```
(15.1a) “Associativity of +”: (a + b) + c = a + (b + c)
(15.1b) “Associativity of ·”: (a • b) • c = a • (b • c)

(15.2a) “Symmetry of +”: a + b = b + a
(15.2b) “Symmetry of ·”: a • b = b • a

(15.3a) “Additive identity” “Identity of +”: 0 + a = a
(15.3b) “Additive identity” “Identity of +”: a + 0 = a

(15.4a) “Multiplicative identity” “Identity of •”: 1 • a = a
(15.4b) “Multiplicative identity” “Identity of •”: a • 1 = a

(15.5a) “Distributivity of · over +”: a • (b + c) = a • b + a • c
(15.5b) “Distributivity of · over +”: (b + c) • a = b • a + c • a

(15.9) “Zero of ·”: a • 0 = 0            .   =⟨ ⟩   ≡   ≔    [ ]   ⇒

(15.13) “Unary minus”: a + (- a) = 0
(15.14) “Subtraction”: a - b = a + (- b)
(15.17) “Self-inverse of unary minus”: - (- a) = a
(15.19) “Distributivity of unary minus over +”: - b + - d = - (b + d)
(15.24) “Right-identity of -”:  a - 0 = a
“Right-identity of subtraction” [Monus version]

(15.25a) “Mutual associativity of + and -”: a + (b - c) = (a + b) − c

(15.25b) “Subtraction of addition”: a - (b + c) = (a - b) − c
Theorem “Subtraction of subtraction”: a - (b - c) = a - b + c

(15.29a) “Distributivity of · over -”: (a - b) • c = a • c - b • c
(15.29b) “Distributivity of · over -”: c • (a - b) = c • a - c • b
```

Table of Precedences

- $[x := e]$ (textual substitution) **(highest precedence)**
- $.$ (function application)
- unary prefix operators $+, -, \neg, \#, \sim, \mathcal{P}$
- $**$
- $\cdot \quad / \quad \div \quad$ **mod** **gcd**
- $+ \quad - \quad \cup \quad \cap \quad \times \quad \circ \quad \bullet$
- $\downarrow \quad \uparrow$
- $\#$
- $\triangleleft \quad \triangleright \quad \hat{}$
- $= \quad \neq \quad < \quad > \quad \in \quad \subset \quad \subseteq \quad \supset \quad \supseteq \quad |$ (conjunctional)
- $\vee \quad \wedge$
- $\Rightarrow \quad \not\Rightarrow \quad \Leftarrow \quad \not\Leftarrow$
- $\equiv \quad \not\equiv$ **(lowest precedence)**

All non-associative binary infix operators associate to the left, except $**$, $\triangleleft$, $\Rightarrow$, $\rightarrow$, which associate to the right.

Truth Values

Boolean constants/values: *false*, *true*

The type of Boolean values: $\mathbb{B}$

— This is the type of propositions, for example: $(x = 1) : \mathbb{B}$

— For any type t, equality $\_{=}\_$ can be used on expressions of that type: $\_{=}\_ : t \to t \to \mathbb{B}$

Boolean operators:

- $\neg\_ : \mathbb{B} \to \mathbb{B}$ — negation, complement, "logical not"
- $\_\wedge\_ : \mathbb{B} \to \mathbb{B} \to \mathbb{B}$ — conjunction, "logical and"
- $\_\vee\_ : \mathbb{B} \to \mathbb{B} \to \mathbb{B}$ — disjunction, "logical or"
- $\_\Rightarrow\_ : \mathbb{B} \to \mathbb{B} \to \mathbb{B}$ — implication, "implies", "if … then …"
- $\_\equiv\_ : \mathbb{B} \to \mathbb{B} \to \mathbb{B}$ — equivalence, "if and only if", "iff"
- $\_\not\equiv\_ : \mathbb{B} \to \mathbb{B} \to \mathbb{B}$ — inequivalence, "exclusive or"

```
Subtraction Theorems

(15.15) x + a = 0 = x = -a
(15.16) -a = -b = a = b
(15.17) “Self-inverse of unary minus”: -(-a) = a
(15.18) “Fixpoint of unary minus”: -0 = 0
(15.19) “Distributivity of unary minus over +”: - (a +b) = (-a) + (-b)
(15.20) -a = (-1) · a
(15.21) (-a) · b = a · (-b)
(15.22) a · (-b) = - (a · b)
(15.23) (-a) · (-b) = a · b
(15.24) “Right-identity of -”: a - 0 = a
(15.25) (a - b) + (c - d) = (a + c) - (b + d)
(15.26) (a - b) - (c - d) = (a + d) - (b + c)
(15.27) (a - b) · (c - d) = (a · c + b · d) - (a · d + b · c)
(15.28) a - b = c - d = a + d = b + c
(15.29) “Distributivity of · over -”: (a - b) · c = a · c – b · c
Theorem “Subtraction of subtraction”: a - (b - c) = a - b + c
```

```
(3.12) “Double negation”:             ¬ ¬ p ≡ p
(3.8) “Definition of `false`”:        false ≡ ¬ true
(3.13) “Negation of `false`”:       ¬ false ≡ true
----------------------------------------------------------------------
(3.24) “Symmetry of ∨”:                p ∨ q ≡ q ∨ p
(3.25) “Associativity of ∨”:   (p ∨ q) ∨ r ≡ p ∨ (q ∨ r)
(3.26) “Idempotency of ∨”:             p ∨ p ≡ p
(3.29) (3.29a) “Zero of ∨”:         p ∨ true ≡ true
(3.29) (3.29b) “Zero of ∨”:         true ∨ p ≡ true
(3.30) (3.30a) “Identity of ∨”:  p ∨ false ≡ p
(3.30) (3.30b) “Identity of ∨”:  false ∨ p ≡ p
(3.28) “Excluded middle” “LEM”:    p ∨ ¬ p ≡ true
----------------------------------------------------------------------
(3.36) “Symmetry of ∧”:                p ∧ q ≡ q ∧ p
(3.37) “Associativity of ∧”:   (p ∧ q) ∧ r ≡ p ∧ (q ∧ r)
(3.38) “Idempotency of ∧”:             p ∧ p ≡ p
(3.39) (3.39a) “Identity of ∧”:   p ∧ true ≡ p
(3.39) (3.39b) “Identity of ∧”:   true ∧ p ≡ p
(3.40) (3.40a) “Zero of ∧”:      p ∧ false ≡ false
(3.40) (3.40b) “Zero of ∧”:      false ∧ p ≡ false
(3.42) “Contradiction”:            p ∧ ¬ p ≡ false
----------------------------------------------------------------------
(3.47) (3.47a) “De Morgan”:      ¬ (p ∧ q) ≡ ¬ p ∨ ¬ q
(3.47) (3.47b) “De Morgan”:      ¬ (p ∨ q) ≡ ¬ p ∧ ¬ q
Axiom “Conjunction” “Definition of ∧”: p ∧ q ≡ ¬ (¬ p ∨ ¬ q)
----------------------------------------------------------------------
(3.45a) “Distributivity of ∨ over ∧”: p ∨ (q ∧ r) ≡ (p ∨ q) ∧ (p ∨ r)
(3.45b) “Distributivity of ∨ over ∧”: (q ∧ r) ∨ p ≡ (q ∨ p) ∧ (r ∨ p)
(3.46a) “Distributivity of ∧ over ∨”: p ∧ (q ∨ r) ≡ (p ∧ q) ∨ (p ∧ r)
(3.46b) “Distributivity of ∧ over ∨”: (q ∨ r) ∧ p ≡ (q ∧ p) ∨ (r ∧ p)
----------------------------------------------------------------------
“ex falso quodlibet”:      false ⇒ p ≡ true
“Left-identity of ⇒”:       true ⇒ p ≡ p

“Right-zero of ⇒”:          p ⇒ true ≡ true
“Definition of ¬ via ⇒”:    ¬ p ≡ p ⇒ false
----------------------------------------------------------------------
```

```
Axiom “Definition of ≡”: (p ≡ q) = (p = q)
Axiom (3.1) “Associativity of ≡”: ((p ≡ q) ≡ r) ≡ (p ≡ (q ≡ r))
Axiom (3.2) “Symmetry of ≡”: p ≡ q ≡ q ≡ p
Axiom (3.3) “Identity of ≡”: true ≡ q ≡ q
Theorem (3.4): true
Theorem (3.5) “Reflexivity of ≡”: p ≡ p
Axiom (3.8) “Definition of `false`”: false ≡ ¬ true
----------------------------------------------------------------------
Axiom (3.9) “Commutativity of ¬ with ≡”:  ¬(p ≡ q) ≡ ¬ p ≡ q
Theorem (3.11) “¬ connection”: (¬ p ≡ q) ≡ (p ≡ ¬ q)
Theorem (3.12) “Double negation”: ¬ ¬ p ≡ p
Axiom (3.10) “Definition of ≢”: (p ≢ q) ≡ ¬(p ≡ q)
(3.14): (p ≢ q) ≡ ¬ p ≡ q
(3.15) “Definition of ¬ from ≡”: ¬ p ≡ p ≡ false
Theorem (3.16) “Symmetry of ≢”: (p ≢ q) ≡ (q ≢ p)
Theorem “Associativity of ≢”:  ((p ≢ q) ≢ r) = (p ≢ (q ≢ r))
Theorem “Left-identity of ≢”: (false ≢ p) ≡ p
----------------------------------------------------------------------
Axiom “Definition of ≠”: x ≠ y  ≡  ¬ (x = y)
Theorem “Irreflexivity of ≠”: ¬ (x ≠ x)
Theorem “Irreflexivity of ≠”: x ≠ x  ≡  false
Theorem “Symmetry of ≠”:  x ≠ y  ≡  y ≠ x
Activate symmetry property “Symmetry of ≠”
----------------------------------------------------------------------
Theorem “Symmetry of ∧”: p ∧ q ≡ q ∧ p
Theorem (3.37) “Associativity of ∧”: (p ∧ q) ∧ r ≡ p ∧ (q ∧ r)
Theorem (3.38) “Idempotency of ∧”: p ∧ p ≡ p
Theorem (3.39) “Identity of ∧”: p ∧ true ≡ p
Theorem (3.40) “Zero of ∧”: p ∧ false ≡ false
Theorem (3.41) “Distributivity of ∧ over ∧”:
p ∧ (q ∧ r) ≡ (p ∧ q) ∧ (p ∧ r)
Theorem (3.42) “Contradiction”: p ∧ ¬ p ≡ false
Theorem (3.43) (3.43a) “Absorption”: p ∧ (p ∨ q) ≡ p
Theorem (3.43) (3.43b) “Absorption”: p ∨ (p ∧ q) ≡ p
Theorem (3.44) (3.44a) “Absorption”: p ∧ (¬ p ∨ q) ≡ p ∧ q
Theorem (3.44) (3.44b) “Absorption”: p ∨ (¬ p ∧ q) ≡ p ∨ q
Theorem (3.44) (3.44b) “Absorption”: ¬ p ∨ (p ∧ q) ≡ ¬ p ∨ q
----------------------------------------------------------------------
(3.32) : (p ∨ q) ≡ (p ∨ ¬ q) ≡ p
Theorem (3.48): p ∧ q ≡ p ∧ ¬ q ≡ ¬ p
Lemma (3.55):
(p ∧ q) ∧ r ≡ p ≡ q ≡ r ≡ p ∨ q  ≡ q ∨ r ≡ r ∨ p ≡ p ∨ q ∨ r
----------------------------------------------------------------------
Axiom (3.35) “Golden rule”: p ∧ q ≡ p ≡ q ≡ p ∨ q
Theorem (3.36) “Symmetry of ∧”: p ∧ q ≡ q ∧ p
```

```
----------------------------------------------------------------------
Axiom “Zero is not successor”:  0 = suc n  ≡  false
Theorem “Zero is not successor”: 0 ≠ suc n
Theorem “Zero is not one”: 0 ≠ 1
Theorem “Zero is not one”: 0 = 1  ≡  false
Axiom “Cancellation of `suc`”: suc m = suc n  ≡  m = n
----------------------------------------------------------------------
Theorem “Cancellation of +”: k + m = k + n  ≡  m = n
Theorem “Zero product”: 0 = a · b  ≡  0 = a ∨ 0 = b
Theorem “Zero sum”: 0 = a + b  ≡  0 = a  ∧  0 = b
----------------------------------------------------------------------
Axiom “Definition of !”: 0 ! = 1
Axiom “Definition of !”: (suc n)! = (suc n) · n !
Theorem “factorial of one”: 1 ! = 1
----------------------------------------------------------------------

“Replacement in equality with addition”:
        a = b + c ∧ c = d   ≡   a = b + d ∧ c = d

----------------------------------------------------------------------
```

```
Axiom “Associativity of ⊕”: (x ⊕ y) ⊕ z = x ⊕ (y ⊕ z)
Axiom “Left-identity of ⊕”:   x = Id ⊕ x
Axiom “Right-identity of ⊕”:  x = x ⊕ Id
Axiom “Left-zero of ⊕”: 0₁ ⊕ x = 0₁
Axiom “Right-zero of ⊕”: x ⊕ 0₂ = 0₂
Axiom “Symmetry of ⊕”:  x ⊕ y = y ⊕ x

Axiom “Left-inverses”: invL x ⊕ x = Id
Axiom “Right-inverses”: x ⊕ invR x = Id

Axiom “Left-inverse of ⊕”: inv x ⊕ x = Id
Axiom “Right-inverse of ⊕”: x ⊕ inv x = Id

Axiom “Left cancellation”:  l ⊕ x = l ⊕ y  ≡  x = y
Axiom “Right cancellation”: x ⊕ r = y ⊕ r  ≡  x = y

Theorem “Self-connection of inverse” “inv connection”:
inv x = y  ≡  x = inv y
Theorem “Unique idempotence”: x ⊕ x = x  ≡  x = Id
Theorem “From Id to inverses”: x ⊕ y = Id  ≡  x = inv y
Theorem “From Id to inverses”: x ⊕ y = Id  ≡  y = inv x
Theorem “Inverse of Id is Id”: inv Id = Id
Theorem “Involutionarity of `inv`”: inv (inv x) = x
Axiom “Inverse of Id is Id”:              inv Id = Id
Axiom “Involutionarity of `inv`”:         inv (inv x) = x
Axiom “Cancellation of inverse” “Injectivity of inverse”:
inv x = inv y ≡ x = y
Axiom “Co-Distributivity of `inv` over ⊕”:
inv (x ⊕ y) = inv y ⊕ inv x

Axiom “Definition of ⊖”: x ⊖ y = x ⊕ inv y
Theorem “Mutual associativity of ⊕ and ⊖”:
x ⊕ (y ⊖ z) = (x ⊕ y) ⊖ z
Theorem “Right-identity of inverse”: x ⊖ Id = x
Theorem “Self-cancellation of inverse”: x ⊖ x = Id
Theorem “Inverse of composition” “Subtraction of sum”:
    x ⊖ (y ⊕ z) = (x ⊖ z) ⊖ y

Axiom “Definition of ⁅_⁆⇐”:   Q ⁅ C ⁆⇐ P  ≡  P ⇒⁅ C ⁆ Q
```

```
Axiom “Zero is even”:     even 0     ---- read this as: `even 0 ≡ true`
Axiom “Even successor”:   even (suc n) ≡ ¬ (even n)
Axiom “Zero is not odd”:  ¬ odd 0
Axiom “Odd successor”:  odd (suc n) ≡ ¬ (odd n)
Theorem “Odd is not even”:  odd n ≡ ¬ (even n)
----------------------------------------------------------------------
Axiom “Definition of + for 0”
      “Left-identity of +”:           0 + n = n
      “Right-identity of +”:          m + 0 = m
----------------------------------------------------------------------
Axiom “Definition of + for `suc`”:  (suc m) + n = suc (m + n)
Theorem “Successor”: suc n = n + 1
Theorem “Adding the successor”: m + (suc n) = suc (m + n)
Theorem “Symmetry of +”: m + n = n + m

“Definition of · for `suc`” = suc a · b = b + a · b
----------------------------------------------------------------------

Axiom (3.83) “Leibniz”: e = f  ⇒  E[z ≔ e] = E[z ≔ f]
Theorem (3.84) (3.84a) “Replacement”:
    (e = f) ∧ E[z ≔ e]  ≡  (e = f) ∧ E[z ≔ f]
Lemma “Replacement in equality with addition”:
    a = b + c ∧ c = d  ≡  a = b + d ∧ c = d

----------------------------------------------------------------------
```

```
Axiom (3.57) “Definition of ⇒”: p ⇒ q ≡ p ∨ q ≡ q
Theorem “Characterisation of ⇒”:  (k ∧ m) ⇒ n  ≡  k ⇒ (m ⇒ n)
Theorem “Sub-cancellation of ⇐”:  (a ⇐ b) ∧ b   ⇒   a
Axiom (3.58) “Consequence” “Definition of ⇐”: p ⇐ q ≡ q ⇒ p
Theorem “Characterisation of ⇐”:  (k ∧ m) ⇒ n  ≡  k ⇒ (n ⇐ m)
Theorem (3.59) “Definition of ⇒”: p ⇒ q ≡ ¬ p ∨ q
Theorem (3.59) “Material implication”: p ⇒ q ≡ ¬ p ∨ q
Theorem (3.60) “Definition of ⇒”: p ⇒ q ≡ p ∧ q ≡ p
Theorem (3.61) “Contrapositive”: p ⇒ q ≡ ¬ q ⇒ ¬ p
Theorem (3.62): p ⇒ (q ≡ r) ≡ p ∧ q ≡ p ∧ r
Theorem (3.63) “Distributivity of ⇒ over ≡”:
                                          p ⇒ (q ≡ r) ≡ p ⇒ q ≡ p ⇒ r
Theorem (3.64): p ⇒ (q ⇒ r) ≡ (p ⇒ q) ⇒ (p ⇒ r)
Theorem (3.65) “Shunting”: p ∧ q ⇒ r ≡ p ⇒ (q ⇒ r)
Theorem (3.66) “Strong modus ponens”: p ∧ (p ⇒ q) ≡ p ∧ q
Theorem (3.67): p ∧ (q ⇒ p) ≡ p
Theorem (3.68): p ∨ (p ⇒ q) ≡ true
Axiom “Subtraction of successor from successor”: suc m - suc n = m - n
Theorem (3.69): p ∨ (q ⇒ p) ≡ q ⇒ p
Theorem (3.70): p ∨ q ⇒ p ∧ q ≡ p ≡ q
Theorem (3.71) “Reflexivity of ⇒”: (p ⇒ p) ≡ true
Theorem (3.72) “Right zero of ⇒”: (p ⇒ true) ≡ true
Theorem (3.73) “Left identity of ⇒”: (true ⇒ p) ≡ p
Theorem (3.74) “Definition of ¬ from ⇒”: (p ⇒ false) ≡ ¬ p
Theorem (3.75) “ex falso quodlibet”: (false ⇒ p) ≡ true
Theorem (3.76a) “Weakening” “Strengthening”: p ⇒ p ∨ q
Theorem (3.76a) “Weakening” “Strengthening”: p ⇒ p ∨ q
Theorem (3.76b) “Weakening” “Strengthening”: p ∧ q ⇒ p
Theorem (3.76c) “Weakening” “Strengthening”: p ∧ q ⇒ p ∨ q
Theorem (3.76d) “Weakening” “Strengthening”: p ∨ (q ∧ r) ⇒ p ∨ q
Theorem (3.76e) “Weakening” “Strengthening”: p ∧ q ⇒ p ∧ (q ∨ r)
Theorem (3.77) “Modus ponens”: p ∧ (p ⇒ q) ⇒ q
Theorem (3.78): (p ⇒ r) ∧ (q ⇒ r) ≡ (p ∨ q ⇒ r)
Theorem (3.79): (p ⇒ r) ∧ (¬ p ⇒ r) ≡ r
Theorem (3.80) “Mutual implication”: (p ⇒ q) ∧ (q ⇒ p) ≡ p ≡ q
Theorem (3.81) “Antisymmetry of ⇒”: (p ⇒ q) ∧ (q ⇒ p) ≡ (p ≡ q)
Theorem (3.82a) “Transitivity of ⇒”: (p ⇒ q) ∧ (q ⇒ r) ⇒ (p ⇒ r)
Theorem (3.82b) “Transitivity of ⇒”: (p ≡ q) ∧ (q ⇒ r) ⇒ (p ⇒ r)
Theorem (3.82c) “Transitivity of ⇒”: (p ⇒ q) ∧ (q ≡ r) ⇒ (p ⇒ r)
Theorem “Indirect reflexivity of ⇒”: (p ≡ q) ⇒ (p ⇒ q)
“Antisymmetry of ⇒”: (x ⇒ y) ∧ (y ⇒ x) ⇒ x = y
Theorem  “Indirect equality”: (∀ z • z ⇒ x  ≡  z ⇒ y)  ≡  x = y
Theorem (4.2) “Left-monotonicity of ∨” “Monotonicity of ∨”:
                                  (p ⇒ q) ⇒ (p ∨ r) ⇒ (q ∨ r)
```

```
Theorem “Distributivity of ∨ over ⇒”: p ∨ (q ⇒ r) ≡ p ∨ q ⇒ p ∨ r
Theorem “Antitonicity of ¬”: (p ⇒ q) ⇒ (¬ q ⇒ ¬ p)
Theorem “Monotonicity of ⇒” “Right-monotonicity of ⇒”:
                                   (p ⇒ q) ⇒ ((r ⇒ p) ⇒ (r ⇒ q))
Theorem “Antitonicity of ⇒” “Left-antitonicity of ⇒”:
                                   (p ⇒ q) ⇒ ((q ⇒ r) ⇒ (p ⇒ r))
Theorem “Proof by contradiction”:  ¬ p ⇒ false  ≡  p
----------------------------------------------------------------------
“<-Monotonicity of +”:            a < b  ⇒  a + d < b + d
“≤-Monotonicity of +”:            a ≤ b  ⇒  a + d ≤ b + d
“≤-Antitonicity of unary minus”:  a ≤ b  ⇒    - b ≤   - a
“≤-Monotonicity of -”:            a ≤ b  ⇒  a - d ≤ b - d
“≤-Antitonicity of -”:            c ≤ b  ⇒  a - b ≤ a – c
----------------------------------------------------------------------
“Reflexivity of ≤”: a ≤ a
“Transitivity of ≤”: a ≤ b ⇒ b ≤ c ⇒ a ≤ c
“Antisymmetry of ≤”: a ≤ b ⇒ b ≤ a ⇒ a = b
Axiom “Zero is less than successor”: 0 < suc a
Axiom “<-Isotonicity of successor”: suc a < suc b   ≡   a < b
Axiom “Nothing is less than zero”: a < 0   ≡   false
Axiom “Zero is least element”:                0 ≤ a
Axiom “Isotonicity of successor”:         suc a ≤ suc b  ≡  a ≤ b
Axiom “Successor is not at most zero”:    suc a ≤ 0      ≡ false
Theorem “Zero is <-least element”: 0 < a ∨ 0 = a
Theorem “Less than successor”: a < suc b  ≡  a < b ∨ a = b
Theorem “Less than successor”: a < suc a
Theorem “Only zero is less than one”: a < 1  ≡  a = 0
Theorem “Empty range”: a < b < a ⇒ false
Theorem “Empty range”: a < b < a ≡ false
Theorem “Asymmetry of <”: a < b ⇒ ¬ (b < a)
Theorem “Mutual inclusion”: x ≤ y ∧ y ≤ x  ≡  x = y
----------------------------------------------------------------------
Theorem  “Left-antitonicity of <”: (p ≤ q) ⇒ ((q < r) ⇒ (p < r))
Theorem “Right-monotonicity of <”: (p ≤ q) ⇒ ((r < p) ⇒ (r < q))
Theorem  “Left-antitonicity of ≤”: (p ≤ q) ⇒ ((q ≤ r) ⇒ (p ≤ r))
Theorem “Right-monotonicity of ≤”: (p ≤ q) ⇒ ((r ≤ p) ⇒ (r ≤ q))
Theorem  “Weak left-antitonicity of <”: (p < q) ⇒ ((q < r) ⇒ (p < r))
Theorem “Weak right-monotonicity of <”: (p < q) ⇒ ((r < p) ⇒ (r < q))
----------------------------------------------------------------------
Axiom “Predecessor of zero”:       pred 0       = 0
Axiom “Predecessor of successor”:  pred (suc n) = n
Theorem “Predecessor”:  pred n = n – 1
Theorem “Predecessor is non-increasing”: pred a ≤ a
suc (pred 0) = suc 0 = 1
Theorem “Predecessor of non-zero”:  n ≠ 0  ≡  suc (pred n) = n
```

```
Theorem “Monotonicity of predecessor”: a ≤ b ⇒ pred a ≤ pred b

Theorem “Non-<-monotonicity of predecessor”:
       ¬ (a < b ⇒ pred a < pred b)

Theorem “<-Monotonicity of predecessor”:
    suc a < b ⇒ pred (suc a) < pred b
-----------------------------------------------------------------------
“Empty range for ∑”:    (∑ x ❙ false • E)  =  0

“Split off term” “Split off term at top”:
     (∑ i : ℕ ❙ i < suc n • E) = (∑ i : ℕ ❙ i < n • E) + E[i ≔ n]

Axiom (8.11) “Substitution into ∑”: Provided ¬occurs(`y`, `x, F`):
     (∑ y ❙ R • E)[x ≔ F]  =  ∑ y ❙ R[x ≔ F] • E[x ≔ F]

Axiom (8.21) “Dummy renaming”, “α-conversion”: Provided ¬occurs(`y`,
`E, R`):
     (∑ x ❙ R • E) = (∑ y ❙ R[x ≔ y] • E[x ≔ y])

Calculation:
    (∑ i : ℕ ❙ i < k • (∑ j : ℕ ❙ j < i • m · j))
  =⟨ “Reflexivity of =” ⟩
    (∑ j : ℕ ❙ j < k • (∑ k : ℕ ❙ k < j • m · k))
-----------------------------------------------------------------------
Axiom “if true”:   if true  then x else y fi  =  x
Axiom “if false”:  if false then x else y fi  =  y

(3.89) “Shannon”: E[z ≔ p]≡(p ∧ E[z ≔ true]) ∨ (¬ p ∧ E[z ≔ false])
“Zero of ∨”

Theorem “`if` to ∨”:
    P[z ≔ if b then x else y fi]
  ≡ (b ∧ P[z ≔ x]) ∨ (¬ b ∧ P[z ≔ y])

Theorem “if swap”:
      if   b then x else y fi
   =  if ¬ b then y else x fi
-----------------------------------------------------------------------
Axiom “Reflexivity of ⊑”: a ⊑ a
Axiom “Transitivity of ⊑”: a ⊑ b  ∧  b ⊑ c  ⇒  a ⊑ c
Axiom “Antisymmetry of ⊑”: a ⊑ b  ∧  b ⊑ a  ⇒  a = b

Theorem “Indirect reflexivity of ⊑”:  a = b  ⇒  a ⊑ b
```

```
Theorem “Mutual ⊑”: a ⊑ b  ∧  b ⊑ a  ≡  a = b

Theorem “Conjunctional Practice α”: a ⊑ a ⊑ b  ≡  a ⊑ b
Theorem “Conjunctional Practice β” “Sandwhich theorem”:
a ⊑ b ⊑ a  ≡  a = b
Theorem “Conjunctional Practice γ” “Chaining”:
a ⊑ b ⊑ c  ⇒  a ⊑ c
----------------------------------------------------------------------
Axiom “First bottom”:  ⊥₁ ⊑ a
Axiom “Second bottom”: ⊥₂ ⊑ a
Theorem “Bottoms are unique”: ⊥₁ = ⊥₂
Axiom “Bottom of ⊑”: ⊥ ⊑ a

Axiom “First top”: a ⊑ ⊤₁
Axiom “Second top”: b ⊑ ⊤₂
Axiom “Top is greatest element”: a ⊑ ⊤
----------------------------------------------------------------------
Axiom “Definition of retract `f⊑`”: a f⊑ b   ≡   f a ⊑ f b
Theorem “Reflexivity of retract `f⊑`”: a  f⊑  a
Theorem “Transitivity of retract `f⊑`”: a f⊑ b  ∧  b f⊑ c  ⇒  a f⊑ c

Axiom “Definition of retract equivalence”: a f= b   ≡   f a = f b
Theorem “Reflexivity of retract equivalence”:  a  f=  a
Theorem “Transitivity of retract equivalence”:
                          a f= b  ∧  b f= c  ⇒  a f= c
Theorem “Symmetry of retract equivalence”: a f= b  ≡  b f= a
Theorem “Relative antisymmetry of retract `f⊑`”:
          a f⊑ b  ∧  b f⊑ a  ⇒  a f= b
----------------------------------------------------------------------
Axiom “Definition of induced order”: a ⊕⊑ b ≡ a ⊕ b = b
Axiom “Idempotency of ⊕”: a ⊕ a = a
Theorem “Reflexivity of induced order”: a ⊕⊑ a
Axiom “Symmetry of ⊕”: a ⊕ b  =  b ⊕ a
Theorem “Antisymmetry of induced order”: a ⊕⊑ b  ∧  b ⊕⊑ a ⇒ a = b
Theorem “Transitivity of induced order”: a ⊕⊑ b  ∧  b ⊕⊑ c ⇒a ⊕⊑ c
Axiom “Associativity of ⊕”:  (a ⊕ b) ⊕ c  =  a ⊕ (b ⊕ c)

Axiom “Left-Identity of ⊕”:  Id ⊕ a  =  a
Axiom “Right-Identity of ⊕”:  a ⊕ Id  =  a
----------------------------------------------------------------------
Axiom “Reflexitivity of |”: m | m
Axiom “Antisymmetry of |”: m | n  ∧  n | m  ⇒  n = m
Axiom “Transitivity of |”: m | n  ∧  n | k  ⇒  m | k
Theorem “Mutual divisibility” “Mutual |”:  m | n  ∧  n | m  ≡  n = m
Axiom “Divisibility of multiples”: m | (q · m)
```

```
Theorem “Bottom of |” “Least element of |”: 1 | m
Theorem “Top of |” “Greatest value of |”: m | 0
Theorem “Top of |” “Greatest value of |” “Top is maximal”:
   0 | n  ≡  n = 0
Theorem “Bottom of |” “Least element of |” “Bottom is minimal”:
  m | 1  ≡  m = 1
Axiom “Invariance of Divisibility under semi-linear combinations”:
   k | x  ∧  k | y  ≡  k | (x + a · y) ∧ k | y
   k | y ⇒ (k | (x + a · y) ≡ k | x)
Theorem “|-Weakening” “|-Strengthening”:
  m | n  ⇒  m | (q · n)
Theorem “Divisibility of sums”: a | b  ∧  a | c  ⇒  a | (b + c)
Theorem “Divisiblity of linear combinations”:
            a | b  ∧  a | c  ⇒  a | (b · x + c · y)
----------------------------------------------------------------------
Axiom “Characterisation of ⊓”:  c ⊑ a  ∧  c ⊑ b  ≡  c  ⊑  a ⊓ b
Theorem “Weakening for ⊓”: a ⊓ b  ⊑  a
Theorem “Weakening for ⊓”: a ⊓ b  ⊑  b
Theorem “Left-Monotonicity of ⊓”: a ⊑ b  ⇒  a ⊓ c ⊑ b ⊓ c
Theorem “Idempotency of ⊓”: a ⊓ a  =  a
Theorem “Induced definition of inclusion”: a ⊑ b  ≡  a ⊓ b = a
----------------------------------------------------------------------
Axiom “Characterisation of ⊔”:   a ⊑ c  ∧  b ⊑ c  ≡  a ⊔ b  ⊑  c
Theorem “Weakening for ⊔”: a  ⊑  a ⊔ b
Theorem (3.76l) “Weakening for ⊔”: b  ⊑  a ⊔ b
Theorem “Idempotency of ⊔”:  a ⊔ a = a
Theorem “Induced definition of inclusion”: a ⊑ b  ≡ a ⊔ b = b
Theorem “Absorption” “Squeeze Law” “Sandwich Theorem”: a ⊓ (b ⊔ a) = a
Theorem “Absorption” “Squeeze Law” “Sandwich Theorem”: a ⊔ (b ⊓ a) = a
Theorem “Weakening from ⊓ to ⊔” “Strengthening from ⊔ to ⊓”:
                                                       a ⊓ b  ⊑  a ⊔ b
----------------------------------------------------------------------
Theorem “Symmetry of ⊓”: a ⊓ b = b ⊓ a
Theorem “Symmetry of ⊔”: a ⊔ b = b ⊔ a
Theorem “Golden rule for ⊓ and ⊔”: b ⊓ a = a  ≡   b = a ⊔ b
Theorem “Golden rule for ⊓ and ⊔”: b ⊓ a = a ⊔ b  ≡   a = b
Theorem “Indirect zero of ⊔”:   a ⊔ ⊤ ⊑ c  ≡  ⊤ ⊑ c
----------------------------------------------------------------------
Axiom “Characterisation of ÷”:  k · m ≤ n  ≡  k ≤ n ÷ m
Theorem “Sub-cancellation of ÷”:  (a ÷ b) · b ≤ a
Theorem “Mutual inclusion”: x ≤ y ∧ y ≤ x  ≡  x = y
Theorem “Dividing a division”: (a ÷ b) ÷ c  =  a ÷ (b · c)
Theorem “Indirect equality (from below)”: x = y ≡(∀ z • z ≤ x ≡ z ≤ y)
Theorem “Dividing a division, elegantly”: (a ÷ b) ÷ c  =  a ÷ (b · c)
Theorem “Linearity”: m ≤ n ∨ n ≤ m
```

```
Theorem “Mutual inclusion” “Weak trichotomy”: (m ≤ n ≡ n ≤ m) ≡ n = m

Theorem “Indirect equality (from below)”:
                                          x = y ≡(∀ z • z ⊑ x ≡ z ⊑ y)
Theorem “Indirect inclusion (from below)”:
                                          x ⊑ y≡(∀ z • z ⊑ x ⇒ z ⊑y)


----------------------------------------------------------------------
Theorem “Associativity of ⊓”: (a ⊓ b) ⊓ c  =  a ⊓ (b ⊓ c)
Theorem “Monotonicity of ⊓”: a ⊑ a’  ⇒  b ⊑ b’  ⇒  a ⊓ b ⊑ a’ ⊓ b’
Axiom “Definition of ⊏”: a ⊏ b  ≡  a ⊑ b  ∧  a ≠ b
Theorem “Irreflexivity of ⊏”: a ⊏ a  ≡  false
Theorem “Irreflexivity of ⊏”:  a ⊏ b  ⇒  ¬ (a = b)
Theorem “Transitivity of ⊏”: a ⊏ b ∧ b ⊏ c ⇒ a ⊏ c
Theorem “Reflexivity of ⊑”: a = b  ⇒  a ⊑ b
Theorem “Definition of ⊑ in terms of ⊏”: a ⊑ b  ≡  a ⊏ b ∨ a = b
Theorem “Empty Range”: a ⊏ b ⊏ a ⇒ false
Theorem “Empty Range”: a ⊏ b ⊏ a ≡ false
Theorem “Empty Range”: a ⊑ b ⊏ a ≡ false
Theorem “⊏-⊑-Transitivity”: k ⊏ m ⊑ n ⇒ k ⊏ n
Axiom “Converse of ⊏”: a ⊐ b ≡ b ⊏ a
Axiom “Converse of ⊑”: a ⊒ b ≡ b ⊑ a
Theorem “Asymmetry of ⊏”: a ⊏ b ⇒ ¬ (b ⊏ a)
----------------------------------------------------------------------
Theorem (9.13) “Instantiation”: (∀ x • P) ⇒ P[x ≔ E]
Axiom (3): (∀ x : ℤ • f x = f (x + 2))
Axiom (5): g x = x · x
----------------------------------------------------------------------
Axiom “Zero is not suc”: 0 = n + 1  ≡  false
Axiom “Definition of +”: 0 + n = n
Theorem “Right-identity of +”: ∀ m : ℕ • m + 0 = m
Theorem “Adding the successor”: m + (n + 1) = (m + n) + 1
Axiom “Definition of +”: (m + 1) + n = (m + n) + 1
Theorem “Symmetry of +”: ∀ m • ∀ n • m + n = n + m
Theorem “Associativity of +”: ∀ k• ∀ m• ∀ n• (k + m) + n = k + (m + n)
Theorem “Zero sum”: ∀ m • ∀ n • 0 = m + n  ≡  0 = m  ∧  0 = n
----------------------------------------------------------------------
Axiom (13.3) “Cons is not empty”: x ◃ xs ≠ ϵ
Axiom (13.4) “Cancellation of ◃”: x ◃ xs = y ◃ ys  ≡  x = y ∧ xs = ys
Axiom (13.12) “Definition of ▹ for ϵ”:        ϵ ▹ a = a ◃ ϵ
Axiom (13.13) “Definition of ▹ for ◃”:   (a ◃ s) ▹ b = a ◃ (s ▹ b)
Theorem (13.14) “Snoc is not empty”:  xs ▹ x ≠ ϵ
----------------------------------------------------------------------
```

```
----------------------------------------------------------------------
Axiom (13.17)
      “Left-identity of ⌢”
      “Definition of ⌢ for ϵ”:             ϵ ⌢ ys = ys
Axiom (13.18)
      “Mutual associativity of ◃ with ⌢”
      “Definition of ⌢ for ◃”:      (x ◃ xs) ⌢ ys = x ◃ (xs ⌢ ys)
Theorem (13.19) x ⌢ ys:
    xs ⌢ ϵ = xs
Theorem (13.20) “Associativity of ⌢”:
Theorem (13.23) “Empty concatenation”: xs ⌢ ys = ϵ  ≡  xs = ϵ ∧ ys = ϵ
----------------------------------------------------------------------
Axiom “Under”: x ⊕ y =                        z  ≡  y = x ╲ z
Axiom “Over”:  x ⊕ y =                        z  ≡  x = z ╱ y
Theorem “Under with ⊕ in the numerator”:      y = x ╲ (x ⊕ y)
Theorem “⊕ then Under”:                       x ⊕ (x ╲ z) = z
Theorem “Over with ⊕ in the numerator”:       x = (x ⊕ y) ╱ y
Theorem “Over then ⊕”:                        (z ╱ y) ⊕ y = z
Theorem “Fractions”:                          a ╲ b  =  b ╱ a
Axiom “Definition of percentage”: x %-of y  =  (x div 100) · y
Axiom “Into the numerator”: (x div z) · y = (x · y) div z
----------------------------------------------------------------------
Axiom (15.53) (15.53a) “Definition of ↓”: z ≤ x ↓ y  ≡  z ≤ x ∧ z ≤ y
Axiom (15.53) (15.53b) “Definition of ↑”: x ↑ y ≤ z ≡  x ≤ z ∧ y ≤ z
Theorem (15.54) “Symmetry of ↓”:  x ↓ y = y ↓ x
Theorem (15.54) “Symmetry of ↑”:  x ↑ y = y ↑ x
Theorem (15.55) “Associativity of ↓”: (x ↓ y) ↓ z = x ↓ (y ↓ z)
Theorem (15.55) “Associativity of ↑”: (x ↑ y) ↑ z = x ↑ (y ↑ z)
Theorem (15.56) “Idempotency of ↓”: x ↓ x = x
Theorem (15.56) “Idempotency of ↑”:  x ↑ x = x
Theorem (15.57) “Minimum is lower bound”: x ↓ y ≤ x  ∧  x ↓ y ≤ y
Theorem (15.57) “Maximum is upper bound”: x ≤ x ↑ y  ∧  y ≤ x ↑ y
Theorem (15.58) “At most via minimum”: x ≤ y  ≡  x ↓ y = x
Theorem (15.58) “At most via maximum”: x ≤ y  ≡  x ↑ y = y
----------------------------------------------------------------------
Axiom “Associativity of ⨾”:  (x ⨾ y) ⨾ z  =  x ⨾ (y ⨾ z)
Axiom “Left-identity of ⨾”:  Id ⨾ x = x
Axiom “Right-Identity of ⨾”: x ⨾ Id = x
Axiom “Characterisation of ╱”:  a ⨾ b ⊑ c  ≡  a ⊑ c ╱ b
Axiom “Characterisation of ╲”:  a ⨾ b ⊑ c  ≡  b ⊑ a ╲ c
Theorem “Cancellation of ╱”: (a ╱ b) ⨾ b ⊑ a
Theorem “Cancellation of ╲”: a ⨾ (a ╲ b) ⊑ b
Theorem “Right-division of multiples”: a ⊑ (a ⨾ b) ╱ b
Theorem “Left-division of multiples”: b ⊑ a ╲ (a ⨾ b)
```

```
Theorem “Dividing a division”: (a ╱ b) ╱ c  =  a ╱ (c ⨾ b)
Theorem “Dividing a division”: a ╲ (b ╲ c)  =  (b ⨾ a) ╲ c
Theorem “Monotonicity of ⨾”: a ⊑ a′ ⇒ a ⨾ b ⊑ a′ ⨾ b
Theorem “Monotonicity of ⨾”: b ⊑ b′ ⇒ a ⨾ b ⊑ a ⨾ b′
Theorem “Monotonicity of ⨾”: a ⊑ a′ ∧ b ⊑ b′ ⇒ a ⨾ b ⊑ a′ ⨾ b′
Theorem “Numerator monotonicity”: a ⊑ a′ ⇒  a ╱ b ⊑ a′ ╱ b
Theorem “Numerator monotonicity”: b ⊑ b′ ⇒  a ╲ b ⊑ a ╲ b′
Theorem “Denominator antitonicity”: b′ ⊑ b ⇒  a ╱ b ⊑ a ╱ b′
Theorem “Denominator antitonicity”: a′ ⊑ a ⇒  a ╲ b ⊑ a′ ╲ b

Theorem “Dividing a division”: ((a ⇐ b) ⇐ c)  =  (a ⇐ (c ∧ b))


----------------------------------------------------------------------
Axiom (11.4) “Set extensionality”:
   S = T  ≡  (∀ e  •  e ∈ S  ≡  e ∈ T)
Axiom (11.13) “Subset” “Definition of ⊆” “Set inclusion”:
                                       S ⊆ T  ≡  (∀ e ❙ e ∈ S • e ∈ T)
Corollary “Subset” “Definition of ⊆” “Set inclusion”:
                                      S ⊆ T  ≡  (∀ e • e ∈ S ⇒ e ∈ T)
Theorem “Subset membership” “Casting”:  X ⊆ Y ⇒ x ∈ X ⇒ x ∈ Y
Theorem (11.59) “Transitivity of ⊆”: X ⊆ Y ⇒ Y ⊆ Z ⇒ X ⊆ Z
Theorem (11.58) “Reflexivity of ⊆”: X ⊆ X
Theorem (11.57) “Antisymmetry of ⊆”: X ⊆ Y ⇒ Y ⊆ X ⇒ X = Y
Theorem (11.57) “Antisymmetry of ⊆”: X ⊆ Y ⇒ Y ⊆ X ⇒ X = Y
Theorem (11.57) “Antisymmetry of ⊆”: X ⊆ Y ⇒ Y ⊆ X ⇒ X = Y
----------------------------------------------------------------------
Axiom “Complement”: e ∈ ~ S  ≡ ¬ (e ∈ S)
Theorem (11.19) “Self-inverse of complement”: ~ (~ S) = S
Theorem “Lower ~ connection for ⊆”:  ~ X ⊆ Y  ≡  ~ Y ⊆ X
Theorem “Upper ~ connection for ⊆”:  X ⊆ ~ Y  ≡  Y ⊆ ~ X
Theorem “Upper ~ connection for ⊆”:  X ⊆ ~ Y  ≡  Y ⊆ ~ X
----------------------------------------------------------------------
Axiom “Union”:          e ∈ S ∪ T  ≡  e ∈ S  ∨  e ∈ T
Axiom “Intersection”:   e ∈ S ∩ T  ≡  e ∈ S  ∧  e ∈ T
Theorem (11.45) “Inclusion via ∪”:  S ⊆ T  ≡  S ∪ T = T
----------------------------------------------------------------------
Theorem “Set Abbreviation”:{ x ❙ P } = { x ❙ P • x }
Theorem (11.7) (11.7s) “Simple Membership”: e ∈ { x ❙ P }  ≡ P[x ≔ e]
Theorem (11.7) (11.7x) “Simple Membership”:  x ∈ { x ❙ P }  ≡ P
Theorem (11.7) (11.7∀) “Simple Membership”:  ∀ x • x ∈ { x ❙ P }  ≡ P
Axiom (11.4) “Set extensionality”: S = T  ≡  (∀ e  •  e ∈ S  ≡  e ∈ T)
Theorem (11.6) “Mathematical formulation of set comprehension”:
                          {x ❙ P • E } = { y ❙ (∃ x ❙ P • y = E) }
Theorem (11.9) “Simple set comprehension equality”:
```

```
                            {x ❙ Q} = {x ❙ R}  ≡  (∀ x • Q ≡ R)
----------------------------------------------------------------------
Axiom (14.2) “Pair equality”: ⟨ b, c ⟩ =  ⟨ b', c' ⟩  ≡  b = b' ∧ c = c'
Axiom “Definition of `fst`”: fst ⟨ x, y ⟩ = x
Axiom “Definition of `snd`”: snd ⟨ x, y ⟩ = y
Axiom “Pair equality”: p = q  ≡  fst p = fst q  ∧  snd p = snd q
Axiom “Membership in ×”:p ∈ S × T  ≡  fst p ∈ S ∧ snd p ∈ T
Theorem (14.4) “Membership in ×”: ⟨ x , y ⟩ ∈ S × T  ≡  x ∈ S ∧ y ∈ T
Theorem “Pair extensionality”: p = ⟨ fst p , snd p ⟩
Theorem (14.5) “Membership in swapped ×”:
                     ⟨ x , y ⟩ ∈ S × T  ≡  ⟨ y , x ⟩ ∈ T × S
Theorem (14.6) “Empty factor in ×”:S = {}  ⇒  S × T = {}
Theorem “fst after swap-×”: fst (swap-× p) = snd p
Theorem “snd after swap-×”: snd (swap-× p) = fst p
Axiom (11.22) “Set difference”: v ∈ S - T ≡ v ∈ S ∧ ¬ (v ∈ T)
----------------------------------------------------------------------
“Definition of ↔”:  t₁ ↔ t₂  =  set ❰ t₁ , t₂ ❱
Axiom “Infix relationship” “Definition of `_⦗_⦘_`”:
    a ⦗ R ⦘ b  ≡  ⟨ a , b ⟩ ∈ R
Axiom “Relation extensionality”:
                     R = S  ≡  (∀ x • ∀ y • x ⦗ R ⦘ y  ≡  x ⦗ S ⦘ y)
Axiom “Relation inclusion”:
                     R ⊆ S  ≡  (∀ x • ∀ y • x ⦗ R ⦘ y  ⇒  x ⦗ S ⦘ y)
Theorem “Empty relation”: a ⦗ {} ⦘ b  ≡ false
Lemma “Singleton relation”: a₁ ⦗ { ⟨ a₂ , b₂ ⟩ } ⦘ b₁ ≡ a₁ = a₂ ∧ b₁= b₂
Lemma “Singleton relation inclusion”:  { ⟨ a , b ⟩ } ⊆ R  ≡  a ⦗ R ⦘ b
Theorem “Relation complement”: a ⦗ ~ R ⦘ b  ≡  ¬ (a ⦗ R ⦘ b)
Theorem “Relation union”:  a ⦗ R ∪ S ⦘ b  ≡  a ⦗ R ⦘ b  ∨  a ⦗ S ⦘ b
Theorem “Relation intersection”: a ⦗ R ∩ S ⦘ b  ≡  a ⦗ R ⦘ b ∧ a ⦗ S ⦘ b
Theorem “Relation difference”: a ⦗ R - S ⦘ b  ≡  a ⦗ R ⦘ b ∧ ¬ (a⦗ S ⦘b)
----------------------------------------------------------------------
Axiom “Definition of 𝕀”: 𝕀 B = { x ❙ x ∈ B • ⟨ x , x ⟩ }
Theorem “Relationship via 𝕀”: x ⦗ 𝕀 B ⦘ y  ≡  x = y ∈ B


----------------------------------------------------------------------
Axiom “Membership in `Dom`”:  x ∈ Dom R  ≡  ∃ y • x ⦗ R ⦘ y
Axiom “Membership in `Ran`”:  y ∈ Ran R  ≡  ∃ x • x ⦗ R ⦘ y
Theorem “Domain of union”: Dom (R ∪ S) = Dom R ∪ Dom S
Theorem “Domain of intersection”: Dom (R ∩ S) ⊆ Dom R ∩ Dom S
Axiom “Relation converse” “Relationship via ˘”:y ⦗ R ˘ ⦘ x  ≡  x ⦗ R ⦘ y
Theorem “Self-inverse of ˘”:   R ˘ ˘  =  R
Theorem “Monotonicity of ˘”: R ⊆ S      ⇒  R ˘ ⊆ S ˘
Theorem “Isotonicity of ˘”: R ⊆ S   ≡   R ˘ ⊆ S ˘
Theorem “Domain of converse”: Dom (R ˘) = Ran R
```

```
Theorem “Converse of ∩”:     (R ∩ S) ˘  =  R ˘ ∩ S ˘
Axiom “Relation composition”: a ⦗ R ⨾ S ⦘ c ≡ ∃ b • a ⦗ R ⦘ b ∧ b ⦗ S ⦘ c
Theorem “Converse of ⨾”:    (R ⨾ S) ˘    =  S ˘ ⨾ R ˘
Axiom “Definition of `Id` via 𝕀”: Id = 𝕀 𝐔
Theorem “Identity relation” “Relationship via `Id`”:
                                                x ⦗ Id ⦘ y  ≡  x = y
Theorem “Converse of `Id`”: Id ˘   =  Id
Theorem “Left-identity of ⨾” “Identity of ⨾”: Id ⨾ R = R
Theorem “Right-identity of ⨾” “Identity of ⨾”: R ⨾ Id = R
Axiom “Definition of reflexivity”:  reflexive R  ≡  ∀ x • x ⦗ R ⦘ x
Theorem “`Id` is reflexive”: reflexive Id
Theorem “Reflexivity”:  reflexive R  ≡  Id ⊆ R
Theorem “Composition of reflexive relations”:
       reflexive R ⇒ reflexive S ⇒ reflexive (R ⨾ S)
Theorem “Composition of reflexive relations”:
       reflexive R ⇒ reflexive S ⇒ reflexive (R ⨾ S)
Theorem “Converse of reflexive relations”:
                             reflexive R ⇒ reflexive (R ˘)
Theorem “Converse reflects reflectivity”:
                             reflexive (R ˘) ⇒ reflexive R
Axiom “Definition of transitivity”:
              transitive R   ≡  ∀ x • ∀ y • ∀ z •
                               x ⦗ R ⦘ y ⦗ R ⦘ z  ⇒  x ⦗ R ⦘ z
----------------------------------------------------------------------
Summing to zero:     x  +  y  = 0  ≡  x  = 0  ∧  y  = 0
Catenating to empty: xs ⌢ ys = ϵ   ≡  xs = ϵ  ∧  ys = ϵ
Axiom “Definition of reverse”: reverse ϵ = ϵ
Axiom “Definition of reverse”: reverse (x ◃ xs) = reverse xs ▹ x
Theorem “Reverse co-distributes over catenation”:
                      reverse (xs ⌢ ys) = reverse ys ⌢ reverse xs
Axiom “˘⨾˘” “Converse co-distributes over composition”:
                                                 (x ⨾ y) ˘ = y ˘ ⨾ x ˘
Axiom “˘˘” “Converse is involutive”:  (x ˘) ˘ = x
Axiom “Monotonicity of _˘”:  a ⊑ b  ⇒  a ˘  ⊑  b ˘
Theorem “Converse is self-connected”:  a ˘ ⊑  b  ≡  a  ⊑  b ˘
Theorem “Cancellation of converse”:  a ˘ = b ˘  ≡  a = b
Axiom “Definition of `univalent`” “Univalence”:
   univalent f  ≡  f ˘ ⨾ f  ⊑  Id
Axiom “Definition of `surjective`” “Surjectivity”:
   surjective f  ≡  Id  ⊑ f ˘ ⨾ f
Axiom “Definition of `total`” “Totality”:
   total f  ≡  Id  ⊑  f ⨾ f ˘
Axiom “Definition of `injective`” “Injectivity”:
   injective f  ≡  f ⨾ f ˘  ⊑ Id
```

```
Axiom “Definition of `mapping`” “Mapping”:
   mapping f  ≡  total f  ∧  univalent f
Axiom “Definition of `bijective`” “Bijectivity”:
   bijective f  ≡ surjective f  ∧  injective f
Theorem “Duality of univalence and injectivity”:
                                  univalent (x ˘) ≡ injective x
Theorem “Duality of totality and surjectivity”:
                                  total (x ˘) = surjective x
Theorem “Duality of mapping and bijectivity”:
                                  mapping (x ˘) = bijective x
----------------------------------------------------------------------
Theorem “Total injectives are precisely the right-invertibles”:
      total f  ∧  injective f  ⇒  f ⨾ f ˘ = Id
Theorem “Proof route for masochists”:
      total f  ∧  injective f  ⇒  f ⨾ f ˘ = Id
Axiom “Definition of iso” “Isomorphism”:
      iso f  ≡ mapping f  ∧ bijective f
Theorem “Isos are precisely the invertibles”:
      iso f  ≡  f ⨾ f ˘ = Id  ∧  f ˘ ⨾ f = Id
Theorem “Iso via ∃”: iso x  ⇒  (∃ y • x ⨾ y = Id = y ⨾ x)
Theorem “Exact division”: (∃ z • y = x ⨾ z) ⇒ x ⨾ (x ╲ y) = y
Theorem “Exact division”: (∃ z • y = x ╲ z)  ⇒  x ╲ (x ⨾ y) = y
----------------------------------------------------------------------
Theorem “Shunting of univalents”:
                    univalent f  ⇒  ( x ⨾ f ⊑ y  ⇐  x ⊑ y ⨾ f ˘ )
Theorem “Shunting of totals”:
                    total f ⇒ ( x ⨾ f ⊑ y  ⇒  x ⊑ y ⨾ f ˘ )
Theorem “Shunting of mappings”:
              univalent f  ⇒ total f ⇒ ( x ⨾ f ⊑ y  ≡  x ⊑ y ⨾ f ˘ )
Theorem “Multiplying by converse of univalents is division”:
                    univalent f  ⇒  x ⨾ f ˘  ⊑  x ╱ f
Theorem “Dividing by totals is multiplying by converse”:
                    total f  ⇒  x ╱ f  ⊑  x ⨾ f ˘
Theorem “Division by mappings is precisely multiplying by converse”:
                    univalent f  ⇒ total f ⇒ x ╱ f  =  x ⨾ f ˘
----------------------------------------------------------------------
Theorem “Modular law”:  a ╲ b  ⊓ c  ⊑  a ╲ (b ⊓ a ⨾ c)
Theorem “Numerators preserve meets”: a ╲ (b ⊓ c)  =  a ╲ b ⊓ a ╲ c


----------------------------------------------------------------------
Theorem “Monotonicity of ∪”: A₁ ⊆ A₂ ⇒ (A₁ ∪ B) ⊆ (A₂ ∪ B)
Theorem “Monotonicity of ∪”: A₁ ⊆ A₂ ⇒ B₁ ⊆ B₂ ⇒(A₁ ∪ B₁)⊆(A₂ ∪ B₂)
Theorem “Distributivity of ⨾ over ∪ to the left”
        “Distributivity of ⨾ over ∪”: (Q ∪ R) ⨾ S  =  Q ⨾ S  ∪  R ⨾ S
```

Axiom “Definition of univalence”: is-univalent R ≡ R ˘ ⨾ R ⊆ Id
Theorem “Univalence of composition”:
is-univalent R ⇒ is-univalent S ⇒ is-univalent (R ⨾ S)
Theorem “Univalence”:
is-univalent R ≡ ∀ b_1 • ∀ b_2 • ∀ a • a [R] b_1 ∧ a [R] b_2 ⇒ b_1 = b_2
Axiom “Definition of totality”: is-total R ≡ Id ⊆ R ⨾ R ˘
Theorem “Totality of union”: is-total R ⇒ is-total S ⇒is-total(R ∪ S)
Theorem “Totality”: is-total R ≡ ∀ a • ∃ b • a [R] b
Theorem “Domain of total relations”: is-total R ≡ **U** ⊆ Dom R
Theorem “Domain of total relations”: is-total R ≡ Dom R = **U**
Axiom “Definition of injectivity”:
is-injective R ≡ R ⨾ R ˘ ⊆ Id
Theorem “Injectivity of converse”:
is-injective (R ˘) ≡ is-univalent R

“Relationship via ×”: x [S × T] y ≡ x ∈ S ∧ y ∈ T
“Distributivity of × over ∪”: S × (T ∪ U) = (S × T) ∪ (S × U)
“Distributivity of × over ∪”: (S ∪ T) × U = (S × U) ∪ (T × U)
“Distributivity of × over ∩”: S × (T ∩ U) = (S × T) ∩ (S × U)
“Distributivity of × over ∩”: (S ∩ T) × U = (S × U) ∩ (T × U)
Theorem “Converse of ×”: (A × B) ˘ = B × A

“Relation extensionality”: R = S ≡ (∀x•(∀ y • x [R] y ≡ x [S] y))

Axiom “Definition of ◁”: A ◁ R = R ∩ (A × **U**)
Axiom “Definition of ▷”: R ▷ B = R ∩ (**U** × B)
Axiom “Definition of ⩤”: A ⩤ R = R ∩ (~ A × **U**)
Axiom “Definition of ⩥”: R ⩥ B = R ∩ (**U** × ~ B)

Lemma “Definition of ⩤ via ◁”: A ⩤ R = ~ A ◁ R
Lemma “Definition of ⩥ via ▷”: R ⩥ B = R ▷ ~ B

Theorem “Distributivity of ◁ over set intersection”:
(A ∩ B) ◁ R = (A ◁ R) ∩ (B ◁ R)
Theorem “Distributivity of ◁ over relation union”:
A ◁ (R ∪ S) = (A ◁ R) ∪ (A ◁ S)
Theorem “Definition of ▷ via ◁”: R ▷ B = (B ◁ R ˘) ˘
Theorem “Definition of ◁ via ▷”: A ◁ R = (R ˘ ▷ A) ˘
Theorem “Distributivity of ▷ over set intersection”:
R ▷ (B ∩ C) = (R ▷ B) ∩ (R ▷ C)
Theorem “Distributivity of ▷ over relation union”:
(R ∪ S) ▷ B = (R ▷ B) ∪ (S ▷ B)
Theorem “Range of ◁”: Ran (R ▷ B) = Ran R ∩ B

```
Theorem “Relationship via ◁” “Domain restriction”:
    x ⁅ A ◁ R ⁆ y  ≡  x ∈ A ∧ x ⁅ R ⁆ y
Theorem “Relationship via ▷” “Range restriction”:
    x ⁅ R ▷ B ⁆ y  ≡  x ⁅ R ⁆ y ∈ B
Theorem “Relationship via ⩤” “Domain antirestriction”:
    x ⁅ A ⩤ R ⁆ y  ≡  ¬ (x ∈ A) ∧ x ⁅ R ⁆ y
Theorem “Domain restriction by `Dom`”:  Dom S ◁ S = S
Theorem “Domain restriction via ⨾”:   A ◁ R = 𝕀 A ⨾ R
----------------------------------------------------------------------
Axiom “Pr completeness”: (∑ e • pr e) = 1
Axiom “Pr min”: 0 ≤ pr e
Axiom “Pr max”: pr e ≤ 1
Axiom “Pr of a compound event”: Pr A = (∑ e ❙ e ∈ A • pr e)
Theorem “Pr of a compound event”: Pr {e ❙ R} = (∑ e ❙ R • pr e)
Theorem “Pr likelihood of the absurd”: Pr {} = 0
Theorem “Pr likelihood of the certain”: Pr 𝐔 = 1
Theorem “Pr non-negativity”:  ∀ e • pr e ≥ 0
Theorem “Pr Principle of Inclusion-Exclusion” “PIE”:
  Pr A + Pr B = Pr (A ∪ B) + Pr (A ∩ B)
Theorem “Pr Principle of Inclusion-Exclusion” “PIE”:
  Pr (A ∪ B) = Pr A + Pr B - Pr (A ∩ B)
Theorem “Pr Principle of Inclusion-Exclusion” “PIE”:
  Pr (A ∩ B) = Pr A + Pr B - Pr (A ∪ B)
Theorem “Pr Law of the Excluded Middle”:  Pr A + Pr (~ A) = 1
Theorem “Pr of the complement of an event”: Pr (~ A ) = 1 - Pr A
Theorem “Set inclusion via complement”: S ⊆ T  ≡  ~ S ∪ T  = 𝐔
Theorem “Pr distributivity over minus”:
       A ⊆ B  ⇒  Pr (B - A) = Pr B - Pr A
Axiom “Definition of `E`”:  E X = (∑ e • X(e) · pr e)
Axiom “Definition of pointwise sum”: (X +˙ Y)(e)  =  X(e) + Y(e)
Theorem “E over sum”: E (X +˙ Y) = E X + E Y
Axiom “Pr for dice”: pr e = 1 / 36
Axiom “Number of die faces”: # ⌞ 𝔻 ⌟ = 6
Axiom “Simultaneity” (M5-1):
     (∑ p : ❰ τ₁ , τ₂ ❱ ❙ R[p₁ ≔ fst p][p₂ ≔ snd p]
                          • B[p₁ ≔ fst p][p₂ ≔ snd p])
  =  (∑ p₁ : τ₁; p₂ : τ₂ ❙ R • B : ℝ)
----------------------------------------------------------------------
Axiom “Partial characterisation of /”:  n ≠ 0 ⇒ x · n = k ⇒ x = k / n
Theorem “Cancellation of /”:  n ≠ 0  ⇒  (k · n) / n = k
Axiom “Characterisation of P”: P (n + r) r · n ! = (n + r) !
Theorem “Definition of P via !”:  P (n + r) r = (n + r) ! / n !
Theorem “Definition of P via ! with -”:
Theorem “Universal permutations”: P r r = r !
```

```
Theorem “Almost-universal permutations”: P (n + 1) n = (n + 1) !
Axiom “Characterisation of choose”: ((n + r)choose r)·r! = P(n + r)r
Theorem “Definition of choose via /”:
    ((n + r) choose r)  =  (n + r) ! / (n ! · r !)
Theorem “Definition of choose via / and -”:
    r ≤ n   ⇒   (n choose r)  =  n ! / (r ! · (n - r) !)
Theorem “Almost-universal choose”: (n + 1) choose n = n + 1
Theorem “Universal choose”: n choose n = 1
Theorem (16.14+) “Symmetry of choose”:
        (n + r) choose r = (n + r) choose n
“Cancellation of - by +”:  a ≤ b  ⇒  (b - a) + a = b
“Greater than zero means successor”: 0 < n  ≡  n = suc (pred n)
Theorem (16.14) “Symmetry of choose”:
         r ≤ n ⇒ n choose r = n choose (n - r)
----------------------------------------------------------------------
```

TREES TREES TREES TREES TREES TREES TREES TREES

```
----------------------------------------------------------------------
Axiom “Singleton tree”: ⌈ x ⌋ = ◬ ⍰ x ⍰ ◬
Axiom “Mirror”: ◬ ˘  = ◬
Axiom “Mirror”: (l ⍰ x ⍰ r) ˘  =  (r ˘) ⍰ x ⍰ (l ˘)
Axiom “Tree induction”:
     P[t ≔ ◬]
  ∧  ( ∀ l, r : Tree A; x : A
       • P[t ≔ l] ∧ P[t ≔ r]  ⇒  P[t ≔ l ⍰ x ⍰ r]
     )
  ⇒  (∀ t : Tree A • P)
Theorem “Self-inverse of tree mirror”: ∀ t : Tree A • (t ˘) ˘ = t
----------------------------------------------------------------------
Axiom “Tree size”: size ◬  = 0
Axiom “Tree size”: size (l ⍰ x ⍰ r)  =  size l + 1 + size r
Lemma “Singleton tree size”: size ⌈ x ⌋ = 1
Theorem “Size of mirrored tree”:
    ∀ t : Tree A • size (t ˘) = size t
----------------------------------------------------------------------
Axiom “Tree map”: map f ◬ = ◬
Axiom “Tree map”: map f (l ⍰ x ⍰ r) = (map f l) ⍰ (f x) ⍰ (map f r)
Theorem “Size of mapped tree”:
    ∀ t •  size (map f t) = size t
----------------------------------------------------------------------
Axiom “Definition of `preOrder`”:
     preOrder ◬ = ϵ
  ∧  preOrder (l ⍰ x ⍰ r) = x ◃ preOrder l ⌢ preOrder r

Lemma “Singleton `preOrder`”: preOrder ⌈ x ⌋ = x ◃ ϵ
```

```
Axiom “Definition of `inOrder`”:
     inOrder ▵ = ϵ
  ∧  inOrder (l ⟨ x ⟩ r) = inOrder l ⌢ x ◃ inOrder r

Axiom “Definition of `postOrder`”:
     postOrder ▵ = ϵ
  ∧  postOrder (l ⟨ x ⟩ r) = postOrder l ⌢ postOrder r ▹ x
----------------------------------------------------------------------
Axiom “Mirror”:
     ⌜ x ⌟ ˘ = ⌜ x ⌟ ∧ (l ⟨⟩ r) ˘  =  (r ˘) ⟨⟩ (l ˘)
Axiom “HTree induction”:
     (∀ x : A • P[ t ≔ ⌜ x ⌟ ])
  ∧  ( ∀ l, r : HTree A ❙ P[t ≔ l] ∧ P[t ≔ r]   •  P[t ≔ l ⟨⟩ r] )
  ⇒  (∀ t : HTree A • P)
Axiom “HTree size”: size ⌜ x ⌟  = 1
Axiom “HTree size”: size (l ⟨⟩ r)  =  size l + size r
Axiom “Definition of `decode1`”:
     decode1 (l ⟨⟩ r) (false ◃ bs) = decode1 l bs
  ∧  decode1 (l ⟨⟩ r) (true  ◃ bs) = decode1 r bs
  ∧  decode1 ⌜ x ⌟ bs = ⟨ x, bs ⟩
Axiom “Definition of `second`” “second”: second f ⟨ a, b ⟩ = ⟨ a, f b ⟩
Axiom “Just is not nothing”: just x = nothing  ≡  false
Corollary  “Just is not nothing”: just x ≠ nothing
Axiom “Cancellation of `just`”:  just x = just y  ≡  x = y
----------------------------------------------------------------------
Axiom (8.11) “Substitution into ⋃”:
   (⋃ x ❙ R • E)[y ≔ F]  =  ⋃ x ❙ R[y ≔ F] • E[y ≔ F]
Axiom “Leibniz for ⋃ range”:
    (∀ x • R₁ ≡ R₂) ⇒ (⋃ x ❙ R₁ • E) = (⋃ x ❙ R₂ • E)
Axiom “Leibniz for ⋃ body”:
    (∀ x • E₁ = E₂) ⇒ (⋃ x ❙ R • E₁) = (⋃ x ❙ R • E₂)
Axiom (8.13) “Empty ⋃ range” “Empty range for ⋃”:
  (⋃ x ❙ false • E)  =  ⊥
Axiom (8.14) “One-point rule for ⋃”:
  (⋃ x ❙ x = D • E)  =  E[x ≔ D]
Axiom (8.15) “Distributivity of ⋃ over ∪”:
  (⋃ x ❙ R • E₁) ∪ (⋃ x ❙ R • E₂) = (⋃ x ❙ R • E₁ ∪ E₂)
Axiom (8.18) “Range split for ⋃”:
     (⋃ x ❙ Q ∨ R  • E)  =  (⋃ x ❙ Q • E)  ∪  (⋃ x ❙ R • E)
Axiom (8.20) “Nesting for ⋃”:
    (⋃ x, y ❙ Q ∧ R • E) = (⋃ x ❙ Q • (⋃ y ❙ R • E))
Theorem “Replacement in ⋃”:
    (⋃ x ❙ R ∧ e = f • E[y ≔ e]) = (⋃ x ❙ R ∧ e = f • E[y ≔ f])
```

```
----------------------------------------------------------------------
```

```
    (q = (n + 1) · (n + 1) ∧ s = 2 · (n + 1) + 1)
  ≡⟨ Substitution ⟩
    (q = n · n ∧ s = 2 · n + 1)[n ≔ n + 1]
  ⇒⁅ n := n + 1 ⁆   ⟨ “Assignment” ⟩
    (q = n · n ∧ s = 2 · n + 1)
```

```
Proof:
  By cases: `m = 0`, `m = suc (pred m)`
    Completeness: By “Zero or successor of predecessor”
    Case `m = 0`:
        m - 0 = m
      ≡⟨ Assumption `m = 0` ⟩
        0 - 0 = 0
      — This is “Subtraction from zero”
    Case `m = suc (pred m)`:
        m - 0
      =⟨ Assumption `m = suc (pred m)` ⟩
        (suc (pred m)) - 0
      =⟨ “Subtraction of zero from successor” ⟩
        suc (pred m)
      =⟨ Assumption `m = suc (pred m)` ⟩
        m
```

```
Theorem “Mutual ⊑”: a ⊑ b  ∧  b ⊑ a  ≡  a = b
Proof:
  Using “Mutual implication”:
    Subproof for `a ⊑ b  ∧  b ⊑ a  ⇒  a = b`:
        By “Antisymmetry of ⊑”
    Subproof for `a = b  ⇒  a ⊑ b  ∧  b ⊑ a`:
        Assuming `a = b`:
            a ⊑ b  ∧  b ⊑ a
          ≡⟨ Assumption `a = b`, “Reflexivity of ⊑” ⟩
            true ∧ true
          ≡⟨ “Identity of ∧” ⟩
            True
```

```
Theorem “Even is not odd”:  even n ≡ ¬ (odd n)
Proof:
  By induction on `n : ℕ`:
    Base case:
```

```
        even 0
      ≡⟨ “Zero is even” ⟩
        true
      ≡⟨ “Zero is not odd” ⟩
        ¬ (odd 0)
    Induction step:
        even (suc n)
      ≡⟨ “Even successor” ⟩
        ¬ (even n)
      ≡⟨ Induction hypothesis ⟩
        ¬ ¬ (odd n)
      ≡⟨ “Odd successor” ⟩
        ¬ odd (suc n)
```

```
Theorem “Factorial Program”:
      true
    ⇒⁅  f := 1 ;
        n := 0 ;
        while n ≠ N
          do
            n := suc n ;
            f := f · n
          od
      ⁆
      f = N !
Proof:
    f = N !
  ⇐⟨ “Weakening” ⟩
    n = N ∧ f = N !
  ≡⟨ Substitution, “Replacement” ⟩
    n = N ∧ (f = z !) [ z ≔ n ]
  ≡⟨ Substitution ⟩
    n = N ∧ f = n !
  ≡⟨ “Double negation”, “Definition of ≠” ⟩
    ¬ (n ≠ N) ∧ f = n !
  ⁅ while n ≠ N do
       n := suc n ;
       f := f · n
     od ⁆⇐ ⟨ “While” with subproof:
        f = n !
      ⁅ f := f · n ⁆⇐ ⟨ “Assignment” with substitution ⟩
        f · n = n !
      ⁅ n := suc n ⁆⇐ ⟨ “Assignment” with substitution ⟩
        f · (suc n) = (suc n) !
```

```
      ≡⟨ “Definition of !” ⟩
        f · (suc n) = suc n · n !
      ≡⟨ “Cancellation of multiplication with successor” ⟩
        f = n !
      ⇐⟨ “Weakening” ⟩
        n ≠ N ∧ f = n !
    ⟩
    f = n !
  ⁅ n := 0 ⁆⇐ ⟨ “Assignment” with substitution ⟩
    f = 0 !
  ⁅ f := 1 ⁆⇐ ⟨ “Assignment” with substitution ⟩
    1 = 0 !
  ≡⟨ “Definition of !”, “Reflexivity of =” ⟩
    True
```

```
Theorem “Cancellation of converse”:  a ˘ = b ˘  ≡  a = b
Proof:
  Using “Mutual implication”:
    Subproof for `a ˘ = b ˘ ⇒  a = b`:
      Assuming `a ˘ = b ˘`:
          a = b
        ≡⟨ “Converse is involutive” ⟩
          a ˘ ˘ = b ˘ ˘
        ≡⟨ Assumption `a ˘ = b ˘`, “Reflexivity of =” ⟩
          true
    Subproof for `a = b ⇒  a ˘ = b ˘`:
      Assuming `a = b`:
          a ˘ = b ˘
        ≡⟨ Assumption `a = b`, “Reflexivity of =” ⟩
          True
```

```
Theorem “Self-inverse of tree mirror”: ∀ t : Tree A • (t ˘) ˘ = t
Proof:
  Using “Tree induction”:
    Subproof for `△ ˘ ˘ = △`: By “Mirror”
    Subproof for `∀ l, r : Tree A; x : A
         • (l ˘) ˘ = l ∧ (r ˘) ˘ = r
         ⇒ (l ◻ x ◻ r)˘ ˘ = (l ◻ x ◻ r)`:
      For any `l, r, x`:
        Assuming “IHL” `(l ˘) ˘ = l`,
                 “IHR” `(r ˘) ˘ = r`:
            (l ◻ x ◻ r) ˘ ˘
          =⟨ “Mirror” ⟩
            (l ˘ ˘) ◻ x ◻ (r ˘ ˘)
```

```
          =⟨ Assumptions “IHL” and “IHR” ⟩
            l ? x ? r
```