

# 1 Set Theory

## 1.1 Set Axioms

### 1.1.1 Undefined notions

Set:  $A, B, C, \dots$

### 1.1.2 Axioms

1. *Extension:*  $\forall A \forall B [\forall C (C \in A \Leftrightarrow C \in B) \Rightarrow A = B]$
2. *Regularity:*  $\forall A [\exists C (C \in A) \Rightarrow \exists B (B \in A \wedge \neg \exists D (D \in B \wedge D \in A))]$   
(Every nonempty set contains a set that is disjoint from it. Also known as "Axiom of Foundation.")
3. *Schema of Specification:*  $\forall B \forall X_1 \forall X_2 \dots \forall X_n \exists A \forall C [C \in A \Leftrightarrow (C \in B \wedge \phi)]$
4. *Pairing:*  $\forall X_1 \forall X_2 \exists A (X_1 \in A \wedge X_2 \in A)$
5. *Union:*  $\forall \mathcal{F}_A \exists U \forall A \forall X [(X \in A \wedge A \in \mathcal{F}_A) \Rightarrow X \in U]$
6. *Schema of Replacement:*  $\forall A \forall X_1 \forall X_2 \dots \forall X_n [\forall B (B \in A \Rightarrow \exists! D \phi) \Rightarrow \exists B \forall C (C \in A \Rightarrow \exists D (D \in B \wedge \phi))]$
7. *Infinity:*  $\exists \omega [\emptyset \in \omega \wedge \forall X (X \in \omega \Rightarrow X \cup X \in \omega)]$
8. *Power Set:*  $\forall X \exists \mathcal{P}(X) \forall S [S \subseteq X \Rightarrow S \in \mathcal{P}(X)]$
9. *Empty Set:*  $\exists A \forall X (X \notin A)$
10. *Choice:*  $\forall X [\emptyset \notin X \Rightarrow \exists (f : X \rightarrow \bigcup X) \forall A \in X (f(A) \in A)]$

**Proposition 1.1.1.** *The empty set axiom is implied by the other nine axioms.*

*Proof.* Just choose any formula that is always false such as  $\phi(X) = X \in B \wedge X \notin B$  and apply the axiom schema of specification. This will give the empty set. The axiom of extension proves uniqueness vacuously.  $\square$

### 1.1.3 Universe

A set  $U$  is defined with the following properties...

1.  $x \in u \in U \Rightarrow x \in U$
2.  $u \in U \wedge v \in U \Rightarrow \{u, v\}, \langle u, v \rangle, u \times v \in U$
3.  $X \in U \Rightarrow \mathcal{P}(X) \in U \wedge \bigcup X \in U$
4.  $\omega \in U$  is the set of finite ordinals
5. if  $f : A \rightarrow B$  is a surjective function with  $A \in U \wedge B \subset U$ , then  $B \in U$   
(See: Set Constructions.)

In category theory, *small sets* are members of  $U$ .

## 1.2 Set Constructions

### 1.2.1 Union

- $A \cup B := \{x | x \in A \vee x \in B\}$
- $\bigcup \mathcal{F} := \{x | x \in X \text{ for some } X \in \mathcal{F}\}$

**Proposition 1.2.1.** *For sets  $A, B, C$ , the following hold...*

- Identity:  $A \cup \emptyset = A$
- Idempotence:  $A \cup A = A$
- Absorption:  $A \subseteq B \Leftrightarrow A \cup B = B$
- Commutative:  $A \cup B = B \cup A$
- Associative:  $A \cup (B \cup C) = (A \cup B) \cup C$

### 1.2.2 Intersection

- $A \cap B := \{x \in A | x \in B\} = \{x \in B | x \in A\}$
- $\bigcap \mathcal{F} := \{x | x \in X \text{ for all } X \in \mathcal{F}\}$

**Proposition 1.2.2.** *For sets  $A, B, C$ , the following hold...*

- Zero:  $A \cap \emptyset = \emptyset$
- Idempotence:  $A \cap A = A$
- Absorption:  $A \subseteq B \Leftrightarrow A \cap B = A$
- Commutative:  $A \cap B = B \cap A$
- Associative:  $A \cap (B \cap C) = (A \cap B) \cap C$

### 1.2.3 Complement

- *Relative Complement:*  $A \setminus B := \{x \in A | x \notin B\}$
- *Absolute Complement:* For some universe  $U$  and  $A \subseteq U$ ,  $A^c := U \setminus A$

**Proposition 1.2.3.** *For a universe  $U$  and sets  $A, B \subseteq U$ ...*

- $(A^c)^c = A$
- $\emptyset^c = U$
- $U^c = \emptyset$
- $A \cap A^c = \emptyset$

- $A \cup A^c = U$
- $A \subseteq B \Leftrightarrow B^c \subseteq A^c$

**Proposition 1.2.4** (DeMorgan's Laws). *For a universe  $U$  and sets  $A, B \subseteq U$ ...*

- $(A \cup B)^c = A^c \cap B^c$
- $(A \cap B)^c = A^c \cup B^c$

**Proposition 1.2.5.** *For sets  $A, B$ ...*

- $A \setminus B = A \cap B^c$
- $A \subseteq B \Leftrightarrow A \setminus B = \emptyset$
- $A \setminus (A \setminus B) = A \cap B$
- $A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C)$
- $A \cap B \subseteq (A \cap C) \cup (B \cap C^c)$
- $(A \cup C) \cap (B \cup C^c) \subseteq A \cup B$

**Proposition 1.2.6.** *For a family  $\mathcal{F}$ ...*

- $\forall X \in \mathcal{F}, \bigcup_{k \in K} X_k = \bigcup_{j \in J} (\bigcup_{i \in I_j} X_i)$
- $\forall X \in \mathcal{F}, \bigcap_{k \in K} X_k = \bigcap_{j \in J} (\bigcap_{i \in I_j} X_i)$
- $\forall X \in \mathcal{F}, \bigcup_{i \in I} X_i = \bigcup_{j \in J} X_j$
- $\forall X \in \mathcal{F}, \bigcap_{i \in I} X_i = \bigcap_{j \in J} X_j$
- $(\bigcup_{i \in I} A_i) \cap (\bigcup_{j \in J} B_j) = \bigcup_{i,j} (A_i \cap B_j)$
- $(\bigcap_{i \in I} A_i) \cup (\bigcap_{j \in J} B_j) = \bigcap_{i,j} (A_i \cup B_j)$

**Proposition 1.2.7** (Generalized DeMorgan's Laws). *For a universe  $U$  and a family  $\mathcal{F}$ ...*

- $(\bigcup_{X \in \mathcal{F}} X)^c = \bigcap_{X \in \mathcal{F}} X^c$
- $(\bigcap_{X \in \mathcal{F}} X)^c = \bigcup_{X \in \mathcal{F}} X^c$

#### 1.2.4 Symmetric Difference

$$A \triangle B := (A \setminus B) \cup (B \setminus A)$$

### 1.2.5 Power Set

$$\mathcal{P}(X) := \{S \mid S \subseteq X\}$$

**Proposition 1.2.8.** *For sets  $A, B$  and a family  $\mathcal{F} \dots$*

- $\mathcal{P}(A) \cap \mathcal{P}(B) = \mathcal{P}(A \cap B)$
- $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$
- $\bigcap_{X \in \mathcal{F}} \mathcal{P}(X) = \mathcal{P}(\bigcap_{X \in \mathcal{F}} X)$
- $\bigcup_{X \in \mathcal{F}} \mathcal{P}(X) \subseteq \mathcal{P}(\bigcup_{X \in \mathcal{F}} X)$

#### 1.2.5.1 Characteristic Function of a subset

For  $A \subseteq X$ ,  $\chi_A : X \rightarrow 2$  where...

$$\chi_A(x) := \begin{cases} 0 & x \in X \setminus A \\ 1 & x \in A \end{cases}$$

### 1.2.6 $n$ -Tuple

- *Ordered pair:*  $\langle a, b \rangle := \{\{a\}, \{a, b\}\}$
- $\langle a_1, a_2, a_3, \dots, a_n \rangle := \langle \langle \langle a_1, a_2 \rangle, a_3 \rangle \dots \rangle, a_n \rangle$

### 1.2.7 Cartesian Product

- $A \times B := \{\langle a, b \rangle \mid \text{for some } a \in A \text{ and for some } b \in B\}$
- $\times \mathcal{F} := \{\langle a_1, a_2, \dots, a_n \rangle \mid \text{for } a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n \text{ where } A_1, A_2, \dots, A_n \in \mathcal{F}\}$

**Proposition 1.2.9.** *For sets  $A, B \dots$*

- $(A \cup B) \times X = (A \times X) \cup (B \times X)$
- $(A \cap B) \times (X \cap Y) = (A \times X) \cap (B \times X)$
- $(A \setminus B) \times X = (A \times X) \setminus (B \times X)$

**Proposition 1.2.10.** *For families  $\{A_i\}_{i \in I}, \{B_j\}_{j \in J}, \{X_i\}_{i \in I} \dots$*

- $(\bigcup_{i \in I} A_i) \times (\bigcup_{j \in J} B_j) = \bigcup_{i,j} (A_i \times B_j)$
- $(\bigcap_{i \in I} A_i) \times (\bigcap_{j \in J} B_j) = \bigcap_{i,j} (A_i \times B_j)$
- $\bigcap_i X_i \subseteq X_j \subseteq \bigcup_i X_i$

### 1.2.8 Quotient by Equivalence Relation

$X / \sim := \{[a]_{\sim} \mid a \in X\}$  (See: equivalence relations)

### 1.2.9 Family

Given a set  $X$  and an index set  $I$ , a family is a function  $\mathcal{F} : I \rightarrow X$ . A cleaner way of denoting the concept is...

$$\mathcal{F}(i) := S_i, \{S_i\}_{i \in I}$$

## 1.3 Relations

$\mathcal{R} : \subseteq A \times B$  for some  $A \times B$

### 1.3.1 Equivalence Relations

Relations  $\sim \subseteq A \times A$  such that  $\forall a, b, c \in A \dots$

- *Reflexive*:  $a \sim a$
- *Symmetric*:  $a \sim b \Rightarrow b \sim a$
- *Transitive*:  $a \sim b \wedge b \sim c \Rightarrow a \sim c$

#### 1.3.1.1 Equivalence Class

$$[a]_{\sim} := \{b \in S \mid b \sim a\}$$

#### 1.3.1.2 Set Partition

A set  $P : \subseteq \mathcal{P}(X)$  such that...

- $\bigcup P = X$
- $\forall S_1, S_2 \in P (S_1 \cap S_2 \neq \emptyset \Rightarrow S_1 = S_2)$

### 1.3.2 Functions

A relation  $f : A \rightarrow B$  satisfying  $\forall a \in A \exists! b \in B$  such that  $afb$ , denoted  $f(a) = b$ .

#### 1.3.2.1 Injection

A function  $f : A \hookrightarrow B$  such that  $\forall x, y \in A$  if  $x \neq y$ , then  $f(x) \neq f(y)$ . (See: monomorphism. Injections have right inverses.)

#### 1.3.2.2 Surjection

A function  $f : A \twoheadrightarrow B$  such that  $\forall b \in B \exists a \in A$  such that  $f(a) = b$ . (See: epimorphism. Surjections have left inverses, called *sections*.)

#### 1.3.2.3 Bijection

A function  $f : A \xrightarrow{\sim} B$  which is an injection and a surjection. (See: isomorphism)

#### 1.3.2.4 Restriction

For  $C \subseteq A$  and  $f : A \rightarrow B$ ,  $f|_C : C \rightarrow B$  where  $\forall c \in C \ f|_C(c) := f(c)$

#### 1.3.2.5 Image

$$f(A) := \{f(a) | a \in A\}$$

**Proposition 1.3.1.** *For a function  $f : A \rightarrow B$  and a family  $\{X_i\}_{i \in I}$  where  $\forall i \in I \ X_i \subseteq A \dots$*

- $f(\bigcup_i X_i) = \bigcup_i f(X_i)$
- In general,  $f(\bigcap_i X_i) \neq \bigcap_i f(X_i)$
- In general,  $f(X)^c \neq f(X^c)$

#### 1.3.2.6 Preimage

$$f^{-1}(A) := \{a \in A | f(a) \in B\}$$

**Proposition 1.3.2.** *Given a function  $f : X \rightarrow Y$ ,  $f$  is surjective if and only if  $\forall A \subseteq Y$ , where  $A \neq \emptyset$ ,  $f^{-1}(A) \neq \emptyset$ .*

**Proposition 1.3.3.** *Given a function  $f : X \rightarrow Y$ ,  $f$  is injective if and only if  $\forall A \subseteq \text{ran } f$ , where  $A$  is a singleton,  $f^{-1}(A)$  is a singleton.*

**Proposition 1.3.4.** *Given a function  $f : X \rightarrow Y \dots$*

- If  $B \subseteq Y$ , then  $f(f^{-1}(B)) \subseteq B$ .
- If  $f$  is surjective, then  $f(f^{-1}(B)) = B$ .
- If  $A \subseteq X$ , then  $A \subseteq f^{-1}(f(A))$ .
- If  $f$  is injective, then  $A = f^{-1}(f(A))$ .
- If  $\{B_i\}$  is a family of subset of  $Y$ , then  $f^{-1}(\bigcup_i B_i) = \bigcup_i f^{-1}(B_i)$  and  $f^{-1}(\bigcap_i B_i) = \bigcap_i f^{-1}(B_i)$ .

#### 1.3.2.7 Function Composition

$f : X \rightarrow Y$  and  $g : Y \rightarrow Z \Rightarrow g \circ f : X \rightarrow Z$  where  $\forall x \in X$ ,  $g \circ f(x) := g(f(x))$

### 1.4 Natural Numbers

#### 1.4.1 Successor

For a set  $n$ , its *successor*  $n^+$  is defined by...

$$n^+ = n \cup \{n\}$$

### 1.4.2 Inductive

A set  $N$  is *inductive* if and only if  $\emptyset \in N$  and  $(\forall n \in N) n^+ \in N$ .

The Axiom of Infinity may be restated in terms of "inductiveness," i.e. . . .

*There exists an inductive set  $\omega$ .*

### 1.4.3 Natural Number

A *natural number* is a set that belongs to every inductive set, i.e. the intersection of them all.

The following theorem is a consequence of the definition. . .

**Theorem 1.4.1** (Induction on  $\omega$ ). *Any inductive subset of  $\omega$  coincides with  $\omega$ .*

**Proposition 1.4.1.** *Every natural number except 0 is the successor of some natural number.*

*Proof.* Let  $T = \{n \in \omega \mid n = 0 \vee (\exists p \in \omega) n = p^+\}$  and use induction.  $\square$

### 1.4.4 Peano's Postulates

#### 1.4.4.1 Peano System

An ordered triple  $\langle N, S, e \rangle$  consisting of a set  $N$ , a function  $S : N \rightarrow N$ , and a member  $e \in N$  such that the following three conditions are met:

1.  $e \notin \text{ran} S$ .
2.  $S$  is injective.
3. Any subset  $A \subseteq N$  that contains  $e$  and is closed under  $S$  equals  $N$  itself.

**Proposition 1.4.2.** *Let  $\sigma = \{\langle n, n^+ \rangle \mid n \in \omega\}$ . Then  $\langle \omega, \sigma, 0 \rangle$  is a Peano system.*

#### 1.4.4.2 Transitive Set

A set  $A$  is said to be a *transitive set* if and only if  $x \in a \in A \Rightarrow x \in A$ .

**Proposition 1.4.3.** *For a transitive set  $a$ ,*

$$\bigcup (a^+) = a.$$

**Proposition 1.4.4.** *Every natural number is a transitive set and  $\omega$  is a transitive set.*

*Proof.* Use induction.  $\square$

### 1.4.5 Recursion

**Theorem 1.4.2** (Recursion Theorem on  $\omega$ ). *Let  $A$  be a set,  $a \in A$ , and  $F : A \rightarrow A$ . Then there exists an unique function  $h : \omega \rightarrow A$  such that...*

$$h(0) = a,$$

and for every  $n \in \omega$ ,

$$h(n^+) = F(h(n)).$$

*Proof.* The idea is to let  $h$  be the union of many approximating functions. For the purposes of this proof, call a function  $v$  *acceptable* if and only if  $\text{dom } v \subseteq \omega$ ,  $\text{ran } v \subseteq A$ , and the following conditions hold:

1. If  $0 \in \text{dom } v$ , then  $v(0) = a$ .
2. If  $n^+ \in \text{dom } v$  (where  $n \in \omega$ ), then also  $n \in \text{dom } v$  and  $v(n^+) = F(v(n))$ .

Let  $\mathcal{H}$  be the collection of all acceptable functions, and let  $h = \bigcup \mathcal{H}$ . Thus...

$$\begin{aligned} (\star) \quad \langle n, y \rangle \in h &\Leftrightarrow \langle n, y \rangle \text{ is a member of some acceptable } v \\ &\Leftrightarrow v(n) = y \text{ for some acceptable } v. \end{aligned}$$

We claim that this  $h$  meets the demands of the theorem. This claim can be broken down into four parts. The four parts involve showing that (I)  $h$  is a function, (II)  $h$  is acceptable, (III)  $\text{dom } h$  is all of  $\omega$ , and (IV)  $h$  is unique.

I. We first claim that  $h$  is a function. Let...

$$S = \{n \in \omega \mid \text{for at most one } y, \langle n, y \rangle \in h\}.$$

We must check that  $S$  is inductive. If  $\langle 0, y_1 \rangle \in h$  and  $\langle 0, y_2 \rangle \in h$ , then by  $(\star)$  there exist acceptable  $v_1$  and  $v_2$  such that  $v_1(0) = y_1$  and  $v_2(0) = y_2$ . But by (1) it follows that  $y_1 = a = y_2$ . Thus  $0 \in S$ .

Next suppose that  $k \in S$ . Consider  $\langle k^+, y_1 \rangle \in h$  and  $\langle k^+, y_2 \rangle \in h$ . As before there must exist acceptable  $v_1$  and  $v_2$  such that  $v_1(k^+) = y_1$  and  $v_2(k^+) = y_2$ . By condition (2) it follows that...

$$y_1 = v_1(k^+) = F(v_1(k)) \quad \text{and} \quad y_2 = v_2(k^+) = F(v_2(k)).$$

But since  $k \in S$ , we have  $v_1(k) = v_2(k)$ . Therefore...

$$y_1 = F(v_1(k)) = F(v_2(k)) = y_2.$$

So  $k^+ \in S$ , proving  $S$  is inductive and coincides with  $\omega$ . Consequently  $h$  is a function.

II. Next we claim that  $h$  itself is acceptable. We have just seen that  $h$  is a function, and it is clear from  $(\star)$  that  $\text{dom } h \subseteq \omega$  and  $\text{ran } h \subseteq A$ .



First examine (1). If  $0 \in \text{dom } h$ , then there must be some acceptable  $v$  with  $v(0) = h(0)$ . Since  $v(0) = a$ , we have  $h(0) = a$ .

Next examine (2). Assume  $n^+ \in \text{dom } h$ . Again there must be some acceptable  $v$  with  $v(n^+) = h(n^+)$ . Since  $v$  is acceptable we have  $n \in \text{dom } v$  (and  $v(n) = h(n)$ ) and

$$h(n^+) = v(n^+) = F(v(n)) = F(h(n)).$$

Thus  $h$  satisfies (2) and so is acceptable.

III. We now claim that  $\text{dom } h = \omega$  (the function is nonempty). It suffices to show that  $\text{dom } h$  is inductive. The function  $\{\langle 0, a \rangle\}$  is acceptable and hence  $0 \in \text{dom } h$ . Suppose the  $k \in \text{dom } h$ . If  $k^+ \notin \text{dom } h$ , then let...

$$v = h \cup \{\langle k^+, F(h(k)) \rangle\}.$$

Then  $v$  is a function,  $\text{dom } v \subseteq \omega$ , and  $\text{ran } v \subseteq A$ . We will show that  $v$  is acceptable.

Condition (1) holds since  $v(0) = h(0) = a$ . For condition (2) there are two cases. If  $n^+ \in \text{dom } v$  where  $n^+ \neq k^+$ , then  $n^+ \in \text{dom } h$  and  $v(n^+) = h(n^+) = F(h(n)) = F(v(n))$ . The other case occurs if  $n^+ = k^+$ . Since the successor operation is injective,  $n = k$ . By assumption  $k \in \text{dom } h$ . Thus...

$$v(k^+) = F(h(k)) = F(v(k))$$

and (2) holds. Hence  $v$  is acceptable. But then  $v \subseteq h$ , so that  $k^+ \in \text{dom } h$  after all. So  $\text{dom } h$  is inductive and therefore coincides with  $\omega$ .

IV. Finally we claim that  $h$  is unique. For let  $h_1$  and  $h_2$  both satisfy the conclusion for the theorem. Let...

$$S = \{n \in \omega \mid h_1(n) = h_2(n)\}.$$

$S$  is inductive, showing  $h_1 = h_2$ . Thus  $h$  is unique.  $\square$

**Example 1.4.2.1.** *There is no function  $h : \mathbb{Z} \rightarrow \mathbb{Z}$  such that for every  $a \in \mathbb{Z}$ ,*

$$h(a+1) = h(a)^2 + 1.$$

*Proof.* Note  $h(a) > h(a-1) > h(a-2) > \dots > 0$ . Recursion on  $\omega$  relies on there being a starting point 0.  $\mathbb{Z}$  has no analogous starting point.  $\square$

**Theorem 1.4.3.** *Let  $\langle N, S, e \rangle$  be a Peano system. Then  $\langle \omega, \sigma, 0 \rangle$  is isomorphic to  $\langle N, S, e \rangle$ , i.e. there is a function  $h$  mapping  $\omega$  bijectively to  $N$  in a way that preserves the successor operation*

$$h(\sigma(n)) = S(h(n))$$

*and the zero element*

$$h(0) = e.$$

### 1.4.6 Arithmetic

#### 1.4.6.1 Addition

*Addition*  $(+)$  is the binary operation on  $\omega$  such that for any  $m$  and  $n \in \omega$ ,

$$m + n = A_m(n),$$

where  $A_m : \omega \rightarrow \omega$  is the unique function given by the recursion theorem for which...

- $A_m(0) = m$
- $A_m(n^+) = A_m(n)^+ \forall n \in \omega$ .

**Proposition 1.4.5.** *For natural numbers  $m$  and  $n$ ,*

- $m + 0 = m$ ,
- $m + n^+ = (m + n)^+$

#### 1.4.6.2 Multiplication

*Multiplication*  $(\cdot)$  is the binary operation on  $\omega$  such that for any  $m$  and  $n \in \omega$ ,

$$m \cdot n = M_m(n),$$

where  $M_m : \omega \rightarrow \omega$  is the unique function given by the recursion theorem for which...

- $M_m(0) = 0$
- $M_m(n^+) = M_m(n) + m$ .

**Proposition 1.4.6.** *For natural numbers  $m$  and  $n$ ,*

- $m \cdot 0 = 0$ ,
- $m \cdot n^+ = m \cdot n + m$

#### 1.4.6.3 Exponentiation

*Exponentiation* is the binary operation on  $\omega$  such that for any  $m$  and  $n \in \omega$ ,

$$m^n = E_m(n),$$

where  $E_m : \omega \rightarrow \omega$  is the unique function given by the recursion theorem for which...

- $E_m(0) = 1$
- $E_m(n^+) = E_m(n) \cdot m$ .

**Proposition 1.4.7.** *For natural numbers  $m$  and  $n$ ,*

- $m^0 = 1$ ,
- $m^{(n^+)} = m^n \cdot m$ .

### 1.4.7 Ordering on the natural numbers

Define  $m < n$  if and only if  $m \in n$ .

**Lemma 1.4.4.** *For any natural numbers  $m$  and  $n$ ...*

- $m \in n \Leftrightarrow m^+ \in n^+$ .
- $n \notin n$

**Theorem 1.4.5** (Trichotomy Law for  $\omega$ ). *For any natural numbers  $m$  and  $n$ , exactly one of the three conditions...*

- $m \in n$
- $m = n$
- $n \in m$

holds.

**Corollary 1.4.5.1.** *For any natural numbers  $m$  and  $n$ ,*

- $m \in n \Leftrightarrow m \subset n$
- $(m \in n) \vee (m = n) \Leftrightarrow m \subseteq n$

**Proposition 1.4.8.** *For any natural numbers  $m, n$  and  $p$ ,...*

- $m \in n \Leftrightarrow m + p \in n + p$ .
- If, in addition,  $p \neq 0$ , then  $m \in n \Leftrightarrow m \cdot p \in n \cdot p$ .

**Corollary 1.4.5.2.** *The following cancellation laws hold for  $m, n, p \in \omega$ ...*

- $m + p \in n + p \Rightarrow m = n$
- If, in addition,  $p \neq 0$ , then  $m \cdot p \in n \cdot p \Rightarrow m = n$

**Theorem 1.4.6** (Well Ordering of  $\omega$ ). *Let  $A$  be a nonempty set of  $\omega$ . Then there is some  $m \in A$  such that  $(m \in n) \vee (m = n)$  for all  $n \in A$ .*

*Proof.* Assume that  $A$  is a subset of  $\omega$  without a least element; we will show that  $A = \emptyset$ . We could attempt to do this by showing that the complement  $\omega \setminus A$  is inductive. But in order to show that  $k^+ \in \omega \setminus A$ , it is not enough to know merely that  $k \in \omega \setminus A$ , we must know that all numbers smaller than  $k$  are in  $\omega \setminus A$  as well. Given this additional information, we can argue that  $k^+ \in \omega \setminus A$  lest it be a least element of  $A$ .

To write down what is approximately this argument, let...

$$B = \{m \in \omega \mid \text{no number less than } m \text{ belongs to } A\}.$$

We claim that  $B$  is inductive.  $0 \in B$  vacuously. Suppose that  $k \in B$ . Then if  $n$  is less than  $k^+$ , either  $n$  is less than  $k$  (in which case  $n \notin A$  since  $k \in B$ ) or  $n = k$  (in which case  $n \notin A$  lest, by trichotomy, it be least in  $A$ ). In either case,  $n$  is outside of  $A$ . Hence  $k^+ \in B$  and  $B$  is inductive. It clearly follows that  $A = \emptyset$ .  $\square$

**Corollary 1.4.6.1.** *There is no function  $f : \omega \rightarrow \omega$  such that  $f(n^+) \in f(n)$  for every natural number  $n$ .*

**Theorem 1.4.7** (Strong Induction Principle for  $\omega$ ). *Let  $A$  be a subset of  $\omega$ , and assume that for every  $n \in \omega$ , if every number less than  $n$  is in  $A$ , then  $n \in A$ . Then  $A = \omega$ .*

## 1.5 Constructing Number Systems

For the purposes of this subsection let  $\mathbb{N} := \omega$ .

### 1.5.1 The Integers

Let  $\sim_{\mathbb{Z}}$  be the equivalence relation on  $\mathbb{N} \times \mathbb{N}$  for which...

$$\langle m, n \rangle \Leftrightarrow m + q = p + n.$$

Then the set of *Integers*, denoted  $\mathbb{Z}$ , is the set  $\mathbb{N} \times \mathbb{N} / \sim_{\mathbb{Z}}$ .

#### 1.5.1.1 Addition

Addition of integers  $a = \langle m, n \rangle$  and  $b = \langle p, q \rangle$  is defined as...

$$a +_{\mathbb{Z}} b = [\langle m + p, n + q \rangle]$$

**Lemma 1.5.1.** *Addition of integers ( $+_{\mathbb{Z}}$ ) is well defined, i.e. if  $\langle m, n \rangle \sim_{\mathbb{Z}} \langle m', n' \rangle$  and  $\langle p, q \rangle \sim_{\mathbb{Z}} \langle p', q' \rangle$ , then...*

$$\langle m + p, n + q \rangle \sim_{\mathbb{Z}} \langle m' + p', n' + q' \rangle$$

The integers under addition form an abelian group.

#### 1.5.1.2 Multiplication

Multiplication of integers  $a = \langle m, n \rangle$  and  $b = \langle p, q \rangle$  is defined as...

$$a \cdot_{\mathbb{Z}} b = [\langle mp + nq, mq + np \rangle]$$

**Lemma 1.5.2.** *Multiplication of integers ( $\cdot_{\mathbb{Z}}$ ) is well defined, i.e. if  $\langle m, n \rangle \sim_{\mathbb{Z}} \langle m', n' \rangle$  and  $\langle p, q \rangle \sim_{\mathbb{Z}} \langle p', q' \rangle$ , then...*

$$\langle mp + nq, mq + np \rangle \sim_{\mathbb{Z}} \langle m'p' + n'q', m'q' + n'p' \rangle$$

The integers under multiplication form an abelian group.

### 1.5.1.3 Order

Order of integers  $a = \langle m, n \rangle$  and  $b = \langle p, q \rangle$  is defined as. . .

$$a <_{\mathbb{Z}} b \Leftrightarrow m + q \in p + n$$

**Lemma 1.5.3.** *Order of integers ( $<_{\mathbb{Z}}$ ) is well defined, i.e. if  $\langle m, n \rangle \sim_{\mathbb{Z}} \langle m', n' \rangle$  and  $\langle p, q \rangle \sim_{\mathbb{Z}} \langle p', q' \rangle$ , then. . .*

$$m + q \in p + n \Leftrightarrow m' + q' \in p' + n'$$

The order relation so defined linearly orders the integers.

### 1.5.2 The Rational Numbers

Let  $\sim_{\mathbb{Q}}$  be the equivalence relation on  $\mathbb{Z} \times (\mathbb{Z} \setminus \{0_{\mathbb{Z}}\})$  for which. . .

$$\langle a, b \rangle \sim \langle c, d \rangle \Leftrightarrow a \cdot_{\mathbb{Z}} d = c \cdot_{\mathbb{Z}} b.$$

Then the set of *Rational Numbers*, denoted  $\mathbb{Q}$ , is the set  $\mathbb{Z} \times (\mathbb{Z} \setminus \{0_{\mathbb{Z}}\}) / \sim_{\mathbb{Q}}$ .

#### 1.5.2.1 Addition

Addition of rational numbers  $p = \langle a, b \rangle$  and  $q = \langle c, d \rangle$  is defined as. . .

$$p +_{\mathbb{Q}} q = [\langle ad + cb, bd \rangle]$$

**Lemma 1.5.4.** *Addition of rational numbers is well defined.*

The rational numbers under addition form an abelian group.

#### 1.5.2.2 Multiplication

Multiplication of rational numbers  $p = \langle a, b \rangle$  and  $q = \langle c, d \rangle$  is defined as. . .

$$p \cdot_{\mathbb{Q}} q = [\langle ac, bd \rangle]$$

**Lemma 1.5.5.** *Multiplication of rational numbers is well defined.*

The rational numbers under addition and multiplication form a field.

#### 1.5.2.3 Order

Order of rational numbers  $p = \langle a, b \rangle$  and  $q = \langle c, d \rangle$  is defined as. . .

$$p <_{\mathbb{Q}} q \Leftrightarrow ad < cb.$$

**Lemma 1.5.6.** *The order of rational numbers is well-defined.*

The order relation so defined linearly orders the rational numbers.

### 1.5.3 The Real Numbers with Cauchy Sequences

Define a *Cauchy sequence* to be a function  $s : \omega \rightarrow \mathbb{Q}$  such that...

$$(\forall \varepsilon > 0)(\exists k \in \omega)(\forall m > k)(\forall n > k)|s_m - s_n| < \varepsilon.$$

Let  $C$  be the set of all Cauchy sequences. For  $r, s \in C$ , define  $r \sim_{\mathbb{R}} s$  if and only if  $|r_n - s_n|$  is arbitrarily small for large  $n$ .

With more work we can define  $\mathbb{R} := C / \sim$ .

### 1.5.4 The Real Numbers with Dedekind Cuts

A *Dedekind cut* is a subset  $x$  of  $\mathbb{Q}$  such that:

1.  $\emptyset \neq x \neq \mathbb{Q}$
2.  $x$  is "closed downward," i.e.,

$$q \in x \wedge r < q \Rightarrow r \in x.$$

3.  $x$  has no largest member

$\mathbb{R}$  is the set of Dedekind cuts.

#### 1.5.4.1 Order

Define an ordering on  $\mathbb{R}$  as...

$$x <_{\mathbb{R}} y \Leftrightarrow x \subset y$$

**Proposition 1.5.1.**  $<_{\mathbb{R}}$  is a linear ordering.

*Proof.*  $<_{\mathbb{R}}$  is clearly transitive; so it suffices to show that  $<_{\mathbb{R}}$  satisfies trichotomy on  $\mathbb{R}$ . So consider  $x, y \in \mathbb{R}$ . Obviously *at most* one of the alternatives,

$$x \subset y, \quad x = y, \quad y \subset x,$$

can hold, but we must prove that at least one holds. Without loss of generality, suppose that the first two fail, i.e., that  $x \not\subseteq y$ .

Since  $x \not\subseteq y$  there is some rational  $r$  in the relative complement  $x \setminus y$ . Consider any  $q \in y$ . If  $r \subseteq q$ , then since  $y$  is closed downward, we would have  $r \in y$ . But  $r \notin y$ , so we must have  $q < r$ . Since  $x$  is closed downward, it follows that  $q \in x$ . Since  $q$  was arbitrary (and  $x \neq y$ ), we have  $y \subset x$ .  $\square$

**Theorem 1.5.7** (Least Upper Bound Property). *Any bounded nonempty subset of  $\mathbb{R}$  has a least upper bound in  $\mathbb{R}$ .*

*Proof.* Let  $A$  be a set of real numbers. The least upper bound is just  $\bigcup A$ .  $\square$

### 1.5.4.2 Addition

Addition of real number  $x, y$  is defined as...

$$x +_{\mathbb{R}} y = q + r \mid q \in x \wedge r \in y$$

### 1.5.4.3 Multiplication

The *absolute value* of a real number  $x$  is defined as...

$$|x| = x \cup -x$$

Multiplication of real number  $x, y$  is defined as follows...

- If  $x$  and  $y$  are nonnegative real numbers, then...

$$x \cdot_{\mathbb{R}} y = 0_{\mathbb{R}} \cup \{rs \mid 0 \leq r \in x \wedge 0 \leq s \in y\}.$$

- If  $x$  and  $y$  are both negative real numbers, then...

$$x \cdot_{\mathbb{R}} y = |x| \cdot_{\mathbb{R}} |y|.$$

- If one of the real numbers  $x$  and  $y$  is negative and one is nonnegative, then...

$$x \cdot_{\mathbb{R}} y = -(|x| \cdot_{\mathbb{R}} |y|).$$

Real numbers under addition, multiplication, and their order relation form an ordered field.

## 1.6 Cardinal Numbers

### 1.6.1 Equinumerosity

Two sets  $A$  and  $B$  are *equinumerous*, denoted  $A \approx B$ , if and only if there is a bijection  $f : A \rightarrow B$ .

**Proposition 1.6.1.** *Equinumerosity is an equivalence relation. (See: isomorphism)*

**Theorem 1.6.1** (Diagonalization). *The set  $\omega$  is not equinumerous to the set  $\mathbb{R}$  of real numbers.*

*Proof.* Suppose for the sake of contradiction that there is a bijection  $f : \omega \rightarrow \mathbb{R}$ . Thus we can imagine a list of successive values...

$$f(0) = 236.001 \dots$$

$$f(1) = -7.777 \dots$$

$$f(2) = 3.1415 \dots$$

$\vdots$

Then consider the real number  $0.a_1a_2a_3\dots$  where:

$$a_n = \begin{cases} 7 & \text{if the } n\text{th decimal of } f(n) \neq 7 \\ 6 & \text{otherwise.} \end{cases}$$

This number cannot be in the range of  $f$ , so it is not a bijection.  $\nexists$

**Theorem 1.6.2** (Diagonalization). *No set is equinumerous to its power set.*

*Proof.* Let  $g : A \rightarrow \mathcal{P}(A)$ . Consider...

$$B = \{x \in A \mid x \notin g(x)\}.$$

Then  $B \subseteq A$ , but for each  $x \in A$ ,

$$x \in B \Leftrightarrow x \notin g(x).$$

Hence  $B \notin \text{ran } g$  and  $g$  is not a bijection.  $\square$

### 1.6.2 Finite/Infinite

A set is *finite* if and only if it is equinumerous to some natural number. Otherwise it is *infinite*.

**Theorem 1.6.3** (Pigeonhole Principle). *No natural number is equinumerous to a proper subset of itself.*

*Proof.* Suppose  $f : N \rightarrow N$  is a bijection from a finite set to itself. We will show that  $\text{ran } f$  is all of the set  $n$ . This suffices to prove the theorem.

We use the induction on  $n$ . Define:

$$T = \{n \in \omega \mid \text{every injection from } n \text{ into } n \text{ has range } n\}$$

We have that  $0 \in T$ ; the only function from the set  $0$  into the set  $0$  is the empty function, which has range  $0$ . Now suppose that  $k \in T$  and that  $f$  is an injection from  $k^+$  into  $k^+$ . Note that the restriction  $f|_k$  maps  $k$  injectively into  $k^+$ . There are two cases...

Case I: The set  $k$  is closed under  $f$ . Then  $f|_k$  maps the set  $k$  into the set  $k$ . Then because  $k \in T$  we may conclude that  $\text{ran } (f|_k) = k$ . Since  $f$  is injective, the only possible value for  $f(k)$  is the number  $k$ . Hence  $\text{ran } f$  is  $k \cup \{k\}$ , which is the set  $k^+$ .

Case II: Otherwise  $f(p) = k$  for some number  $p$  less than  $k$ . In this case we interchange two values of the function. Define  $\hat{f}$  by...

$$\hat{f}(p) = f(k),$$

$$\hat{f}(k) = f(p) = k,$$



$$\hat{f}(x) = f(x) \text{ for other } x \in k^+.$$

The  $\hat{f}$  maps the set  $k^+$  injectively into the set  $k^+$ , and the set  $k$  is closed under  $\hat{f}$ . So we can apply Case I.

Thus  $\text{ran } f = k^+$ . □

**Corollary 1.6.3.1.** *No finite set is equinumerous to a proper subset of itself.*

**Corollary 1.6.3.2.** *Any set equinumerous to a proper subset of itself is infinite.*

**Corollary 1.6.3.3.** *The set  $\omega$  is infinite.*

**Corollary 1.6.3.4.** *Any finite set is equinumerous to a unique natural number.*

**Lemma 1.6.4.** *If  $C$  is a proper subset of a natural number  $n$ , the  $C \approx m$  for some  $m$  less than  $n$ .*

**Corollary 1.6.4.1.** *Any subset of a finite set is finite.*

### 1.6.3 Cardinal Numbers

For any set  $A$ , the cardinal number of  $A$ , denoted  $\text{card } A$ , is a set...

1. For any sets  $A, B \dots$

$$\text{card } A = \text{card } B \Leftrightarrow A \approx B.$$

2. For a finite set  $A$ ,  $\text{card } A$  is the natural number  $n$  for which  $A \approx n$ .

#### 1.6.3.1 Cardinal Arithmetic

Let  $\kappa$  and  $\lambda$  be any cardinal numbers.

- $\kappa + \lambda = \text{card}(K \cup L)$ , where  $K$  and  $L$  are any disjoint sets of cardinality  $\kappa$  and  $\lambda$ , respectively.
- $\kappa \cdot \lambda = \text{card}(K \times L)$ , where  $K$  and  $L$  are any sets of cardinality  $\kappa$  and  $\lambda$ , respectively.
- $\kappa^\lambda = \text{card}^L K$ , where  $K$  and  $L$  are any sets of cardinality  $\kappa$  and  $\lambda$ , respectively.

**Proposition 1.6.2.** *Assume that  $K_1 \approx K_2$  and  $L_1 \approx L_2$ .*

1. *If  $K_1 \cap L_1 = K_2 \cap L_2 = \emptyset$ , then  $K_1 \cup L_1 \approx K_2 \cup L_2$ .*
2.  *$K_1 \times L_1 \approx K_2 \times L_2$ .*
3.  *${}^{L_1}K_1 \approx {}^{L_2}K_2$ .*

**Proposition 1.6.3.** *For any cardinal numbers  $\kappa, \lambda$ , and  $\mu \dots$*

- $\kappa + \lambda = \lambda + \kappa$  and  $\kappa \cdot \lambda = \lambda \cdot \kappa$ .

- $\kappa + (\lambda + \mu) = (\kappa + \lambda) + \mu$  and  $\kappa \cdot (\lambda \cdot \mu) = (\kappa \cdot \lambda) \cdot \mu$ .
- $\kappa \cdot (\lambda + \mu) = \kappa \cdot \lambda + \kappa \cdot \mu$ .
- $\kappa^{\lambda+\mu} = \kappa^\lambda \cdot \kappa^\mu$ .
- $(\kappa \cdot \lambda)^\mu = \kappa^\mu \cdot \lambda^\mu$ .
- $(\kappa^\lambda)^\mu = \kappa^{\lambda \cdot \mu}$

**Proposition 1.6.4.** *Let  $m$  and  $n$  be finite cardinals. Then...*

- $m + n = m +_\omega n$
- $m \cdot n = m \cdot_\omega n$
- $m^n = m^n$

(See: natural number arithmetic.)

**Corollary 1.6.4.2.** *If  $A$  and  $B$  are finite, then  $A \cup B$ ,  $A \times B$ , and  ${}^B A$  are also finite.*

### 1.6.3.2 Ordering Cardinal Numbers

A set  $A$  is *dominated* by a set  $B$  (written  $A \preceq B$ ) if and only if there is an injective function from  $A$  into  $B$ .

**Theorem 1.6.5** (Schröder-Bernstein Theorem). *If  $A \preceq B$  and  $B \preceq A$ , then  $A \approx B$ .*

*Proof.* The proof is accomplished with mirrors. Given injections  $f : A \rightarrow B$  and  $g : B \rightarrow A$ . Define  $C_n$  by recursion, using the formulas

$$C_0 = A \setminus \text{ran } g \quad \text{and} \quad C_{n+} = g[f[C_n]].$$

Thus  $C_0$  is the troublesome part that keeps  $g$  from being a bijection. We bounce it back and forth, obtaining  $C_1, C_2, \dots$ . This function showing that  $A \approx B$  is the function  $h : A \rightarrow B$  defined by...

$$h(x) = \begin{cases} f(x) & \text{if } x \in C_n \text{ for some } n, \\ g^{-1}(x) & \text{otherwise.} \end{cases}$$

Note that in the second case ( $x \in A$  but  $x \notin C_n$  for any  $n$ ) it follows that  $x \notin C_0$  and hence  $x \in \text{ran } g$ . So  $g^{-1}(x)$  makes sense in this case. We verify that  $h$  is indeed a bijection. Define  $D_n = f[C_n]$ , so that  $C_{n+} = g[D_n]$ . Consider distinct  $x, y \in A$ . Since both  $f$  and  $g^{-1}$  are injective, the only possible problem arises when, say,  $x \in C_m$  and  $y \in \bigcup_{n \in \omega} C_n$ . In this case,

$$h(x) = f(x) \in D_m,$$

whereas,

$$h(y) = g^{-1}(y) \notin D_m,$$

lest  $y \in C_{m^+}$ . So  $h(x) \neq h(x')$ , showing  $h$  is injective.

Finally, we show  $h$  is surjective. Certainly each  $D_n \subseteq \text{ran } h$ , because  $D_n = h[C_n]$ . Consider then a point  $y$  in  $B \setminus \bigcup_{n \in \omega} D_n$ . Where is  $g(y)$ ? Certainly  $g(y) \notin C_0$ . Also  $g(y) \notin C_{n^+}$ , because  $C_{n^+} = g[D_n]$ ,  $y \notin D_n$ , and  $g$  is injective. So  $g(y) \notin C_n$  for any  $n$ . Therefore  $h(g(y)) = g^{-1}(g(y)) = y$ . This shows that  $y \in \text{ran } h$ , thereby proving part (a).  $\square$

**Theorem 1.6.6** (Restated Schröder-Bernstein Theorem). *For cardinal numbers  $\kappa$  and  $\lambda$ , if  $\kappa \leq \lambda$  and  $\lambda \leq \kappa$ , then  $\kappa = \lambda$ .*

**Proposition 1.6.5.** *Let  $\kappa, \lambda$  and  $\mu$  be cardinal numbers.*

- $\kappa \leq \lambda \Rightarrow \kappa + \mu \leq \lambda + \mu$
- $\kappa \leq \lambda \Rightarrow \kappa \cdot \mu \leq \lambda \cdot \mu$
- $\kappa \leq \lambda \Rightarrow \kappa^\mu \leq \lambda^\mu$
- $\kappa \leq \lambda \Rightarrow \mu^\kappa \leq \mu^\lambda$ ; if not both  $\kappa$  and  $\mu$  equal zero.

### 1.6.3.3 Infinite Cardinal Arithmetic

**Lemma 1.6.7.** *For any infinite cardinal  $\kappa$ , we have  $\kappa \cdot \kappa = \kappa$ .*

**Theorem 1.6.8** (Absorption Law of Cardinal Arithmetic). *Let  $\kappa$  and  $\lambda$  be cardinal numbers, the larger of which is infinite and the smaller of which is nonzero. Then...*

$$\kappa + \lambda = \kappa \cdot \lambda = \max(\kappa, \lambda).$$

## 1.7 Countable Sets

A set  $A$  is *countable* if and only if  $A \preceq \omega$ , i.e. if and only if  $\text{card } A \leq \aleph_0$ .

**Theorem 1.7.1.** *A countable union of countable sets is countable.*

*Proof.* We may suppose that  $\emptyset \notin \mathcal{A}$ , for otherwise we could simply remove it without affecting  $\bigcup \mathcal{A}$ . We may further suppose that  $\mathcal{A} \neq \emptyset$ , since  $\bigcup \emptyset$  is certainly countable. Thus  $\mathcal{A}$  is a countable (but nonempty) function from  $\omega \times \omega$  onto  $\bigcup \mathcal{A}$ . It is easy to find a function from  $\omega$  onto  $\omega \times \omega$ , and the composition will map  $\omega$  onto  $\bigcup \mathcal{A}$ , thereby showing that  $\bigcup \mathcal{A}$  is countable. Since  $\mathcal{A}$  is countable but nonempty, there is a function  $G$  from  $\omega$  onto  $\mathcal{A}$ . We are given that each set  $G(m)$  is countable and nonempty. Hence for each  $m$  there is a function from  $\omega$  onto  $G(m)$ . We must then use the axiom of choice to select such a function for each  $m$ . Let  $H : \omega \rightarrow^\omega (\bigcup \mathcal{A})$  be defined by...

$$H(m) = \{g \mid g \text{ is a function from } \omega \text{ onto } G(m)\}.$$

We know that  $H(m)$  is nonempty for each  $m$ . Hence there is function  $F$  with domain  $\omega$  such that for each  $m$ ,  $F(m)$  is a function from  $\omega$  onto  $G(m)$ . To conclude the proof we have only to let  $f(m, n) = F(m)(n)$ . Then  $f$  is a function from  $\omega \times \omega$  onto  $\bigcup \mathcal{A}$ .  $\square$

## 1.8 Continuum Hypothesis

There is no set  $\mathcal{S}$  such that  $\aleph_0 < \text{card } \mathcal{S} < 2^{\aleph_0}$ .

## 1.9 Ordinal Numbers

### 1.9.1 Partial Orderings

A *partial ordering* is a relation  $R$  such that...

1.  $R$  is transitive
2.  $R$  is irreflexive, that is for all  $x$  we have  $x \not R x$

**Proposition 1.9.1.** *Assume that  $<$  is a partial ordering. Then for  $x, y$ , and  $z$ :*

1. At most one of the alternatives,

$$x < y, \quad x = y, \quad y < x,$$

*can hold.*

2.  $x \leq y \leq x \Rightarrow x = y$ .

### 1.9.2 Linear Orderings

A *linear ordering* is a partial ordering  $R$  that satisfies trichotomy.

### 1.9.3 Well Orderings

A *well ordering* is a linear ordering  $R$  on  $A$  such that every nonempty subset of  $A$  has a least element.

**Theorem 1.9.1.** *Let  $<$  be a linear ordering on  $A$ . Then it is a well ordering if and only if there does not exist any function  $f : \omega \rightarrow A$  with  $f(n^+) < f(n)$  for every  $n \in \omega$ .*

**Theorem 1.9.2** (Transfinite Induction Principle). *Assume that  $<$  is a well ordering on  $A$ . Assume that  $B$  is a subset of  $A$  with the special property that for every  $t \in A$ ,*

$$\text{seg } t \subseteq B \Rightarrow t \in B.$$

*Then  $B$  coincides with  $A$ .*

*Proof.* If  $B \subset A$ , then  $A \setminus B$  has a least element  $m$ . But the leastness,  $y \in B$  for any  $y < m$ . But this is to say that  $\text{seg } m \subseteq B$ , so by assumption  $m \in B$  after all.  $\square$

## 2 Combinatorics

(See: Cardinality)

### 2.1 Basic Methods

#### 2.1.1 Addition

**Theorem 2.1.1** (Addition principle). *If  $A$  and  $B$  are two disjoint finite sets, then...*

$$|A \cup B| = |A| + |B|.$$

**Theorem 2.1.2** (Generalized addition principle). *Let  $A_1, A_2, \dots, A_n$  be finite sets that are pairwise disjoint. Then...*

$$|\bigcup_{i=1}^n A_i| = \sum_{i=1}^n |A_i|$$

#### 2.1.2 Subtraction

**Theorem 2.1.3** (Subtraction principle). *Let  $A$  be a finite set, and let  $B \subseteq A$ . Then  $|A \setminus B| = |A| - |B|$ .*

*Proof.* Observe  $|A \setminus B| + |B| = |A|$  by the addition principle.  $\square$

#### 2.1.3 Multiplication

**Theorem 2.1.4** (Product principle). *Let  $X$  and  $Y$  be two finite sets. Then  $|X \times Y| = |X| \times |Y|$ .*

**Theorem 2.1.5** (Generalized product principle). *Let  $X_1, X_2, \dots, X_n$  be finite sets. Then  $|\times_{i \in I}^n X_i| = \prod_{i \in I}^n |X_i|$ .*

#### 2.1.4 Division

**Theorem 2.1.6.** *Let  $S$  and  $T$  be finite sets so that a  $d$ -to-one function  $f : T \rightarrow S$  exists. Then*

$$|S| = \frac{|T|}{d}.$$

#### 2.1.5 Binomial Coefficients

See permutations.

**Theorem 2.1.7.** *Let  $n$  be a positive integer, and let  $k \leq n$  be a nonnegative integer. Then the number of all  $k$ -element subsets of  $[n]$  is*

$$\binom{n}{k} = \frac{(n)_k}{k!} = \frac{n!}{k!(n-k)!}.$$

Note:  $\binom{n}{k} = \binom{n}{n-k}$  exhibits duality.

**Theorem 2.1.8** (Binomial theorem). *If  $n$  is a positive integer, then...*

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

*Proof.* The left-hand side of the equation contains the factor  $(x + y)$   $n$  times. To compute the product we choose an  $x$  or  $y$  term from each factor and multiply those  $n$  terms together, then do this in all  $2^n$  possible ways, adding all the resulting products. It suffices to show that there are exactly  $\binom{n}{k}$  products of the form  $x^k y^{n-k}$ , which is immediately obvious from the way we compute the product.  $\square$

**Theorem 2.1.9.** *Let  $n$  and  $k$  be nonnegative integers so that  $k < n$ . Then...*

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$$

**Theorem 2.1.10.** *For all positive integers  $n$ ,*

$$\binom{2n}{n} = \sum_{k=0}^n \binom{n}{k}^2.$$

### 2.1.6 Pigeonhole Principle

**Theorem 2.1.11** (Pigeonhole Principle). *Let  $A_1, A_2, \dots, A_k$  be finite sets that are pairwise disjoint. Let us assume that*

$$|A_1 \cup A_2 \cup \dots \cup A_k| > kr.$$

*Then there exists at least one index  $i$  so that  $|A_i| > r$ . (See: Pigeonhole Principle in Set Theory)*

**Example 2.1.11.1.** *Consider the sequence  $1, 3, 7, 15, 31, \dots$ , in other words, the sequence whose  $i$ th element is  $a_i = 2^i - 1$ . Let  $q$  be any odd integer. Then our sequence contains an element that is divisible by  $q$ .*

*Proof.* Consider the first  $q$  elements of our sequence. If one of them is divisible by  $q$ , then we are done. If not, then consider their remainders modulo  $q$ . That is, let us write...

$$a_i = d_i q + r_i$$

where  $0 < r_i < q$ , and  $d_i = \lfloor a_i/q \rfloor$ . As the integers  $r_1, r_2, \dots, r_q$  all come from the open interval  $(0, q)$ , there are  $q - 1$  possibilities for their values. On the other hand, their number is  $q$ , so, by the pigeonhole principle, there have to be two of them that are equal. Say these are  $r_n$  and  $r_m$ , with  $n > m$ . Then  $a_n = d_n q + r_n$  and  $a_m = d_m q + r_m$ , so...

$$a_n - a_m = (d_n - d_m)q$$

or, after rearranging,

$$\begin{aligned}
(d_n - d_m)q &= a_n - a_m \\
&= (2^n - 1) - (2^m - 1) \\
&= 2^m(2^{n-m} - 1) \\
&= 2^m a_{n-m}
\end{aligned}$$

As the first expression of our chain of equations is divisible by  $q$ , so too must be the last expression. Note that  $2^{n-m}$  is relatively prime to any odd number  $q$ , that is, the largest common divisor of  $2^{n-m}$  and  $q$  is 1. Therefore, the equality  $(d_n - d_m)q = 2^{n-m}a_{n-m}$  implies that  $a_{n-m}$  is divisible by  $q$ .  $\square$

## 2.2 Applications of Basic Methods

### 2.2.1 Multisets

Given a set  $A$ , a *multiset* is defined via a function  $m : A \rightarrow \mathbb{N} \cup \{0\}$ . It is a set containing  $a \in A$   $m(a)$  many times.

#### 2.2.1.1 Multinomial Coefficients

**Theorem 2.2.1.** *Given a multiset  $A$  of  $n$  elements over a  $k$  element sets. The number of ways to linearly order the elements of  $A$  is...*

$$\binom{n}{a_1, a_2, \dots, a_k} = \frac{n!}{a_1! a_2! \dots a_k!}.$$

#### 2.2.2 Weak Compositions

Let  $a_1, a_2, \dots, a_k$  be nonnegative integers satisfying

$$\sum_{i=1}^k a_i = n.$$

Then the ordered  $k$ -tuple  $(a_1, a_2, \dots, a_k)$  is called a *weak composition* of  $n$  into  $k$  parts.

**Theorem 2.2.2.** *The number of weak compositions of  $n$  into  $k$  parts is...*

$$\binom{n+k-1}{n} = \binom{n+k-1}{k-1}.$$

**Corollary 2.2.2.1.** *The number of  $n$ -element multisets over a  $k$ -element set is...*

$$\binom{n+k-1}{n} = \binom{n+k-1}{k-1}.$$

### 2.2.3 Compositions

Let  $a_1, a_2, \dots, a_k$  be positive integers satisfying

$$\sum_{i=1}^k a_i = n.$$

Then the ordered  $k$ -tuple  $(a_1, a_2, \dots, a_k)$  is called a *composition* of  $n$  into  $k$  parts.

**Corollary 2.2.2.2.** *The number of compositions of  $n$  into  $k$  parts is...*

$$\binom{n-1}{k-1}.$$

### 2.2.4 Stirling numbers of the second kind

Given a finite set  $A$ ,  $|A| = n$ , the number of set partitions of  $A$  into  $0 < k \leq n$  classes is denoted  $S(n, k)$ , the *Stirling number of the second kind*.

## 2.3 Permutations

Given a set  $A$ , a *permutation* of  $A$  is a bijection  $f : A \rightarrow A$ .

**Proposition 2.3.1.** *Given a finite set  $A$ , if  $n = |A|$  the number of permutations of  $A$  is  $n!$ .*

Intuitively permutations represent the reordering of an ordered list. Looking at the idea of "sub-orderings" of lists we come up with the following proposition...

**Proposition 2.3.2** (k-lists). *Let  $n$  and  $k$  be positive integers so that  $n \geq k$ . Then the number of injections  $f : [k] \rightarrow [n]$  is...*

$$(n)_k := n(n-1)(n-2) \cdots (n-k+1).$$

## 2.4 Graphs

# 3 Category Theory

## 3.1 Metacategories

### 3.1.1 Undefined notions

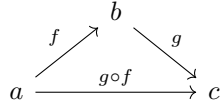
- *Objects:*  $a, b, c \dots$
- *Arrows:*  $f, g, h \dots$



### 3.1.2 Operations

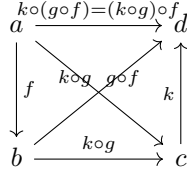
Given  $f : a \rightarrow b \dots$

- *Domain*: **dom**: arrows  $\rightarrow$  objects,  $f \mapsto a$
- *Codomain*: **cod**: arrows  $\rightarrow$  objects,  $f \mapsto b$
- *Identity*: **id**: objects  $\rightarrow$  arrows,  $a \mapsto \text{id}_a = 1_a$
- *Composition*: **comp**: arrows  $\times$  : arrows  $\rightarrow$  arrows,  $\langle g, f \rangle \mapsto g \circ f$ ,  
 $g \circ f : \text{dom}f \rightarrow \text{cod}g$

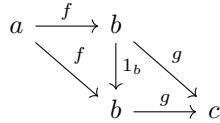


### 3.1.3 Axioms

- *Associativity*:  $a \xrightarrow{f} b \xrightarrow{g} c \xrightarrow{k} d$ ,  $k \circ (g \circ f) = (k \circ g) \circ f$



- *Unit Law*:  $1_a \circ f = f$  and  $g \circ 1_b = g$



## 3.2 Categories

### 3.2.1 Directed Graph

- $A$  - a set of arrows
- $O$  - a set of objects
- **dom** :  $A \rightarrow O$ , **cod** :  $A \rightarrow O$

Set of composable pairs of arrows:

$$A \times_O A = \{\langle g, f \rangle | g, f \in A \text{ and } \mathbf{dom}(g) = \mathbf{cod}(f)\}$$

### 3.2.2 Categories

Add the following structure to a directed graph. . .

- $O \xrightarrow{id} A, c \mapsto id_C$
- $A \times_O A \xrightarrow{\circ} A, \langle g, f \rangle \mapsto g \circ f$

which satisfy  $\forall a \in O$  and  $\forall \langle g, f \rangle \in A \times_O A$  . . .

- $\mathbf{dom}(\mathbf{id}(a)) = a = \mathbf{cod}(\mathbf{id}(a))$
- $\mathbf{dom}(g \circ f) = \mathbf{dom}(f)$
- $\mathbf{cod}(g \circ f) = \mathbf{cod}(g)$
- metacategorical axioms

Small categories use small sets for their objects.

### 3.2.3 Hom Sets

$hom(b, c) = \{f | f \in C, \mathbf{dom}(f) = b, \mathbf{cod}(f) = c\}$

### 3.2.4 Groupoids

A category in which every arrow is an isomorphism.

## 3.3 Morphisms

Arrows in categories.

### 3.3.1 Isomorphisms

A morphism  $f \in hom(b, c)$  that has a two-sided inverse  $g \in hom(c, b)$  under composition such that

$$gf = 1_b, fg = 1_c.$$

**Proposition 3.3.1.** *The inverse of an isomorphism is unique.*

*Proof.* For inverses  $g_1, g_2$  of  $f$  observe. . .

$$g_1 = g_1 1_c = g_1 (f g_2) = (g_1 f) g_2 = 1_b g_2 = g_2$$

□

**Proposition 3.3.2.** *Supposing  $f^{-1}$  is the inverse of  $f$  . . .*

- Each identity  $1_c$  is an isomorphism and is its own inverse.
- If  $f$  is an isomorphism, then  $f^{-1}$  is an isomorphism and further  $(f^{-1})^{-1} = f$ .
- If  $f \in hom(a, b)$ ,  $g \in hom(b, c)$  are isomorphisms, then the composition  $gf$  is an isomorphism and  $(gf)^{-1} = f^{-1}g^{-1}$ .

### 3.3.2 Automorphisms

An isomorphism of an object to itself. Denoted:

$$\text{hom}(c, c) = \text{aut}(c)$$

Observe  $\text{aut}(c)$  is a group.

### 3.3.3 Monomorphisms

A morphism  $f \in \text{hom}(b, c)$  such that  $\forall z \in C$  and  $\forall \alpha', \alpha'' \in \text{hom}(z, b)$ :

$$f \circ \alpha' = f \circ \alpha'' \Rightarrow \alpha' = \alpha''$$

### 3.3.4 Epimorphisms

A morphism  $f \in \text{hom}(b, c)$  such that  $\forall z \in C$  and  $\forall \beta', \beta'' \in \text{hom}(b, z)$ :

$$\beta' \circ f = \beta'' \circ f \Rightarrow \beta' = \beta''$$

## 3.4 Functors

Morphisms  $T : C \rightarrow B$  with domain and codomain both categories. It consists of two suitably related functions

- object function  $T, c \mapsto Tc$
- arrow function  $T, f : c \rightarrow c' \mapsto Tf : Tc \rightarrow Tc'$

which satisfy...

- $T(1_c) = 1_{Tc}$
- $T(g \circ f) = Tg \circ Tf$

### 3.4.1 Full

$\forall c, c' \in C$  and  $g : Tc \rightarrow Tc' \in B, \exists f : c \rightarrow c' \in C$  s.t.  $g \in Tf$

### 3.4.2 Faithful

$\forall c, c' \in C$  and  $f_1, f_2 : c \rightarrow c', Tf_1 = Tf_2 \Rightarrow f_1 = f_2$

- 3.5 Duality
- 4 Group Theory
- 5 Ring Theory
- 6 Modules
- 7 Homology
- 8 Topology
- 9 Homotopy