

1 Set Theory

1.1 Set Axioms

1.1.1 Undefined notions

Set: A, B, C, \dots

1.1.2 Axioms

1. *Extension:* $\forall A \forall B [\forall C (C \in A \Leftrightarrow C \in B) \Rightarrow A = B]$
2. *Regularity:* $\forall A [\exists C (C \in A) \Rightarrow \exists B (B \in A \wedge \neg \exists D (D \in B \wedge D \in A))]$
(Every nonempty set contains a set that is disjoint from it. Also known as "Axiom of Foundation.")
3. *Schema of Specification:* $\forall B \forall X_1 \forall X_2 \dots \forall X_n \exists A \forall C [C \in A \Leftrightarrow (C \in B \wedge \phi)]$
4. *Pairing:* $\forall X_1 \forall X_2 \exists A (X_1 \in A \wedge X_2 \in A)$
5. *Union:* $\forall \mathcal{F}_A \exists U \forall A \forall X [(X \in A \wedge A \in \mathcal{F}_A) \Rightarrow X \in U]$
6. *Schema of Replacement:* $\forall A \forall X_1 \forall X_2 \dots \forall X_n [\forall B (B \in A \Rightarrow \exists! D \phi) \Rightarrow \exists B \forall C (C \in A \Rightarrow \exists D (D \in B \wedge \phi))]$
7. *Infinity:* $\exists \omega_0 [\emptyset \in \omega_0 \wedge \forall X (X \in \omega_0 \Rightarrow X \cup X \in \omega_0)]$
8. *Power Set:* $\forall X \exists \mathcal{P}(X) \forall S [S \subseteq X \Rightarrow S \in \mathcal{P}(X)]$
9. *Empty Set:* $\exists A \forall X (X \notin A)$
10. *Choice:* $\forall X [\emptyset \notin X \Rightarrow \exists (f : X \rightarrow \bigcup X) \forall A \in X (f(A) \in A)]$

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

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

1.1.3 Universe

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

1. $x \in u \in U \Rightarrow x \in U$
2. $u \in U \wedge v \in U \Rightarrow \{u, v\}, \langle u, v \rangle, u \times v \in U$
3. $X \in U \Rightarrow \mathcal{P}(X) \in U \wedge \bigcup X \in U$
4. $\omega_0 \in U$ is the set of finite ordinals
5. if $f : A \rightarrow B$ is a surjective function with $A \in U \wedge B \subset U$, then $B \in U$
(See: Set Constructions.)

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

1.2 Set Constructions

1.2.1 Union

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

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

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

1.2.2 Intersection

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

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

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

1.2.3 Complement

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

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

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

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

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

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

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

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

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

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

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

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

1.2.4 Symmetric Difference

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

1.2.5 Power Set

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

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

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

1.2.5.1 Characteristic Function of a subset

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

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

1.2.6 n -Tuple

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

1.2.7 Cartesian Product

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

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

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

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

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

1.2.8 Quotient by Equivalence Relation

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

1.2.9 Family

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

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

1.3 Relations

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

1.3.1 Equivalence Relations

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

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

1.3.1.1 Equivalence Class

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

1.3.1.2 Set Partition

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

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

1.3.2 Functions

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

1.3.2.1 Injection

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

1.3.2.2 Surjection

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

1.3.2.3 Bijection

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

1.3.2.4 Restriction

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

1.3.2.5 Image

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

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

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

1.3.2.6 Preimage

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

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

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

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

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

1.3.2.7 Function Composition

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

2 Combinatorics

2.1 Basic Methods

2.1.1 Addition

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

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

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

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

2.1.2 Subtraction

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

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

2.1.3 Multiplication

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

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

2.1.4 Division

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

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

2.1.5 Binomial Coefficients

See permutations.

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

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

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

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

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

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

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

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

Theorem 2.1.10. *For all positive integers n ,*

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

2.1.6 Pigeonhole Principle

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

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

Then there exists at least one index i so that $|A_i| > r$.

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

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

$$a_i = d_i q + r_i$$

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

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

or, after rearranging,

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

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

2.2 Applications of Basic Methods

2.2.1 Multisets

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

2.2.1.1 Multinomial Coefficients

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

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

2.2.2 Weak Compositions

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

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

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

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

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

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

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

2.2.3 Compositions

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

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

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

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

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

2.2.4 Stirling numbers of the second kind

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

2.3 Permutations

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

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

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

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

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

2.4 Graphs

3 Category Theory

3.1 Metacategories

3.1.1 Undefined notions

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

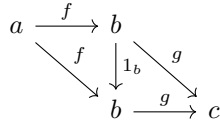
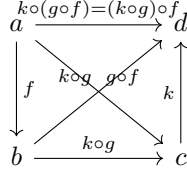
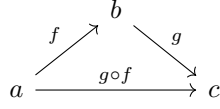
3.1.2 Operations

Given $f : a \rightarrow b \dots$

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

3.1.3 Axioms

- *Associativity:* $a \xrightarrow{f} b \xrightarrow{g} c \xrightarrow{k} d$, $k \circ (g \circ f) = (k \circ g) \circ f$
- *Unit Law:* $1_a \circ f = f$ and $g \circ 1_b = g$



3.2 Categories

3.2.1 Directed Graph

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

Set of composable pairs of arrows:

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

3.2.2 Categories

Add the following structure to a directed graph. . .

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

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

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

Small categories use small sets for their objects.

3.2.3 Hom Sets

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

3.2.4 Groupoids

A category in which every arrow is an isomorphism.

3.3 Morphisms

Arrows in categories.

3.3.1 Isomorphisms

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

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

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

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

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

□

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

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

3.3.2 Automorphisms

An isomorphism of an object to itself. Denoted:

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

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

3.3.3 Monomorphisms

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

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

3.3.4 Epimorphisms

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

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

3.4 Functors

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

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

which satisfy...

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

3.4.1 Full

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

3.4.2 Faithful

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

3.5 Duality

4 Group Theory

5 Ring Theory

6 Modules

7 Homology

8 Topology

9 Homotopy