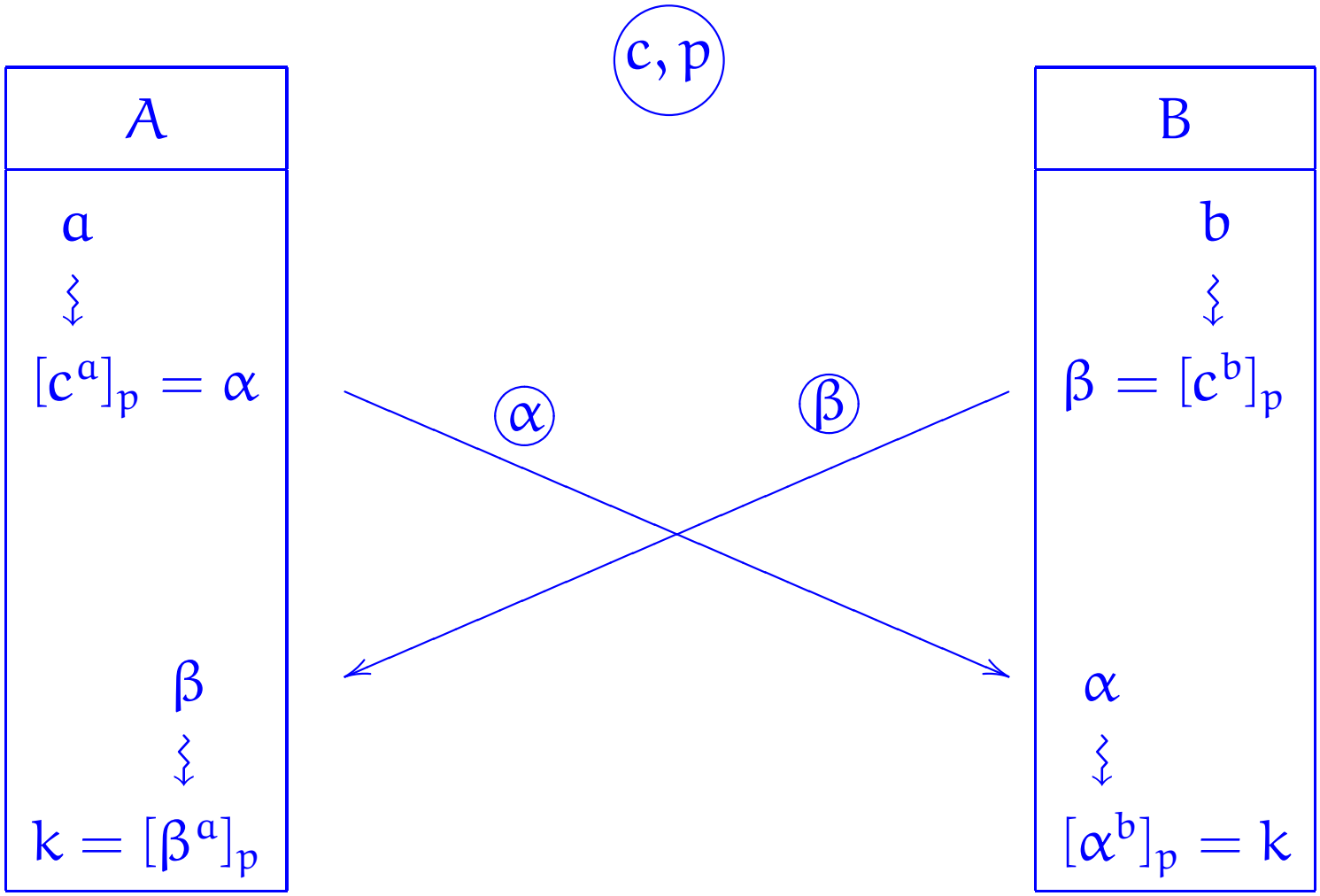
Diffie-Hellman cryptographic method

Shared secret key



Diffie-Hellman cryptographic method

Shared secret key



Key exchange

Mathematical modelling:

- Encrypt and decrypt by means of modular exponentiation:

$$[k^e]_p \qquad\qquad [\ell^d]_p$$

- Encrypting-decrypting have no effect:

By Fermat's Little Theorem,

$$k^{1+c\cdot(p-1)} \equiv k \pmod{p}$$

for every natural number c, integer k, and prime p.

- Consider d, e, p such that $e \cdot d = 1 + c \cdot (p-1)$; equivalently,

$$d \cdot e \equiv 1 \pmod{p-1} \ .$$

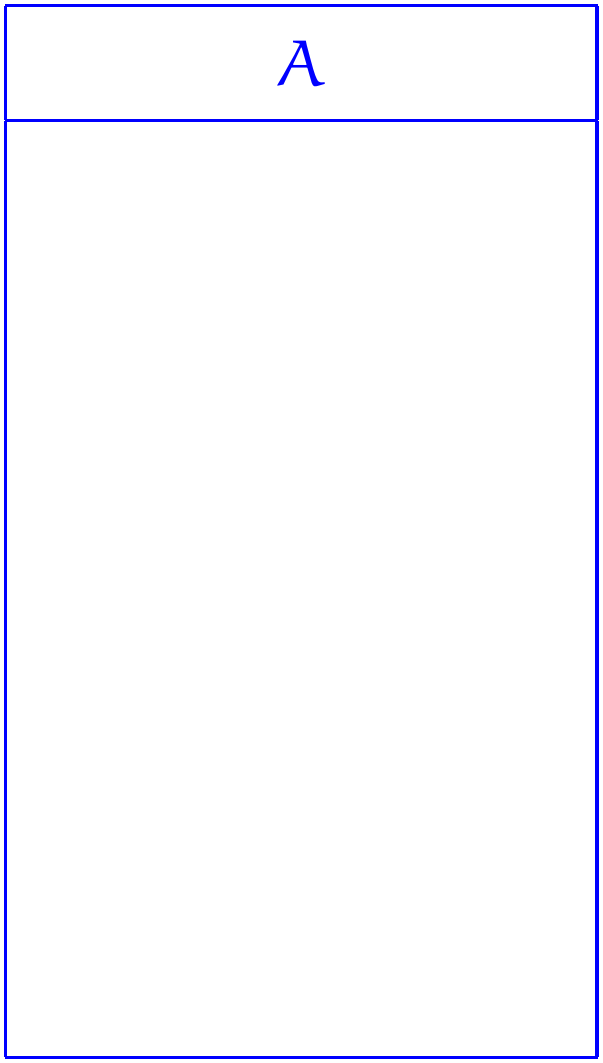
Lemma 93 *Let* p *be a prime and* e *a positive integer with* $\gcd(p-1, e) = 1$*. Define*

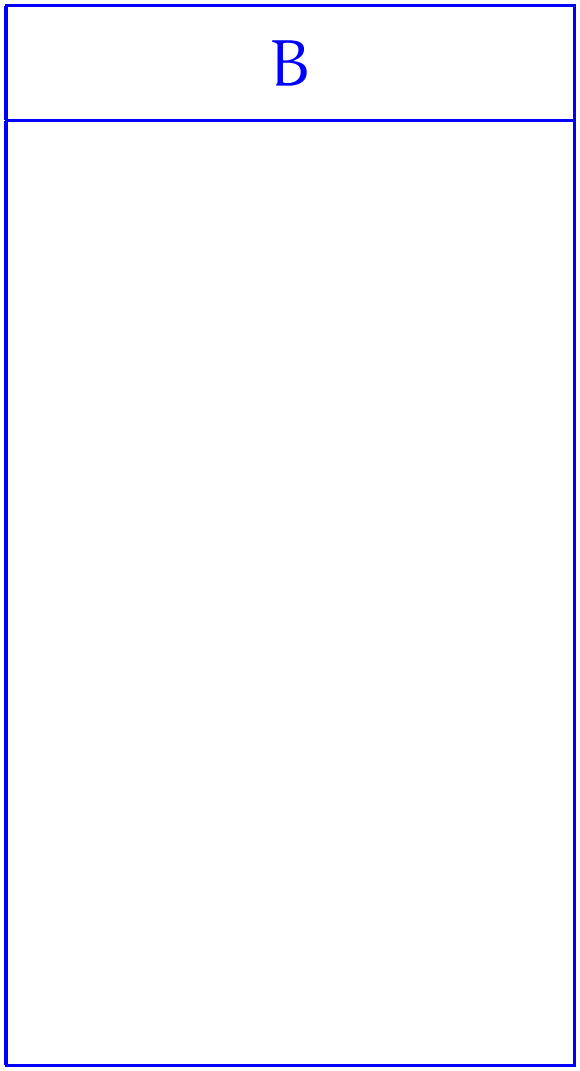
$$d = \left[\mathrm{lc}_2(p-1, e) \right]_{p-1} \ .$$

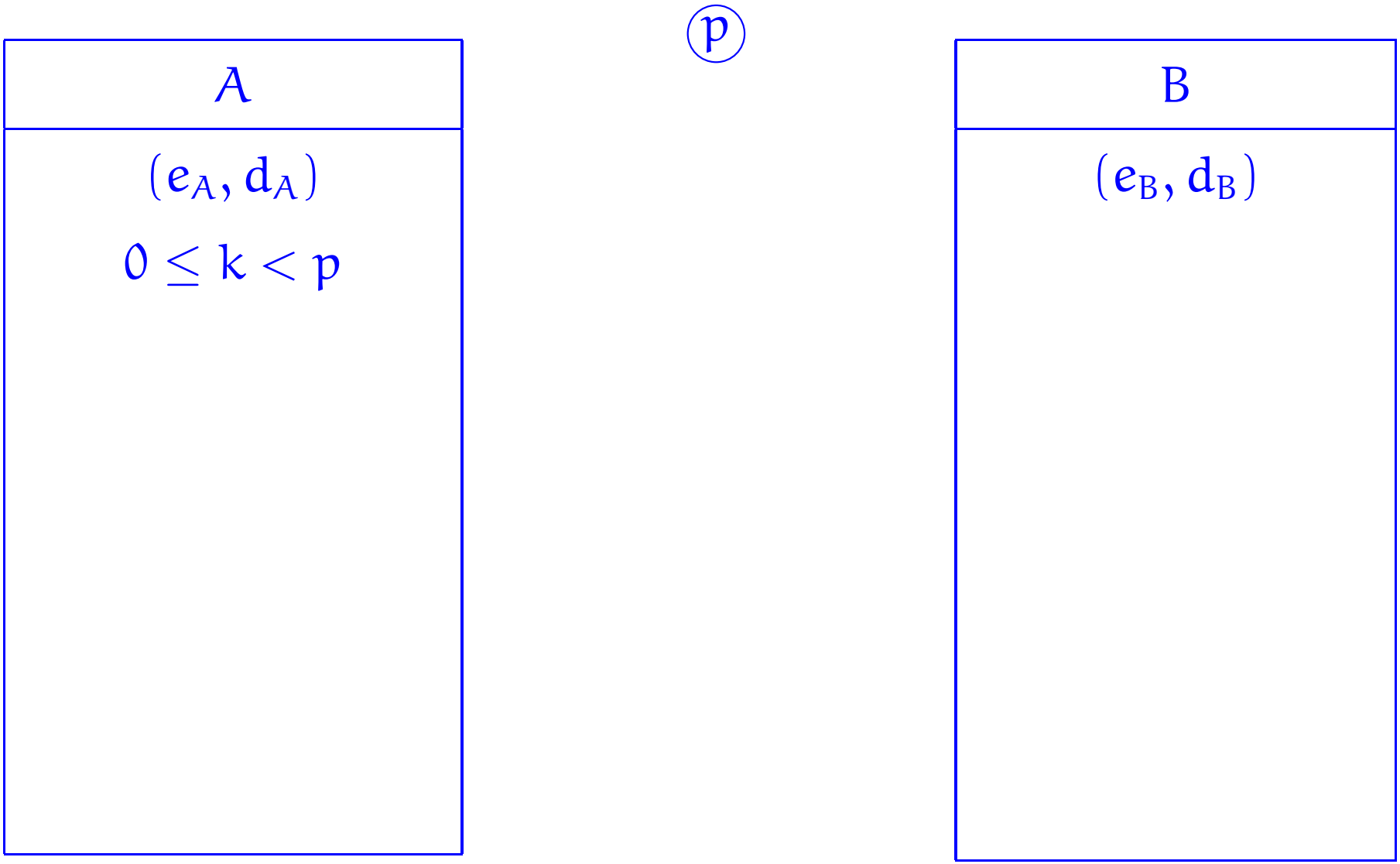
Then, for all integers k*,*

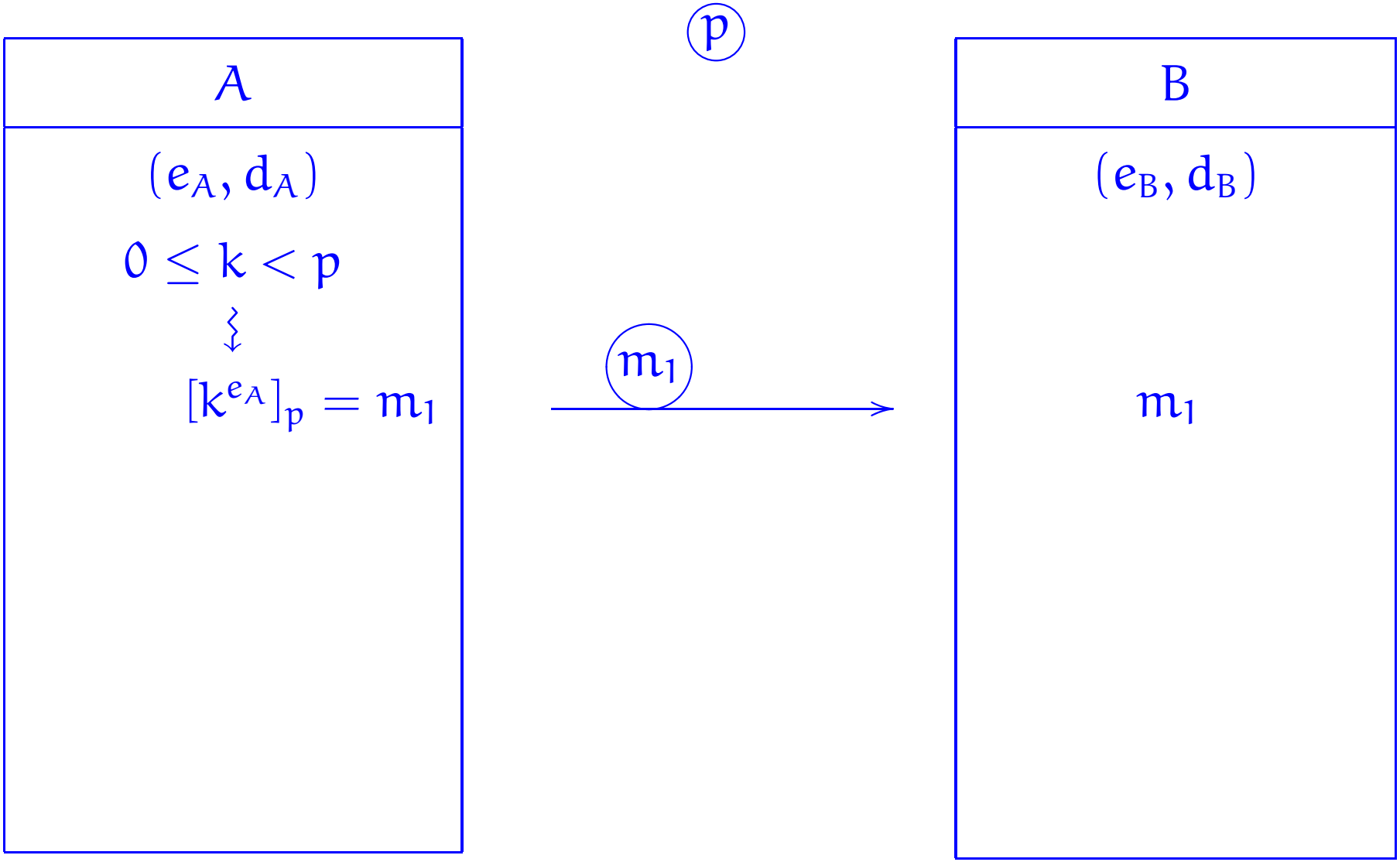
$$(k^e)^d \equiv k \pmod{p} \ .$$

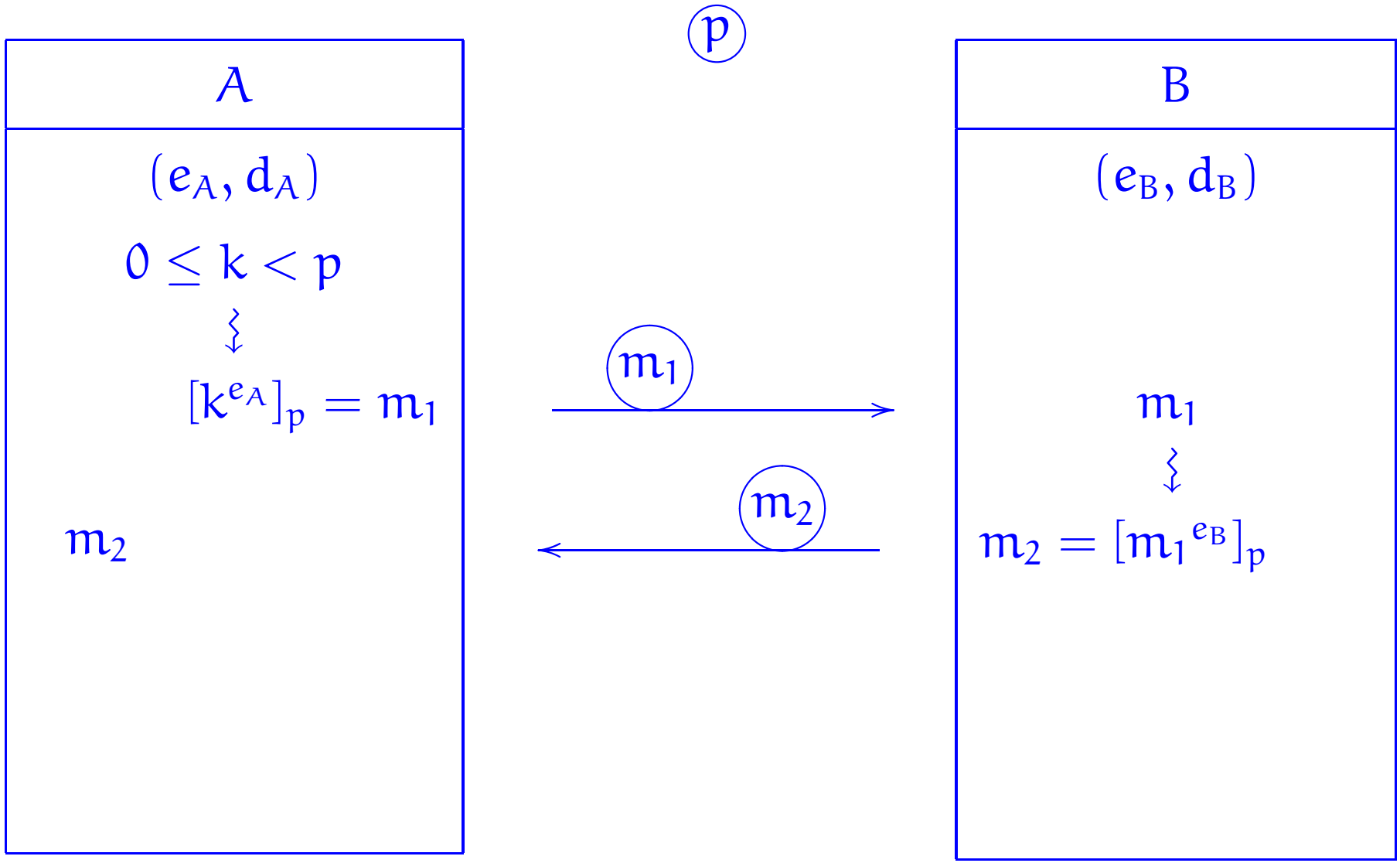
PROOF:

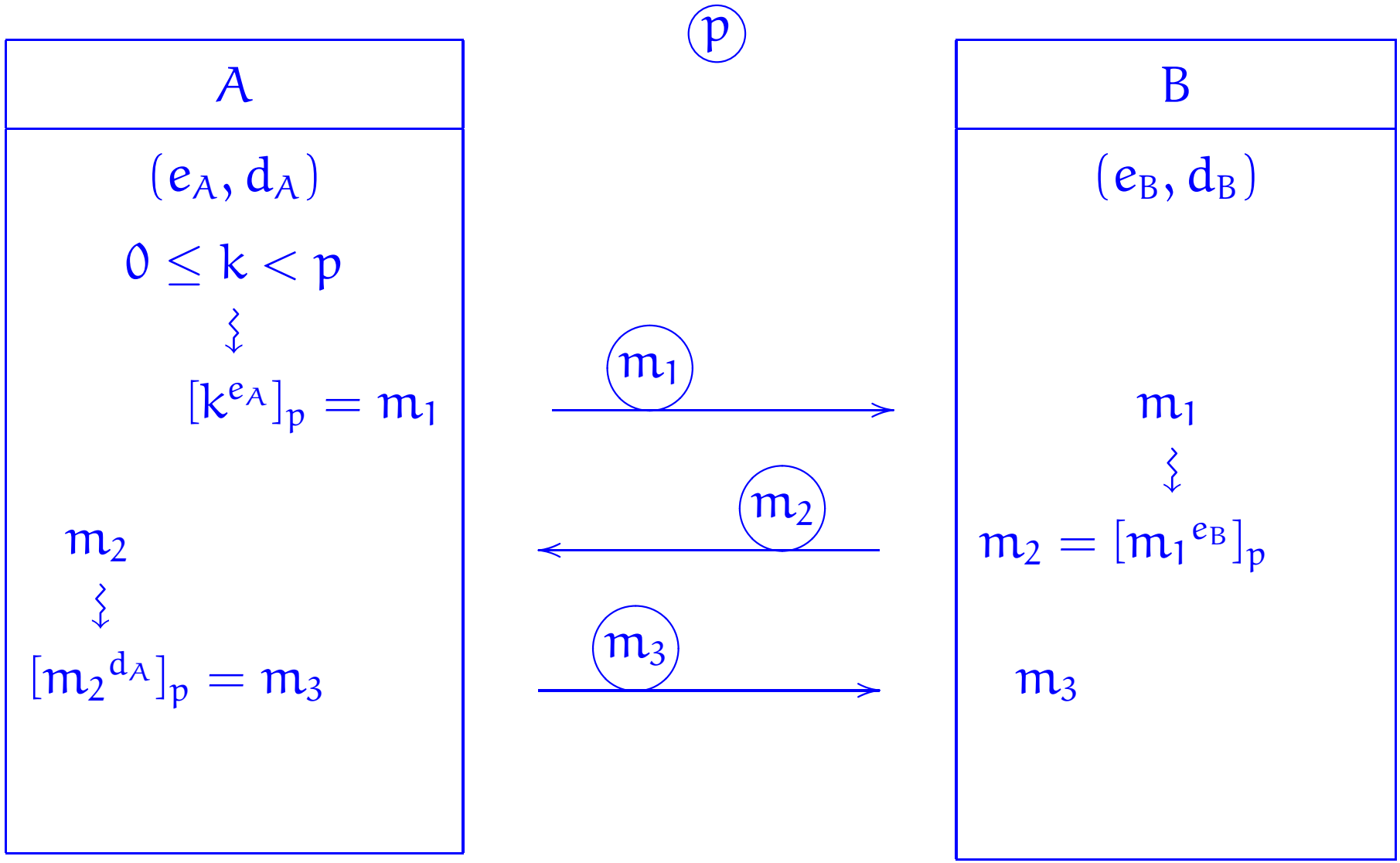

A

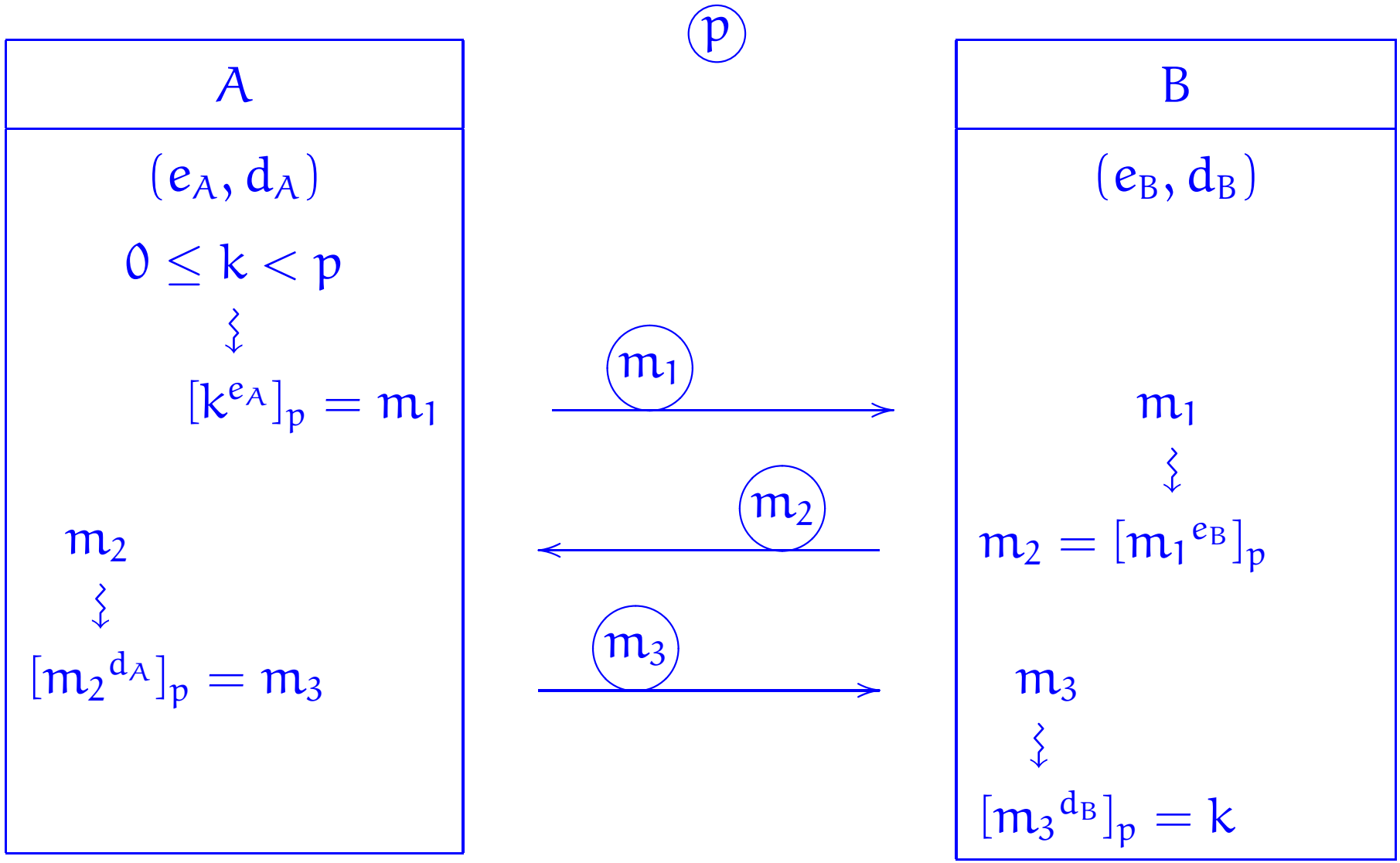

B


p
A
(e_A, d_A)
$0 \leq k < p$
B
(e_B, d_B)


p
A
(e_A, d_A)
$0 \leq k < p$
$[k^{e_A}]_p = m_1$
m_1
B
(e_B, d_B)
m_1


p
A
B
(e_A, d_A)
$0 \leq k < p$
$[k^{e_A}]_p = m_1$
m_2
m_1
m_2
m_1
$m_2 = [m_1{}^{e_B}]_p$


p
A
B
(e_A, d_A)
$0 \leq k < p$
$[k^{e_A}]_p = m_1$
m_2
$[m_2{}^{d_A}]_p = m_3$
m_1
m_2
m_3
m_1
$m_2 = [m_1{}^{e_B}]_p$
m_3
(e_B, d_B)


p
A
B
(e_A, d_A)
$0 \leq k < p$
$[k^{e_A}]_p = m_1$
m_2
$[m_2{}^{d_A}]_p = m_3$
m_1
m_2
m_3
(e_B, d_B)
m_1
$m_2 = [m_1{}^{e_B}]_p$
m_3
$[m_3{}^{d_B}]_p = k$

Natural Numbers and mathematical induction

We have mentioned in passing that the natural numbers are generated from zero by succesive increments. This is in fact the defining property of the set of natural numbers, and endows it with a very important and powerful reasoning principle, that of *Mathematical Induction*, for establishing universal properties of natural numbers.

Principle of Induction

Let $P(m)$ be a statement for m ranging over the set of natural numbers $\mathbb{N}$.

If

- the statement $P(0)$ holds, and
- the statement

  $$\forall n \in \mathbb{N}.\ \big(\ P(n) \implies P(n+1)\ \big)$$

  also holds

then

- the statement

  $$\forall m \in \mathbb{N}.\, P(m)$$

  holds.

Binomial Theorem

Theorem 29 *For all* $n \in \mathbb{N}$,

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} \cdot x^{n-k} \cdot y^k \quad .$$

PROOF:

Principle of Induction

from basis ℓ

Let $P(m)$ be a statement for m ranging over the natural numbers greater than or equal a fixed natural number ℓ. If

- $P(\ell)$ holds, and
- $\forall\, n \geq \ell$ in $\mathbb{N}$. $\big(\, P(n) \implies P(n+1) \,\big)$ also holds

then

- $\forall\, m \geq \ell$ in $\mathbb{N}$. $P(m)$ holds.

Principle of Strong Induction

from basis ℓ and Induction Hypothesis $P(m)$.

Let $P(m)$ be a statement for m ranging over the natural numbers greater than or equal a fixed natural number ℓ. If both

- $P(\ell)$ and
- $\forall\, n \geq \ell$ in $\mathbb{N}.\ \Big(\ \big(\forall\, k \in [\ell..n].\, P(k)\big)\ \Longrightarrow\ P(n+1)\ \Big)$

hold, then

- $\forall\, m \geq \ell$ in $\mathbb{N}.\, P(m)$ holds.

Fundamental Theorem of Arithmetic

Proposition 95 *Every positive integer greater than or equal* 2 *is a prime or a product of primes.*

PROOF:

Theorem 96 (Fundamental Theorem of Arithmetic) *For every positive integer* $\mathfrak{n}$ *there is a unique finite ordered sequence of primes* $(\mathfrak{p}_1 \leq \cdots \leq \mathfrak{p}_\ell)$ *with* $\ell \in \mathbb{N}$ *such that*

$$\mathfrak{n} = \prod(\mathfrak{p}_1, \ldots, \mathfrak{p}_\ell) \ .$$

PROOF:

Euclid's infinitude of primes

Theorem 99 *The set of primes is infinite.*

PROOF:

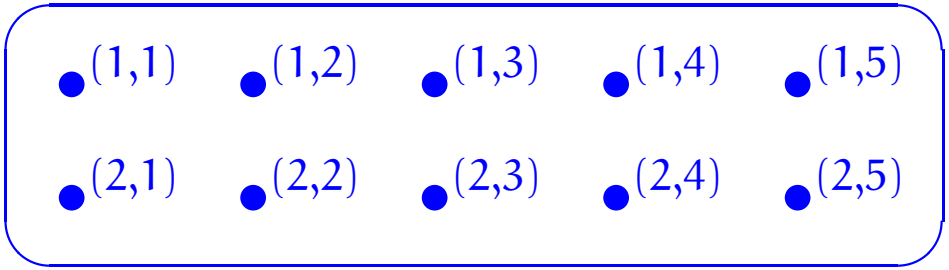
Sets

Objectives

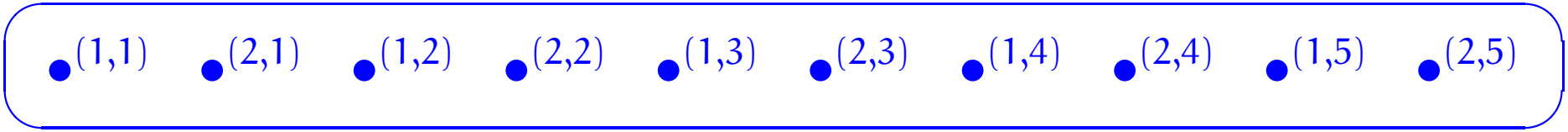
To introduce the basics of the theory of sets and some of its uses.

Abstract sets

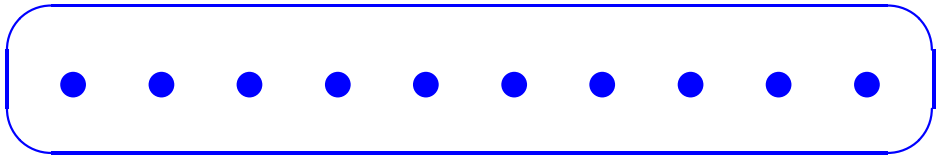
It has been said that a set is like a mental "bag of dots", except of course that the bag has no shape; thus,



may be a convenient way of picturing a certain set for some considerations, but what is apparently the same set may be pictured as



or even simply as



for other considerations.

Naive Set Theory

We are not going to be formally studying Set Theory here; rather, we will be *naively* looking at ubiquituous structures that are available within it.

Set membership

We write $\in$ for the *membership predicate*; so that

$x \in A$ stands for x is an element of A .

We further write

$x \notin A$ for $\neg(x \in A)$.

Example: $0 \in \{0, 1\}$ and $1 \notin \{0\}$ are true statements.

Extensionality axiom

Two sets are equal if they have the same elements.

Thus,

$$\forall \text{ sets } A, B.\ A = B \iff (\ \forall x.\, x \in A \iff x \in B\ )\quad .$$

Example:

$$\{0\} \neq \{0,1\} = \{1,0\} \neq \{2\} = \{2,2\}$$

Proposition 100 *For* $b, c \in \mathbb{R}$, *let*

$$\begin{aligned} A &= \{x \in \mathbb{C} \mid x^2 - 2bx + c = 0\} \\ B &= \{b + \sqrt{b^2 - c}, b - \sqrt{b^2 - c}\} \\ C &= \{b\} \end{aligned}$$

Then,

1. $A = B$, *and*
2. $B = C \iff b^2 = c$.

Subsets and supersets

Lemma 103

1. *Reflexivity.*

   For all sets A, $\mathrm{A} \subseteq \mathrm{A}$.

2. *Transitivity.*

   For all sets A, B, C, $(\mathrm{A} \subseteq \mathrm{B} \land \mathrm{B} \subseteq \mathrm{C}) \implies \mathrm{A} \subseteq \mathrm{C}$.

3. *Antisymmetry.*

   For all sets A, B, $(\mathrm{A} \subseteq \mathrm{B} \land \mathrm{B} \subseteq \mathrm{A}) \implies \mathrm{A} = \mathrm{B}$.

Separation principle

For any set A and any definable property P, there is a set containing precisely those elements of A for which the property P holds.

$$\{ x \in A \mid P(x) \}$$

Russell's paradox

Empty set

Set theory has an

empty set ,

typically denoted

$\emptyset$ or $\{\}$,

with no elements.

Cardinality

The *cardinality* of a set specifies its size. If this is a natural number, then the set is said to be *finite*.

Typical notations for the cardinality of a set S are $\#S$ or $|S|$.

Example:

$$\#\emptyset = 0$$

Finite sets

The *finite sets* are those with cardinality a natural number.

Example: For $n \in \mathbb{N}$,

$$[n] = \{x \in \mathbb{N} \mid x < n\}$$

is finite of cardinality n.

Powerset axiom

For any set, there is a set consisting of all its subsets.

$$\mathcal{P}(U)$$

$$\forall X.\ X \in \mathcal{P}(U) \iff X \subseteq U \quad .$$

NB: The powerset construction can be iterated. In particular,

$$\mathcal{F} \in \mathcal{P}\big(\mathcal{P}(\mathcal{U})\big) \iff \mathcal{F} \subseteq \mathcal{P}(\mathcal{U}) \ ;$$

that is, $\mathcal{F}$ is a set of subsets of $\mathcal{U}$, sometimes referred to as a *family*.

Example: The family $\mathcal{E} \subseteq \mathcal{P}\big([5]\big)$ consisting of the non-empty subsets of $[5] = \{0,1,2,3,4\}$ whose elements are even is

$$\mathcal{E} \ = \ \big\{\, \{0\}, \{2\}, \{4\}, \{0,2\}, \{0,4\}, \{2,4\}, \{0,2,4\} \,\big\} \ .$$

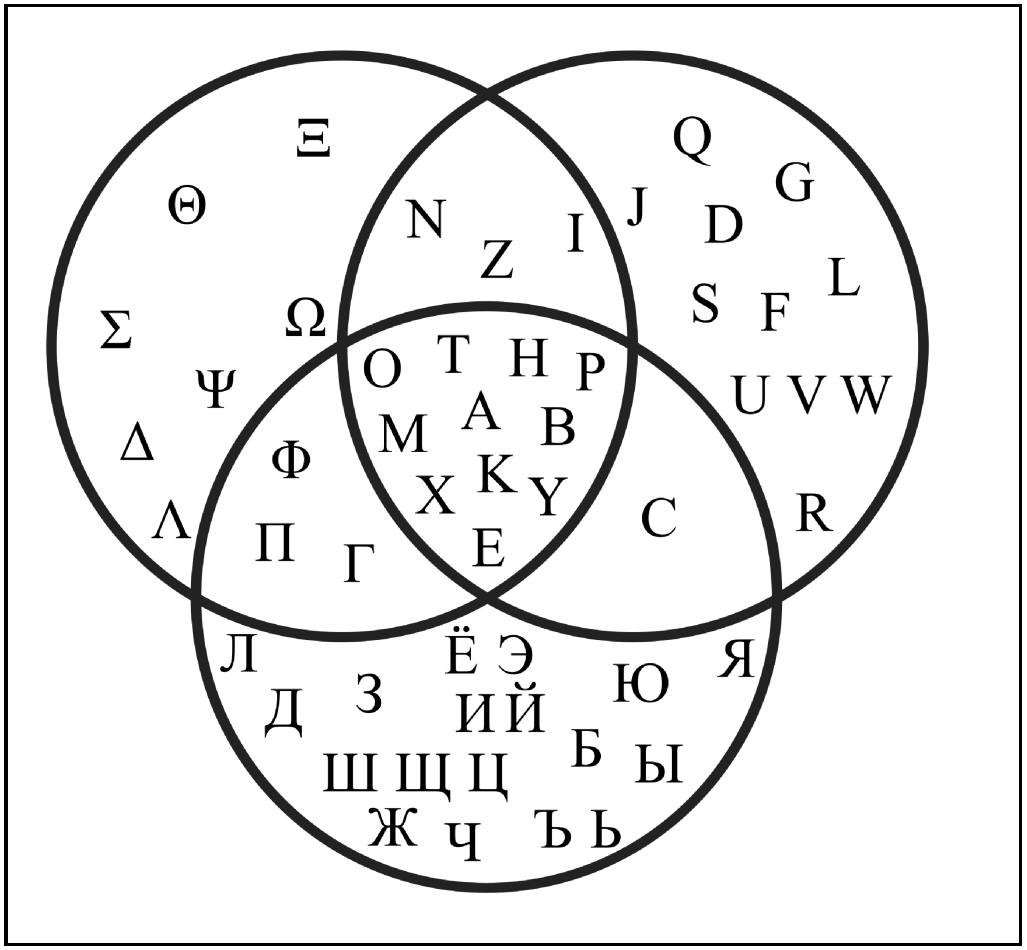
Hasse diagrams

Proposition 104 *For all finite sets* $\mathfrak{U}$*,*

$$\#\,\mathcal{P}(\mathfrak{U}) = 2^{\#\mathfrak{U}} \quad .$$

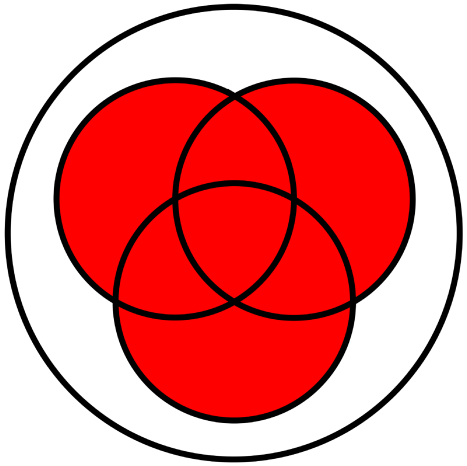
PROOF IDEA:

Venn diagrams[a]

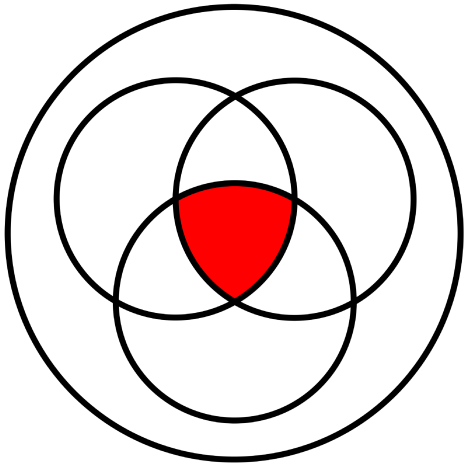


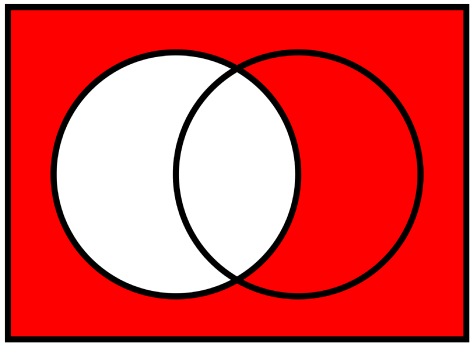
[a]From http://en.wikipedia.org/wiki/Intersection_(set_theory) .

Union



Intersection





Complement

The powerset Boolean algebra

$$(\quad \mathcal{P}(U) \ , \quad \emptyset \ , \quad U \ , \quad \cup \ , \quad \cap \ , \quad (\cdot)^c \quad)$$

For all $A, B \in \mathcal{P}(U)$,

$$A \cup B = \{x \in U \mid x \in A \vee x \in B\} \in \mathcal{P}(U)$$

$$A \cap B = \{x \in U \mid x \in A \wedge x \in B\} \in \mathcal{P}(U)$$

$$A^c = \{x \in U \mid \neg(x \in A)\} \in \mathcal{P}(U)$$

- The union operation $\cup$ and the intersection operation $\cap$ are associative, commutative, and idempotent.

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

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

- The union operation $\cup$ and the intersection operation $\cap$ are associative, commutative, and idempotent.

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

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

- The *empty set* $\emptyset$ is a neutral element for $\cup$ and the *universal set* $\mathcal{U}$ is a neutral element for $\cap$.

$$\emptyset \cup A = A = \mathcal{U} \cap A$$

- The empty set $\emptyset$ is an annihilator for $\cap$ and the universal set $\mathcal{U}$ is an annihilator for $\cup$.

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

$$\mathcal{U} \cup A = \mathcal{U}$$

- The empty set $\emptyset$ is an annihilator for $\cap$ and the universal set $\mathcal{U}$ is an annihilator for $\cup$.

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

$$\mathcal{U} \cup A = \mathcal{U}$$

- With respect to each other, the union operation $\cup$ and the intersection operation $\cap$ are distributive and absorptive.

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

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

- The complement operation $(\cdot)^c$ satisfies complementation laws.

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

Proposition 105 *Let* $\mathcal{U}$ *be a set and let* $A, B \in \mathcal{P}(\mathcal{U})$.

1. $\forall X \in \mathcal{P}(\mathcal{U}).\ A \cup B \subseteq X \iff \big(A \subseteq X \wedge B \subseteq X\big)$.

2. $\forall X \in \mathcal{P}(\mathcal{U}).\ X \subseteq A \cap B \iff \big(X \subseteq A \wedge X \subseteq B\big)$.

PROOF:

Corollary 106 *Let* U *be a set and let* $\mathrm{A}, \mathrm{B}, \mathrm{C} \in \mathcal{P}(\mathrm{U})$.

1. $\mathrm{C} = \mathrm{A} \cup \mathrm{B}$

iff

$$\left[\mathrm{A} \subseteq \mathrm{C} \wedge \mathrm{B} \subseteq \mathrm{C}\right]$$

$$\wedge$$

$$\left[\forall \mathrm{X} \in \mathcal{P}(\mathrm{U}).\ \left(\mathrm{A} \subseteq \mathrm{X} \wedge \mathrm{B} \subseteq \mathrm{X}\right) \implies \mathrm{C} \subseteq \mathrm{X}\right]$$

2. $\mathrm{C} = \mathrm{A} \cap \mathrm{B}$

iff

$$\left[\mathrm{C} \subseteq \mathrm{A} \wedge \mathrm{C} \subseteq \mathrm{B}\right]$$

$$\wedge$$

$$\left[\forall \mathrm{X} \in \mathcal{P}(\mathrm{U}).\ \left(\mathrm{X} \subseteq \mathrm{A} \wedge \mathrm{X} \subseteq \mathrm{B}\right) \implies \mathrm{X} \subseteq \mathrm{C}\right]$$

Sets and logic

$\mathcal{P}(\mathsf{U})$	$\{\,\mathbf{false}\,,\,\mathbf{true}\,\}$
$\emptyset$	**false**
U	**true**
$\cup$	$\vee$
$\cap$	$\wedge$
$(\cdot)^{\mathsf{c}}$	$\neg(\cdot)$

Pairing axiom

For every a and b, there is a set with a and b as its only elements.

$$\{a, b\}$$

defined by

$$\forall x.\, x \in \{a, b\} \iff (x = a \vee x = b)$$

NB The set $\{a, a\}$ is abbreviated as $\{a\}$, and referred to as a *singleton*.

Examples:

- $\#\{\emptyset\} = 1$
- $\#\{\{\emptyset\}\} = 1$
- $\#\{\emptyset, \{\emptyset\}\} = 2$

Proposition 107 *For all* a, b, c, x, y,

1. $\{x, y\} \subseteq \{a\} \implies x = y = a$
2. $\{c, x\} = \{c, y\} \implies x = y$

PROOF:

Ordered pairing

Notation:

$$(a, b) \quad \text{or} \quad \langle a, b \rangle$$

Fundamental property:

$$(a, b) = (x, y) \implies a = x \wedge b = y$$

A construction:

For every pair a and b,

$$\langle a, b \rangle = \{ \{ a \}, \{ a, b \} \}$$

defines an *ordered pairing* of a and b.

Proposition 108 (Fundamental property of ordered pairing)
For all a, b, x, y*,*

$$\langle a, b\rangle = \langle x, y\rangle \iff (a = x \wedge b = y) \quad .$$

PROOF:

Products

The *product* $A \times B$ of two sets A and B is the set

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

where

$$\forall a_1, a_2 \in A, b_1, b_2 \in B.$$
$$(a_1, b_1) = (a_2, b_2) \iff (a_1 = a_2 \wedge b_1 = b_2) \quad .$$

Thus,

$$\forall\, x \in A \times B.\, \exists!\, a \in A.\, \exists!\, b \in B.\, x = (a, b) \quad .$$

Pattern-matching notation

Example: The subset of ordered pairs from a set A with equal components is formally

$$\{x \in A \times A \mid \exists\, a_1 \in A.\, \exists\, a_2 \in A.\, x = (a_1, a_2) \wedge a_1 = a_2\}$$

but often abbreviated using *pattern-matching notation* as

$$\{(a_1, a_2) \in A \times A \mid a_1 = a_2\}\ .$$

Pattern-matching notation

Example: The subset of ordered pairs from a set A with equal components is formally

$$\{x \in A \times A \mid \exists\, a_1 \in A.\, \exists\, a_2 \in A.\, x = (a_1, a_2) \wedge a_1 = a_2\}$$

but often abbreviated using *pattern-matching notation* as

$$\{(a_1, a_2) \in A \times A \mid a_1 = a_2\} \ .$$

Notation: For a property $P(a, b)$ with a ranging over a set A and b ranging over a set B,

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

abbreviates

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

Proposition 110 *For all finite sets* A *and* B*,*

$$\#(A \times B) = \#A \cdot \#B \quad .$$

PROOF IDEA:

Sets and logic

$\mathcal{P}(\mathcal{U})$	$\{\,\mathbf{false}\,,\,\mathbf{true}\,\}$
$\emptyset$	**false**
$\mathcal{U}$	**true**
$\cup$	$\vee$
$\cap$	$\wedge$
$(\cdot)^{\mathrm{c}}$	$\neg(\cdot)$
$\bigcup$	$\exists$
$\bigcap$	$\forall$

Big unions

Example:

- Consider the family of sets

$$\mathcal{T} = \left\{ T \subseteq [5] \;\middle|\; \begin{array}{l} \text{the sum of the elements of} \\ T \text{ is less than or equal } 2 \end{array} \right\}$$

$$= \{ \emptyset, \{0\}, \{1\}, \{2\}, \{0,1\}, \{0,2\} \}$$

- The *big union* of the family $\mathcal{T}$ is the set $\bigcup \mathcal{T}$ given by the union of the sets in $\mathcal{T}$:

$$n \in \bigcup \mathcal{T} \iff \exists T \in \mathcal{T}. n \in T \quad .$$

Hence, $\bigcup \mathcal{T} = \{0,1,2\}$.

Definition 111 *Let $\mathfrak{U}$ be a set. For a collection of sets $\mathcal{F} \in \mathcal{P}(\mathcal{P}(\mathfrak{U}))$, we let the* big union *(relative to $\mathfrak{U}$) be defined as*

$$\bigcup \mathcal{F} \;=\; \left\{ x \in \mathfrak{U} \mid \exists A \in \mathcal{F}. x \in A \right\} \;\in \mathcal{P}(\mathfrak{U}) \quad .$$

Proposition 112 *For all* $\mathcal{F} \in \mathcal{P}(\mathcal{P}(\mathcal{P}(\mathfrak{U})))$,

$$\bigcup\left(\bigcup\mathcal{F}\right) = \bigcup\left\{\bigcup\mathcal{A} \in \mathcal{P}(\mathfrak{U}) \;\middle|\; \mathcal{A} \in \mathcal{F}\right\} \in \mathcal{P}(\mathfrak{U}) \quad .$$

PROOF:

Big intersections

Example:

- Consider the family of sets

$$\mathcal{S} = \left\{ S \subseteq [5] \;\middle|\; \text{the sum of the elements of } S \text{ is } 6 \right\}$$

$$= \{\{2,4\},\{0,2,4\},\{1,2,3\},\{0,1,2,3\}\}$$

- The *big intersection* of the family $\mathcal{S}$ is the set $\bigcap \mathcal{S}$ given by the intersection of the sets in $\mathcal{S}$:

$$n \in \bigcap \mathcal{S} \iff \forall S \in \mathcal{S}. n \in S \quad .$$

Hence, $\bigcap \mathcal{S} = \{2\}$.

Definition 113 *Let $\mathcal{U}$ be a set. For a collection of sets $\mathcal{F} \subseteq \mathcal{P}(\mathcal{U})$, we let the* big intersection *(relative to $\mathcal{U}$) be defined as*

$$\bigcap \mathcal{F} = \left\{ x \in \mathcal{U} \mid \forall A \in \mathcal{F}. x \in A \right\} \quad .$$

Theorem 114 *Let*

$$\mathcal{F} = \left\{ S \subseteq \mathbb{R} \,\middle|\, (0 \in S) \wedge \left(\forall x \in \mathbb{R}. x \in S \implies (x+1) \in S\right) \right\} .$$

Then, (i) $\mathbb{N} \in \mathcal{F}$ *and* (ii) $\mathbb{N} \subseteq \bigcap \mathcal{F}$. *Hence,* $\bigcap \mathcal{F} = \mathbb{N}$.

PROOF:

Proposition 115 *Let* $\mathcal{U}$ *be a set and let* $\mathcal{F} \subseteq \mathcal{P}(\mathcal{U})$ *be a family of subsets of* $\mathcal{U}$.

1. *For all* $S \in \mathcal{P}(\mathcal{U})$,

$$S = \bigcup \mathcal{F}$$

iff

$$\left[\forall A \in \mathcal{F}. A \subseteq S\right] \wedge \left[\forall X \in \mathcal{P}(\mathcal{U}). (\forall A \in \mathcal{F}. A \subseteq X) \Rightarrow S \subseteq X\right]$$

2. *For all* $T \in \mathcal{P}(\mathcal{U})$,

$$T = \bigcap \mathcal{F}$$

iff

$$\left[\forall A \in \mathcal{F}. T \subseteq A\right] \wedge \left[\forall Y \in \mathcal{P}(\mathcal{U}). (\forall A \in \mathcal{F}. Y \subseteq A) \Rightarrow Y \subseteq T\right]$$

Union axiom

Every collection of sets has a union.

$$\bigcup \mathcal{F}$$

$$x \in \bigcup \mathcal{F} \iff \exists X \in \mathcal{F}. x \in X$$

For *non-empty* $\mathcal{F}$ we also have

$$\bigcap \mathcal{F}$$

defined by

$$\forall x.\ x \in \bigcap \mathcal{F} \iff (\forall X \in \mathcal{F}.\, x \in X) \quad .$$

Disjoint unions

Definition 116 *The* disjoint union $A \uplus B$ *of two sets* A *and* B *is the set*

$$A \uplus B \;=\; \big(\{1\} \times A\big) \cup \big(\{2\} \times B\big) \quad .$$

Thus,

$$\forall x.\, x \in (A \uplus B) \iff \big(\exists a \in A.\, x = (1, a)\big) \vee \big(\exists b \in B.\, x = (2, b)\big) .$$

Proposition 118 *For all finite sets* A *and* B*,*

$$A \cap B = \emptyset \implies \#(A \cup B) = \#A + \#B \quad .$$

PROOF IDEA:

Corollary 119 *For all finite sets* A *and* B*,*

$$\#(A \uplus B) = \#A + \#B \quad .$$

Relations

Definition 121 *A (binary) relation* R *from a set* A *to a set* B

$$R : A \nrightarrow B \quad \textit{or} \quad R \in \mathrm{Rel}(A, B) \quad ,$$

is

$$R \subseteq A \times B \quad \textit{or} \quad R \in \mathcal{P}(A \times B) \quad .$$

Notation 122 *One typically writes* $a \, R \, b$ *for* $(a, b) \in R$.

Informal examples:

- Computation.
- Typing.
- Program equivalence.
- Networks.
- Databases.

Examples:

- Empty relation.
  $\emptyset : A \rightarrowtail\!\!\!\!\!+\; B$ $\qquad (a \;\emptyset\; b \iff \mathbf{false})$
- Full relation.
  $(A \times B) : A \rightarrowtail\!\!\!\!\!+\; B$ $\qquad (a \;(A \times B)\; b \iff \mathbf{true})$
- Identity (or equality) relation.
  $\mathrm{id}_A = \{\, (a, a) \mid a \in A \,\} : A \rightarrowtail\!\!\!\!\!+\; A$ $\qquad (a \;\mathrm{id}_A\; a' \iff a = a')$
- Integer square root.
  $R_2 = \{\, (m, n) \mid m = n^2 \,\} : \mathbb{N} \rightarrowtail\!\!\!\!\!+\; \mathbb{Z}$ $\qquad (m \;R_2\; n \iff m = n^2)$

Internal diagrams

Example:

$$R = \{ (0,0), (0,-1), (0,1), (1,2), (1,1), (2,1) \} : \mathbb{N} \rightarrowtail \mathbb{Z}$$

$$S = \{ (1,0), (1,2), (2,1), (2,3) \} : \mathbb{Z} \rightarrowtail \mathbb{Z}$$

Relational extensionality

$$R = S : A \rightarrowtail\!\!\!\!\!+\; B$$

iff

$$\forall a \in A. \forall b \in B.\ a\,R\,b \iff a\,S\,b$$

Relational composition

Theorem 124 *Relational composition is associative and has the identity relation as neutral element.*

- *Associativity.*

  For all $R : A \rightarrowtail\!\!\!\!\!+\; B$, $S : B \rightarrowtail\!\!\!\!\!+\; C$, *and* $T : C \rightarrowtail\!\!\!\!\!+\; D$,

  $$(T \circ S) \circ R \;=\; T \circ (S \circ R)$$

- *Neutral element.*

  For all $R : A \rightarrowtail\!\!\!\!\!+\; B$,

  $$R \circ \mathrm{id}_A \;=\; R \;=\; \mathrm{id}_B \circ R \quad .$$

Relations and matrices

Definition 125

1. *For positive integers* m *and* n*, an* $(\mathrm{m} \times \mathrm{n})$*-*matrix *over a semiring* $(\mathrm{S}, 0, \oplus, 1, \odot)$ *is given by entries* $\mathrm{M}_{\mathrm{i},\mathrm{j}} \in \mathrm{S}$ *for all* $0 \leq \mathrm{i} < \mathrm{m}$ *and* $0 \leq \mathrm{j} < \mathrm{n}$*.*

Theorem 126 *Matrix multiplication is associative and has the identity matrix as neutral element.*

Relations from $[m]$ to $[n]$ and $(m \times n)$-matrices over Booleans provide two alternative views of the same structure.

This carries over to identities and to composition/multiplication .

Directed graphs

Definition 130 *A directed graph* (A, R) *consists of a set* A *and a relation* R *on* A *(i.e. a relation from* A *to* A*).*

Corollary 132 *For every set* A*, the structure*

$$\left(\mathrm{Rel}(A) \, , \, \mathrm{id}_A \, , \circ \right)$$

is a monoid.

Definition 133 *For* $R \in \mathrm{Rel}(A)$ *and* $n \in \mathbb{N}$*, we let*

$$R^{\circ n} = \underbrace{R \circ \cdots \circ R}_{n \text{ times}} \in \mathrm{Rel}(A)$$

be defined as id_A *for* $n = 0$*, and as* $R \circ R^{\circ m}$ *for* $n = m + 1$*.*

Paths

Proposition 135 *Let* (A, R) *be a directed graph. For all* $n \in \mathbb{N}$ *and* $s, t \in A$, $s\ R^{\circ n}\ t$ *iff there exists a path of length* n *in* R *with source* s *and target* t.

PROOF:

Definition 136 *For* $\mathrm{R} \in \mathrm{Rel}(\mathrm{A})$*, let*

$$\mathrm{R}^{\circ *} \;=\; \bigcup \left\{ \mathrm{R}^{\circ \mathrm{n}} \in \mathrm{Rel}(\mathrm{A}) \mid \mathrm{n} \in \mathbb{N} \right\} \;=\; \bigcup_{\mathrm{n} \in \mathbb{N}} \mathrm{R}^{\circ \mathrm{n}} \quad .$$

Corollary 137 *Let* (A, R) *be a directed graph. For all* $\mathrm{s}, \mathrm{t} \in \mathrm{A}$*,* $\mathrm{s}\ \mathrm{R}^{\circ *}\ \mathrm{t}$ *iff there exists a path with source* s *and target* t *in* R*.*

The $(n \times n)$-matrix $M = \mathrm{mat}(R)$ of a finite directed graph $\big([n], R\big)$ for n a positive integer is called its *adjacency matrix*.

The adjacency matrix $M^* = \mathrm{mat}(R^{\circ *})$ can be computed by matrix multiplication and addition as M_n where

$$\begin{cases} M_0 &= I_n \\ M_{k+1} &= I_n + \big(M \cdot M_k\big) \end{cases}$$

This gives an algorithm for establishing or refuting the existence of paths in finite directed graphs.

Preorders

Definition 138 *A* preorder $(P, \sqsubseteq)$ *consists of a set* P *and a relation* $\sqsubseteq$ *on* P *(i.e.* $\sqsubseteq \in \mathcal{P}(P \times P)$*) satisfying the following two axioms.*

- *Reflexivity.*

$$\forall x \in P.\ x \sqsubseteq x$$

- *Transitivity.*

$$\forall x, y, z \in P.\ (x \sqsubseteq y \wedge y \sqsubseteq z) \implies x \sqsubseteq z$$

Examples:

- $(\mathbb{R}, \leq)$ and $(\mathbb{R}, \geq)$.
- $(\mathcal{P}(A), \subseteq)$ and $(\mathcal{P}(A), \supseteq)$.
- $(\ \mathbb{Z}\ ,\ |\ )$.

Theorem 140 *For* $\mathrm{R} \subseteq \mathrm{A} \times \mathrm{A}$, *let*

$$\mathcal{F}_{\mathrm{R}} = \left\{ \mathrm{Q} \subseteq \mathrm{A} \times \mathrm{A} \mid \mathrm{R} \subseteq \mathrm{Q} \wedge \mathrm{Q} \textit{ is a preorder} \right\} .$$

Then, (i) $\mathrm{R}^{\circ *} \in \mathcal{F}_{\mathrm{R}}$ *and* (ii) $\mathrm{R}^{\circ *} \subseteq \bigcap \mathcal{F}_{\mathrm{R}}$. *Hence,* $\mathrm{R}^{\circ *} = \bigcap \mathcal{F}_{\mathrm{R}}$.

PROOF:

Partial functions

Definition 141 *A relation* $R : A \rightarrowtail\!\!\!\!\!\!+\; B$ *is said to be* functional*, and called a* partial function*, whenever it is such that*

$$\forall a \in A. \forall b_1, b_2 \in B.\ a\,R\,b_1 \wedge a\,R\,b_2 \implies b_1 = b_2 \quad .$$

Theorem 143 *The identity relation is a partial function, and the composition of partial functions yields a partial function.*

NB

$$f = g : A \rightharpoonup B$$

iff

$$\forall a \in A. \left(f(a)\downarrow \iff g(a)\downarrow \right) \wedge f(a) = g(a)$$

Example: The following are examples of partial functions.

- rational division $\div : \mathbb{Q} \times \mathbb{Q} \rightharpoonup \mathbb{Q}$, with domain of definition $\{(r, s) \in \mathbb{Q} \times \mathbb{Q} \mid s \neq 0\}$;
- integer square root $\sqrt{-} : \mathbb{Z} \rightharpoonup \mathbb{Z}$, with domain of definition $\{m \in \mathbb{Z} \mid \exists n \in \mathbb{Z}. m = n^2\}$;
- real square root $\sqrt{-} : \mathbb{R} \rightharpoonup \mathbb{R}$, whose domain of definition is $\{x \in \mathbb{R} \mid x \geq 0\}$.

Proposition 144 *For all finite sets* A *and* B*,*

$$\#(A \rightleftharpoons B) \;=\; (\#B + 1)^{\#A} \quad .$$

PROOF IDEA:

Functions (or maps)

Definition 145 *A partial function is said to be* total*, and referred to as a* (total) function *or* map*, whenever its domain of definition coincides with its source.*

Theorem 146 *For all* $f \in \mathrm{Rel}(A, B)$*,*

$$f \in (A \Rightarrow B) \iff \forall a \in A.\, \exists! b \in B.\ a\, f\, b \quad .$$

Proposition 147 *For all finite sets* A *and* B*,*

$$\#(A \Rightarrow B) \;=\; \#B^{\#A} \quad .$$

PROOF IDEA:

Theorem 148 *The identity partial function is a function, and the composition of functions yields a function.*

NB

1. $f = g : A \to B$ iff $\forall\, a \in A.\, f(a) = g(a)$.
2. For all sets A, the identity function $\mathrm{id}_A : A \to A$ is given by the rule

   $$\mathrm{id}_A(a) = a$$

   and, for all functions $f : A \to B$ and $g : B \to C$, the composition function $g \circ f : A \to C$ is given by the rule

   $$\big(g \circ f\big)(a) = g\big(f(a)\big) \quad .$$

Inductive definitions

Examples:

- $\mathrm{add} : \mathbb{N}^2 \to \mathbb{N}$

$$\begin{cases} \mathrm{add}(m, 0) &= m \\ \mathrm{add}(m, n+1) &= \mathrm{add}(m, n) + 1 \end{cases}$$

- $S : \mathbb{N} \to \mathbb{N}$

$$\begin{cases} S(0) &= 0 \\ S(n+1) &= \mathrm{add}(n, S(n)) \end{cases}$$

The function

$$\rho_{a,f} : \mathbb{N} \to A$$

inductively defined from

$$\begin{cases} a \in A \\ f : \mathbb{N} \times A \to A \end{cases}$$

is the unique such that

$$\begin{cases} \rho_{a,f}(0) & = & a \\ \rho_{a,f}(n+1) & = & f\big(n, \rho_{a,f}(n)\big) \end{cases}$$

Examples:

- $\mathrm{add} : \mathbb{N}^2 \to \mathbb{N}$

  $\mathrm{add}(m, n) = \rho_{m,f}(n)$ for $f(x, y) = y + 1$

- $S : \mathbb{N} \to \mathbb{N}$

  $S = \rho_{0,\mathrm{add}}$

For a set A, consider $a \in A$ and a function $f : \mathbb{N} \times A \to A$.

Definition 149 *Define $R \subseteq \mathbb{N} \times A$ to be (a, f)-closed whenever*

- $0 \, R \, a$, *and*
- $\forall n \in \mathbb{N}. \forall x \in A. \, n \, R \, x \implies (n+1) \, R \, f(n, x)$.

Theorem 150 *Let $\rho_{a,f} = \bigcap \{ R \subseteq \mathbb{N} \times A \mid R$ is (a, f)-closed $\}$.*

1. *The relation $\rho_{a,f} : \mathbb{N} \rightarrowtail A$ is functional and total.*
2. *The function $\rho_{a,f} : \mathbb{N} \to A$ is the unique such that $\rho_{a,f}(0) = a$ and $\rho_{a,f}(n+1) = f\big(n, \rho_{a,f}(n)\big)$ for all $n \in \mathbb{N}$.*

Bijections

Definition 151 *A function* $\mathrm{f} : \mathrm{A} \to \mathrm{B}$ *is said to be* bijective*, or a* bijection*, whenever there exists a (necessarily unique) function* $\mathrm{g} : \mathrm{B} \to \mathrm{A}$ *(referred to as the* inverse *of* f*) such that*

1. g *is a* retraction *(or* left inverse*) for* f*:*

$$\mathrm{g} \circ \mathrm{f} = \mathrm{id}_{\mathrm{A}} \quad ,$$

2. g *is a* section *(or* right inverse*) for* f*:*

$$\mathrm{f} \circ \mathrm{g} = \mathrm{id}_{\mathrm{B}} \quad .$$

Proposition 153 *For all finite sets* A *and* B*,*

$$\#\,\mathrm{Bij}(A,B) \;=\; \begin{cases} 0 & \text{, if } \#A \neq \#B \\ n! & \text{, if } \#A = \#B = n \end{cases}$$

PROOF IDEA:

Theorem 154 *The identity function is a bijection, and the composition of bijections yields a bijection.*

Definition 155 *Two sets* A *and* B *are said to be* isomorphic *(and to have the* same cardinatity*) whenever there is a bijection between them; in which case we write*

$$\mathrm{A} \cong \mathrm{B} \quad \textit{or} \quad \#\mathrm{A} = \#\mathrm{B} \quad .$$

Examples:

1. $\{0, 1\} \cong \{\mathbf{false}, \mathbf{true}\}$.
2. $\mathbb{N} \cong \mathbb{N}^{+}$, $\mathbb{N} \cong \mathbb{Z}$, $\mathbb{N} \cong \mathbb{N} \times \mathbb{N}$, $\mathbb{N} \cong \mathbb{Q}$.

Equivalence relations and set partitions

- Equivalence relations.

- Set partitions.

Theorem 158 *For every set* A*,*

$$\mathrm{EqRel}(A) \cong \mathrm{Part}(A) \quad .$$

PROOF:

Calculus of bijections

- $A \cong A$, $A \cong B \implies B \cong A$, $(A \cong B \wedge B \cong C) \implies A \cong C$
- If $A \cong X$ and $B \cong Y$ then

$$\mathcal{P}(A) \cong \mathcal{P}(X) \quad , \quad A \times B \cong X \times Y \quad , \quad A \uplus B \cong X \uplus Y \quad ,$$

$$\mathrm{Rel}(A, B) \cong \mathrm{Rel}(X, Y) \quad , \quad (A \rightleftharpoons B) \cong (X \rightleftharpoons Y) \quad ,$$

$$(A \Rightarrow B) \cong (X \Rightarrow Y) \quad , \quad \mathrm{Bij}(A, B) \cong \mathrm{Bij}(X, Y)$$

- $A \cong [1] \times A \;,\; (A \times B) \times C \cong A \times (B \times C) \;,\; A \times B \cong B \times A$
- $[0] \uplus A \cong A \;,\; (A \uplus B) \uplus C \cong A \uplus (B \uplus C) \;,\; A \uplus B \cong B \uplus A$
- $[0] \times A \cong [0] \;,\; (A \uplus B) \times C \cong (A \times C) \uplus (B \times C)$
- $\big(A \Rightarrow [1]\big) \cong [1] \;,\; \big(A \Rightarrow (B \times C)\big) \cong (A \Rightarrow B) \times (A \Rightarrow C)$
- $\big([0] \Rightarrow A\big) \cong [1] \;,\; \big((A \uplus B) \Rightarrow C\big) \cong (A \Rightarrow C) \times (B \Rightarrow C)$
- $([1] \Rightarrow A) \cong A \;,\; \big((A \times B) \Rightarrow C\big) \cong \big(A \Rightarrow (B \Rightarrow C)\big)$
- $(A \rightleftharpoons B) \cong \big(A \Rightarrow (B \uplus [1])\big)$
- $\mathcal{P}(A) \cong \big(A \Rightarrow [2]\big)$

Characteristic (or indicator) functions

$$\mathcal{P}(\mathbf{A}) \cong \left(\mathbf{A} \Rightarrow [\mathbf{2}]\right)$$

Finite cardinality

Definition 160 *A set* A *is said to be* finite *whenever* $\mathrm{A} \cong [\mathrm{n}]$ *for some* $\mathrm{n} \in \mathbb{N}$*, in which case we write* $\#\mathrm{A} = \mathrm{n}$*.*

Theorem 161 *For all* $m, n \in \mathbb{N}$,

1. $\mathcal{P}\big([n]\big) \cong [2^n]$
2. $[m] \times [n] \cong [m \cdot n]$
3. $[m] \uplus [n] \cong [m + n]$
4. $\big([m] \rightharpoonup [n]\big) \cong \big[(n+1)^m\big]$
5. $\big([m] \Rightarrow [n]\big) \cong [n^m]$
6. $\mathrm{Bij}\big([n], [n]\big) \cong [n!]$

Infinity axiom

There is an infinite set, containing $\emptyset$ and closed under successor.

Bijections

Proposition 162 *For a function $f : A \to B$, the following are equivalent.*

1. f *is bijective.*
2. $\forall\, b \in B.\, \exists!\, a \in A.\, f(a) = b$.
3. $$\begin{aligned} &\big(\forall\, b \in B.\, \exists\, a \in A.\, f(a) = b\big) \\ \wedge\ &\big(\forall\, a_1, a_2 \in A.\, f(a_1) = f(a_2) \implies a_1 = a_2\big) \end{aligned}$$

Surjections

Definition 163 *A function* $f : A \to B$ *is said to be* surjective*, or a* surjection*, and indicated* $f : A \twoheadrightarrow B$ *whenever*

$$\forall\, b \in B.\, \exists\, a \in A.\, f(a) = b \quad .$$

Theorem 164 *The identity function is a surjection, and the composition of surjections yields a surjection.*

The set of surjections from A to B is denoted

$$\mathrm{Sur}(A, B)$$

and we thus have

$$\mathrm{Bij}(A, B) \subseteq \mathrm{Sur}(A, B) \subseteq \mathrm{Fun}(A, B) \subseteq \mathrm{PFun}(A, B) \subseteq \mathrm{Rel}(A, B) \ .$$

Enumerability

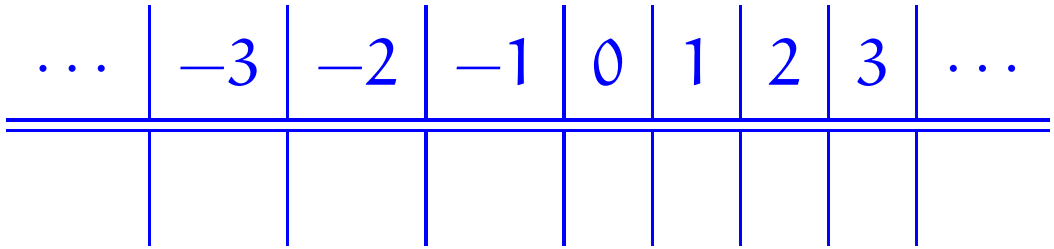
Definition 166

1. *A set* A *is said to be* enumerable *whenever there exists a surjection* $\mathbb{N} \twoheadrightarrow A$*, referred to as an* enumeration*.*

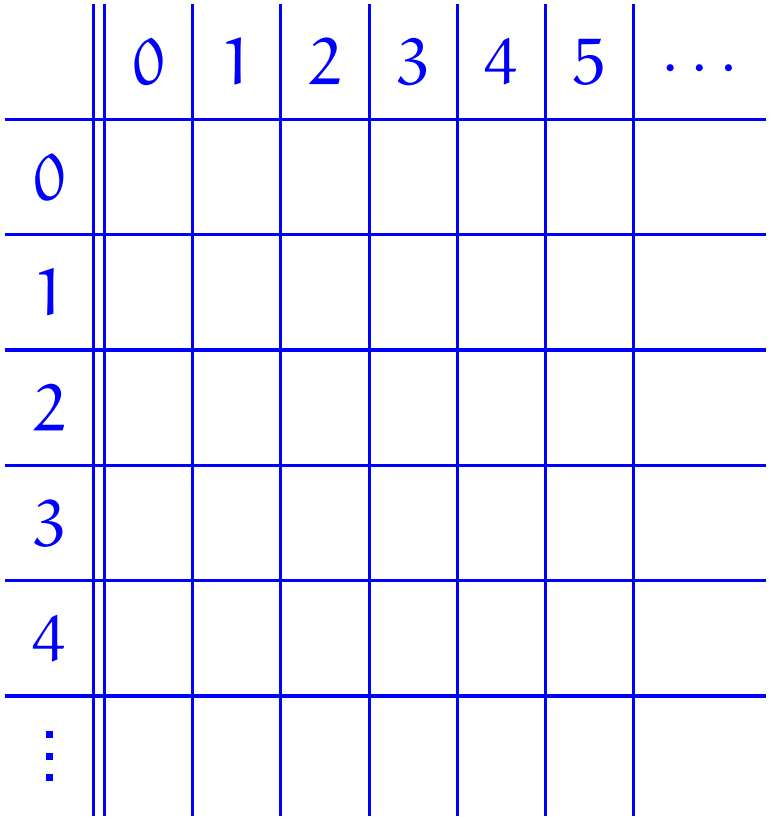
2. *A* countable *set is one that is either empty or enumerable.*

Examples:

1. A bijective enumeration of $\mathbb{Z}$.



2. A bijective enumeration of $\mathbb{N} \times \mathbb{N}$.



Proposition 167 *Every non-empty subset of an enumerable set is enumerable.*

PROOF:

Countability

Proposition 168

1. $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ *are countable sets.*
2. *The product and disjoint union of countable sets is countable.*
3. *Every finite set is countable.*
4. *Every subset of a countable set is countable.*

Axiom of choice

Every surjection has a section.

Injections

Definition 169 *A function* $f : A \to B$ *is said to be* injective*, or an* injection*, and indicated* $f : A \rightarrowtail B$ *whenever*

$$\forall a_1, a_2 \in A. \left(f(a_1) = f(a_2)\right) \implies a_1 = a_2 \quad .$$

Theorem 170 *The identity function is an injection, and the composition of injections yields an injection.*

The set of injections from A to B is denoted

$$\mathrm{Inj}(A, B)$$

and we thus have

$$\begin{array}{ccccc}
 & & \mathrm{Sur}(A, B) & & \\
 & \rotatebox{45}{$\subseteq$} & & \rotatebox{-45}{$\subseteq$} & \\
\mathrm{Bij}(A, B) & & & & \mathrm{Fun}(A, B) \subseteq \mathrm{PFun}(A, B) \subseteq \mathrm{Rel}(A, B) \\
 & \rotatebox{-45}{$\subseteq$} & & \rotatebox{45}{$\subseteq$} & \\
 & & \mathrm{Inj}(A, B) & &
\end{array}$$

with

$$\mathrm{Bij}(A, B) = \mathrm{Sur}(A, B) \cap \mathrm{Inj}(A, B) \quad .$$

Proposition 171 *For all finite sets* A *and* B*,*

$$\#\mathrm{Inj}(\mathrm{A},\mathrm{B}) = \begin{cases} \binom{\#\mathrm{B}}{\#\mathrm{A}} \cdot (\#\mathrm{A})! & \text{, if } \#\mathrm{A} \leq \#\mathrm{B} \\ 0 & \text{, otherwise} \end{cases}$$

PROOF IDEA:

Relational images

Definition 174 *Let* $R : A \rightarrowtail\!\!\!\!\!\!+\; B$ *be a relation.*

- *The* direct image *of* $X \subseteq A$ *under* R *is the set* $\overrightarrow{R}(X) \subseteq B$*, defined as*

$$\overrightarrow{R}(X) \;=\; \{b \in B \mid \exists x \in X.\, x\, R\, b\}\ .$$

NB *This construction yields a function* $\overrightarrow{R} : \mathcal{P}(A) \to \mathcal{P}(B)$.

- *The* inverse image *of* $Y \subseteq B$ *under* R *is the set* $\overleftarrow{R}(Y) \subseteq A$, *defined as*

$$\overleftarrow{R}(Y) \;=\; \{\, a \in A \mid \forall\, b \in B.\, a\, R\, b \implies b \in Y \,\}$$

NB *This construction yields a function* $\overleftarrow{R} : \mathcal{P}(B) \to \mathcal{P}(A)$.

Replacement axiom

The direct image of every definable functional property on a set is a set.

Set-indexed constructions

For every mapping associating a set A_i to each element of a set I, we have the set

$$\bigcup_{i\in I} A_i \;=\; \bigcup \left\{A_i \mid i \in I\right\} \;=\; \left\{a \mid \exists\, i \in I.\, a \in A_i\right\} \quad .$$

Examples:

1. Indexed disjoint unions:

$$\biguplus_{i\in I} A_i \;=\; \bigcup_{i\in I} \{i\} \times A_i$$

2. Finite sequences on a set A:

$$A^* \;=\; \biguplus_{n\in\mathbb{N}} A^n$$

3. Finite partial functions from a set A to a set B:

$$(A \rightharpoonup_{\text{fin}} B) \;=\; \biguplus_{S \in \mathcal{P}_{\text{fin}}(A)} (S \Rightarrow B)$$

where

$$\mathcal{P}_{\text{fin}}(A) = \{\, S \subseteq A \mid S \text{ is finite} \,\}$$

4. Non-empty indexed intersections: for $I \neq \emptyset$,

$$\bigcap_{i \in I} A_i \;=\; \{\, x \in \bigcup_{i \in I} A_i \mid \forall\, i \in I.\, x \in A_i \,\}$$

5. Indexed products:

$$\prod_{i \in I} A_i \;=\; \left\{\; \alpha \in \left(I \Rightarrow \bigcup_{i \in I} A_i\right) \;\middle|\; \forall\, i \in I.\, \alpha(i) \in A_i \;\right\}$$

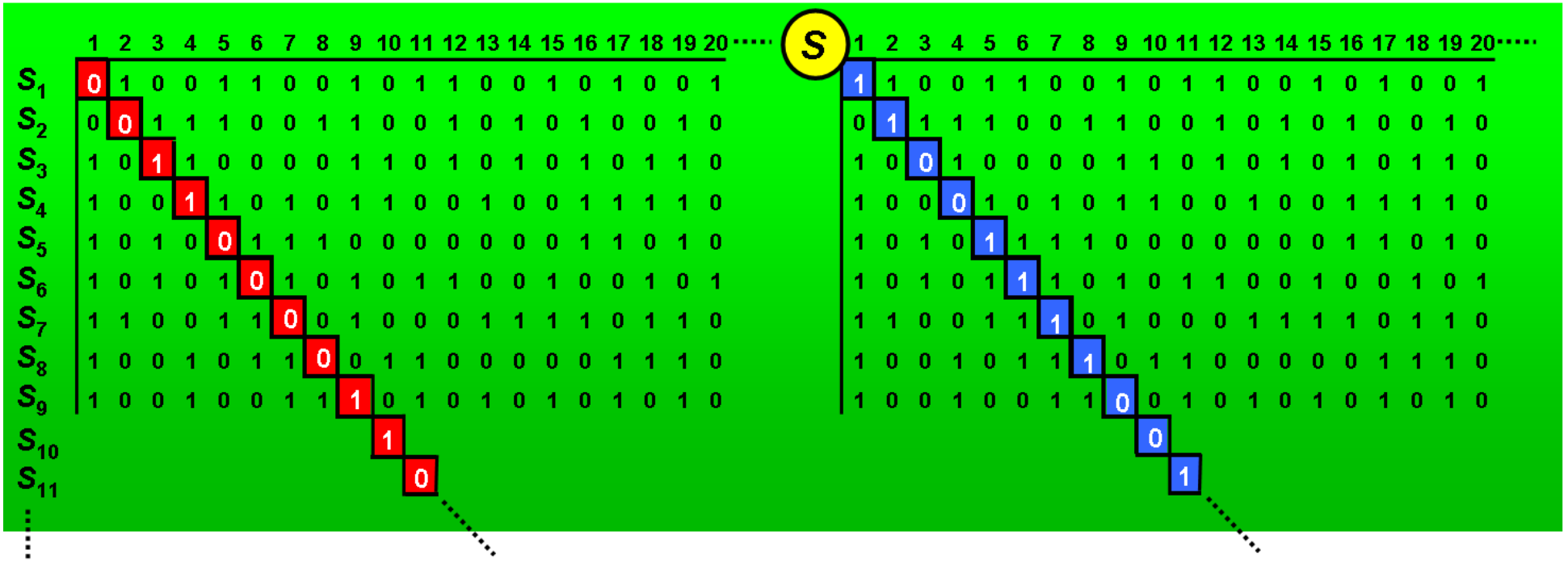
Proposition 177 *An enumerable indexed disjoint union of enumerable sets is enumerable.*

PROOF:

Corollary 179 *If* X *and* A *are countable sets then so are* A^*, $\mathcal{P}_{\mathrm{fin}}(\mathrm{A})$, *and* $(\mathrm{X} \rightleftharpoons_{\mathrm{fin}} \mathrm{A})$.

THEOREM OF THE DAY

Cantor's Uncountability Theorem *There are uncountably many infinite 0-1 sequences.*



Proof: Suppose you *could* count the sequences. Label them in order: S_1, S_2, S_3, ..., and denote by $S_i(j)$ the j-th entry of sequence S_i. Now define a new sequence, S, whose i-th entry is $S_i(i)+1 \pmod 2$. So S is $S_1(1)+1$, $S_2(2)+1$, $S_3(3)+1$, $S_4(4)+1$, ..., with all entries remaindered modulo 2. S is certainly an infinite sequence of 0s and 1s. So it must appear in our list: it is, say, S_k, so its k-th entry is $S_k(k)$. But this is, by definition, $S_k(k) + 1 \pmod 2 \neq S_k(k)$. So we have contradicted the possibility of forming our enumeration. QED.

The theorem establishes that the real numbers are *uncountable* — that is, they cannot be enumerated in a list indexed by the positive integers $(1, 2, 3, \ldots)$. To see this informally, consider the infinite sequences of 0s and 1s to be the binary expansions of fractions (e.g. $0.010011\ldots = 0/2 + 1/4 + 0/8 + 0/16 + 1/32 + 1/64 + \ldots$). More generally, it says that the set of subsets of a countably infinite set is uncountable, and to see *that*, imagine every 0-1 sequence being a different recipe for building a subset: the i-th entry tells you whether to include the i-th element (1) or exclude it (0).

Georg Cantor (1845–1918) discovered this theorem in 1874 but it apparently took another twenty years of thought about what were then new and controversial concepts: 'sets', 'cardinalities', 'orders of infinity', to invent the important proof given here, using the so-called *diagonalisation method*.

Web link: www.math.hawaii.edu/~dale/godel/godel.html. There is an interesting discussion on mathoverflow.net about the history of diagonalisation: type 'earliest diagonal' into their search box.

Further reading: *Mathematics: the Loss of Certainty* by Morris Kline, Oxford University Press, New York, 1980.

Unbounded cardinality

Theorem 180 (Cantor's diagonalisation argument) *For every set A, no surjection from A to $\mathcal{P}(A)$ exists.*

PROOF:

Definition 181 *A fixed-point of a function $f : X \to X$ is an element $x \in X$ such that $f(x) = x$.*

Theorem 182 (Lawvere's fixed-point argument) *For sets A and X, if there exists a surjection $A \twoheadrightarrow (A \Rightarrow X)$ then every function $X \to X$ has a fixed-point; and hence X is a singleton.*

PROOF:

Corollary 183 *The sets*

$$\mathcal{P}(\mathbb{N}) \;\cong\; \big(\mathbb{N} \Rightarrow [2]\big) \;\cong\; [0,1] \;\cong\; \mathbb{R}$$

are not enumerable.

Corollary 184 *There are* non-computable *infinite sequences of bits.*

Foundation axiom

The membership relation is well-founded.

Thereby, providing a

Principle of $\in$-Induction .