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

.

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

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

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

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

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

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

They are the unique nat. k s.t. (1) $k \mid l \wedge k \mid m \wedge k \mid n$
(2) $\forall d.\ d \mid l \wedge d \mid m \wedge d \mid n \Rightarrow d \mid k$

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

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

PROOF: (1)

$$D(\gcd(m,n)) = CD(m,n)$$
$$\parallel$$
$$D(\gcd(n,m)) = CD(n,m)$$
$$\Rightarrow \gcd(m,n) = \gcd(n,m).$$

[a] Aka (Distributivity).

(3) $\gcd(l\cdot m, l\cdot n) \overset{?}{=} l\cdot\gcd(m,n)$

Lemma $x \mid y \Rightarrow zx \mid zy$

(i) $\gcd(l\cdot m, l\cdot n) \mid l\cdot\gcd(m,n)$?

(ii) $l\cdot\gcd(m,n) \mid \gcd(l\cdot m, l\cdot n)$? ✓

(ii) ~~$\gcd(lm, ln) \mid lm \wedge \gcd(lm, ln) \mid ln$~~

$\gcd(m,n) \mid m \wedge \gcd(m,n) \mid n$

$\Rightarrow l\gcd(m,n) \mid lm \wedge l\cdot\gcd(m,n) \mid ln$

$\Rightarrow l\cdot\gcd(m,n) \mid \gcd(l\cdot m, l\cdot n)$.

(i) $\underline{\gcd}(\ell \cdot m, \ell \cdot n) \mid \ell \cdot \underline{\gcd}(m, n)$

Exercise

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: $m \cdot n = k \cdot \ell$

$\gcd(k, m) = 1 \implies n \cdot \gcd(k, m) = n$

$\| $

$\gcd(n \cdot k, n \cdot m)$

$\|$

$k \cdot \gcd(n, \ell) = \gcd(n \cdot k, k \cdot \ell)$

$\boxtimes$

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

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

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

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

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

$$\begin{bmatrix} \mathrm{lc}_1(m, n) & \mathrm{lc}_2(m, n) \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = \gcd(m, n) \quad ,$$

can be efficiently computed.

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

1. $\left[\, \overset{1}{\cancel{?_1}} \;\; \overset{0}{\cancel{?_2}} \,\right] \cdot \begin{bmatrix} m \\ n \end{bmatrix} = m \;\; \wedge \;\; \left[\, \overset{0}{\cancel{?_1}} \;\; \overset{1}{\cancel{?_2}} \,\right] \cdot \begin{bmatrix} m \\ n \end{bmatrix} = n$;

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

$$\begin{bmatrix} \overset{s_1+s_2}{\cancel{?_1}} & \overset{t_1+t_2}{\cancel{?_2}} \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r_1 + r_2 \;;$$

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,

$$\begin{bmatrix} s & t \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r \text{ implies } \begin{bmatrix} \overset{ks}{\cancel{?_1}} & \overset{kt}{\cancel{?_2}} \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = k \cdot r \;.$$

We extend Euclid's Algorithm $\mathtt{gcd}(m, n)$ from computing on pairs of positive integers to computing on pairs of triples $((s, t), r)$ 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( ((s1,t1),r1) ,  c as ((s2,t2),r2) )
    = let
        val (q,r) = divalg(r1,r2)    (* r = r1-q*r2 *)
      in
        if r = 0
        then  c
        else  gcditer(  c , ((s1-q s2 , t1-q t2), r) )
      end
  in
    gcditer( ((1,0),m) , ((0,1),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*,*

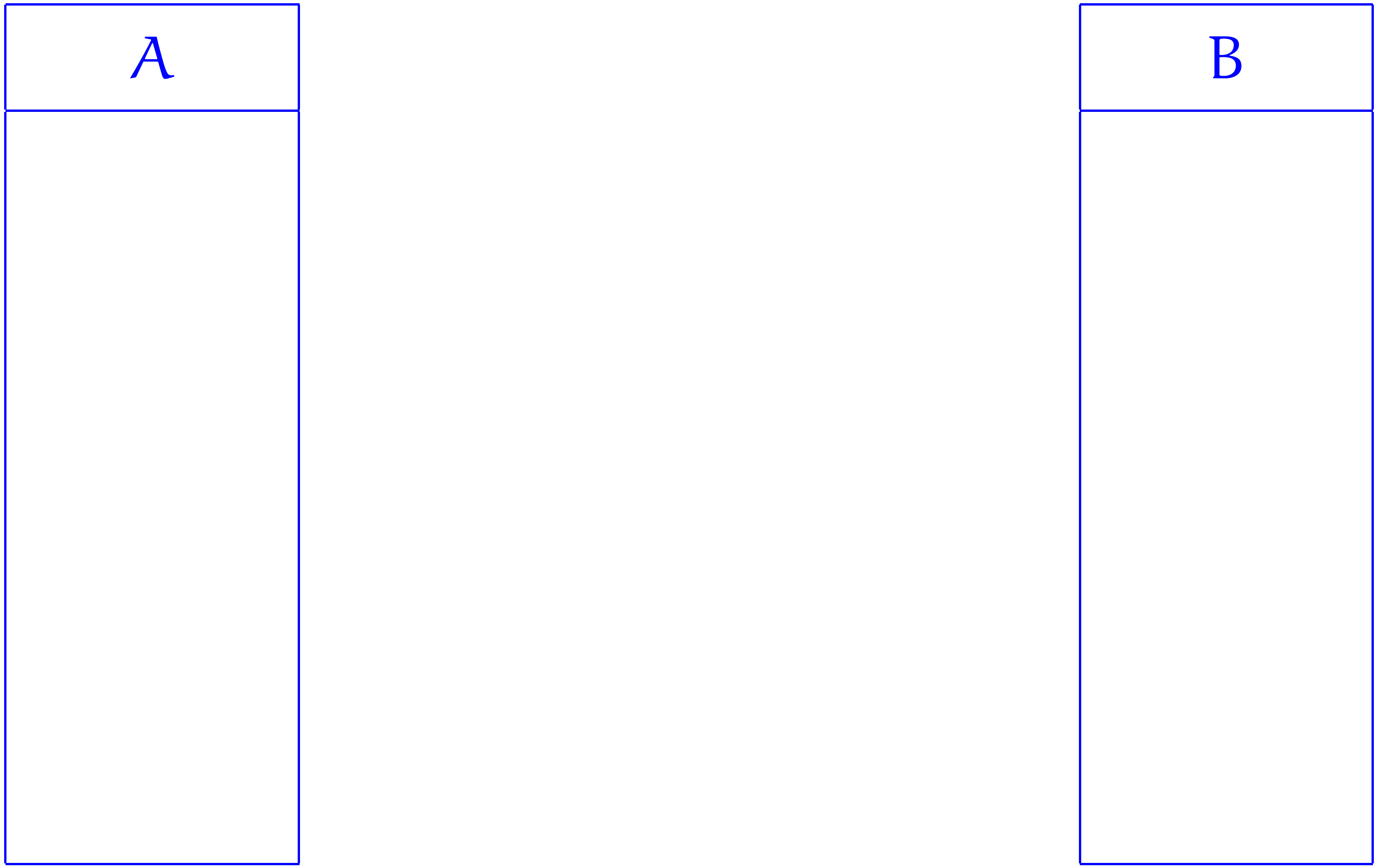
1. $n \cdot \mathrm{lc}_2(m,n) \equiv \gcd(m,n) \pmod{m}$*, and*

2. *whenever* $\gcd(m,n) = 1$*,*

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

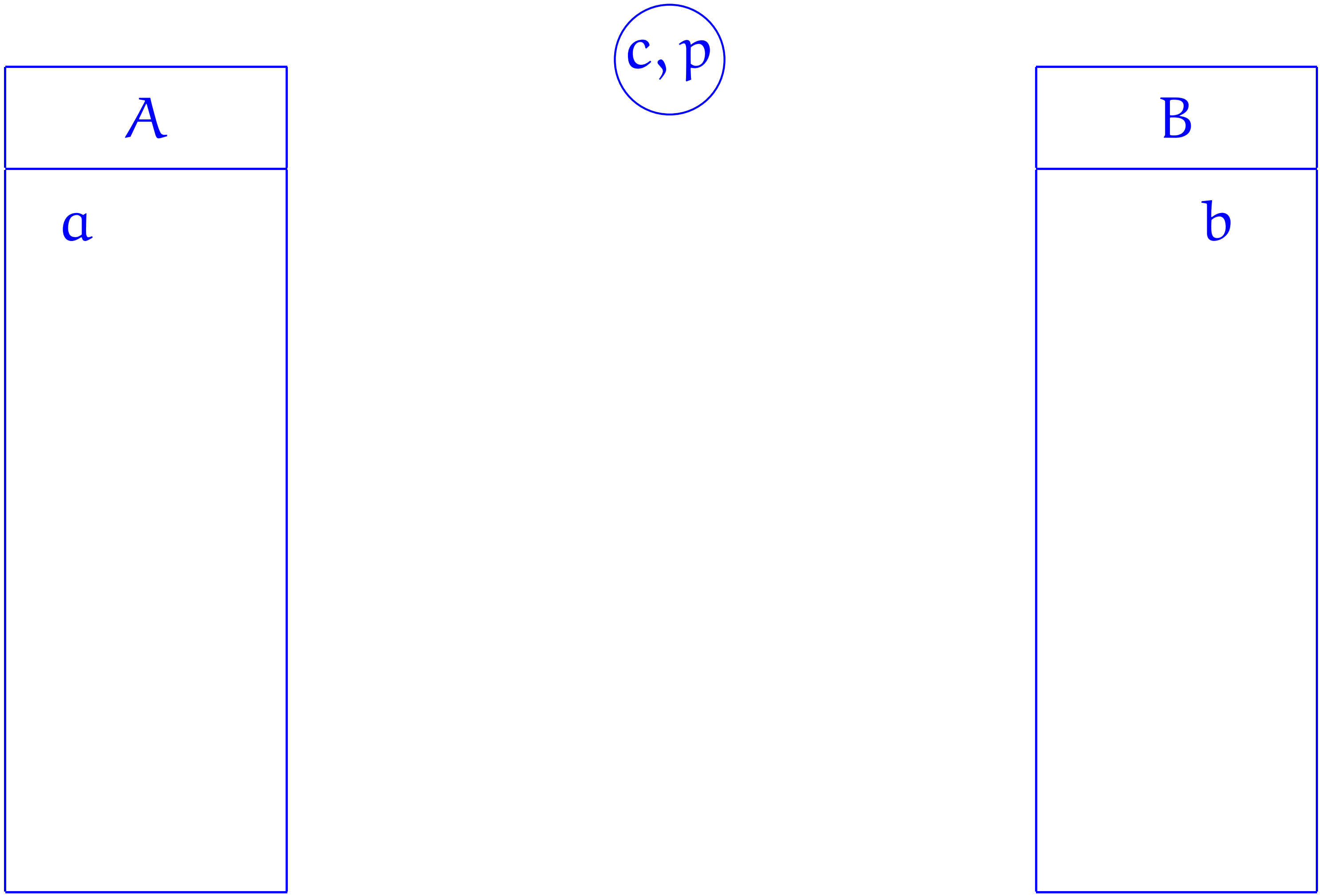
Diffie-Hellman cryptographic method

Shared secret key



Diffie-Hellman cryptographic method

Shared secret key



Diffie-Hellman cryptographic method

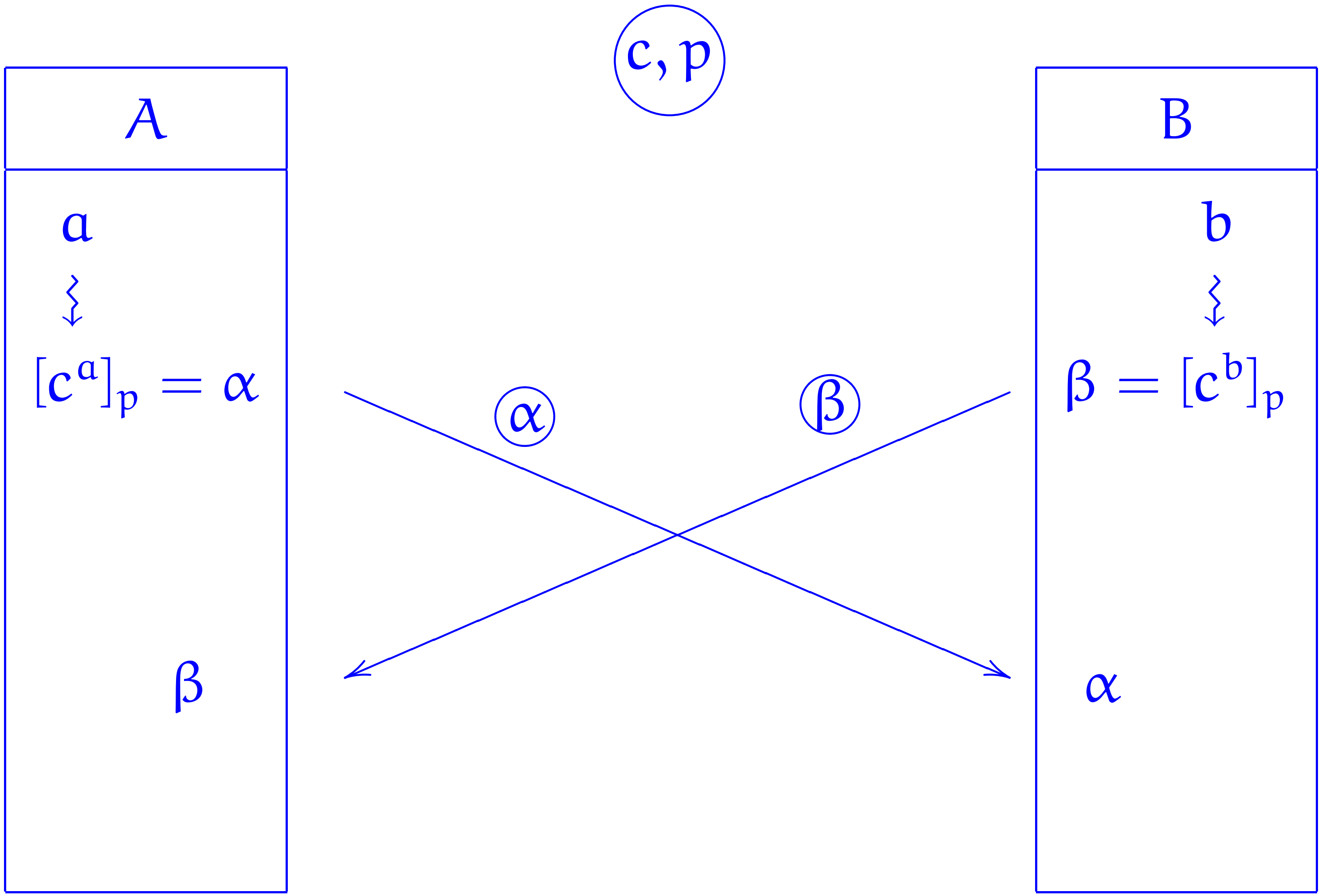
Shared secret key

c, p

A	B
a	b
$\Downarrow$	$\Downarrow$
$[c^a]_p = \alpha$	$\beta = [c^b]_p$

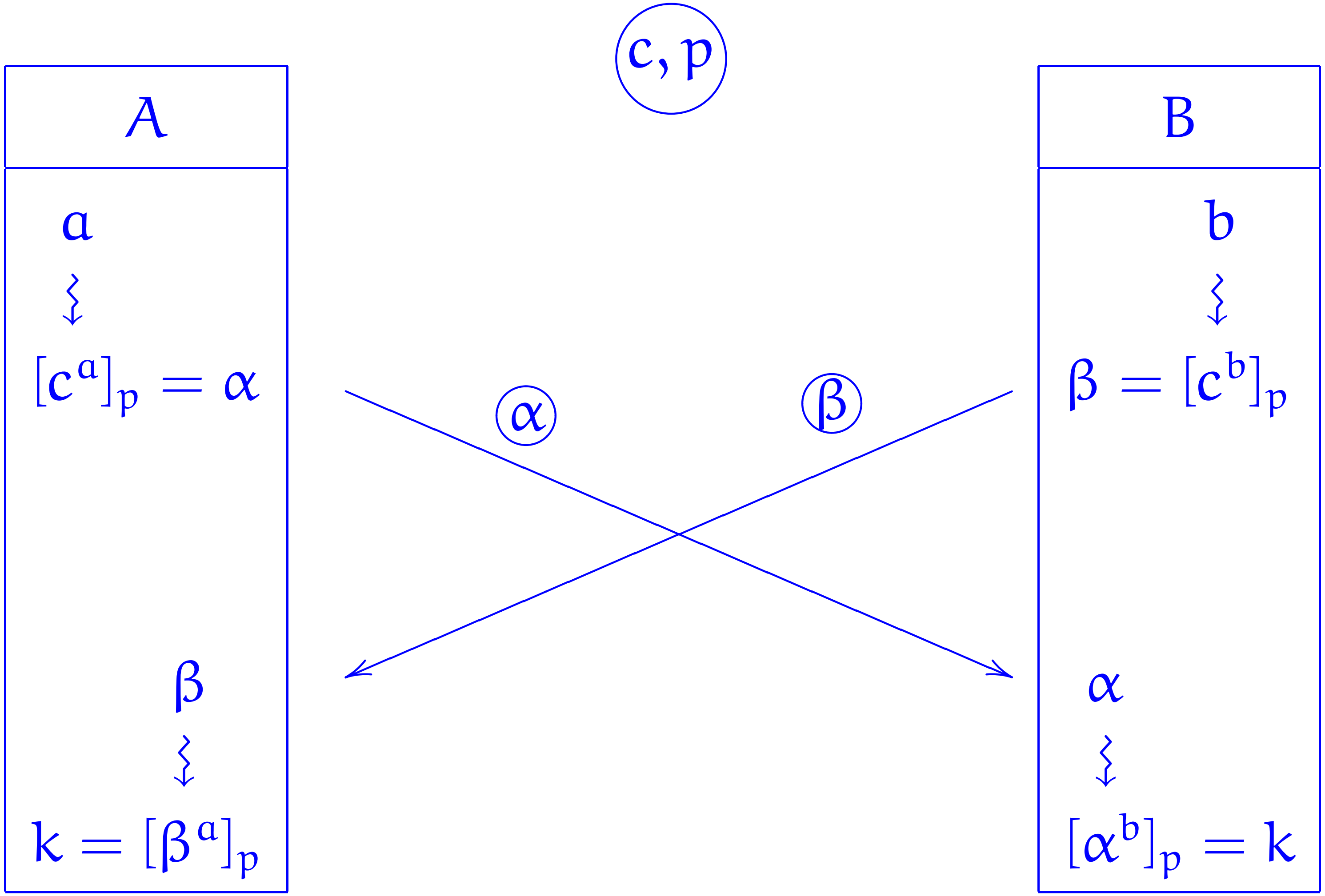
Diffie-Hellman cryptographic method

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*

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

Then, for all integers k*,*

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

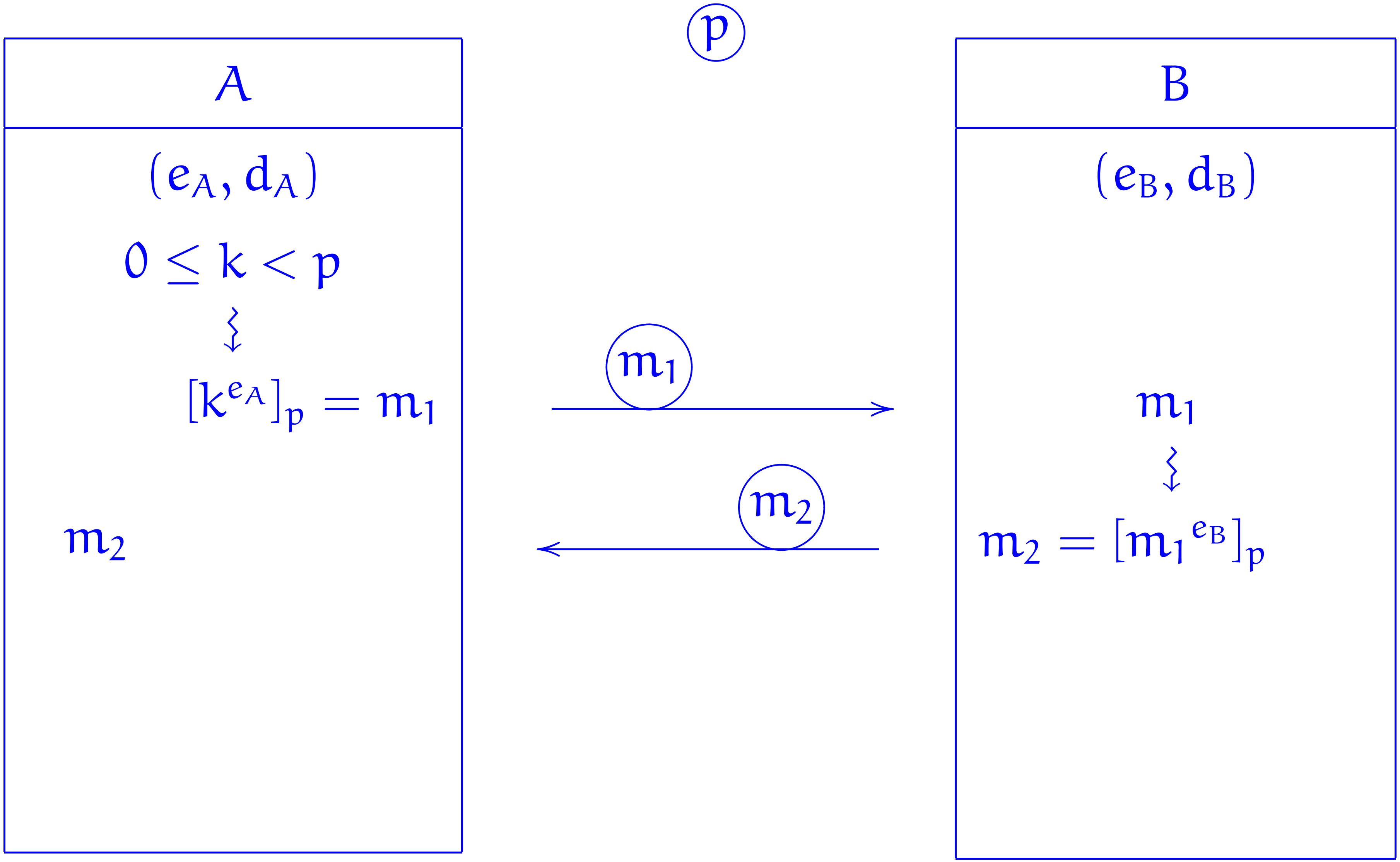
PROOF:

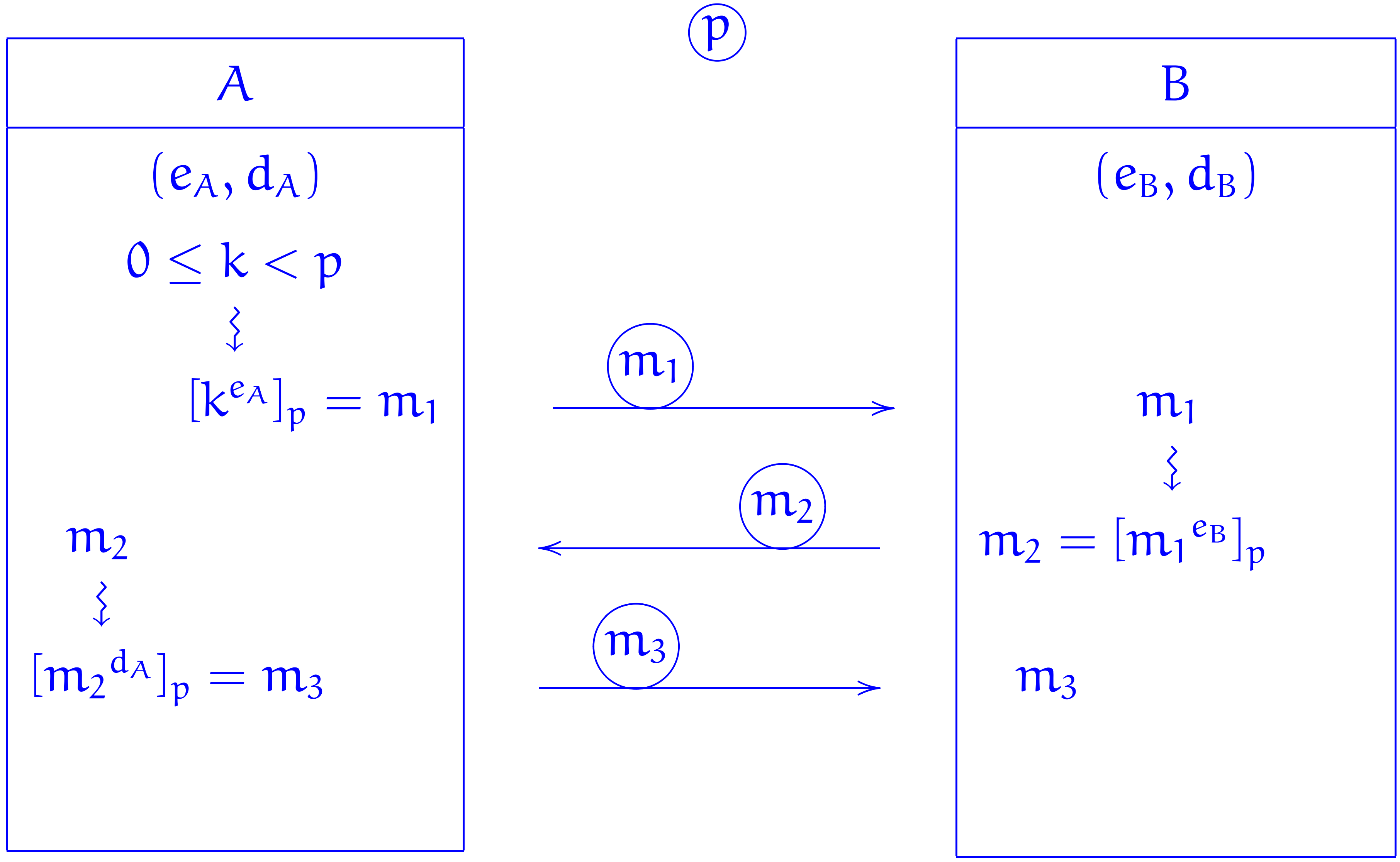
p

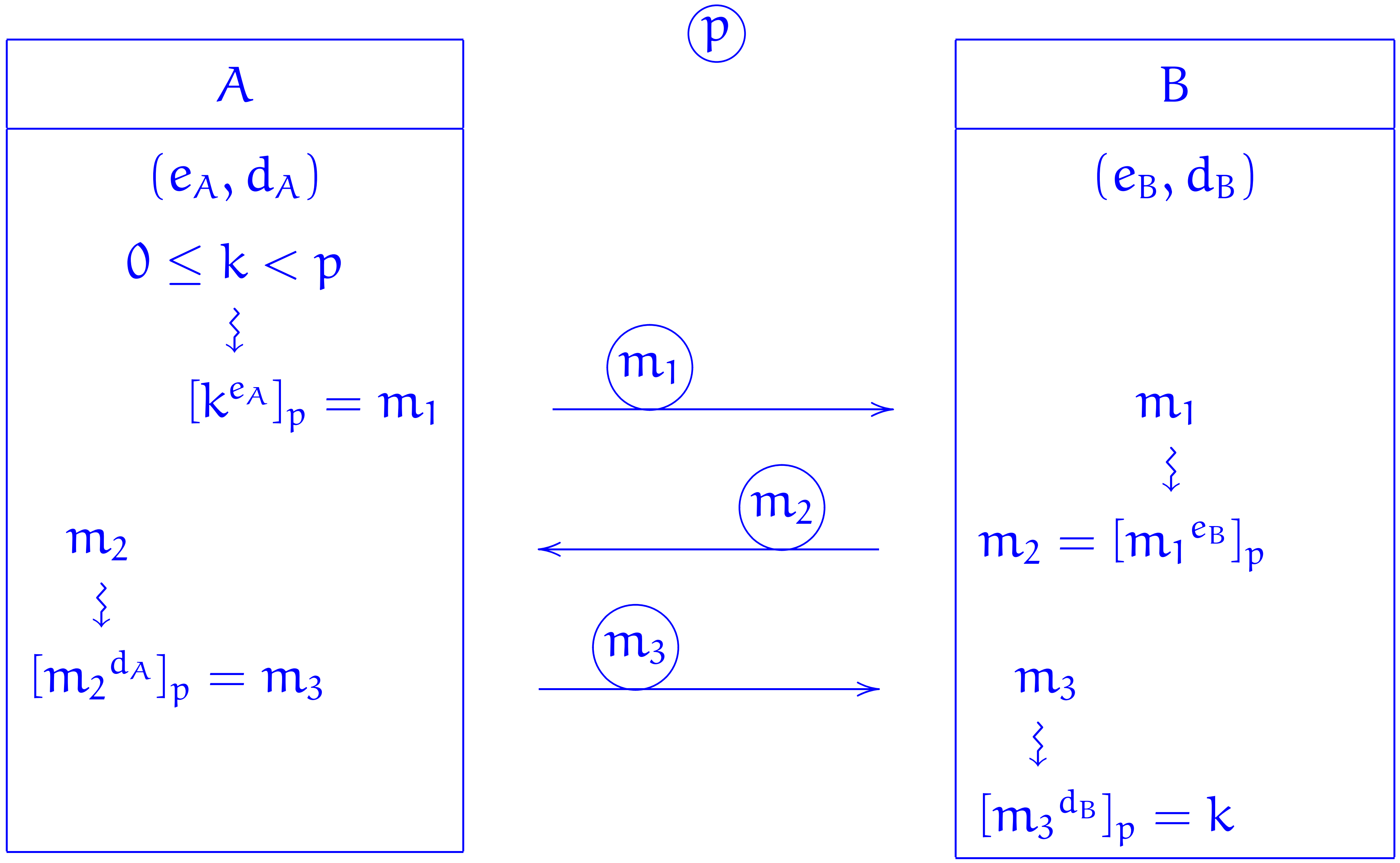
A	B
(e_A, d_A)	(e_B, d_B)
$0 \le k < p$	

p

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


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


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


p
A
(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
B
(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 $\mathbb{N}.\ \Big(\ \big(\forall\, k \in [\ell..n].\, P(k)\,\big) \implies P(n+1)\ \Big)$

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* n *there is a unique finite ordered sequence of primes* $(p_1 \leq \cdots \leq p_\ell)$ *with* $\ell \in \mathbb{N}$ *such that*

$$n = \prod(p_1, \ldots, p_\ell) \quad .$$

PROOF:

Euclid's infinitude of primes

Theorem 99 *The set of primes is infinite.*

PROOF:

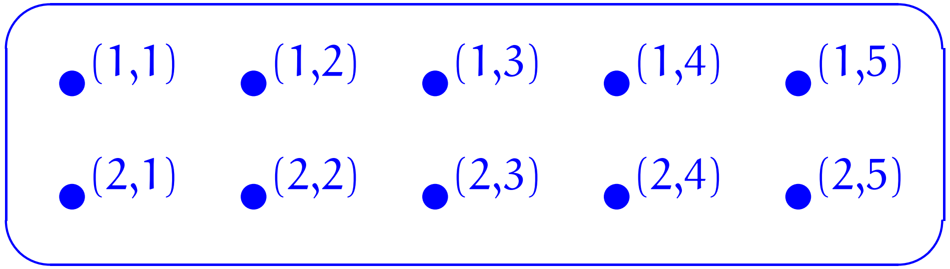
Sets

Objectives

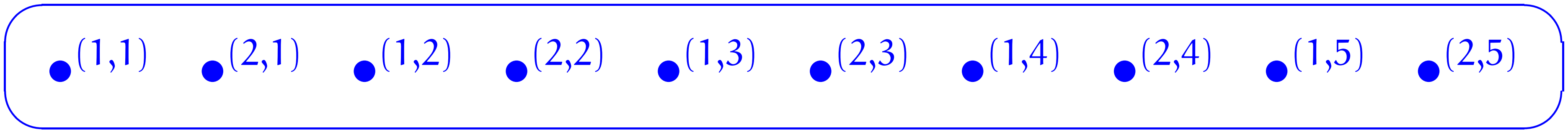
To introduce the basics of the theory of sets and some of its uses.

Abstract sets

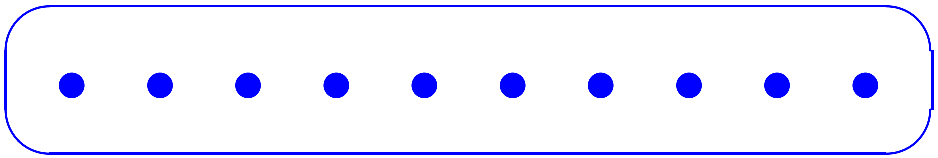
It has been said that a set is like a mental "bag of dots", except of course that the bag has no shape; thus,



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 ubiquitous structures that are available within it.

Set membership

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

$$x \in A \text{ stands for } x \text{ is an element of } A \quad .$$

We further write

$$x \notin A \text{ for } \neg(x \in A) \quad .$$

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

Extensionality axiom

$\boxed{\text{Two sets are equal if they have the same elements.}}$

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*

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

Then,

1. $A = B$, *and*

2. $B = C \iff b^2 = c$.

Subsets and supersets

Lemma 103

1. *Reflexivity.*

   For all sets A, $A \subseteq A$.

2. *Transitivity.*

   For all sets A, B, C, $(A \subseteq B \ \wedge \ B \subseteq C) \implies A \subseteq C$.

3. *Antisymmetry.*

   For all sets A, B, $(A \subseteq B \ \wedge \ B \subseteq A) \implies A = B$.

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

$\boxed{\text{For any set, there is a set consisting of all its subsets.}}$

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

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

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

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

that is, $\mathcal{F}$ is a set of subsets of 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

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

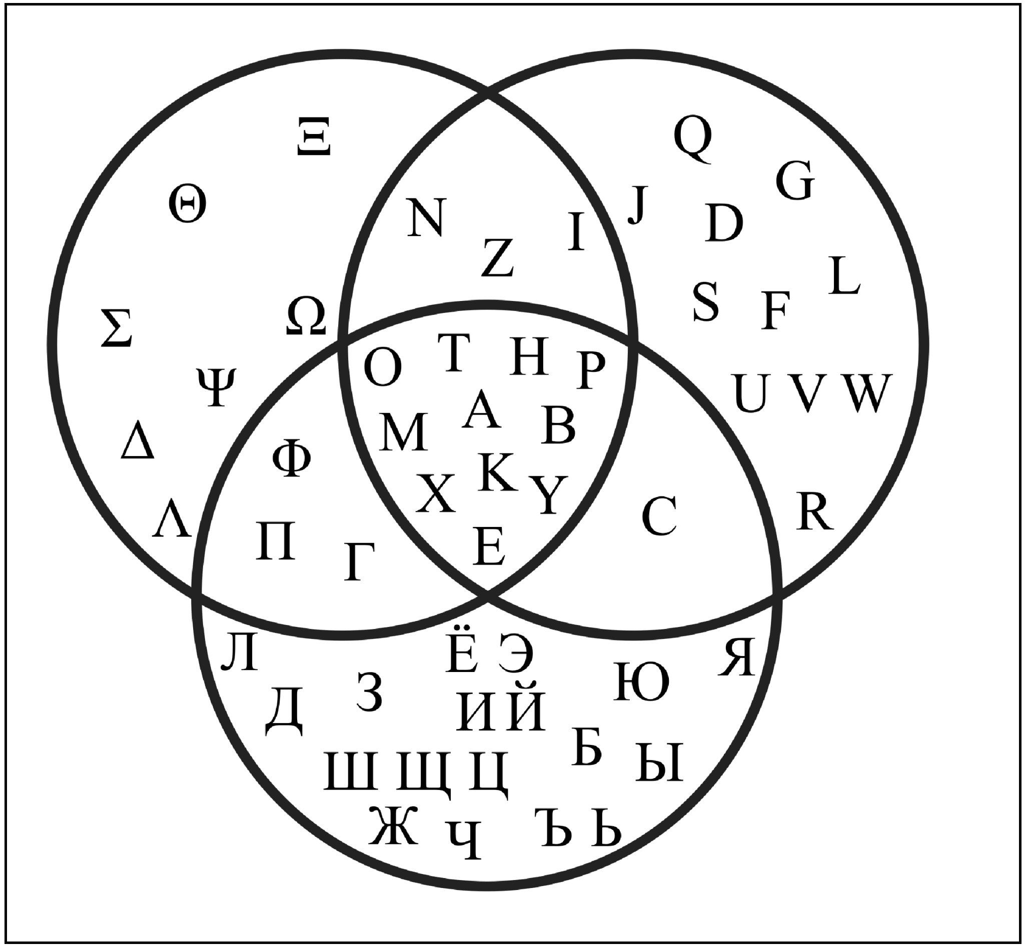
Hasse diagrams

Proposition 104 *For all finite sets U,*

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

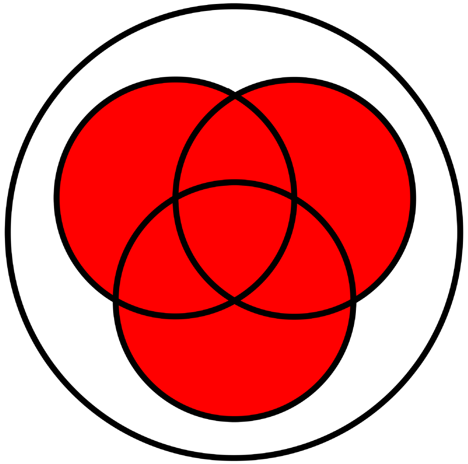
PROOF IDEA:

Venn diagrams[a]

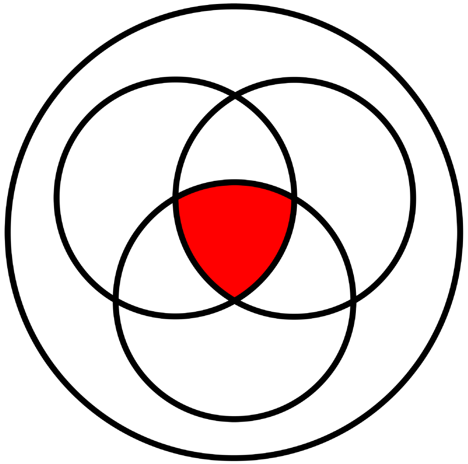


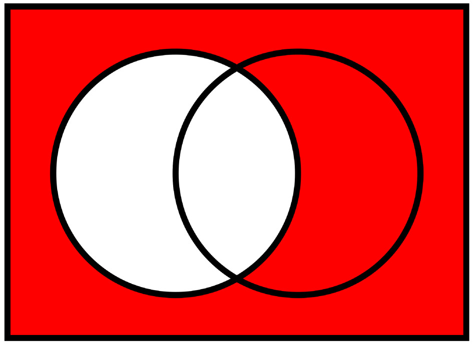
[a]From http://en.wikipedia.org/wiki/Intersection_(set_theory) .

Union



Intersection





Complement

The powerset Boolean algebra

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

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

$$\begin{aligned} A \cup B &= \{ x \in U \mid x \in A \ \vee\ x \in B \} && \in \mathcal{P}(U) \\ A \cap B &= \{ x \in U \mid x \in A \ \wedge\ x \in B \} && \in \mathcal{P}(U) \\ A^c &= \{ x \in U \mid \neg(x \in A) \} && \in \mathcal{P}(U) \end{aligned}$$

- 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* $\mathbb{U}$ is a neutral element for $\cap$.

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

- 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.

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

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

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

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

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

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

PROOF:

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

1. $$C = A \cup B$$

iff

$$[A \subseteq C \wedge B \subseteq C]$$

$$\wedge$$

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

2. $$C = A \cap B$$

iff

$$[C \subseteq A \wedge C \subseteq B]$$

$$\wedge$$

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

Sets and logic

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

Pairing axiom

$\boxed{\text{For every } a \text{ and } b\text{, there is a set with } a \text{ and } b \text{ as its only elements.}}$

$$\{ a , b \}$$

defined by

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

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. $\{a\} = \{x, y\} \implies x = y = a$
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,

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

defines an *ordered pairing* of a and b.

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

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

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

$$\begin{array}{l} \forall a_1, a_2 \in A, b_1, b_2 \in B. \\ \quad (a_1, b_1) = (a_2, b_2) \iff (a_1 = a_2 \ \wedge\ b_1 = b_2) \end{array}$$.

Thus,

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

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

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

Big unions

Example:

- Consider the family of sets

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

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

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

$$\bigcup \mathcal{F} = \{ x \in \mathcal{U} \mid \exists A \in \mathcal{F} .\, x \in A \} \in \mathcal{P}(\mathcal{U}) \quad .$$

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

$$\bigcup \Big(\bigcup \mathcal{F} \Big) = \bigcup \Big\{ \bigcup \mathcal{A} \in \mathcal{P}(\mathbf{U}) \;\Big|\; \mathcal{A} \in \mathcal{F} \Big\} \in \mathcal{P}(\mathbf{U}) \quad .$$

PROOF:

Big intersections

Example:

- Consider the family of sets
$$\mathcal{S} = \left\{ S \subseteq [5] \;\middle|\; \text{the sum of the elements of } S \text{ is } 6 \right\}$$
$$= \big\{ \{2,4\}, \{0,2,4\}, \{1,2,3\} \big\}$$

- 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*

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

Theorem 114 *Let*

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

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

$$\begin{aligned} & \big[\,\forall A \in \mathcal{F}.\, A \subseteq S\,\big] \\ & \quad \wedge \ \big[\,\forall X \in \mathcal{P}(\mathcal{U}).\, (\forall A \in \mathcal{F}.\, A \subseteq X) \Rightarrow S \subseteq X\,\big] \end{aligned}$$

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

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

iff

$$\begin{aligned} & \big[\,\forall A \in \mathcal{F}.\, T \subseteq A\,\big] \\ & \quad \wedge \ \big[\,\forall Y \in \mathcal{P}(\mathcal{U}).\, (\forall A \in \mathcal{F}.\, Y \subseteq A) \Rightarrow Y \subseteq T\,\big] \end{aligned}$$

Union axiom

$$\boxed{\text{Every collection of sets has a union.}}$$

$$\bigcup \mathcal{F}$$

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

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

$$\bigcap \mathcal{F}$$

defined by

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

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* <u>(binary) relation</u> R *from a set* A *to a set* B

$$R : A \longrightarrow\!\!\!\!\!\!\!+\;\; B \qquad \textit{or} \qquad R \in \mathrm{Rel}(A, B) \quad ,$$

is

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

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

Informal examples:

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

Examples:

- Empty relation.

  $\emptyset : A \twoheadrightarrow B$ $\quad$ ($a \; \emptyset \; b \iff \textbf{false}$)

- Full relation.

  $(A \times B) : A \twoheadrightarrow B$ $\quad$ ($a \; (A \times B) \; b \iff \textbf{true}$)

- Identity (or equality) relation.

  $\mathrm{id}_A = \{ (a, a) \mid a \in A \} : A \twoheadrightarrow A$ $\quad$ ($a \; \mathrm{id}_A \; a' \iff a = a'$)

- Integer square root.

  $R_2 = \{ (m, n) \mid m = n^2 \} : \mathbb{N} \twoheadrightarrow \mathbb{Z}$ $\quad$ ($m \; R_2 \; n \iff m = n^2$)

Internal diagrams

Example:

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

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

Relational extensionality

$$R = S : A \rightarrow\!\!\!\!\!+\!\!\!\!\rightarrow B$$

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 $R : A \nrightarrow B$, $S : B \nrightarrow C$, *and* $T : C \nrightarrow D$,

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

- *Neutral element.*

  For all $R : A \nrightarrow B$,

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

Definition 125

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

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 $n = m + 1$.

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

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

Corollary 137 *Let* (A, R) *be a directed graph. For all* $s, t \in A$, $s \; R^{\circ *} \; t$ *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 $([n], R)$ 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

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

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 $(\mathcal{P}(A), \supseteq)$.
- $(\ \mathbb{Z}\ ,\ \mid\ )$.

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

$$\mathcal{F}_R = \{\, Q \subseteq A \times A \mid R \subseteq Q \wedge Q \textit{ is a preorder} \,\} \quad .$$

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

PROOF:

Partial functions

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

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

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

$$\forall a \in A.\, \big(\, f(a)\!\downarrow \iff g(a)\!\downarrow \,\big) \;\wedge\; f(a) = g(a)$$

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*,*

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

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:

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

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

- $\mathrm{S} : \mathbb{N} \longrightarrow \mathbb{N}$

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

The function

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

inductively defined from

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

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:

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

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

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

  $\mathrm{S} = \boldsymbol{\rho}_{0,\mathrm{add}}$

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*

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

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

1. *The relation* $\rho_{a,f} : \mathbb{N} \rightarrowtriangle A$ *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* $f : A \to B$ *is said to be* bijective*, or a* bijection*, whenever there exists a (necessarily unique) function* $g : B \to A$ *(referred to as the* inverse *of* f*) such that*

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

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

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

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

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*

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

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

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

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

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

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

Characteristic (or indicator) functions

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

Finite cardinality

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

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

$\boxed{\text{There is an infinite set, containing } \emptyset \text{ and closed under successor.}}$

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. $$\begin{array}{l} \big(\forall\, b \in B.\, \exists\, a \in A.\, f(a) = b\big) \\ \wedge \\ \big(\forall\, a_1, a_2 \in A.\, f(a_1) = f(a_2) \implies a_1 = a_2\big) \end{array}$$

Surjections

Definition 163 *A function* $f : A \longrightarrow B$ *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

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

and we thus have

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

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 $\mathbb{Z}$.

$\cdots$	-3	-2	-1	0	1	2	3	$\cdots$

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

	0	1	2	3	4	5	$\cdots$
0							
1							
2							
3							
4							
$\vdots$							

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

$\boxed{\text{Every surjection has a section.}}$

Injections

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

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

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

$$\begin{tikzcd}[column sep=small, row sep=small]
 & \mathrm{Sur}(A, B) \arrow[dr, phantom, sloped, "\subseteq"] & \\
\mathrm{Bij}(A, B) \arrow[ur, phantom, sloped, "\subseteq"] \arrow[dr, phantom, sloped, "\subseteq"] & & \mathrm{Fun}(A, B) \subseteq \mathrm{PFun}(A, B) \subseteq \mathrm{Rel}(A, B) \\
 & \mathrm{Inj}(A, B) \arrow[ur, phantom, sloped, "\subseteq"] &
\end{tikzcd}$$

with

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

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

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

PROOF IDEA:

Relational images

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

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

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

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

$\boxed{\text{The direct image of every definable functional property on a set is a set.}}$

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:

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

where

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

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:

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

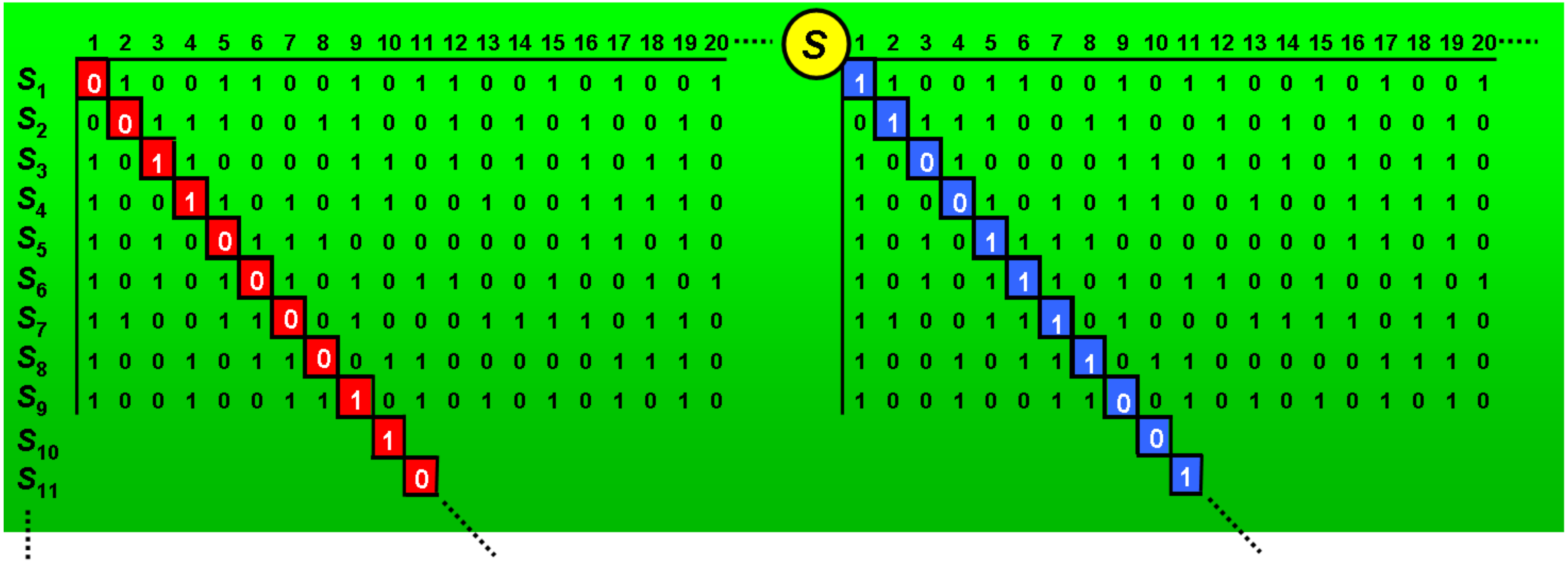
Proposition 177 *An enumerable indexed disjoint union of enumerable sets is enumerable.*

PROOF:

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

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: $S_1, S_2, S_3, \ldots$, 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 $S_1(1)+1, S_2(2)+1, S_3(3)+1, S_4(4)+1, \ldots$, 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.

Created by Robin Whitty for www.theoremoftheday.org

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

$\boxed{\text{The membership relation is well-founded.}}$

Thereby, providing a

Principle of $\in$*-Induction* .