1 Set Theory

1.1 Set Axioms

1.1.1 Undefined notions

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

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 know as "Axiom of Foundation.")
3. *Schema of Specification:* $\forall B \forall X_1 \forall X_2 \ldots \forall X_n \exists A \forall C[C \in A \Leftrightarrow (C \in B \wedge \phi)]$
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:* $\forall A \forall X_1 \forall X_2 \ldots \forall X_n[\forall B(B \in A \Rightarrow \exists! D\phi) \Rightarrow \exists B \forall C(C \in A \Rightarrow \exists D(D \in B \wedge \phi))]$
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:* $\forall X[\emptyset \notin X \Rightarrow \exists (f : X \to \bigcup X) \forall A \in X(f(A) \in A)]$

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 $f : A \to B$ 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

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

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

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

1.2.5.1 Characteristic Function of a subset

For $A \subseteq X$, $\chi_A : X \to 2$ 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:* $\langle a, b \rangle := \{\{a\}, \{a, b\}\}$
- $\langle a_1, a_2, a_3, \dots a_n \rangle := \langle \langle \langle \langle a_1, a_2 \rangle, a_3 \rangle \dots \rangle, a_n \rangle$

1.2.7 Cartesian Product

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

Proposition 1.2.9. *For sets A, B...*

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

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

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

1.2.8 Quotient by Equivalence Relation

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

1.2.9 Family

Given a set X and an index set I, a family is a function $\mathcal{F} : I \to X$. 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 $\forall a, b, c \in A$...

- *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

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

1.3.1.2 Set of Equivalence Classes

$[A] = \{[a]_\sim | a \in A\}$

1.3.1.3 Set Partition

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

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

Proposition 1.3.1. *Let A is a set and $\sim$ an equivalence relation on A. Then $[A]$ is a partition of A.*

Proposition 1.3.2. *Let A be a set and P be a partition of A. Define a relation $x \sim y$ if and only if $x, y \in C \in P$. Then $\sim$ is an equivalence relation.*

1.3.1.4 Congruence Relation

A congruence $\sim$ of a set A with a binary operation $\mu : A \times A \to A$ is an equivalence relation such that...

$$\overline{\mu}([a], [b]) = [\mu(a, b)]$$

induces a well-defined binary operation on $[A]$.

Proposition 1.3.3. *An equivalence relation $\sim$ on A with $\mu : A \times A \to A$ is a congruence relation if for any $a, a', b, b' \in A$, whenever $[a] = [a']$ and [b] = [b'], we have $[\mu(a,b)] = [\mu(a',b')]$.*

1.3.2 Functions

A relation $f : A \to B$ 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, Stirling numbers of the second kind. 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 $f : A \to B$, $f\restriction_C : C \to B$ where $\forall c \in C\ f\restriction_C(c) := f(c)$

1.3.2.5 Image

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

Proposition 1.3.4. *For a function $f : A \to B$ and a family $\{X_i\}_{i \in I}$ where $\forall i \in I\ X_i \subseteq A \ldots$*

- $f(\bigcup_i X_i) = \bigcup_i f(X_i)$
- *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 1.3.5. *Given a function $f : X \to Y$, f is surjective if and only if $\forall A \subseteq Y$, where $A \neq \emptyset$, $f^{-1}(A) \neq \emptyset$.*

Proposition 1.3.6. *Given a function $f : X \to Y$, f is injective if and only if $\forall A \subseteq$ ran f, where A is a singleton, $f^{-1}(A)$ is a singleton.*

Proposition 1.3.7. *Given a function $f : X \to Y \dots$*

- *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 $A = f(f^{-1}(A))$.*
- *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

$f : X \to Y$ and $g : Y \to Z \Rightarrow g \circ f : X \to Z$ 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 ω.

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 ω)**.** *Any inductive subset of ω coincides with ω.*

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

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

1.4.4 Peano's Postulates

1.4.4.1 Peano System

An ordered triple $\langle N, S, e\rangle$ consiting of a set N, a function $S : N \to N$, 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* $\sigma = \{\langle n, n^+\rangle | n \in \omega\}$. *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* ω *is a transitive set.*

Proof. Use induction. □

1.4.5 Recursion

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

$$h(0) = a,$$

and for every $n \in \omega$*,*

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

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

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

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

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) dom h is all of ω, and (IV) h is unique.

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

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

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 acceptabel 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 conincides with ω. Consequently h is a function.

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

First examine (1). If $0 \in$ 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 $n^+ \in$ dom h. Again there must be some acceptable v with $v(n^+) = h(n^+)$. Since v is acceptable we have $n \in$ 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 dom $h = \omega$ (the function is nonempty). It suffices to show that dom h is inductive. The function $\{\langle 0, a\rangle\}$ is acceptable and hence $0 \in$ dom h. Suppose the $k \in$ dome h. If $k^+ \notin$ dom h, then let...

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

Then v is a function, dom $v \subseteq \omega$, and 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 $n^+ \in$ dom v where $n^+ \neq k^+$, then $n^+ \in$ 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 $k \in$ 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 dom h is inductive and therefore coincides with ω.

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

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

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

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

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

Proof. Note $h(a) > h(a-1) > h(a-2) > \cdots > 0$. Recursion on ω reliex on there being a starting point 0. $\mathbb{Z}$ has no analogous starting point. □

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 funciton h mapping ω 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 ω such that for any m and $n \in \omega$,

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

where $A_m : \omega \to \omega$ 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 ω such that for any m and $n \in \omega$,

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

where $M_m : \omega \to \omega$ 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 ω such that for any m and $n \in \omega$,

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

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

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

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 ω)**.** *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 canncellation 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 ω)**.** *Let A be a nonempty set of ω. 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 ω 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 $k^+ \in \omega - A$, 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...

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

We claim that B is inductive. $0 \in B$ vacuously. Suppose that $k \in B$. Then if n is less that 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 $A = \emptyset$. □

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

Theorem 1.4.7 (Strong Induction Principle for ω)**.** *Let A be a subset of ω, and assume the 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 $s : \omega \to \mathbb{Q}$ 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 $x \nsubseteq y$.

Since $x \nsubseteq y$ there is some rational r in the relative complement $x \backslash y$. 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 $y \subset x$. □

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 $\bigcup A$. □

1.5.4.2 Addition

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

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

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

1.6.1 Equinumerosity

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

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

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

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

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

$$f(1) = -7.777\ldots$$
$$f(2) = 3.1415\ldots$$
$$\vdots$$

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

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

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

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

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

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

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

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

Hence $B \notin \operatorname{ran} g$ 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 $f : N \to N$ is a bijection from a finite set to itself. We will show that ran f is all of the set n. This suffices to prove the theorem.

We use the induction on n. Define:

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

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 $f\restriction_k$ maps k injectively into k^+. There are two cases...

Case I: The set k is closed under f. Then $f\restriction_k$ maps the set k into the set k. Then because $k \in T$ we may conclude that ran $(f\restriction_k) = k$. Since f is injective, the only possible value for $f(k)$ is the number k. Hence 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 teh functino. 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 ran $f = k^+$. $\square$

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 ω 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 if finite.*

1.6.3 Cardinal Numbers

For any set A, the cardinal number of A, denoted card A, is a set...

1. For any sets A, B...

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

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

(See: cardinal number definition using ordinals)

1.6.3.1 Cardinal Arithmetic

Let κ and λ be any cardinal numbers.

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

- *$\kappa + \lambda = \lambda + \kappa$ 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 $f : A \to B$ and $g : B \to A$. Define C_n by recursion, using the formulas

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

Thus C_0 is the troublesome part that keeps g from being a bijection. We bounce it back and forth, obtaining $C_1, C_2, \ldots$. This function showing that $A \approx B$ is the function $h : A \to B$ 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 $x \in \operatorname{ran} g$. 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 abd 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 $D_n \subseteq \operatorname{ran} h$, 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 $y \in \operatorname{ran} h$, thereby proving part (a). □

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

Proposition 1.6.5. *Let κ, λ and μ 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 κ and μ equal zero.*

1.6.3.3 Infinite Cardinal Arithmetic

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

Theorem 1.6.8 (Absorption Law of Cardinal Arithmetic)**.** *Let κ and λ 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 card $A \leq \aleph_0$.

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

Proof. We may suppose that $\notin \mathcal{A}$, 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 ω onto $\omega \times \omega$, and the composition will map ω 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 ω onto $\mathcal{A}$. We are given that each set $G(m)$ is countable and nonempty. Hence for each m there is a function from ω 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...

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

We know that $H(m)$ is nonempty for each m. Hence there is function F with domain ω such that for each m, $F(m)$ is a function from ω ontop $G(m)$. 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 $\bigcup \mathcal{A}$. □

1.8 Axiom of Choice

(See: set axioms)

Theorem 1.8.1 (Axiom of Choice)**.** *The following statements are equivalent.*

1. *For any relation R, there is a function $F \subseteq R$ with dom $F =$ dom R.*

2. *The Cartesian product of nonempty sets is always nonempty. That is, if H is a function with domain I and if $(\forall i \in I) H(i) \neq \emptyset$, then there is a function f with domain I such that $(\forall i \in I) f(i) \in H(i)$.*

3. *For any set A there is a function F (a "choice function" for A) such that $F(B) \in B$ for every nonempty $B \subseteq A$.*

4. *Let $\mathcal{A}$ be a set such that (a) each member of $\mathcal{A}$ is a nonempty set, and (b) any two distinct members of $\mathcal{A}$ are disjoint. Then there exists a set C containing exactly one element from each member of $\mathcal{A}$ (i.e., for each $B \in \mathcal{A}$ the set $C \cap B$ is a singleton $\{x\}$ for some x).*

There are other theorems that are equivalent to the axiom of choice.

Theorem 1.8.2 (Cardinal Comparability)**.** *For any sets C and D, either $C \preceq D$ or $D \preceq C$. For any two cardinal numbers κ and λ, either $\kappa \leq \lambda$ or $\lambda \leq \kappa$.*

Theorem 1.8.3 (Zorn's Lemma)**.** *Let $\mathcal{A}$ be a set such that for every chain $\mathcal{B} \subseteq \mathcal{A}$, we have $\bigcup \mathcal{B} \in \mathcal{A}$. ($\mathcal{B}$ is called a* chain *if and only if for any C and D in $\mathcal{B}$, either $C \subseteq D$ or $D \subseteq C$.) Then $\mathcal{A}$ contains an element M (a "maximal" element) such that M is not a subset of any other set in $\mathcal{A}$.*

1.9 Continuum Hypothesis

Proposition 1.9.1. *For any infinite set A, we have $\omega \preceq A$.*

Proposition 1.9.2. $\aleph_0 \leq \kappa$ *for any infinite cardinal κ.*

Corollary 1.9.0.1. *A set is infinite if and only if it is equinumerous to a proper subset of itself.*

The *continuum hypothesis* is:

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

1.10 Ordinal Numbers

1.10.1 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 1.10.1. *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. $x \leq y \leq x \Rightarrow x = y$.

1.10.2 Linear Orderings

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

1.10.3 Well Orderings

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

Theorem 1.10.1. *Let $<$ be a linear ordering on A. Then if is a well ordering if and only if there does not exist any function $f : \omega \to A$ with $f(n^+) < f(n)$ for every $n \in \omega$.*

Theorem 1.10.2 (Transifinite 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 $t \in A$,*

$$seg\ t \subseteq B \Rightarrow t \in B.$$

Then B coincides with A.

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

Proposition 1.10.2. *Assume that $<$ is a linear ordering on A. Further assume that the only subset of A such that $\forall\, t \in A,\ seg\ t \subseteq B \Rightarrow t \in B$ is A itself. Then $<$ is a well ordering on A.*

1.10.4 Transfinite Recursion

Theorem 1.10.3 (Transfinite Recursion Theorem Schema)**.** *For any formula $\gamma(x, y)$ the following is a theorem:*

Assume that $<$ is a well ordering on a set A. Assume that for any f there is a unique y such that $\gamma(f, y)$. Then there exists a unique function F with domain A such that...

$$\gamma(F \restriction\ seg\ t,\ F(t))$$

for all $t \in A$.

The following axiom is used to prove the transfinite recursion theorem schema.

For any formula $\varphi(x, y)$ not containing the letter B, the following is an axiom:

$$\begin{aligned} &\forall[(\forall x \in A)\forall y_1 \forall y_2(\varphi(x, y_1) \wedge \varphi(x, y_2) \Rightarrow y_1 = y_2) \\ &\qquad \Rightarrow \exists B \forall y(y \in B \Leftrightarrow (\exists x \in A)\varphi(x, y))]. \end{aligned}$$

1.10.5 Epsilon Images

Let $<$ be a well ordering on A and let $\gamma(x, y)$ be the formulat $y =$ ran x. Then the transfinite recursion theorem gives an unique function E with domain A such that $\forall t \in A$:

$$\begin{aligned} E(t) &= \text{ ran } (E \restriction \text{ seg } t) \\ &= E[\text{seg } t] \\ &= \{E(x) | x < t\}. \end{aligned}$$

The ϵ-image of $\langle A, < \rangle$ is the range of E.

Proposition 1.10.3. *Let $<$ be a well ordering on A and let E be as above and α its epsilon image.*

1. *$E(t) \notin E(t)$ for any $t \in A$.*
2. *E maps A bijectively to α.*
3. *For any s and t in A,*

$$s < t \text{ if and only if } E(s) \in E(t)$$

4. *α is a transitive set.*

1.10.6 Ordinal Numbers

Proposition 1.10.4. *Two well-ordered structures are isomorphic if and only if they have the same ϵ-image. That is, if $<_1$ and $<_2$ are well orderings on A_1 and A_2, respectively, then $\langle A_1, <_1 \rangle \cong \langle A_2, <_2 \rangle$ if and only if the ϵ-image of $\langle A_1, <_1 \rangle$ is the same as the ϵ-image of $\langle A_2, <_2 \rangle$.*

The *ordinal number* of $\langle A, < \rangle$ is its ϵ-image. An *ordinal number* is a set that is the ordinal number of some well-ordered structure.

1.10.7 Cardinal Numbers

Theorem 1.10.4 (Numeration Theorem)**.** *Any set is equinumerous to some ordinal number.*

For any set A, define the cardinal number of A (card A) to be the least ordinal equinumerous to A.

2 Combinatorics

2.1 Basic Methods

Use Cardinality to derive the most basic results.

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 $A_1, A_2, \ldots, A_n$ 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. □

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 $X_1, X_2, \ldots, X_n$ be finite sets. Then $|\bigtimes_{i\in I}^{n} X_i| = \prod_{i\in I}^{n} |X_i|$.*

2.1.4 Division

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

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 $A_1, A_2, \ldots, A_k$ be finite sets that are pairwise disjoint. Let us assume that*

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

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

Example 2.1.11.1. *Consider the sequence $1, 3, 7, 15, 31, \ldots,$ in other words, the sequence whose ith 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 $r_1, r_2, \ldots, r_q$ 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 $a_m = d_m q + r_n$, 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. □

2.2 Applications of Basic Methods

2.2.1 Inclusion-Exclusion

Theorem 2.2.1 (Inclusin-exclusion principle)**.** *Let $A_1, A_2, \ldots, A_n$ be finite sets. Then...*

$$|A_1 \cup A_2 \cdots \cup A_n| = \sum_{j=1}^{n}(-1)^{j-1} \sum_{i_1,i_2,\ldots,i_j} |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_j}|,$$

where $(i_1, i_2, \ldots, i_j)$ ranges all j-element subsets of $[n]$.

Proof. We prove the two follwoing claims:

1. If x is contained in the set represented on the left side of the equation, then the right side conts it exactly once.

2. If x is not contained in any A_i, then the right-hand side counts x zero times.

(1) Assume that x is contained in exactly k of the n A_i-sets, with $k > 0$. Certainly, x is not in any j-fold intersection where $j > k$. On the otherhand $j \leq k$, then x is contained in exactly $\binom{k}{j}$ different j-fold intersections. If we take the signs into accoount, this means that the right side counts x exactly...

$$m = \sum_{j=1}^{k}(-1)^{j-1}\binom{k}{j}$$

times. Now we show that $m = 1$ necessarily. Observe...

$$1 - m = \sum_{j=0}^{k}(-1)^{j}\binom{k}{j} = (1-1)^k = 0,$$

since k is positive.

(2) We repeat the above argument with $k = 0$. Then the binomial theorem technique we use above gives us $(1-1)^0 = 1$, implying $m = 0$.

Thus the left-hand side and the right-hand side count the same objects. □

2.2.2 Multisets

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

2.2.2.1 Multinomial Coefficients

Theorem 2.2.2. *Given a multiset A of n elements over a k element sets. The number of ways to linearly order the elements of A is...*

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

2.2.3 Weak Compositions

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

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

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

Theorem 2.2.3. *The number of weak compositions of n into k parts is...*

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

Corollary 2.2.3.1. *The number of n-element multisets over a k-elemnt set is...*

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

2.2.4 Compositions

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

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

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

Corollary 2.2.3.2. *The number of compositions of n into k parts is...*

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

2.2.5 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.*

Theorem 2.2.4. *For all positive integers n and k satisfying $n \leq k$, the equality...*

$$S(n,k) = S(n-1,k-1) + kS(n-1,k)$$

Theorem 2.2.5. *For all positive integers n and k satisfying $n \geq k$.*

$$S(n+1,k) = \sum_{i=0}^{n} \binom{n}{i} S(n-i,k-1)$$

Theorem 2.2.6. *The number of surjections from $[n]$ to $[k]$ is equal to*

$$\sum_{j=0}^{k} (-1)^j \binom{k}{j} (k-j)^n.$$

Corollary 2.2.6.1. *For all positive integers $k \leq n$,*

$$S(n,k) = \frac{1}{k!} \sum_{j=0}^{k} (-1)^j \binom{k}{j} (k-j)^n.$$

2.2.5.1 Bell numbers

The number of all partitions of a finite set A, where $|A| = n$, is denoted $B(n)$ and is called a *Bell number.*

Theorem 2.2.7. *Set $B(0) = 1$. Then, for all positive integers n,*

$$B(n+1) = \sum_{k=0}^{n} B(k) \binom{n}{k}.$$

2.2.6 Partitions of integers

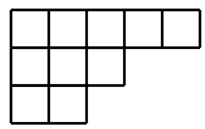
A *partition of an integer n* is a finite sequence $(a_1, a_2, \ldots, a_k)$ of positive integers satisfying $a_1 \geq a_2 \geq \cdots \geq a_k$ and $a_1 + a_2 + \cdot + a_k = n$.

Theorem 2.2.8. *As $n \to \infty$, the function $p(n)$ satisfies...*

$$p(n) \sim \frac{1}{4\sqrt{3}} \exp\left(\pi \sqrt{\frac{2n}{3}}\right)$$

2.2.7 Ferrers shapes

The *Ferrers shape* of the partition $(a_1, a_2, \ldots, a_k)$ is a row diagram of squares, with non-increasing amounts of squares in lower rows. For example the Ferrers shape fo $(5, 3, 2)$ is...



Proposition 2.2.1. *For all positive integers $k \leq n$, the number of partitions of n that have at least k parts is equal to the number of partitions of n in which the largest part is at least k.*

Proposition 2.2.2. *For every positive integer n, the number of partitions of n in which the first two parts are equal is equal to the number of partitions of n in which each part is at least 2.*

Lemma 2.2.9. *Let $m > k \geq 1$. Let S be the set of partitions of n into m parts, the smallest of which is equal to k, and let T be the set of partitions of n into $m-1$ parts, in which the kth part is larger than the $(k+1)$st part and the smallest part is at least k. Then $|S| = |T|$.*

2.2.8 Euler's totient function

For any positive integer n, let $\phi(n)$ denote the number of positive integers $k \leq n$ that are relatively prime to n.

Proposition 2.2.3. *Let $n = pq$, where p and q are distinct prinmes. Then $\phi(n) = (p-1)(q-1)$.*

Proof. Use the inclusion-exclusion principle on $[pq]$, followed by the subtraction principle. □

Proposition 2.2.4. *Let $n = p_1 p_2 \ldots p_t$, where the p_i are pairwise distinct primes. Then...*

$$\phi(n) = \prod_{i=1}^{t} (p_i - 1).$$

Lemma 2.2.10. *Let a and b be two positive integers whose greates common divisor is 1, and let $n = ab$. Then $\phi(n) = \phi(a)\phi(b)$.*

Proposition 2.2.5. *For any prime p, and any positive integer d,*

$$\phi(p^d) = (p-1)p^{d-1}.$$

Proposition 2.2.6. *Let $n = p_1^{d_1} p_2^{d_2} \ldots p_t^{d_t}$, where the p_i are distinct primes. Then...*

$$\phi(n) = \prod_{i=1}^{t} p_i^{d_i - 1}(p_i - 1)$$

2.3 Permutations

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

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 $f : [k] \to [n]$ is...*

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

2.4 Twelvefold Way

There are 12 fundamental counting problems. Sometimes they are formulated in terms of putting *balls* into *baskets*.

Let N and K be finite sets and n and k be their cardinality respectively...

2.4.1 Functions from K to N

Count with sequences of k elements in N, $|{}^K N|$.

2.4.2 Injections from K to N

Count with k-lists, $(n)_k$.

2.4.3 Surjections from K to N

Count with the number of surjections from $[k]$ to $[n]$, $\sum_{j=0}^{n}(-1)^j\binom{n}{j}(n-j)^k$.

2.4.4 Injections from K to N, up to a permutation of K

Count subsets, k-lists without order, $\binom{n}{k}$.

2.4.5 Functions from K to N, up to a permutation of K

Count multisets with k elements from N, $\binom{n+k-1}{k}$.

2.4.6 Surjections from K to N, up to a permutation of K

Count compositions of k into n parts, $\binom{k-1}{n-1}$.

2.4.7 Injections from K to N, up to a permutation of N

Provided $k \leq n$, there is only 1 of these.

2.4.8 Surjections from K to N, up to a permutation of N

Count partitions of K into n non-empty subsets, $S(k, n)$.

2.4.9 Functions from K to N, up to a permutation of N

Count all the partitions of K up to n classes, $\sum_{i=0}^{n} \binom{k}{i}$. If $k \leq n$, $B(k)$.

2.4.10 Functions from K to N, up to a permutation of K and N

Count partitions of k into $\leq n$ non-empty subsets, $\sum_{i=0}^{n} p_i(k)$.

2.4.11 Injections from K to N, up to a permutation of K and N

Provided $k \leq n$, there is only 1 of these.

2.4.12 Surjections from K to N, up to a permutation of K and N

Count partitions of k into n non-empty subsets, $p_n(k)$.

2.5 Graphs

A *graph* is an ordered pair $G = \langle V, E\rangle$ comprising a set V of *nodes* and E of *edges*, which are 2-element subsets of V.

Proposition 2.5.1. *Let $d_1, d_2, \ldots, d_n$ be the degrees of the vertices of a graph G on n vertices that has e edges. Then we have...*

$$d_1 + d_2 + \cdots + d_n = 2e.$$

2.5.1 Simple Graph

A *simple graph* is a graph that contains no loops and no multiple edges.

2.5.1.1 Walk

A *walk* is a series $e_1 e_2 \ldots e_k$ of edges that lead from a vertex to another one.

2.5.1.2 Cycle

A *cycle* is a walk whose starting point.

2.5.2 Graph Isomorphisms

An isomorphism f of two graphs G, H is a bijection from $V(G)$ to $V(H)$ such that if $\{a, b\} \in E(G)$, then $\{f(a), f(b)\} \in E(H)$.

2.5.2.1 Group of Automorphisms

Define the group of automorphisms of a graph G, $Aut(G)$, as normal.

Let J be a graph on n unlabeled vertices. Then define $\ell(J)$ as the number of possible ways to bijectively label J so that the resulting graphs are non-isomorphic.

Proposition 2.5.2. *For any graph H on vertex set $[n]$,*

$$|Aut(H)| \cdot \ell(H) = n!$$

2.5.3 Trees

A *tree* is a simple graph that is minimally connected.

2.5.3.1 Minimally Connected Graph

A *minimally connected* graph is contains the least number of edges in order to be connected.

Lemma 2.5.1. *Let G be a connected simple graph on n vertices. Then the following are equivalent.*

1. *The graph G is minimally connected.*
2. *There are no cycles in G.*
3. *The graph G has exactly $n-1$ edges.*

Proof. (1) $\Rightarrow$ (2) Assume there is a cycle C in G. Then G cannot be minimally connected since any one edge e of C can be omitted, and the obtained graph G' is still connected. Indeed, if a path uv used the edge e, then there would be a walk from u to v in which the edge e is replaced by the set edges of C that are different from e.

(2) $\Rightarrow$ (3) Pick any vertex $x \in G$ and start walking in some direction, never revisiting a vertex. As there is no cycle in G, eventually we will get stuck, meaning that we will hit a vertex of degree 1. This means that a connected simple graph with no cycles contains a vertex of degree 1. Removing such a vertex (and the only edge adjacent to it) from G, we get a graph $G*$ with one less vertex and one less edge, and the statement is proved by induction on n.

(3) $\Rightarrow$ (1) Suppose for the sake of contradiction that a graph on n vertices and $n-2$ edges cannot be connected. Let H be such a graph with a minimum number of vertices. Then H mus have more than 3 vertices. As H has $n-2$ edges, there has to be a vertex y of degree 1 in H, otherwise H would need to have at least n edges. Removing y from H, we get an even smaller counterexample for our statement, which is a contradiction. $\square$

Theorem 2.5.2 (Cayley's formula)**.** *For all positive integers n, the number of all trees on vertex set $[n]$ is n^{n-2}.*

Proof. We need to prove that $T_n = n^{n-2}$, which is the number of all functions from $[n-2]$ to $[n]$. This is certainly equivalent to proving the identity...

$$n^2 T_n = n^n.$$

Here the right-hand side is the number of all functions from $[n]$ into $[n]$. The left-hand side, on the other hand, is equal to the number of all trees on $[n]$ in which we select two vertices, called Start and End (which may be identical). Let us call these trees *doubly rooted trees*.

We construct a bijection G to prove the above formula. Let $f \in End_{Set}([n])$ and draw its *short diagram*, that is, represent $x \in [n]$ as a vertex in a graph, where there is an arrow $\langle x, y \rangle$ if and only if $f(x) = y$. This creates two kinds of vertices, namely, those that are in a directed cycle and those that are not. Let C and N, respectively, denote these two subsets of $[n]$.

Now we start creating the doubly rooted tree $G(f)$. First, note that f acts as a permutation on C. If $C = \{c_1, c_2, \dots c_k\}$ so that $c_1 < c_2 < \cdots < c_k$, call $f(c_1)$ Start and $f(c_k)$ End, and create a path with vertices $f(c_1), f(c_2), \dots, f(c_k)$. Note that so far we have defined a graph with k vertices and $k-1$ edges.

If $x \in N$, then simply connect x to $f(x)$, just as in the short diagram of f. This will define $n-k$ more edges. Therefore, we now have a graph on $[n]$ that has $n-1$ edges and has two vertices (called Start and End, respectively). This is the graph that we want to call $G(f)$. In order to justify that name, we must prove that $G(f)$ is connected. This is true, however, since, in the short diagram of f, each directed path starting at any $x \in N$ must reach a vertex of C at some point (there is no other way it could end). So indeed, $G(f)$ is a doubly rooted tree for all $f \in End_{Set}([n])$.

In order to show that G is a bijection, we prove it has an inverse. Let t be a doubly rooted tree. Then there is a unique path p from Start to End in t. To find $f = G^{-1}(t)$, just put the vertices along p into C, and put all the other vertices to N. If $x \in N$, then define $f(x)$ as the unique neighbor of $x \in t$ that is closer to p than x. For the vertices $x \in C$, we define f so that the ith vertex of the Start-End path is the image of the ith smallest element of C. It is a direct consequence of the definition of G that this way we will get an $f \in End_{Set}([n])$ satisfying $G(f) = t$, and that this f is the only preimage of t under G. Therefore, G is a bijection. $\square$

3 Category Theory

3.1 Metacategories

3.1.1 Undefined notions

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

3.1.2 Operations

Given $f : a \to b \ldots$

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

$$\begin{tikzcd} & b \arrow[dr, "g"] & \\ a \arrow[ur, "f"] \arrow[rr, "g \circ f"] & & c \end{tikzcd}$$

3.1.3 Axioms

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

$$\begin{tikzcd} a \arrow[r, "k \circ (g \circ f) = (k \circ g) \circ f"] \arrow[d, "f"] \arrow[dr, "g \circ f"'] & d \\ b \arrow[r, "k \circ g"] \arrow[ur, "k \circ g"] & c \arrow[u, "k"'] \end{tikzcd}$$

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

$$\begin{tikzcd} a \arrow[r, "f"] \arrow[dr, "f"] & b \arrow[d, "1_b"] \arrow[dr, "g"] & \\ & b \arrow[r, "g"] & c \end{tikzcd}$$

3.2 Categories

3.2.1 Directed Graph

- A - a set of arrows
- O - a set of objects
- $\mathbf{dom} : A \to O$, $\mathbf{cod} : A \to O$

3.2.1.1 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

3.2.3 Small categories

Small categories use small sets for their objects.

3.2.4 Hom Sets

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

3.2.4.1 Alternate Definition of Categories

Small categories may be defined with hom-sets as follows...

1. A set of objects a, b, c...
2. A function which assigns to each ordered pair $\langle a, b \rangle$ of objects a set $\hom(a, b)$

3. For each ordered triple $\langle a, b, c\rangle$ of objects a function

$$\hom(b, c) \times \hom(a, b) \to \hom(a, c)$$

called composition, and written $\langle g, f\rangle \to g \circ f$ for $g \in \hom(b, c),\ f \in \hom(a, b)$

4. For each object b, an element $1_b \in \hom(b, b)$, called the identity of b.
5. If $\langle a, b\rangle \neq \langle a', b'\rangle$, then $\hom(a, b) \cap \hom(a', b') = \emptyset$

The above satisfy the meta-categorical axioms.

Functors in terms of hom-sets are the object function with a collection of functions

$$T_{c,c'} : \hom_C(c, c') \to \hom_B(Tc, Tc')$$

such that each $T_{c,c'} 1_c = 1_{Tc}$ and every diagram...

$$\begin{tikzcd}
hom_C(c', c'') \times hom_C(c, c') \arrow[r, "\circ"] \arrow[d, "T_{c',c''} \times T_{c,c'}"] & hom_C(c, c'') \arrow[d, "T_{c',c''}"] \\
hom_B(Tc', Tc'') \times hom_B(Tc, Tc') \arrow[r, "\circ"] & hom_B(Tc, Tc'')
\end{tikzcd}$$

is commutative.

3.2.5 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...

$$g_1 = g_1 1_c = g_1(fg_2) = (g_1 f)g_2 = 1_b g_2 = g_2$$

□

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:

$$hom(c,c) = aut(c)$$

Observe $aut(c)$ is a group.

3.3.3 Monomorphisms

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

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

3.3.4 Epimorphisms

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

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

3.3.5 Split Morphism

A morphism $f : b \to b$ such that $f^2 = f$ and there exist morphisms $g : b \to c$, $h : c \to b$ satisfying...

$$f = hg \quad \wedge \quad gh = 1_c$$

3.4 Some Objects in Categories

3.4.1 Initial Objects

We say that an object i of a category C is *initial* in C if for every object a of C there exists exactly one morphism $i \to a$ in C:

$$\forall a \in Obj(C) : \quad Hom_C(i,a) \text{ is a singleton.}$$

3.4.2 Final Objects

We say that an object f of a category C is *final* in C if for every object a of C there exists exactly one morphism $a \to f$ in C:

$$\forall a \in Obj(C) : \quad Hom_C(a, f) \text{ is a singleton.}$$

Proposition 3.4.1. *Let C be a category.*

- *If i_1, i_2 are both initial objects in C, then $i_1 \cong i_2$.*
- *If f_1, f_2 are both initial objects in C, then $f_1 \cong f_2$.*

3.4.3 Null Objects

An object that is both initial and terminal.

3.4.4 Group Objects

A *group object* in C consists of an object g of C and of morphisms…

$$m : g \times g \to g, \; e : 1 \to g, \; \iota : g \to g$$

in C such that the diagrams…

$$\begin{tikzcd}
(g \times g) \times g \arrow[r, "m \times \mathrm{id}_g"] \arrow[d] & g \times g \arrow[r, "m"] & g \arrow[d, "="] \\
g \times (g \times g) \arrow[r, "\mathrm{id}_g \times m"] & g \times g \arrow[r, "m"] & g
\end{tikzcd}$$

$$\begin{tikzcd}
1 \times g \arrow[r, "e \times \mathrm{id}_g"] \arrow[dr, "\cong"'] & g \times g \arrow[d, "m"] \\
& g
\end{tikzcd}
\qquad
\begin{tikzcd}
g \times 1 \arrow[r, "\mathrm{id}_g \times e"] \arrow[dr, "\cong"'] & g \times g \arrow[d, "m"] \\
& g
\end{tikzcd}$$

$$\begin{tikzcd}
g \arrow[r, "\Delta"] \arrow[d] & g \times g \arrow[r, "\mathrm{id}_g \times \iota"] & g \times g \arrow[d, "m"] \\
1 \arrow[rr, "e"] & & g
\end{tikzcd}
\qquad
\begin{tikzcd}
g \arrow[r, "\Delta"] \arrow[d] & g \times g \arrow[r, "\iota \times \mathrm{id}_g"] & g \times g \arrow[d, "m"] \\
1 \arrow[rr, "e"] & & g
\end{tikzcd}$$

commute.

3.5 Functors

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

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

which satisfy...

- $T(1_c) = 1_c$
- $T(g \circ f) = Tg \circ Tf$

3.5.1 Full

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

3.5.2 Faithful

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

3.5.3 Forgetful

A functor that drops some of the structure of its input. For example, the forgetful functor $U : \mathrm{Cat} \to \mathrm{Graph}$...

- $C \mapsto UC$ where UC is comprised of the underlying objects and arrows of the category
- $F : C \to C' \mapsto UF : UC \to UC'$ where UF is a morphism between corresponding graphs

3.5.3.1 Group Action

If G is a group and a an object of a category C, then a *group action* is a functor...

$$\sigma : G \to \mathrm{Aut}_C(a)$$

3.6 Natural Transformations

Given two functors $S, T : C \to B$ a *natural transformation* $\tau : S \stackrel{\cdot}{\to} T$ is a function which assigns to each object $c \in C$ an arrow

$$\tau_c = \tau c : Sc \to Tc$$

of B in such a way that every arrow $f : c \to c'$ in C yields a diagram...

$$\begin{tikzcd}
c \arrow[d, "f"] & Sc \arrow[r, "\tau c"] \arrow[d, "Sf"] & Tc \arrow[d, "Tf"] \\
c' & Sc' \arrow[r, "\tau c'"] & Tc'
\end{tikzcd}$$

which is commutative.

In the following diagram $\tau a, \tau b, \tau c$ are the components of the natural transformation.

$$\begin{tikzcd}
a \arrow[dr, "f"] \arrow[dd, "h"] & & Sa \arrow[rr, "\tau a"] \arrow[dr, "Sf"] \arrow[dd, "Sh"] & & Ta \arrow[dr, "Tf"] \arrow[dd, "Th"] & \\
& c & & Sc \arrow[rr, "\tau c"] & & Tc \\
b \arrow[ur, "g"] & & Sb \arrow[ur, "Sg"] \arrow[rr, "\tau b"] & & Tb \arrow[ur, "Tg"] &
\end{tikzcd}$$

3.7 Duality

Statement $\sum$	Dual Statement $\sum^*$
$f : a \to b$	$f : b \to a$
$a = \mathrm{dom} f$	$a = \mathrm{cod} f$
$i = 1_a$	$i = 1_a$
$h = g \circ f$	$h = f \circ g$
f is a monomorphism	f is an epimorphism
u is a right inverse of h	u is a left inverse of h
f is invertible	f is invertible
f is a terminal object	f is an initial object

3.8 Contravariance and Opposites

3.8.1 Contravariant Functor

Given a functor $S : C^{op} \to B$ the *contravariant functor* $\overline{S} : C \to B$ satisfies...

- $\overline{S}f = Sf^{op}$,
- $c \mapsto \overline{S}c$,
- $f : a \to b \mapsto \overline{S}f : \overline{S}b \to \overline{S}a$,
- $\overline{S}(1_c) = 1_{\overline{S}c}$,
- $\overline{S}(fg) = (\overline{S}g)(\overline{S}f)$.

3.8.1.1 Covariant Hom-Functor

A hom-functor $C(a, -) = hom(a, -) : C \to \text{Set}$ satisfying...

- $b \mapsto hom(a, b)$
- $k : b \to b' \mapsto hom(a, k) : hom(a, b) \to hom(a, b')$; the right side maps $f \mapsto k \circ f$ and is denoted $k*$

3.8.1.2 Contravariant Hom-Functor

A hom-functor $C(-, b) = hom(-, b) : C^{op} \to \text{Set}$ satisfying...

- $a \mapsto hom(a, b)$
- $g : a \to a' \mapsto hom(g, a) : hom(a', b) \to hom(a, b)$; the right side maps $f \mapsto f \circ g$ and is denoted $g*$

The functions g^*, k^* defined above satify the following commutative diagram.

$$\begin{tikzcd}
hom(a', b) \arrow[r, "g*"] \arrow[d, "k*"] & hom(a, b) \arrow[d, "k*"] \\
hom(a', b') \arrow[r, "g*"] & hom(a, b')
\end{tikzcd}$$

3.9 Category Constructions

3.9.1 Products

Given categories B and C we construct the product category $B \times C$...

- Objects: pairs of objects $\langle b, c \rangle$ ($b \in B$ and $c \in C$)
- Arrows: $\langle b, c \rangle \to \langle b', c' \rangle$ are a pair $\langle f, g \rangle$ of arrows ($f \in B$ and $g \in C$)
- Composition: $\langle f', g' \rangle \circ \langle f, g \rangle = \langle f' \circ f, g' \circ g \rangle$

The corresponding universal property is: for any functors R and T, there is a unique functor F making the digram commute...

$$
\begin{tikzcd}
 & D \arrow[dl, "R"'] \arrow[d, dotted, "F"] \arrow[dr, "T"] & \\
B & B \times C \arrow[l, "P"] \arrow[r, "Q"'] & C
\end{tikzcd}
$$

Note: $P\langle f, g\rangle = f$ and $Q\langle f, g\rangle = g$ are called the *projections* of the product.

3.9.1.1 Products of Functors

Given functors U and V, the functor product $U \times V$ satisfies...

- $(U \times V)\langle b, c\rangle = \langle Ub, Uc\rangle$ for objects
- $(U \times V)\langle f, g\rangle = \langle Uf, Ug\rangle$ for arrows

$$
\begin{tikzcd}
B \arrow[d, "U"] & B \times C \arrow[l, "P"'] \arrow[r, "Q"] \arrow[d, dotted, "U\times V"] & C \arrow[d, "V"] \\
B & B \times C \arrow[l, "P'"'] \arrow[r, "Q'"] & B
\end{tikzcd}
$$

3.9.1.2 Bifunctors

A functor $S : B \times C \to D$. Intuitively, "a functor of two variables."

Determined by the functors that result when any one object of exactly one of the categories is fixed. This is recorded more explicitly in the following proposition...

Proposition 3.9.1. *Let B, C, and D be categories. For all objects $c \in C$ and $b \in B$, let*

$$L_c : B \to D,\ M_b : C \to D$$

be functors such that $M_b(c) = L_c(b)$ for all b and c. Then there exists a bifunctor $S : B \times C \to D$ with $S(-, c) = L_c$ for all c and $S(b, -) = M_b$ for all b if and only if for every pair of arrows $f : b \to b'$ and $g : c \to c'$ one has

$$M_{b'}g \circ L_c f = L_{c'} f \circ M_b g.$$

These equal arrows in D are then the value $S(f, g)$ of the arrow function of S at f and g.

Proof. Observe...

$$\langle b', g\rangle \circ \langle f, c\rangle = \langle b'f, gc\rangle = \langle f, g\rangle = \langle fb, c'g\rangle = \langle f, c'\rangle \circ \langle b, g\rangle$$

(where b, b', c, c' are identity arrows).

This implies...

$$S(b', g)S(f, c) = S(f, c')S(b, g).$$

Which further implies...

$$\begin{tikzcd}
S(b,c) \arrow[r, "S(b,g)"] \arrow[d, "S(f,c)"] & S(b,c') \arrow[d, "S(f,c')"] \\
S(b',c) \arrow[r, "S(b',g)"] & S(b',c')
\end{tikzcd}$$

□

3.9.1.3 Natural transformations between bifunctors

Given $S, S' : B \times C \to D$. Consider $\alpha(b, c) : S(b, c) \to S'(b, c)$. We say α is *natural in* b if $\forall c \in C$ the components $\alpha(b, c)$ for all b define $\alpha(-, c) : S(-, c) \dot{\to} S'(-, c)$, a natural transformation of functors $B \to D$.

Proposition 3.9.2. *For bifunctors S, S', the function α displayed above is a natural transformation $\alpha : S \dot{\to} S'$ (i.e., of bifunctors) if and only if $\alpha(b, c)$ is natural in b for each $c \in C$ and natural in c for each $b \in B$.*

$$\begin{tikzcd}
S(b,c) \arrow[r, "\alpha(f,g)"] \arrow[d, "S(f,g)"] & S(b,c) \arrow[d, "S'(b,c)"] \\
S(b',c') \arrow[r, "\alpha(b',c')"] & S(b',c')
\end{tikzcd}$$

3.9.1.4 The Universal Natural Transformation

Given any natural transformation $\tau : S \dot{\to} T$ between $S, T : C \to B$ there is a unique functor $F : C \times 2 \to B$ with $F\mu c = \tau c$ for any object c.

- $F\langle f, 0\rangle = Sf$
- $F\langle f, 1\rangle = Tf$
- $F\langle f, \downarrow\rangle = Tf \circ \tau c = \tau c' \circ Sf$ (where $\downarrow : 0 \to 1$)

Observe $C \times 2$ below...

$$\begin{tikzcd}
c \arrow[rr, "\mu c"] \arrow[dr] \arrow[dd, "C\times 0 \text{ layer}"'] & & c \arrow[dd] \arrow[dr, "C\times 1 \text{ layer}"] & \\
& c'' \arrow[rr, "\mu c''"] & & c'' \\
c' \arrow[ur] \arrow[rr, "\mu c'"] & & c' \arrow[ur] &
\end{tikzcd}$$

where $\mu c = \langle c, \downarrow \rangle$

3.9.2 Coproducts

Given categories B and C the dual of the product category is coproduct category $B \coprod C$.

The corresponding universal property is: for any functors R and T, there is a unique functor F making the digram commute...

$$\begin{tikzcd}
B \arrow[r, "I"] & B \coprod C & C \arrow[l, "J"'] \\
& D \arrow[ul, "R"] \arrow[u, dotted, "F"] \arrow[ur, "T"'] &
\end{tikzcd}$$

3.9.3 Quotients

The *quotient category* is specified in the following proposition.

Proposition 3.9.3. *For a given category C, let R be a function which assigns to each pair of objects a, b of C a binary relation $R_{a,b}$ on the hom-set $C(a, b)$. Then there exist a category C/R and a functor $Q = Q_R : C \to C/R$ such that...*

1. *If $fR_{a,b}f'$ in C, then $Qf = Qf'$.*
2. *If $H : C \to D$ is any functor from C for which $fR_{a,b}f'$ implies $Hf = Hf'$ for all f and f', then there is a unique functor $H' : C/R \to D$ with $H' \circ Q_R = H$.*

Moreover, the functor Q_R is a bijection on objects.

The corresponding universal property is represented in the following diagram...

$$\begin{tikzcd}
C \arrow[r, "Q_R"] \arrow[dr, "H"'] & C/R \arrow[d, dotted, "H'"] \\
& D
\end{tikzcd}$$

3.9.3.1 Congruence

A *congruence* is a relation R on a category C such that...

- $\forall a, b \in \mathrm{Obj}(C)$, $R_{a,b}$ is an equivalence relation
- if $f, f' : a \to b$ have $f R_{a,b} f'$, then for all $g : a' \to a$ and all $h : b \to b'$ one has $(hfg) R_{a',b'} (hf'g)$.

3.9.4 Free Categories

3.9.4.1 O-graph

The *O-graph* is a directed graph on a fixed set O of objects (not a simple graph).

We define the *product over* O as a set of composable pairs of arrows...

$$A \times_O B = \{\langle g, f\rangle | \delta_0 g = \delta_1 f, g \in A, f \in B\}$$

where δ_0, δ_1, resp., are functions representing the **dom**, **cod**, resp., operations.

A category with objects O is an O-graph equipped with two morphisms $c : A \times_O A \to A$ and $i : O \to A$ of O-graphs making the following diagrams commutative.

$$\begin{tikzcd}
(A \times_O A) \times_O A \arrow[r, "\cong"] \arrow[d, "c\times 1"] & A \times_O (A \times_O A) \arrow[r, "1\times c"] & A \times_O A \arrow[d, "c"] \\
A \times_O A \arrow[rr, "c"] & & A
\end{tikzcd}
\qquad
\begin{tikzcd}
O \times_O A \arrow[r, "i\times 1"] \arrow[d, "\cong"] & A \times_O A \arrow[d, "c"] & A \times_O O \arrow[l, "1\times i"'] \arrow[d, "\cong"] \\
A \arrow[r, "="] & A & A \arrow[l, "="]
\end{tikzcd}$$

3.9.4.2 Free Category

Let $C(G)$ be the *free category* generated by graph G, specified in the subsequent theorem...

Theorem 3.9.1. *Let $G = \{A \rightrightarrows O\}$ be a small graph. There is a small category $C(G)$ with O as its set of objects and a morphism $P : G \to UC$ of graphs from G to the underlying graph UC of C with the following property. Given any category B and any morphism $D : G \to UB$ of graphs, there is a unique functor $D' : C \to B$ with $(UD') \circ P = D$, as in the commutative diagram*

$$\begin{tikzcd}
C \arrow[d, dotted, "D'"] \\
B
\end{tikzcd}
\qquad
\begin{tikzcd}
G \arrow[r, "P"] \arrow[dr, "D"'] & UC \arrow[d, dotted, "UD'"] \\
& UB
\end{tikzcd}$$

In particular, if B had O as set of objects and D is a morphism of O-graphs, then D' is the identity on objects.

Corollary 3.9.1.1. *To any set X there is a monoid M and a function $p : X \to UM$, where UM is the underlying set of M, with the following universal property: for any monoid L and any function $h : X \to UL$ there is a unique morphism $h' : M \to L$ of monoids with $h : Uh' \circ p$.*

$$Hom_{Cat}(C(G), B) \cong Grph(G, UB),\ D' \mapsto D = UD' \circ P$$

3.9.5 Comma Categories

3.9.5.1 Category of objects unber b $(b \downarrow C)$

Objects $\langle f, c\rangle$:

$$\begin{tikzcd} b \arrow[d, "f"] \\ c \end{tikzcd}$$

Arrows $\langle f, c\rangle \xrightarrow{h} \langle f', c'\rangle$:

$$\begin{tikzcd} & b \arrow[dl, "f'"'] \arrow[dr, "f"] & \\ c \arrow[rr, "h"] & & c' \end{tikzcd}$$

3.9.5.2 Category of objects over a $(C \downarrow a)$

Objects $\langle f, c\rangle$:

$$\begin{tikzcd} c \arrow[d, "f"] \\ a \end{tikzcd}$$

Arrows $\langle f, c\rangle \xrightarrow{h} \langle f', c'\rangle$:

$$\begin{tikzcd} c \arrow[rr, "h"] \arrow[dr, "f"'] & & c' \arrow[dl, "f'"] \\ & a & \end{tikzcd}$$

3.9.5.3 Category of objects S-unber b $(b \downarrow S)$

Given a functor $S : D \to C$.

Objects $\langle f, Sd\rangle$:

$$\begin{tikzcd} b \arrow[d, "f"] \\ Sd \end{tikzcd}$$

Arrows $\langle f, Sd\rangle \xrightarrow{Sh} \langle f', Sd'\rangle$:

$$\begin{tikzcd} & b \arrow[dl, "f'"'] \arrow[dr, "f"] & \\ Sd \arrow[rr, "Sh"] & & Sd' \end{tikzcd}$$

3.9.5.4 Category of objects T-over a $(T \downarrow a)$

Given a functor $T : E \to C$.

Objects $\langle f, Te\rangle$:

$$\begin{tikzcd} Te \arrow[d, "f"] \\ a \end{tikzcd}$$

Arrows $\langle f, Te\rangle \xrightarrow{Th} \langle f', Te'\rangle$:

$$\begin{tikzcd} Te \arrow[rr, "Th"] \arrow[dr, "f"'] & & Te' \arrow[dl, "f'"] \\ & a & \end{tikzcd}$$

3.9.5.5 Comma Category $(T \downarrow S)$

Given functors $S : D \to C$ and $T : E \to C$.

Objects $\langle e, d, f\rangle$:

$$\begin{tikzcd} Te \arrow[d, "f"] \\ Sd \end{tikzcd}$$

where $d \in$Obj(D), $e \in$Obj(E), $f : Te \to Sd$.

Arrows $\langle e, d, f\rangle \xrightarrow{\langle k,h\rangle} \langle e', d', f'\rangle$:

$$
\begin{tikzcd}
Te \arrow[r, "Tk"] \arrow[d, "f"] & Te' \arrow[d, "f'"] \\
Sd \arrow[r, "Sh"] & Sd'
\end{tikzcd}
$$

where $k : e \to e'$, $h : d \to d'$ such that $f' \circ Tk = Sh \circ f$.

Composition $\langle k', h' \rangle \circ \langle k, h \rangle = \langle k' \circ k, h' \circ h \rangle$ when defined.

$$
\begin{tikzcd}
 & & T \downarrow S \arrow[dll, "P"'] \arrow[d, "Q"] \arrow[drr, "R"] & & \\
E \arrow[r, "T"'] & C & C^2 \arrow[l, "C^{d_0}"] \arrow[r, "C^{d_1}"'] & C & D \arrow[l, "S"]
\end{tikzcd}
$$

P and Q are the *projections* of the comma category. C^{d_0}, C^{d_1}, resp., send arrows to domain, codomain, resp.

$$
\begin{tikzcd}
 & & \langle e, d, f : Te \to Sd \rangle \arrow[dll, mapsto] \arrow[d, mapsto] \arrow[drr, mapsto] & & \\
e \arrow[r, mapsto] & Te & (f : Te \to Sd) \arrow[l, mapsto] \arrow[r, mapsto] & Sd & d \arrow[l, mapsto]
\end{tikzcd}
$$

3.10 Higher Level Categories

3.10.1 Functor Categories

A *functor category* is a category whose objects are functors and whose arrows are natural transformations. Since compositions of natural transformations are natural transformations, composition can be defined as in the following diagram. . .

$$
\begin{tikzcd}
Rc \arrow[r, "Rf"] \arrow[d, "\sigma c"] \arrow[dd, bend right, "(\tau\circ\sigma)c"'] & Rc' \arrow[d, "\sigma c'"'] \arrow[dd, bend left, "(\tau\circ\sigma)c'"] \\
Sc \arrow[r, "Sf"] \arrow[d, "\tau c"] & Sc' \arrow[d, "\tau c'"'] \\
Tc \arrow[r, "Tf"] & Tc'
\end{tikzcd}
$$

3.10.2 2-Categories

3.10.2.1 Vertical Composition

For natural transformations τ and σ, we have "vertical" composition $\tau\dot{\sigma}$, as in the following diagram...

$$
\begin{tikzcd}
C \arrow[r] \arrow[d, "\sigma"] \arrow[dd, bend right, "\tau\sigma"'] & B \arrow[d, "\sigma"] \arrow[dd, bend left, "\tau\sigma"] \\
C \arrow[r] \arrow[d, "\tau"] & B \arrow[d, "\tau"] \\
C \arrow[r] & B
\end{tikzcd}
$$

3.10.2.2 Horizontal Composition

We can also define "horizontal" composition for natural transformations τ and τ', $\tau' \circ \tau$, as in the following commutative diagrams...

$$
\begin{tikzcd}
C \arrow[r, "S"] \arrow[d, "\tau"] & B \arrow[r, "S'"] \arrow[d, bend right, "\tau"'] \arrow[d, bend left, "\tau'"] & A \arrow[d, "\tau'"] \\
C \arrow[r, "T"] & B \arrow[r, "T'"] & A
\end{tikzcd}
$$

$$
\begin{tikzcd}
S'Sc \arrow[r, "\tau' Sc"] \arrow[d, "S'\tau c"] \arrow[dr, dotted, "(\tau' \circ \tau)c"] & T'Sc \arrow[d, "T'\tau c"] \\
S'Tc \arrow[r, "\tau' Tc"] & T'Tc
\end{tikzcd}
$$

The next diagram shows $\tau' \circ \tau : S'S \dot{\to} T'T$ is natural.

$$
\begin{tikzcd}
c \arrow[d, "f"] & S'Sc \arrow[r, "S'\tau c"] \arrow[d, "S'Sf"] & S'Tc \arrow[r, "\tau' Tc"] \arrow[d, "S'Tf"] & T'Tc \arrow[d, "T'Tf"] \\
b & S'Sb \arrow[r, "T'\tau b"] & S'Tb \arrow[r, "\tau' Tb"] & T'Tb
\end{tikzcd}
$$

So $\tau' \circ \tau = (T' \circ \tau) \cdot (\tau' \circ S) = (\tau' \circ T) \cdot (S' \circ \tau)$, which leads into our next concept.

3.10.2.3 Interchange Law

For natural transformations $\sigma, \sigma', \tau, \tau'$ satisfying...

$$\begin{tikzcd}
C \arrow[r] \arrow[d, "\sigma"] & B \arrow[r] \arrow[d, bend right, "\sigma"'] \arrow[d, bend left, "\sigma'"] & A \arrow[d, "\sigma'"] \\
C \arrow[r] \arrow[d, "\tau"] & B \arrow[r] \arrow[d, bend right, "\tau"'] \arrow[d, bend left, "\tau'"] & A \arrow[d, "\tau'"] \\
C \arrow[r] & B \arrow[r] & A
\end{tikzcd}$$

the *interchange law* is $(\tau' \cdot \sigma') \circ (\tau \cdot \sigma) = (\tau' \circ \tau) \cdot (\sigma' \circ \sigma)$.

The proof of the interchange law derives from the following diagram. Intuitively, the interchange law occurs along the dotted diagonal lines.

$$\begin{tikzcd}
S'Sc \arrow[r, "\sigma' S"] \arrow[d, "S'\sigma"] \arrow[dr, dotted] \arrow[ddrr, dotted, bend left] & T'Sc \arrow[r, "\tau' S"] \arrow[d, "T'\sigma"] & R'Sc \arrow[d, "R'\sigma'"] \\
S'Tc \arrow[r, "\sigma' T"] \arrow[d, "S'\tau"] & T'Tc \arrow[r, "\tau' T"] \arrow[d, "T'\tau"] \arrow[dr, dotted] & R'Tc \arrow[d, "R'\tau'"] \\
S'Rc \arrow[r, "\sigma' R"] & T'Rc \arrow[r, "\tau' R"] & R'Rc
\end{tikzcd}$$

Theorem 3.10.1. *The collection of natural transformations in the set of arrows of two different categories under two different operations of composition, $\cdot$ and $\circ$, which satisfy the interchange law. Moreover, any arrow (transformation) which is an identity for the composition $\circ$ is also an identity for the composition $\cdot$.*

3.10.2.4 Double Category

The set of arrows for two different compositions with two different compositions which together satisfy the interchange law.

3.10.2.5 2-Category

A double category in which every identiy arrow for the first composition is also an identity for the second composition.

3.11 Universal Properties

4 Category Examples

4.1 The category Set

- Objects: Sets
- Arrows: Functions

4.1.1 Morphisms

Proposition 4.1.1. *A function is injective if and only if it is a monomorphism.*

Proposition 4.1.2. *A function is surjective if and only if it is a monomorphism.*

Theorem 4.1.1 (Canonical Decomposition in Set)**.** *Let $f : A \to B$ be any function, and define $\sim$ as above. Then f decomposes as follows:*

$$\begin{tikzcd} A \arrow[r, two heads] \arrow[rrr, bend left, "f"] & (A/\sim) \arrow[r, "\sim", "\tilde{f}"'] & \mathrm{im} f \arrow[r, hook] & B \end{tikzcd}$$

where the first function is the canonical projection $A \to A/\sim$, the third function is the inclusion im$f \subseteq B$, and the bijection $\tilde{f}$ in the middle is defined by

$$\tilde{f}([a]_\sim) := f(a)$$

for all $a \in A$.

4.1.2 Universal Objects

Proposition 4.1.3. *$\emptyset$ is an initial object in Set.*

Proposition 4.1.4. *Singletons are final objects in Set.*

Proposition 4.1.5. *Cartesian products are products in Set.*

Proposition 4.1.6. *Disjoint unions are coproducts in Set.*

Proposition 4.1.7. *Given a set A and an equivalence relation $\sim$ on A, $(A/\sim)$ is a quotient in Set.*

4.2 The category Grp

- Objects: Groups
- Arrows: Homomorphisms

4.2.1 Morphisms

Proposition 4.2.1. *The following are equivalent:*

1. *φ is a monomorphism*
2. *$ker\varphi = \{e_G\}$*
3. *$\varphi : G \to G'$ is injective (as a set function)*

Proof. (1) $\Rightarrow$ (2): Consider the two parallel compositions...

$$\ker\varphi \underset{e}{\overset{\iota}{\rightrightarrows}} G \xrightarrow{\varphi} G'$$

where ι is the inclusion and e is the trivial map. Both $\varphi \circ \iota$ and $\varphi \circ e$ are the trivial map; since φ is a monomorphism, this implies $\iota = e$. But then $\ker\varphi$ is trivial.
(2) $\Rightarrow$ (3): Observe...

$$\begin{aligned} \varphi(g_1) = \varphi(g_2) &\Rightarrow \varphi(g_1)\varphi(g_2)^{-1} = e_G \Rightarrow \varphi(g_1 g_2^{-1}) = e_{G'} \\ &\Rightarrow g_1 g_2^{-1} \in \ker\varphi \overset{!}{\Rightarrow} g_1 g_2^{-1} = e_G \Rightarrow g_1 = g_2. \end{aligned}$$

(3) $\Rightarrow$ (1): If φ is injective, then it satisfies the defining property for monomorphisms in Set. $\square$

4.2.2 Isomorphism Theorems

Theorem 4.2.1 (Canonical Decomposition in Grp)**.** *Every group homomorphism $\varphi : G \to G'$ may be decomposed as follows:*

$$\begin{tikzcd} G \arrow[r, two heads] \arrow[rrr, bend left, "\varphi"] & (G/\ker\varphi) \arrow[r, "\sim", "\tilde{\varphi}"'] & \mathrm{im}\varphi \arrow[r, hook] & G' \end{tikzcd}$$

where the isomorphism $\tilde{\varphi}$ in the middle is the homomorphism induced by φ as in 5.5.2.

Corollary 4.2.1.1 (First Isomorphism Theorem in Grp)**.** *Suppose $\varphi : G \to G'$ is a surjective group homomorphism. Then*

$$G' \cong \frac{G}{ker\varphi}.$$

Theorem 4.2.2 (Second Isomorphism Theorem in Grp)**.** *Let H, K be subgroups of a group G, and assume that H is normal in G. Then...*

- *HK is a subgroup of G, and H is normal in HK*

- *$H \cap K$ is normal in K, and*

$$\frac{HK}{H} \cong \frac{K}{H \cap K}.$$

Proof. To verify that HK is a subgroup of G when H is noraml, note that HK is the union of all cosets Hk, wiht $k \in K$; that is,

$$HK = \pi^{-1}(\pi(K)),$$

where $\pi : G \to G/H$ is the canonical projection. Since $\pi(K)$ is a subgroup of G/H, HK is a subgroup by 5.4.2. It is clear that H is normal in HK.

For the second part, consider the homomorphism...

$$\varphi : K \to HK/H$$

sending $k \in K$ to the coset Hk. This homomorphism is *surjective*: indeed, every element of HK/H may be written as a coset

$$Hhk, \;\; h \in H, \, k \in K;$$

but $Hhk = Hk$, so $Hhk = \varphi(k)$ is the image of φ. By 4.2.1.1,

$$\frac{HK}{H} \cong \frac{K}{\ker\varphi}.$$

To complete the proof note...

$$\ker\varphi = \{k \in K | \varphi(k) = e\} = \{k \in K | Hk = H\} = \{k \in K | k \in H\} = H \cap K.$$

□

Theorem 4.2.3 (Third Isomorphism Theorem in Grp)**.** *Let H be a normal subgroup of a group G, and let N be a subgroup of G containing H. Then N/H is normal in G/H if and only if N is normal in G, and in this case*

$$\frac{G/H}{N/H} \cong \frac{G}{N}$$

Proof. If N is normal, then consider the projection $\pi_N : G \to \frac{G}{N}$. The subgroup H is contained in $N = \ker\varphi$, so by 5.5.2 we get an induced homomorphism $\varphi' : \frac{G}{H} \to \frac{G}{N}$. The subgroup N/H of G/H is a kernel of φ'; therefore it is normal.

Conversely, if N/H is normal in G/H, consider the composition...

$$G \twoheadrightarrow \frac{G}{H} \twoheadrightarrow \frac{G/H}{N/H}.$$

The kernel of this homomorphism is N, therefore N is normal. Further, this homomorphism is surjective; hence the stated isomorphism $(G/H)/(N/H) \cong G/N$ follows immediately from 4.2.1.1. □

4.2.3 Universal Objects

Proposition 4.2.2. *Trivial groups are null objects in Grp.*

Proposition 4.2.3. *Grp has products. (See Group Products)*

Proposition 4.2.4. *Grp has coproducts. (See Free Group Products)*

4.3 The category Ab

- Objects: Abelian Groups
- Arrows: Homomorphisms

4.3.1 Morphisms

Proposition 4.3.1. *The following are equivalent:*

1. φ *is an epimorphism*
2. *coker*$\varphi = \{e_{G'}\}$
3. $\varphi : G \to G'$ *is surjective (as a set function)*

Proof. (1) $\Rightarrow$ (2): Assume (1) holds, and consider the two parallel compositions...

$$G \xrightarrow{\varphi} G' \overset{\pi}{\underset{e}{\rightrightarrows}} \mathrm{coker}\varphi$$

where π is the canonical projection and e is the trivial map. Both $\pi \circ \varphi$ and $e \circ \varphi$ are the trivial map; since φ is an epimorphism, this implies $\pi = e$. But $\pi = e$ implies that cokerφ is trivial.
(2) $\Rightarrow$ (3): If coker$\varphi = G'/\mathrm{im}\varphi$ is trivial, then im$\varphi = G'$; hence φ is surjective.
(3) $\Rightarrow$ (1): If φ is surjective, then it satisfies the universal property for epimorphisms in Set: for any set Z and any two set-functions α' and $\alpha'' : G' \to Z$,

$$\alpha' \circ \varphi = \alpha'' \circ \varphi \Leftrightarrow \alpha' = \alpha''.$$

This must hold in particular if Z is endowed with a group structure and α', α'' are group homomorphisms, so φ is an epimorphism in Grp. □

4.3.2 Universal Objects

Proposition 4.3.2. *Trivial groups are null objects in Ab.*

Proposition 4.3.3. *Ab has products and coproducts. They are the same construct and are called* Direct Sums*, denoted* $G \oplus H$*. (See Group Products)*

4.4 The category Ring

- Objects: Rings
- Arrows: Ring homomorphisms

4.4.1 Morphisms

Proposition 4.4.1. *For a ring homomorphism $\varphi : R \to S$, the following are equivalent:*

1. *φ is a monomorphism;*
2. *$ker\varphi = \{0\}$;*
3. *φ is injective (as a set-function).*

Proof. Only (1) $\Rightarrow$ (2) warrants serious attention. Assume $\varphi : R \to S$ ois a monomorphism and $r \in \ker\varphi$. Applying the extension property given from the universal property of polynomial rings, we obtain unique ring homomorphisms $ev_r : \mathbb{Z}[x] \to R$ such that $ev_r(x) = r$ and $ev_0 : \mathbb{Z}[x] \to R$ such that $ev(x) = 0$. Consider the parallel ring homomorphisms:

$$\mathbb{Z}[x] \underset{ev_0}{\overset{ev_r}{\rightrightarrows}} R \xrightarrow{\varphi} S,$$

since $\varphi(r) = 0 = \varphi(0)$, the two compositions $\varphi \circ ev_r$, $\varphi \circ ev_0$ agree (because they agree on $\mathbb{Z}$ and they agree on x); hence $ev_r = ev_0$ since φ is a monomorphism. Therefore...

$$r = ev_r(x) = ev_0(x) = 0,$$

showing $r \in \ker\varphi$. ☐

In Ring, epimorphisms need not be surjective.

Proposition 4.4.2. *The function $\iota : \mathbb{Z} \hookrightarrow \mathbb{Q}$ is an epimorphism.*

Proof. Suppose α_1 and α_2 are parallel ring homomorphisms...

$$\mathbb{Z} \hookrightarrow \mathbb{Q} \underset{\alpha_2}{\overset{\alpha_1}{\rightrightarrows}} R$$

and α_1, α_2 agree on $\mathbb{Z}$. Then α_1, α_2 must agree on $\mathbb{Q}$: because for $p, q \in \mathbb{Z}, q \neq 0$,

$$\alpha_i \left(\frac{p}{q}\right) = \alpha_i(p)\alpha_i(q^{-1}) = \alpha(p)\alpha(q)^{-1}$$

is the same for both. ☐

4.4.2 Isomorphism Theorems

Theorem 4.4.1 (Canonical Decomposition in Ring)**.** *Every ring homomorphism $\varphi : R \to S$ may be decomposed as follows:*

$$\begin{tikzcd} R \arrow[r, two heads] \arrow[rrr, bend left, "\varphi"] & (R/\ker\varphi) \arrow[r, "\sim", "\tilde{\varphi}"'] & \mathrm{im}\varphi \arrow[r, hook] & S \end{tikzcd}$$

where the isomorphism $\tilde{\varphi}$ in the middle is the homomorphism induced by φ as in 8.3.1.

Corollary 4.4.1.1. *Suppose $\varphi : R \to S$ is a surjective ring homomorphism. Then*

$$S \cong \frac{R}{ker\varphi}.$$

Note: The 'second isomorphism' theorem doesn't quite make sense in the context of Ring.

Theorem 4.4.2. *Let I is an ideal of a ring R, and let J be an ideal of R containing I. Then J/I is an ideal of R/I, and...*

$$\frac{R/I}{J/I} \cong \frac{R}{J}$$

4.4.3 Universal Objects

Proposition 4.4.3. *Zero rings are final objects in Ring.*

Proposition 4.4.4. *The ring of integers $\mathbb{Z}$ is an initial object in Ring.*

Proof. Observe $\varphi : \mathbb{Z} \to R$ defined by $(\forall n \in \mathbb{Z}) : \quad \varphi(n) = n \cdot 1_R$ is a ring homomorphism by...

$$\varphi(mn) = \sum_{i=1}^{mn} 1_R = \sum_{i=1}^{m}(\sum_{j=1}^{n} 1_R) \stackrel{!}{=} (\sum_{i=1}^{m} 1_R) \cdot (\sum_{j=1}^{n} 1_R) = \varphi(m) \cdot \varphi(n),$$

(where ! occurs via the distributivity axiom) and is unique, since it is determined by the requirement that $\varphi(1) = 1_R$ and by the fact that φ preserves addition. $\square$

5 Group Theory

5.1 Definition

A *group* is a groupoid with a single object.

A *group* $\langle G, \cdot \rangle$ is a set G endowed with the binary operation $\cdot$ such that...

1. the operation $\cdot$ is *associative*
2. there exists an *identity element* e_G for $\cdot$
3. every element in G has an *inverse* with respect to $\cdot$

We can repeated elements as follows...

- $g^n = g \cdot g \cdots g \cdot g$ (n times)
- $g^{-n} = g^{-1} \cdot g^{-1} \cdots g^{-1} \cdot g^{-1}$ (n times)

Proposition 5.1.1. *The identity $e_G \in G$ of a group is unique.*

Proof. If h is another identity, then $h = e_G h = e_G$. □

Proposition 5.1.2. *Inverses in a group G are unique.*

Proposition 5.1.3 (Cancellation)**.** *Let G be a group. Then $\forall a, g, h \in G$...*

$$ga = ha \Rightarrow g = h, \quad ag = ah \Rightarrow g = h.$$

5.2 Order

5.2.1 Order of an element

The *order of an element* $g \in G$, denoted $|g|$, is the smallers positive integer n such that $g^n = e$.
g has *finite order* if any such integer exists.

g has *infinite order* if no such integer exists, denoted $|g| = \infty$.

Lemma 5.2.1. *If $g^n = e$ for some positive integer n, then $|g|$ is a divisor of n.*

Proof. As observed, $n \geq |g|$ for $n \in \mathbb{Z}$, that is $n - |g| \geq 0$. Since $\mathbb{Z}$ is a Euclidean domain, there must exist an integer $m > 0$ such that...

$$r = n - |g| \cdot m \geq 0 \text{ and } n - |g| \cdot (m+1) < 0,$$

that is, $r < |g|$. Note that...

$$g^r = g^{n - |g| \cdot m} = g^n \cdot (g^{|g|})^{-m} = e \cdot e^{-m} = e.$$

By definition of order, $|g|$ is the smallest positive integer such that $g^{|g|} = e$. Since r is smaller than $|g|$ and $g^r = e$, r cannot be positive; hence $r = 0$ necessarily. So $n = |g| \cdot m$. □

Corollary 5.2.1.1. *Let g be an element of finite order, and let $N \in \mathbb{Z}$. Then*

$$g^N = e \Leftrightarrow N \text{ is a multiple of } |g|$$

5.2.2 Order of a group

If G is finite as a set, its *order* $|G|$ is the number of its elements; we write $|G| = \infty$ if G is infinite.

Proposition 5.2.1. *Let $g \in G$ be an element of finite order. Then g^m has finite order $\forall m \geq 0$, and in fact*

$$|g^m| = \frac{lcm(m, |g|)}{m} = \frac{|g|}{gcd(m, |g|)}.$$

Proof. The order of g^m is the least positive d for which...

$$g^{md} = e.$$

In other words, $m|g^m|$ is the smallest multiple of m which is also a multiple of $|g|$:

$$m|g^m| = \text{lcm}(m, |g|).$$

□

Proposition 5.2.2. *If $gh = hg$, then $|gh|$ divides $lcm(|g|, |h|)$.*

Proof. Observe...

$$(gh)^{\text{lcm}(m,n)} = (gh)(gh)\cdots(gh) = gg\cdots g \cdot hh\cdots h = g^{\text{lcm}(m,n)}h^{\text{lcm}(m,n)} = e.$$

□

5.2.3 Index of a subgroup

The *index* of H in G, denoted $[G : H]$, is the number of elements $|G/H|$ of G/H, when this is finite, and ∞ otherwise.

Lemma 5.2.2. *Let H be a subgroup of a group G. Then $\forall g \in G$ the functions*

$$H \to gH,\ h \mapsto gh,$$

$$H \to Hg,\ h \mapsto hg$$

are bijections.

Proof. Surjectiveness is clear and cancellation implies that they are injective. □

5.2.3.1 Lagrange's Theorem

Corollary 5.2.2.1. *If G is a finite group and $H \subseteq G$ is a subgroup, then $|G| = [G : H] \cdot |H|$. In particular, $|H|$ is a divisor of $|G|$.*

Proof. Indeed, G is the disjoint union of $|G/H|$ distinct cosets gH, and $|gH| = |H|$ by 5.2.2. □

Corollary 5.2.2.2. *If $g \in G$, then $a \cdot |g| = |G|$ for some positive integer a.*

5.3 Homomorphism

For groups $\langle G, \cdot_G \rangle$, $\langle H, \cdot_H \rangle$, a *group homomorphism...*

$$\varphi : \langle G, \cdot_G \rangle \to \langle H, \cdot_H \rangle$$

is a set-function preserving the binary operations of the groups, i.e. the following diagram commutes...

$$\begin{array}{ccc} G \times G & \xrightarrow{\varphi \times \varphi} & H \times H \\ \Big\downarrow{\scriptstyle \cdot_G} & & \Big\downarrow{\scriptstyle \cdot_H} \\ G & \xrightarrow{\quad\varphi\quad} & H \end{array}$$

i.e. $\forall a, b \in G$ we have $\varphi(a \cdot_G b) = \varphi(a) \cdot_H \varphi(b)$.

Proposition 5.3.1. *Let $\varphi : G \to H$ be a group homomorphism. Then...*

- $\varphi(e_G) = e_H$
- $\forall g \in G, \varphi(g^{-1}) = \varphi(g)^{-1}$.

Proof. For the first item observe...

$$e_H \ldots \varphi(e_G) = \varphi(e_G) = \varphi(e_G \cdot e_G) = \varphi(e_G) \cdot \varphi(e_G) \Rightarrow e_H = \varphi(e_G).$$

For the second item observe...

$$\varphi(g^{-1}) \cdot \varphi(g) = \varphi(g^{-1} \cdot g) = \varphi(e_G) = e_H = \varphi(g)^{-1} \cdot \varphi(g) \Rightarrow \varphi(g^{-1}) = \varphi(g)^{-1}$$

□

5.3.1 Some Important Morphisms

5.3.1.1 Trivial Morphism

Because $\{*\}$ is a null object in Grp (and Ab) we are guaranteed unique morphisms...

$$\varphi : G \to \{*\},\ \psi : \{*\} \to H.$$

We call the resulting composition $\psi \circ \varphi : G \to H$ the *trivial morphism.*

5.3.1.2 Exponential Map

Given a group G, the *exponential map* is the homomorphism $\epsilon : \mathbb{Z} \to G$ defined by $z \mapsto g^z$.

5.3.2 Interaction with order

Proposition 5.3.2. *Let $\varphi : G \to H$ be a group homomorphism, and let $g \in G$ be am element of finite order. Then $|\varphi(g)|$ divides $|g|$.*

Proof. Observe, $\varphi(g)^{|g|} = e_H$ and apply 5.2.1. □

5.3.3 Isomophisms

Proposition 5.3.3. *Let $\varphi : G \to H$ be a group homomorphism. Then φ is an isomorphism of groups if and only if it is a bijection.*

Two groups G, H are *isomorphic* if there is an isomorphism between them.

Proposition 5.3.4. *Let $\varphi : G \to H$ be an isomorphism.*

- $(\forall g \in G) : |\varphi(g)| = |g|$;
- *G is commutative if and only if H is commutative.*

5.4 Subgroup

Let $\langle G, \cdot \rangle$ be a group, and $\langle H, \cdot \rangle$ another group, whose underlying set H is a subset of G.

$\langle H, \cdot \rangle$ is a *subgroup* of G if the inclusion function $\iota : H \hookrightarrow G$ is a group homomorphism.

Proposition 5.4.1. *A nonempty subset H of a group G is a subgroup if and only if $(\forall a, b \in H) : ab^{-1} \in H$.*

Lemma 5.4.1. *If $\{H_\alpha\}_{\alpha \in A}$ is any family of subgroups of a group G, then...*

$$H = \bigcap_{\alpha \in A} H_\alpha$$

is a subgroup of G.

Lemma 5.4.2. *Let $\varphi : G \to G'$ be a group homomorphism, and let H' be a subgroup of G'. Then $\varphi^{-1}(H')$ is a subgroup of G.*

5.4.1 Normal Subgroup

A subgroup N of a group G is *normal* if $\forall g \in G$, $\forall n \in N$,

$$gng^{-1} \in N.$$

5.4.2 Kernel of a Homomorphism

The *kernel* of $\varphi : G \to G'$, $\ker\varphi$, is the subgroup of G consiting of...

$$\ker\varphi := \{g \in G | \varphi(g) = e_{G'}\} = \varphi^{-1}(e_{G'}).$$

Proposition 5.4.2. *Let $\varphi : G \to G'$ be a homomorphism. Then the inclusion $\iota : \ker\varphi \hookrightarrow G$ is final in the category of group homomorphisms $\alpha : K \to G$ such that $\varphi \circ \alpha$ is the trivial morphism. In other words the following diagram commutes.*

$$\begin{tikzcd}
K \arrow[r, "\alpha"] \arrow[rr, bend left, "0"] \arrow[dr, "\exists!\bar{\alpha}"'] & G \arrow[r, "\varphi"] & G' \\
& \ker\varphi \arrow[u, hook, "\iota"'] &
\end{tikzcd}$$

Lemma 5.4.3. *If $\varphi : G \to G'$ is any group homomorphism, then $\ker\varphi$ is a normal subgroup of G.*

Proof. Since $\ker\varphi$ is a subgroup by the previous proposition, we need only verify it is normal. Observe $\forall g \in G, \forall n \in \ker\varphi$...

$$\varphi(gng^{-1}) = \varphi(g)\varphi(n)\varphi(g^{-1}) = \varphi(g)e_{G'}\varphi(g)^{-1} = e_{G'},$$

proving that $gng^{-1} \in \ker\varphi$. □

5.4.3 Image of a Homomorphism

The *image* of $\varphi : G \to G'$, $\mathrm{im}\varphi$, is the subgroup of G' consiting of...

$$\mathrm{im}\varphi := \{\varphi(g) | g \in G\}.$$

5.4.4 Subgroup generated by a subset

If $A \subseteq G$, we are guaranteed a unique group homomorphism

$$\varphi_A : F(A) \to G$$

extending the inclusion map, by the universal property of free groups. Then $\mathrm{im}\varphi_A$ is the *subgroup generated by* A in G, denoted $\langle A \rangle$.

This subgroup may also be constructed as...

$$\langle A \rangle = \bigcap_{H \text{ subgroup of } G, H \supseteq A} H.$$

5.4.4.1 Finitely Generated

A group G is *finitely generated* if there exists a *finite* subset $A \subseteq G$ such that $G = \langle A \rangle$.

5.5 Group Constructions

5.5.1 Product of Groups

Let G and H be two groups. Define $G \times H := \{(g,h)|g \in G, h \in H\}$ with the operation $(g_1,h_1)\cdot_{G\times H}(g_2,h_2) = (g_1 \cdot_G g_2, h_1 \cdot_H h_2)$. Then $G \times H$ is the product group of the groups G and H.

5.5.2 Free Product of Groups

5.5.3 Free Groups

$F(A)$ is a free group on a set A if there is a set-function $j : A \to F(A)$ such that, for all groups G and set-functions $f : A \to G$, there exists a unique group homomorphism $\varphi : F(A) \to G$ such that the following diagram commutes.

$$\begin{tikzcd}
F(A) \arrow[r, "\varphi"] & G \\
A \arrow[u, "j"] \arrow[ur, "f"'] &
\end{tikzcd}$$

5.5.3.1 Concrete construction

Consider the set A as an 'alphabet' and construct 'words' whose letters are elements of A or 'inverses' of elements of A. That is, a *word* on A is an ordered list

$$(a_1, a_2, \ldots, a_n)$$

, which we denote by the juxtaposition

$$w = a_1 a_2 \ldots a_n,$$

where each letter is either an element of A or an inverse of an element in A. Denote the set of words on A as $W(A)$.

Define an 'elementary' reduction $r : W(A) \to W(A)$: given $w \in W(A)$, search for the first occurrence (from left to right) of a pair aa^{-1} or $a^{-1}a$, and let $r(w)$ be the word obtained by removing such a pair.

Note that $r(w) = w$ precisely when 'no cancellation is possible'; We say that w is a 'reduced word' in this case.

Lemma 5.5.1. *If $w \in W(A)$ has length n, then $r^{\lfloor \frac{n}{2} \rfloor}(w)$ is a reduced word.*

Proof. Indeed, either $r(w) = w$ or the length of $r(w)$ is less than the length of w; but one cannot decrease the length of w more than $n/2$ times, since each non-identity application of r decreases the length by two. $\square$

Now define the 'reduction' $R : W(A) \to W(A)$ by setting $R(w) = r^{\lfloor \frac{n}{2} \rfloor}(w)$, where n is the length of w. By the lemma, $R(w)$ is always a reduced word.

Let $F(A)$ be the set of reduced words on A, that is, the image of the reduction map R we have just defined.

Define a binary operation on $F(A)$ by juxtaposition and reduction: $w \cdot w' = R(ww')$. $F(A)$ is a group under this operation.

Proposition 5.5.1. *The pair $(j, F(A))$ satisfies the universal property for free groups on A.*

5.5.4 Quotient Group

5.5.4.1 Quotient Group by $\sim$

Proposition 5.5.2. *The operation...*

$$[a] \cdot [b] := [ab]$$

defines a group structure on $G/\sim$ if and only if $\forall a, a', g \in G$

$$a \sim a' \Rightarrow ga \sim ga' \text{ and } ag \sim a'g.$$

In this case the quotient function $\pi : G \to G/\sim$ is a homomorphism and is universal with respect to homomorphisms $\varphi : G \to G'$ such that $a \sim a' \Rightarrow \varphi(a) = \varphi(a')$.

5.5.4.2 Cosets

Proposition 5.5.3. *Let $\sim$ be an equivalence relation on a group G, satisfying $(\forall g \in G) : \ a \sim b \Rightarrow ga \sim gb$. Then...*

- *the equivalence class of e_G is a subgroup of H of G; and*
- *$a \sim b \Leftrightarrow a^{-1}b \in H \Leftrightarrow aH = bH$.*

Proof. Let $H \subseteq G$ be the equivalence class of the identity; $H \neq \emptyset$ as $e_G \in H$. For $a, b \in H$, we have $e_G \sim b$ and hence $b^{-1} \sim e_G$; hence $ab^{-1} \sim a$; and hence...

$$ab^{-1} \sim a \sim e_G$$

by the transitivity of $\sim$ and since $a \in H$. This shows $ab^{-1} \in H$ for all $a, b \in H$, proving that H is a subgroup.

Next, assume $a, b \in G$ and $a \sim b$. Multiplying on the left by a^{-1}, implies $e_G \sim a^{-1}b$, that is, $a^{-1}b \in H$. Since H is closed under the operation, this implies $a^{-1}bH \subseteq H$, hence $bH \subseteq aH$; as $\sim$ is symmetric, the same reasoning gives $aH \subseteq bH$; and hence $aH = bH$. Thus, we have proved...

$$a \sim b \Rightarrow a^{-1}b \in H \Rightarrow aH = bH.$$

Finally, assume $aH = bH$. Then $a = ae_G \in bH$, and hence $a^{-1}b \in H$. By definition of H, this means $e_G \sim a^{-1}b$. Multiplying on the left by a shows that $a \sim b$. $\square$

The *left-cosets* of a subgroup H in a group G are the sets aH, for $a \in G$. The *right-cosets* of H are the sets Ha, $a \in G$.

Proposition 5.5.4. *If H is any subgroup of a group G, the relation $\sim_L$ defined by*

$$(\forall a, b \in G): \ a \sim_L b \Leftrightarrow a^{-1}b \in H$$

is an equivalence relation satisfying $(\forall g \in G): \ a \sim b \Rightarrow ga \sim gb$.

Taking the previous two propositions together we get...

Proposition 5.5.5. *There is a bijection between the set of subgroups of G and equivalence relations on G satisfying $(\forall g \in G): \ a \sim b \Rightarrow ga \sim gb$; for the relation $\sim_L$ corresponding to a subgroup H, $G/\sim_L$ may be described as the set of left-cosets aH of H.*

Similar statements exist for right cosets and the property $(\forall g \in G): \ a \sim b \Rightarrow ag \sim bg$ leading to...

Proposition 5.5.6. *There is a bijection between the set of subgroups of G and equivalence relations on G satisfying $(\forall g \in G): \ a \sim b \Rightarrow ag \sim bg$; for the relation $\sim_R$ corresponding to a subgroup H, $G/\sim_R$ may be described as the set of left-cosets Ha of H.*

Proposition 5.5.7. *The relations $\sim_L$, $\sim_R$ corresponding to subgroups of H coincide if and only if H is normal.*

5.5.4.3 Definition

Let H be a normal subgroup of G. The *quotient group of G modulo H*, denoted G/H, is the group $G/\sim$ obtained from the relation $\sim$ as defined in the previous propositions. In terms of cosets, the product in G/H is defined by

$$(aH)(bH) := (ab)H.$$

The identity element is H.

5.5.4.4 Universal Property

Theorem 5.5.2. *Let H be a normal subgroup of a group G. Then for every group homomorphism $\varphi : G \to G'$ such that $H \subseteq ker\varphi$ there exists a unique group homomorphism $\tilde{\varphi} : G/H \to G'$ so that the diagram*

$$\begin{tikzcd} G \arrow[rr, "\varphi"] \arrow[dr, "\pi"'] & & G' \\ & G/H \arrow[ur, "\exists!\tilde{\varphi}"'] & \end{tikzcd}$$

commutes.

5.6 Presentations

A *presentation* of a group G is an explicit isomorphism...

$$G \cong \frac{F(A)}{R}$$

where A is a set and R is a subgroup of 'relations.' In other wordsd, a presentation is an explicit surjection...

$$\varphi : F(A) \twoheadrightarrow G$$

of which R is the kernel.

To create a presentation it is enough to list 'enough' relations, i.e create a set $\mathcal{R}$ of words, and then let R be the smallest normal subgroup of $F(A)$ containing $\mathcal{R}$. We can then denote a presentation by $\langle A|\mathcal{R}\rangle$.

5.6.1 Finitely Presented

A group is *finitely presented* if it admits a presentation $\langle A|\mathcal{R}\rangle$ in which both A and $\mathcal{R}$ are finite.

5.7 Group Actions

An action of a group G on a set A is a set-function...

$$\rho : G \times A \to A$$

such that $\rho(e_G, a) = a$ for all $a \in A$ and...

$$(\forall g, h \in G), (\forall a \in A) : \rho(gh, a) = \rho(g, \rho(h, a)).$$

5.7.1 Natural Action

Every group G acts in a natural way on the underlying set G. The action $\rho : G \times G \to G$ is simply the operation in the group...

$$(\forall g, a \in G) : \rho(g, a) = ga$$

Theorem 5.7.1 (Cayley's theorem)**.** *Every group acts faithfully on some set. That is, every group may be realized as a subgroup of a permutation group.*

Proof. The natural action acts faithfully on $Aut_{Set}(G)$. $\square$

5.7.2 Transitive Actions

An action of a group G on a (nonempty) set A is *transitive* if $\forall a, b \in A, \exists g \in G$ such that $b = ga$.

5.7.2.1 Orbit

The *orbit* of $a \in A$ under an action of a group G is the set...

$$O_G(a) := \{ga | g \in G\}.$$

5.7.2.2 Stabilizer Subgroup

Let G act on a set A, and let $a \in A$. The *stabilizer subgroup* of a consists of the elements of G which fix a:

$$\mathrm{Stab}_G(a) := \{g \in G | ga = a\}.$$

5.7.3 Category G-Set

The functor category of group actions. Thus morphisms are commutative diagrams such as...

$$\begin{tikzcd} G \times A \arrow[r, "\mathrm{id}_G \times \varphi"] \arrow[d, "\rho"] & G \times A' \arrow[d, "\rho'"] \\ A \arrow[r, "\varphi"] & A' \end{tikzcd}$$

Intuitively, we think of these objects as sets endowed with a group action, i.e. *G-sets*. Arrows are morphisms (functions) such as φ above which preserve the group action. They are called *G-equivariant*.

Proposition 5.7.1. *Every transitive left-action of G on a nonempty set A is isomorphic to the left-multiplication of G on G/H, for H = the stabilizer of any $a \in A$.*

Proof. Let G act transitively on a set A, let $a \in A$ be any element, and let $H = \mathrm{Stab}_G(a)$. I claim that there is an equivariant bijection...

$$\varphi : G/H \to A$$

defined by...

$$gH \mapsto ga$$

for all $g \in G$.

First of all φ is well-defined: if $g_1H = g_2H$, then $g_1^{-1}g_2 \in H$, hence $(g_1^{-1}g_2)a = a$, and it follows that $g_1a = g_2a$ as needed. To verify that φ is bijective, define a function $\psi : A \to G/H$ by sending an element ga of A to gH; ψ is well-defined becasue if $g_1a = g_2a$, then $g^{-1}(g_2a) = a$, so $g_1^{-1}g_2 \in H$ and $g_1H = g_2H$. It is clear that φ and ψ are inverses of each other; hence φ is a bijection.

Equivariance is immediate: $\varphi(g'(gH)) = g'ga = g'\varphi(gH)$. $\square$

Corollary 5.7.1.1. *If O is an orbit of the action of a finite group G on a set A, then O is a finite set and…*

$$|O| \text{ divides } |G|.$$

Proof. Use Lagrange's theorem (5.2.2.1) and the previous theorem. □

Proposition 5.7.2. *Suppose a group G acts on a set A, and let $a \in A$, $g \in G$, $b = ga$. Then…*

$$Stab_G(b) = gStab_G(a)g^{-1}.$$

Proof. Observe if $h \in \mathrm{Stab}_G(a)$, then…

$$(ghg^{-1})(b) = gh(g^{-1}g)a = gha = ga = b,$$

proving $\supseteq$. For $\subseteq$ note $a = g^{-1}b$ apply the same argument. □

5.7.4 Conjugation Action

Every group G acts by conjugation on the underlying set G. The action $\rho : G \times G \to G$ is the operation in the group…

$$(\forall g, a \in G) : \rho(g, h) = ghg^{-1}$$

6 Abelian Group Theory

6.1 Definition

An *abelian group* is a group such that $\cdot$ (which we denote $+$ for general abelian groups) is commutative.

In this context we write:

- $ng = g + g \cdots g + g$ (n times)
- $-ng = -g - g \cdots - g - g$ (n times)

6.2 Homomorphisms of Abelian Groups

Proposition 6.2.1. *For any two abelian groups G, H, $Hom_{Ab}(G, H)$ is an abelian group under addition inherited from H.*

Proof. Define the operation $\varphi + \psi$ for $\varphi, \psi \in \mathrm{Hom}_{Ab}(G, H)$, where...

$$(\varphi + \psi)(g) = \varphi(g) +_H \psi(g).$$

Observe that $\varphi + \psi$ is a homomorphism...

$$\begin{aligned}(\varphi + \psi)(a +_G b) = \varphi(a +_G b) + \psi(a +_G b) &= (\varphi(a) +_H \varphi(b)) +_H (\psi(a) +_H \psi(b)) \\ &\stackrel{!}{=} (\varphi(a) +_H \psi(a)) +_H (\varphi(b) +_H \psi(b)) = (\varphi + \psi)(a) +_H (\varphi + \psi)(b)\end{aligned}$$

From here it is easy to show that $\mathrm{Hom}_{Ab}(G, H)$ is an abelian group. $\square$

Note: By the same logic, if A is a set and H an abelian group, then H^A is an abelian group.

In fact, by adding the additional operation $\circ$ (treated as multiplication), we transform $\mathrm{End}_{Ab}(G) := \mathrm{Hom}_{Ab}(G, G)$ into a ring.

Proposition 6.2.2. *$End_{Ab}(\mathbb{Z}) \cong \mathbb{Z}$ as rings.*

Proof. Consider the function...

$$\varphi : \mathrm{End}_{Ab}(\mathbb{Z}) \to \mathbb{Z}$$

defined by...

$$\varphi(\alpha) = \alpha(1)$$

for all group homomorphisms $\alpha : \mathbb{Z} \to \mathbb{Z}$. Then φ is a group homomorphism: the addition in $\mathrm{End}_{Ab}(\mathbb{Z})$ is defined so that $\forall n \in \mathbb{Z}$...

$$(\alpha + \beta)(n) = \alpha(n) + \beta(n);$$

in particular...

$$\varphi(\alpha + \beta) = (\alpha + \beta)(1) = \alpha(1) + \beta(1) = \varphi(\alpha) + \varphi(\beta).$$

Further, φ is a ring homomophism. Indeed, for $\alpha, \beta \in \mathrm{End}_{Ab}(\mathbb{Z})$ denote $\alpha(1)$ by a; then...

$$\alpha(n) = n\alpha(1) = na = an$$

for all $n \in \mathbb{Z}$; in particular,

$$\alpha(\beta(1)) = a\beta(1) = \alpha(1)\beta(1).$$

Therefore,

$$\varphi(\alpha \circ \beta) = (\alpha \circ \beta)(1) = \alpha(\beta(1)) = \alpha(1)\beta(1) = \varphi(\alpha)\varphi(\beta)$$

as needed. Also, $\varphi(\mathrm{id}_{\mathbb{Z}}) = id_{\mathbb{Z}}(1) = 1$.

Finally, φ has an inverse: for $a \in \mathbb{Z}$, the $\psi(a)$ be the homomorphism $\alpha : \mathbb{Z} \to \mathbb{Z}$ defined by...

$$(\forall n \in \mathbb{Z}) : \ \alpha_a(n) = an.$$

This inverse is a ring homomorphism...

- $\psi(a + b) = \alpha_{a+b} = \alpha_a + \alpha_b = \psi(a) + \psi(b)$;
- $\psi(a \cdot b) = \alpha_{a \cdot b} = \alpha_a \circ \alpha_b = \psi(a) \circ \psi(b)$;
- $\psi(1) = \alpha_1 = \mathrm{id}_{\mathbb{Z}}$.

□

Proposition 6.2.3. *Let R be a ring. Then the function $r \mapsto \lambda_r$ is an injective ring homomorphism...*

$$\lambda : R \to End_{Ab}(R).$$

Proof. For any $r \in R$ and for all $a, b \in R$, distributivity gives...

$$\lambda_r(a + b) = r(a + b) = ra + rb = \lambda_r(a) + \lambda_r(b) :$$

this shows that λ_r is indeed an endomorphism of the *group* $\langle R, + \rangle$, that is, $\lambda_r \in \mathrm{End}_{Ab}(R)$.

The function $\lambda : R \to \mathrm{End}_{Ab}(R)$ defined by the assignment $r \mapsto \lambda_r$ is clearly injective, since $r \neq s$, then...

$$\lambda_r(1) = r \neq s = \lambda_s(1),$$

so that $\lambda_r \neq \lambda_s$.

Now we show that λ is a homomorphism. Additive preservation follows from 6.2.1 and distributivity. Associativity can be used to show that multiplication is preserved. The identity is clearly preserved. □

6.3 Abelian Subgroups

Every subgroup of an abelian group is normal.

6.3.1 Cokernel of a Homomorphism

The *cokernel* of $\varphi : G \to G'$, cokerφ, is $\frac{G'}{\text{im}\varphi}$.

Proposition 6.3.1. *Let $\varphi : G \to G'$ be a homomorphism. Then the projection $\pi : G' \twoheadrightarrow$ cokerφ is final in the category of group homomorphisms $\alpha : G' \to L$ such that $\alpha \circ \varphi$ is the trivial morphism. In other words the following diagram commutes.*

$$\begin{tikzcd}
G \arrow[r, "\varphi"'] \arrow[rr, bend left, "0"] & G' \arrow[r, "\alpha"'] \arrow[d, two heads, "\pi"'] & L \\
& \text{coker}\varphi \arrow[ur, "\exists!\overline{\alpha}"'] &
\end{tikzcd}$$

6.4 Abelian Group Constructions

6.4.1 Free Abelian Groups

Proposition 6.4.1. *For every set A, $F^{ab}(A) \cong \mathbb{Z}^{\oplus A}$.*

Proof. Note that every element of $\mathbb{Z}^{\oplus A}$ may be written uniquely as a finite sum...

$$\sum_{a\in A} m_a j(a), \;\; m_a \neq 0 \text{ for only finitely many } a.$$

Now let $f : A \to G$ be any function from A to the abelian group G. Define $\varphi : \mathbb{Z}^{\oplus A} \to G$ by...

$$\varphi(\sum_{a\in A} m_a j(a)) := \sum_{a\in A} m_a f(a).$$

This definition is force by the homomorphism condition and the univeral property of free groups and is thus unique.

It is also a homomorphism...

$$\varphi(\sum_{a\in A} m'_a j(a)) + \varphi(\sum_{a\in A} m''_a j(a)) = \sum_{a\in A} m'_a j(a) + \sum_{a\in A} m''_a j(a) \stackrel{!}{=} \sum_{a\in A} (m'_a + m''_a) f(a)$$

because G is commutative,

$$= \varphi(\sum_{a\in A} (m'_a + m''_a) j(a)) = \varphi(\sum_{a\in A} m'_a f(a) + \sum_{a\in A} m''_a f(a))$$

as needed. ☐

Note: $H^{\oplus A}$ is a subgroup of H^A.

7 Group Examples

7.1 Trivial Group

$G = \{e\}$.

7.2 Cyclic Groups

7.2.1 Modular Arithmetic

Let $n \in \mathbb{Z}^+$. Consider the equivalence relation on $\mathbb{Z}$ defined by...

$$a \equiv b \text{ mod } n \Leftrightarrow n|(b-a) \Leftrightarrow b - a \in n\mathbb{Z}.$$

It is called *congruence modulo n*.

7.2.2 Definition

Let $\mathbb{Z}/n\mathbb{Z} = \{[z]_{\text{mod } n} | z \in \mathbb{Z}\}$.

Lemma 7.2.1. *Addition* $([a]_n + [b]_n := [a+b]_n)$ *is well defined on* $\mathbb{Z}/n\mathbb{Z}$.

Thus $C_n := \langle \mathbb{Z}/n\mathbb{Z}, + \rangle$ is a *finite cyclic group*. We take $\langle \mathbb{Z}, + \rangle$ to be the *infinite cyclic group*.

Proposition 7.2.1. *The order of* $[m]_n$ *in* $\mathbb{Z}/n\mathbb{Z}$ *is* 1 *if* $n|m$, *and more generally...*

$$|[m]_n| = \frac{n}{gcd(m,n)}.$$

Proof. If $n|m$, then $[m]_n = [0]_n$. If $n\not| m$, $[m]_n = m[1]_n$ and apply 5.2.1. □

Corollary 7.2.1.1. *The class* $[m]_n$ *generates* $\mathbb{Z}/n\mathbb{Z}$ *if and only if* $gcd(m,n) = 1$.

The *cyclic groups* are an isomorphism class. Explicitly...

A group G is *cyclic* if it is isomorphic to $\mathbb{Z}$ or C_n
for some positive interger n.

Proposition 7.2.2. *If* $|G| = p$ *is a prime integer, then necessarily* $G \cong \mathbb{Z}/p\mathbb{Z}$.

Proof. Use Lagrange's theorem (5.2.2.2). □

7.2.3 Presentation

We say that a group is *cyclic* when it is generated by exactly one of its elements.
Finite: $\langle x | x^n \rangle$

Infinite: $\langle x \rangle$

7.2.4 Subgroups

Proposition 7.2.3. *Let $G \subseteq \mathbb{Z}$ be a subgroup. Then $G = d\mathbb{Z}$ for some $d \geq 0$.*

Proof. If $G = \{0\}$, then $G = 0\mathbb{Z}$. If not, note that if $a \in G$ and $a < 0$, then $-a \in G$ and $-a > 0$. We can then let d be the *smallest positive integer* in G and $G = d\mathbb{Z}$.

The inclusion $d\mathbb{Z} \subseteq G$ is clear. To verify $G \subseteq d\mathbb{Z}$, let $m \in G$, and apply 'division with remainder' to write...

$$m = dq + r,$$

with $0 \leq r < d$. Since $m \in G$ and $d\mathbb{Z} \subseteq G$ and since G is a subgroup, we see that...

$$r = m - dq \in G.$$

But d is the smallest *positive* integer in G, and $r \in G$ is smaller that d; so r cannot be positive. This shows $r = 0$, that is, $m = qd \in d\mathbb{Z}$; $G \subseteq d\mathbb{Z}$ follows. □

Proposition 7.2.4. *Let $n > 0$ be an integer and let $G \subseteq \mathbb{Z}/n\mathbb{Z}$. Then G is the cyclic subgroup of $\mathbb{Z}/n\mathbb{Z}$ generate by $[d]_n$, for some divisor d of n.*

Proof. Let $\pi_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ be the quotient map, and consider $G' := \pi_n^{-1}(G)$. By 5.4.2, G' is a subgroup of $\mathbb{Z}/n\mathbb{Z}$; by 7.2.3, G' is a *cyclic* subgroup of $\mathbb{Z}$, generated by a nonnegative integer d. It follows that...

$$G = \pi_n(G') = \pi_n(\langle d \rangle) = \langle [d]_n \rangle$$

; thus G is indeed a cyclic subgroup of $\mathbb{Z}/n\mathbb{Z}$, generated by a class $[d]_n$. Further, since $n \in G'$ (because $\pi_n(n) = [n]_n = [0]_n \in G$) and $G' = d\mathbb{Z}$, we see that d divides n, as claimed. □

7.3 Multiplicative group of integers modulo n

7.3.1 Definition

Let $(\mathbb{Z}/n\mathbb{Z})^* := \{[m]_n \in \mathbb{Z}/n\mathbb{Z} | \gcd(m, n) = 1\}$.

Lemma 7.3.1. *Multiplication ($[a]_n \cdot [b]_n := [a \cdot b]_n$) is well defined on $\mathbb{Z}/n\mathbb{Z}$.*

Proposition 7.3.1. *Multiplication makes $(\mathbb{Z}/n\mathbb{Z})^*$ into a group.*

7.3.2 Applications

Theorem 7.3.2 (Fermat's Little Theorem)**.** *Let p be a prime integer, and let a be any integer. Then $a^p \equiv a \bmod p$.*

Proof. This is immediate if $p | a$. If $p \nmid a$, then $a \in (\mathbb{Z}/n\mathbb{Z})^*$, which has order $p-1$. Thus...

$$[a]_p^{p-1} = [1]_p$$

via Lagrange's theorem (5.2.2.2). □

7.4 Symmetric Group

7.4.1 Definition

Let A be a set. The *symmetric group*, or *group of permutations* of A, denoted S_A, is the group $Aut_{Set}(A)$. The group of permutations of the set $[n]$ is denoted by S_n.

7.4.2 Presentation

7.5 Dihedral Group

7.5.1 Definition

Intuitively, this group captures the rigid motions (flips and rotations) of regular polygons in the 2D plane. It is denoted D_{2n}, where n is the number of sides/angles of the polygon, and contains $2n$ elements, n rotations and n flips.

7.5.2 Presentation

$\langle x, y | x^2, y^n, xyxy \rangle$

7.6 General Linear Group

7.6.1 Definition

$\mathrm{GL}_n(R)$, the group of invertible $n \times n$ matrices wtih entries in the ring R. It is noncommutative.

7.6.2 Presentation

8 Ring Theory

8.1 Definitions

A *ring* $\langle R, +, \cdot \rangle$ is an abelian group $\langle R, + \rangle$ endowed with a *second* binary operation $\cdot$, satisfying on its onw the requirements of being associative and having a two-sided identity, i.e.

- $(\forall r, s, t \in R): \quad (r \cdot t) \cdot t = r \cdot (s \cdot t)$
- $(\exists 1_R \in R)(\forall r \in R): \quad r \cdot 1_R = r = 1_R \cdot r$

which make $\langle R, \cdot \rangle$ a *monoid*, and further interacting with $+$ via the following *distributive properties*:

$$(\forall r, s, t \in R): \quad (r + s) \cdot t = r \cdot t + s \cdot t \text{ and } t \cdot (r + s) = t \cdot r + t \cdot s.$$

Lemma 8.1.1. *In a ring R,*

$$0 \cdot r = r = r \cdot 0$$

and

$$r + (-1) \cdot r = 0$$

for all $r \in R$.

Proof. Observe...

$$r \cdot 0 = r \cdot (0 + 0) = r \cdot 0 + r \cdot 0 \Rightarrow 0 = r \cdot 0$$

and...

$$r + (-1) \cdot r = (1) \cdot r + (-1) \cdot r = (1 - 1) \cdot r = 0 \cdot r = 0$$

□

8.1.1 Commutative Rings

A ring R is *commutative* if $(\forall r, s \in R): \ r \cdot s = s \cdot r$.

8.1.2 Subrings

A *subring* S of a ring R is a ring whose underlying set is a subset of R and such that the inclusion function $S \hookrightarrow R$ is a ring homomorphism.

8.1.3 Ideals

Let R be a ring. A subgroup I of $\langle R, + \rangle$ is a *left-ideal* of R if $rI \subseteq I$ for all $r \in R$; that is,

$$(\forall r \in R)(\forall a \in I): \ ra \in I;$$

it is a *right-ideal* if $Ir \subseteq I$ for all $r \in R$; that is,

$$(\forall r \in R)(\forall a \in I): \ ar \in I.$$

A *two-sided ideal* is a subgroup I which is both a left- and a right-ideal.
Some important features to keep in mind about ideals are...

- If $\{I_\alpha\}_{\alpha \in A}$ is a collection of ideals of a ring R. Then the intersection $\bigcap_{\alpha \in A}(I_\alpha)$ is an ideal of R; the largest ideal contained in all of the ideals I_α.
- If I, J are ideals of R, then IJ denotes the ideal *generated* by all products ij with $i \in I, j \in J$. More generally, if $I_1, \ldots, I_n$ are ideals in R, then the 'product' $I_1 \cdots I_n$ denotes the ideal generated by all products $i_1 \cdots i_n$ with $i_k \in I_k$.

8.1.3.1 Principal Ideals

Let $a \in R$ be any element of a ring. Then the subset $I = Ra$ of R is a left-ideal of R and aR is a right-ideal.

If R is commutative, then we write (a) for the ideal. It is called the *principal ideal* generated by a.

Some important features to keep in mind about principal ideals are...

- $(a_\alpha)_{\alpha \in A} := \sum_{\alpha \in A}(a_\alpha)$ the ideal *generated by the elements* a_α
- $(R/(a))/(\bar{b}) \cong R/(a, b)$ where $(\bar{b})$ is the class of $b \in R/(a)$

8.1.3.2 Finitely Generated

An ideal I of a commutative ring R is *finitely generated* if $I = (a_1, \ldots, a_n)$ for some $a_1, \ldots, a_n \in R$.

8.1.4 Characteristic

Let R be a ring and consider the unique ring homomorphism $\phi : \mathbb{Z} \to R$. Then $\ker\phi = n\mathbb{Z}$ for some n. The *characteristic* of R is this nonnegative integer n.

8.2 Ring Homomorphisms

A *ring homomorphism* is a function $\varphi : R \to S$ if it preserves both ring operations and the identity element. That is...

- $(\forall a, b \in R) : \varphi(a + b) = \varphi(a) + \varphi(b)$
- $(\forall a, b \in R) : \varphi(ab) = \varphi(a)\varphi(b)$
- $\varphi(1_R) = 1_S$.

8.3 Ring Constructions

8.3.1 Products

If R_1, R_2 are rings, then the product ring $R_1 \times R_2$ may be definted by endowing the direct product of groups $R_1 \times R_2$ with componentwise multiplication.

8.3.2 Quotients

Let R be a ring and $I \subseteq R$ be an ideal. The quotient group R/I is compatible with ring structure (determined by the natural projection) and is called the *quotient ring* of R *modulo* I.

Theorem 8.3.1. *Let I be a two-sided ideal of a ring R. Then for every ring homomorphism $\varphi : R \to S$ such that $I \subseteq ker\varphi$ there exists a unique ring homomorphism $\tilde{\varphi} : R/I \to S$ so that the diagram...*

$$\begin{tikzcd} R \arrow[rr, "\varphi"] \arrow[dr, "\pi"'] & & S \\ & R/I \arrow[ur, "\exists!\tilde{\varphi}"'] & \end{tikzcd}$$

commutes.

8.4 Polynomial Rings

8.4.1 Polynomials

Let R be a ring. A *polynomial* $f(x)$ in the *indeterminate* x and with *coefficients* in R is a finite linear combination of nonnegative 'powers' of x with coefficients in R:

$$f(x) = \sum_{i \geq 0} a_i x^i = a_0 + a_q x + a_2 x^2 + \cdots ,$$

where all a_i are elements of R and we require $a_i = 0$ for $i \gg 0$.

Two polynomials are taken to be equal if...

$$\sum_{i \geq 0} a_i x^i = \sum_{i \geq 0} b_i x^i \Leftrightarrow (\forall i \geq 0) : \quad a_i = b_i.$$

NOTE: a polynomial *actually is* an element of the infinite direct sum of the group $\langle R, + \rangle$.

Operations on polynomials are defined as follows: if...

$$f(x) = \sum_{i \geq 0} a_i x^i \text{ and } g(x) = \sum_{i \geq 0} b_i x^i$$

then...

$$f(x) + f(x) := \sum_{i \geq 0} (a_i + b_i) x^i$$

and...

$$f(x) \cdot f(x) := \sum_{k \geq 0} \sum_{i+j=k} a_i b_i x^{i+j}.$$

8.4.2 Universal Property

Let $\mathcal{R}_A$ be the category of commutative rings under a set A so that...

- Objects: (j, R) such that $j : A \to R$
- Arrows: $(j_1, R_1) \to (j_2, R_2)$ representing...

$$\begin{tikzcd} A \arrow[d, "j_1"] \arrow[dr, "j_2'"] & \\ R_1 \arrow[r, "\varphi"] & R_2 \end{tikzcd}$$

Proposition 8.4.1. *$(i, \mathbb{Z}[x_1, \cdots, x_n])$ is initial in $\mathcal{R}_A$.*

Proof. Let (j, R) be an arbitrary object of $\mathbb{R}_A$; we have to show that there is a unique morphism $(i, \mathbb{Z}[x_1, \cdots, x_n]) \to (j, R)$.

The key point is that the requirements posed on φ force its definition. The postulated commutativity of the diagram means that $\varphi(x_k) = j(a_k)$ for $k = 1, \cdots, n$. Then, since φ must be a ring homomorphism, necessarily...

$$\begin{aligned} \varphi(\sum m_{i_1 \ldots i_n} x_1^{i_1} \cdots x_n^{i_n}) &= \sum \varphi(m_{i_1 \ldots i_n}) \varphi(x_1)^{i_1} \cdots \varphi(x_n)^{i_n} \\ &= \sum \iota(m_{i_1 \ldots i_n}) j(x_1)^{i_1} \cdots j(x_n)^{i_n}, \end{aligned}$$

where $\iota : \mathbb{Z} \to R$ is the unique ring homomorphism (as $\mathbb{Z}$ is initial in Ring).

Thus, if φ exists, then it is unique. On the other hand, the formula we just obtained clearly preserves the operations and sends 1 to 1, so it does define a ring homomorphism, concluding the proof. $\square$

8.4.2.1 Evaluation Map and Polynomial Functions

Let $\alpha : R \to S$ be a fixed ring homomorphism, and $s \in S$ be an element commuting with $\alpha(r)$ for all $r \in R$. Then there is a unique ring homomorphism $\overline{\alpha} : R[x] \to S$ extending α and sending x to s.

This we get an '*evaluation map*' over commutative rings...

$$f(x) = \sum_{i \geq 0} a_i x^i \text{ and } r \in R \Rightarrow f(r) = \sum_{i \geq 0} a_i r^i \in R.$$

This may be viewed as $\overline{\alpha}(f(x))$, where $\overline{\alpha}$ is obtained with $id_R : R \to R$ and $s = r$.

Thus, every polynomial $f(x)$ determines a *polynomial function* $f : R \to R$ defined by $r \mapsto f(r)$.

8.5 Integral Domains

8.5.1 Zero-divisors

An element a in a ring R is a *left-zero-divisor* if there exist elements $b \neq 0$ in R for which $ab = 0$.

Proposition 8.5.1. *In a ring R, $a \in R$ is not a left- (resp., right-) zero-divisor if and only if left (resp., right) multiplication by a is an injective function $R \to R$.*

Proof. ($\Rightarrow$) Assume a is not a left-zero-divisor and $ab = ac$ for $b, c \in R$. Then, by distributivity,

$$a(b - c) = ab - ac = 0,$$

and this implies $b - c = 0$ since a is not a left-zero-divisor; that is, $b = c$.

($\Leftarrow$) If a is a left-zero-divisor, then $\exists b \neq 0$ such that $ab = 0 = a \cdot 0$; this shows that left-multiplication is not injective in this case. $\square$

8.5.2 Definition

An *integral domain* is a nonzero commutative ring R (with 1) such that...

$$(\forall a, b \in R) : \quad ab = 0 \Rightarrow a = 0 \text{ or } b = 0.$$

Proposition 8.5.2. *Assume R is a finite commutative ring; then R is an integral domain if and only if it is a field.*

Proof. ($\Rightarrow$) If $a \in R$ is a non-zero-divisor, then multiplication by a in R is injective by 8.5.1; hence it is surjective, as the ring is finite, by the pigeonhole principle; hence a is a unit via 8.8.1.

($\Leftarrow$) This direction is obvious. $\square$

8.6 Noetherian Rings

A commutative ring R is *Noetherian* if every ideal of R is finitely generated.

8.7 Principla Ideal Domains

An integral domain R is a *PID* if every ideal of R is principal.

Proposition 8.7.1. *$\mathbb{Z}$ is a PID.*

Proof. Let $I \subseteq \mathbb{Z}$ be an ideal. Since I is a subgroup, $I = n\mathbb{Z}$ for some $n \in \mathbb{Z}$, by 7.2.3. Since $n\mathbb{Z} = (n)$, this shows that I is principal. $\square$

8.8 Division Rings

8.8.1 Units

An element u of a ring R is a *left-unit* if $\exists v \in R$ such that $uv = 1$; it is a *right-unit* if $\exists v \in R$ such that $vu = 1$. *Units* are two sided units.

Proposition 8.8.1. *In a ring R:*

- *u is a left- (resp., right-) unit if and only if left- (resp., right-) multiplication by u is a surjective function $R \to R$*
- *if u is a left- (resp., right-) unit, then right- (resp., left-) multiplication by u is injective; that is, u is not a right- (resp., left-) zero-divisor;*
- *the inverse of a two-sided unit is unique;*
- *two-sided units form a group under multiplication.*

8.8.2 Definition

A *division ring* is a ring in which every nonzero element is a two-sided unit.

9 Field Theory

9.1 Definitions

A *field* is a nonzero commutative ring R (with 1) in which every nonzero element is a unit.

10 Modules

11 Topology

11.1 Metric Spaces

A *metric space* $\langle X, d\rangle$ is a set X together with a *metric* $d : X \times X \to \mathbb{R}$ satisfying...

1. $d(x, y) \geq 0$ for all $x, y \in X$ and $d(x, y) = 0$ if and only if $x = y$.
2. $d(x, y) = d(y, x)$ for all $x, y \in X$.
3. (*The Triangle Inequality*): $d(x, y) + d(y, z) \geq d(x, z)$ for all $x, y, z \in X$.

11.1.1 Open Ball

The *open ball* of radius $\varepsilon > 0$ centered at a point x in a metric space $\langle X, d\rangle$ is given by...

$$B_\varepsilon(x) = \{y \in X | d(x, y) < \varepsilon\}.$$

11.1.2 Continuity

Suppose $\langle X, d_X\rangle$ and $\langle Y, d_Y\rangle$ are two metric spaces and $f : X \to Y$ is a function. Then f is *continuous at* $x \in X$ if for any $\epsilon > 0$, there is a $\delta > 0$ so that $B_\delta(x) \subset f^{-1}(B_\varepsilon(f(x)))$.

The function f is *continuous* if it is continous at x for all $x \in X$.

11.1.3 Open Set

The *open set* U of a metric space (X, d) is *open* if for any $u \in U$, there is $\varepsilon > 0$ so that $B_\varepsilon(x) \subseteq U$.

Theorem 11.1.1. *A function $f : X \to Y$ between metric spaces $\langle X, d\rangle$ and $\langle Y, d\rangle$ is continuous if and only if for any open subset V of Y, the subset $f^{-1}(V)$ is open in X.*

11.1.4 Examples

11.1.4.1 Euclidean Metric Space

If for $x, y \in \mathbb{R}^n$...

$$d(x, y) = ||x - y|| = \sqrt{(x_1 - y_1)^2 + \cdots + (x_n - y_n)^n},$$

then $\langle \mathbb{R}^n, d\rangle$ is a metric space.

11.1.4.2 Box Metric Space

If for $x, y \in \mathbb{R}^n$...

$$d(x, y) = \max\{|x_1 - y_1|, \ldots, |x_n - y_n|\},$$

then $\langle \mathbb{R}^n, d \rangle$ is a metric space.

The set of open balls for the previous two metrics form bases that generate the same topology.

11.1.4.3 Bounded Real Functions Metric Space

Let $\mathrm{Bdd}([0,1], \mathbb{R})$ denote the set of *bounded functions* $f : [0,1] \to \mathbb{R}$. If for $f, g \in \mathrm{Bdd}([0,1], \mathbb{R})$...

$$d(f, g) = \mathrm{lub}_{t \in [0,1]}\{f(t) - g(t)\},$$

then $\langle \mathrm{Bdd}([0,1], \mathbb{R}), d \rangle$ is a metric space.

11.1.4.4 Discrete Metric space

Let X be any set and define...

$$d(x, y) = \begin{cases} 0, & \text{if } x = y, \\ 1, & \text{if } x \neq y. \end{cases}$$

Then $\langle X, d \rangle$ is a metric space.

11.2 Topological Spaces

11.2.1 Topological Space

Let X be a set and $\mathcal{T}$ a collection of subsets of X called *open sets*. The collection $\mathcal{T}$ is called a *topology* on X if

1. we have that $\emptyset \in \mathcal{T}$ and $X \in \mathcal{T}$,
2. the union of an arbitrary collection of memebers of $\mathcal{T}$ is in $\mathcal{T}$,
3. the finite intersection of members of $\mathcal{T}$ is in $\mathcal{T}$.

The pair $\langle X, \mathcal{T} \rangle$ is called a *(topological) space*.

11.2.1.1 Finer

Given two topologies $\mathcal{T}, \mathcal{T}'$ on a given set X we say $\mathcal{T}$ is *finer* than $\mathcal{T}'$ if $\mathcal{T}' \subseteq \mathcal{T}$.

11.2.1.2 Coarser

Given two topologies $\mathcal{T}, \mathcal{T}'$ on a given set X we say $\mathcal{T}$ is *coarser* than $\mathcal{T}'$ if $\mathcal{T} \subseteq \mathcal{T}'$.

11.2.2 Basis

A collection of subsets, $\mathcal{B}$, of a set X is a *basis for a topology on* X if

1. for all $x \in X$, there is a $B \in \mathcal{B}$ with $x \in B$,
2. $x \in B_1 \in \mathcal{B}$ and $x \in B_2 \in \mathcal{B}$, then there is some $B_3 \in \mathcal{B}$ with $x \in B_3 \subseteq B_1 \cap B_2$.

Proposition 11.2.1. *If $\mathcal{B}$ is a basis for a topology on a set X, then the collection of subsets...*

$$\mathcal{T}_{\mathcal{B}} = \{\bigcup_{\alpha \in A} B_\alpha | A \textit{ is any index set and } B_\alpha \in \mathcal{B} \textit{ for all } \alpha \in A\}$$

is a topology on X called the topology generated by the basis $\mathcal{B}$.

Proposition 11.2.2. *If $\mathcal{B}_1$ and $\mathcal{B}_2$ are bases for topologies on a set X, and for all $x \in X$ and $x \in B_1 \in \mathcal{B}_1$, there is a B_2 with $x \in B_2 \subseteq B_1$ and $B_2 \in \mathcal{B}_2$, then $\mathcal{T}_{\mathcal{B}_2}$ is finer than $\mathcal{T}_{\mathcal{B}_1}$.*

11.2.3 Continuity

Let $\langle X, \mathcal{T} \rangle$ and $\langle Y, \mathcal{T}' \rangle$ be topological spaces and $f : X \to Y$ a function. We say that f is *continuous* if whenever V is open in Y, $f^{-1}(V)$ is open in X.

Proposition 11.2.3. *If $\mathcal{T}$ and $\mathcal{T}'$ are topologies on a set X, then the identity mapping $id : \langle X, \mathcal{T} \rangle \to \langle X, \mathcal{T}' \rangle$ is continuous if and only if $\mathcal{T}$ is finer that $\mathcal{T}'$.*

Theorem 11.2.1. *Given two continuous functions $f : X \to Y$ and $g : Y \to Z$, the composite function $g \circ f : X \to Z$ is continuous.*

11.2.4 Homeomorphism

A function $f : \langle X, \mathcal{T}_X \rangle \to \langle Y, \mathcal{T}_Y \rangle$ is a *homeomorphism* if f is continuous, bijective, and has a continuous inverse. In other words, a homeomorphism is an isomorphism in the category **Top**.

11.2.4.1 Homeomorphic Spaces

We say $\langle X, \mathcal{T}_X \rangle$ and $\langle Y, \mathcal{T}_Y \rangle$ are *homeomorphic topological spaces* if there is a homeomorphism $f : \langle X, \mathcal{T}_X \rangle \to \langle Y, \mathcal{T}_Y \rangle$.

11.3 Topology Examples

11.3.1 Indiscrete Topology

For any set X, $\mathcal{T} = \{\emptyset, X\}$.

11.3.2 Discrete Topology

For any set X, $\mathcal{T} = \mathcal{P}(X)$.

11.3.3 Finite Complement Topology

Given an infinte set X, define $\mathcal{T}_{FC} = \{U \subseteq X | U = \emptyset \text{ or } X \setminus U \text{ is finite}\}$.

11.4 Topological Properties

A property of a space $\langle X, \mathcal{T}_X \rangle$ is said to be a *topological property* if, whenever $\langle Y, \mathcal{T}_Y \rangle$ is homeomorphic to $\langle X, \mathcal{T}_X \rangle$, then the space $\langle Y, \mathcal{T}_Y \rangle$ also has the property.

11.4.1 Second Countable

A space that has a countable set as a basis for its topology.

12 Homotopy

13 Homology

14 Dimension

Theorem 14.0.1. *There is a one-to-one correspondence* $\mathbb{R} \to \mathbb{R} \times \mathbb{R}$.

Proof. Since the mapping $f : \mathbb{R} \to (0, 1)$ given by $r \mapsto \frac{1}{\pi}(\arctan(r) + \frac{\pi}{2})$ is a bijection, it is sufficient to find a bijection $(0, 1) \to (0, 1) \times (0, 1)$. For this we use the Schröder-Bernstein Theorm.

Observe that $g : (0, 1) \to (0, 1) \times (0, 1)$ given by $t \mapsto (t, t)$ is an injection. So the only real work is in constructing an injection $(0, 1) \times (0, 1) \to (0, 1)$.

To start things off, introduce the following injection $I : (0, 1) \to (0, 1) \cap (\mathbb{R} \setminus \mathbb{Q})$...

$$I(r) = \begin{cases} [0; a_1 + 2, a_2 + 2, \dots, a_n + 2, 2, 2, \dots] & \text{if } r = [0; a_1, a_2, \dots, a_n], \\ [0; a_1 + 2, a_2 + 2, a_3 + 2, \dots] & \text{if } r = [0; a_1, a_2, a_3, \dots]. \end{cases}$$

Composed with another injection, $t : (0, 1) \cap (\mathbb{R} \setminus \mathbb{Q}) \times (0, 1) \cap (\mathbb{R} \setminus \mathbb{Q}) \to (0, 1)$ given by $([0; a_1, a_2, \dots], [0; a_1, a_2, \dots]) \mapsto [0; a_1, b_1, a_2, b_2, \dots]$, we get our desired injection $t \circ (I \times I)$. $\square$

Corollary 14.0.1.1. *There is a bjection* $f : \mathbb{R}^m \to \mathbb{R}^n$ *for all positive integers* m *and* n.