

Learning Uni Maths

gispisquared

If only I had the theorems! Then I
should find the proofs easily
enough.

Bernhard Riemann

Contents

Chapter 1. Set Theory	5
Chapter 2. Ordinals	9
Chapter 3. Cardinality	11
Chapter 4. Number Systems	13
Chapter 5. Vector Spaces	17
Chapter 6. Metric Spaces	19
Appendix A. Proofs	21

CHAPTER 1

Set Theory

AXIOM 1 (Existence). *There exists a set.*

REMARK 2. This is implied by the Axiom of Infinity; however, we include it here so that we may define the empty set.

DEFINITION 3. A *sentence* is made by combining assertions of belonging (eg $x \in A$) and/or assertions of equality (eg $A = B$) using the usual logical operators: *and, or, not, implies, if and only if, there exists, for all.*

DEFINITION 4. Let A and B be sets. If every element of A is an element of B , we say that A is a *subset* of B , denoted $A \subseteq B$.

PROPOSITION 5. *If $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$.*

AXIOM 6 (Extensionality). *$A = B$ iff $A \subseteq B$ and $B \subseteq A$.*

AXIOM 7 (Specification). *For every set A and every sentence $S(x)$ there is a set B whose elements are exactly those elements x of A for which $S(x)$ holds.*

DEFINITION 8. We notate this set B by $\{x \in A : S(x)\}$.

PROPOSITION 9. *There exists a unique set X such that for any x , the sentence $x \in X$ is false.*

DEFINITION 10. We call this set the *empty set*, notated \emptyset .

PROPOSITION 11. *For every set A there is a set B such that $B \notin A$.*

AXIOM 12 (Pairing). *For any two sets A and B there is a set X with $A \in X$ and $B \in X$.*

PROPOSITION 13. *There is a unique set Y such that for any a , a is in Y iff $a = A$ or $a = B$.*

DEFINITION 14. This set is called the *unordered pair* formed by A and B , denoted $\{A, B\}$.

DEFINITION 15. The set $\{A, A\}$ is denoted $\{A\}$, and called the *singleton* of $\{A\}$.

AXIOM 16 (Union). *For any set X of sets there exists a set Y such that for any A in X , and any a in A , a is in Y .*

PROPOSITION 17. *For a nonempty set X of sets there is a unique set Z such that a is in Z if and only if there exists an A in X such that a is in A .*

DEFINITION 18. This set is called the *union* of X , denoted $\bigcup X$.

For two sets A and B we define $A \cup B = \bigcup\{A, B\}$.

DEFINITION 19. Let A and B be sets. The *intersection* of A and B , notated $A \cap B$, is $\{x \in A : x \in B\}$.

If $A \cap B = \emptyset$ then A and B are called *disjoint*.

PROPOSITION 20. We have

- $A \cup \emptyset = A$,
- $A \cup B = B \cup A$ (*commutative*),
- $A \cup (B \cup C) = (A \cup B) \cup C$ (*associative*),
- $A \cup A = A$ (*idempotent*),
- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (*distributive*),
- $A \subseteq B$ iff $A \cup B = B$,
- $A \cap \emptyset = \emptyset$,
- $A \cap B = B \cap A$ (*commutative*),
- $A \cap (B \cap C) = (A \cap B) \cap C$ (*associative*),
- $A \cap A = A$ (*idempotent*),
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (*distributive*),
- $A \subseteq B$ iff $A \cap B = A$.

PROPOSITION 21. For every nonempty set C of sets, there is a unique set Y such that $x \in Y$ iff $x \in X$ for each X in C .

DEFINITION 22. This set Y is called the *intersection* of C , denoted $\bigcap C$.

AXIOM 23 (Powers). For each set X there is a set that contains all subsets of X .

PROPOSITION 24. There is a unique set Y such that $x \in Y$ iff $x \subseteq X$.

DEFINITION 25. This set Y is called the *power set* of X , denoted $\mathcal{P}(X)$.

DEFINITION 26. The *ordered pair* of a and b is the set defined as

$$(a, b) = \{\{a\}, \{a, b\}\}.$$

PROPOSITION 27. For any a, b, c, d , we have $(a, b) = (c, d)$ iff $a = c$ and $b = d$.

DEFINITION 28. Let A and B be sets. The *Cartesian product* $A \times B$ is

$$\{(x, y) : x \in A, y \in B\}.$$

PROPOSITION 29. For any set R of ordered pairs there are sets A and B such that $R \subseteq A \times B$.

DEFINITION 30. A *binary relation* R over sets A and B is a subset of $A \times B$. If (a, b) is in R we write aRb .

If $A = B$ then we call it a *binary relation over A* .

DEFINITION 31. An *equivalence relation* is a binary relation \sim over A such that

- $a \sim a$ (*reflexive*),
- $a \sim b \iff b \sim a$ (*symmetric*), and
- if $a \sim b$ and $b \sim c$ then $a \sim c$ (*transitive*).

The *equivalence class* of a under \sim is

$$[a] = \{x \in A : x \sim a\}.$$

DEFINITION 32. A *partition* of a set A is a disjoint set of subsets of A whose union is A .

A partition X of A *induces* a relation \sim , where $a \sim b$ iff a and b belong to the same element of X .

PROPOSITION 33. *The set of equivalence classes of an equivalence relation exists and is a partition.*

DEFINITION 34. This partition is called the partition *induced* by the equivalence relation \sim .

PROPOSITION 35. *The equivalence relation induced by a partition induces that partition; the partition induced by an equivalence relation induces that relation.*

DEFINITION 36. For any set X we define $X^+ = X \cup \{X\}$.

AXIOM 37 (Infinity). *There exists a set S containing \emptyset and containing X^+ for every X in S .*

PROPOSITION 38. *There exists a unique set ω which is a subset of all such sets S .*

PROPOSITION 39. *For any $a, b \in \omega$, exactly one of $a \in b$, $a = b$, $b \in a$ is true.*

PROPOSITION 40. *For any $a \in \omega$ and any $b \in a$, $b \subseteq a$.*

DEFINITION 41. A function $f : A \rightarrow B$ is a relation f over A and B such that for each $a \in A$ there is exactly one $b \in B$ such that afb . We usually write this as $f(a) = b$.

A function f is *injective* if for each b in B , there is at most one a in A such that $f(a) = b$. It is *surjective* if for each b in B there is at least one a in A such that $f(a) = b$. A function which is both injective and surjective is *bijective*.

THEOREM 42 (Recursion theorem). *If a is an element of a set X , and if $f : X \rightarrow X$ is a function, then there is a function $g : \omega \rightarrow X$ such that $u(0) = a$ and $u(n^+) = f(u(n))$ for all n in ω .*

AXIOM 43 (Substitution). *If $S(a, b)$ is a sentence such that for each a in a set A there exists a set B_a such that $b \in B_a \iff S(a, b)$, then there exists a function F with domain A such that $F(a) = B_a$ for each a in A .*

AXIOM 44 (Foundation). *Every set X contains a set Y such that X and Y are disjoint.*

AXIOM 45 (Choice). *Let X be a set of sets whose members are all nonempty. Then there exists a function $f : X \rightarrow \bigcup X$ such that $f(Y) \in Y$ for all $Y \in X$.*

CHAPTER 2

Ordinals

DEFINITION 46. A *partial order* is a binary relation \leq on a set A such that

- $a \leq a$ (reflexive),
- if $a \leq b$ and $b \leq a$ then $a = b$ (antisymmetric), and
- if $a \leq b$ and $b \leq c$ then $a \leq c$ (transitive).

We define $a < b$ if $a \leq b$ and $a \neq b$.

If for all a and b we have $a \leq b$ or $b \leq a$ (strongly connected), then \leq is a *total order*.

A *chain* is a totally ordered subset of a partially ordered set.

DEFINITION 47. If X is a partially ordered set, and if $a \in X$, the set $s(a) = \{x \in X : x < a\}$ is called the *initial segment* determined by a .

DEFINITION 48. Two partially ordered sets X and Y are *similar* if there is a bijection $f : X \rightarrow Y$ such that $a \leq b \iff f(a) \leq f(b)$. This bijection is called a *similarity*.

DEFINITION 49. Let S be a subset of a partially ordered set A , and let a be an element of A . If $s \leq a$ for every s in S , then we call a an *upper bound* of S . If $a \leq s$ for every s in S , then we call a a *lower bound* of S . If a is an upper bound of S and a lower bound of the set of upper bounds of S , then we call a a *least upper bound* of S .

DEFINITION 50. A *well-order* on A is a total order \leq on A such that every nonempty subset S of A has an element a which is a lower bound for S . The set A together with the relation \leq is then called *well-ordered*.

PROPOSITION 51. *If two well-ordered sets are similar, then the similarity is unique.*

THEOREM 52. *If X and Y are well-ordered, then either X and Y are similar, or one is similar to an initial segment of the other.*

DEFINITION 53. An *ordinal number* is a well-ordered set α such that for any $\xi \in \alpha$ we have $s(\xi) = \xi$.

PROPOSITION 54. ω is an ordinal number.

PROPOSITION 55. *If α is an ordinal number then so is α^+ , and so is any element of α .*

THEOREM 56. *If two ordinal numbers are similar, then they are equal. Otherwise, one is an element of the other.*

PROPOSITION 57. *If a set α can be well-ordered such that it is an ordinal, then the ordering is unique.*

PROPOSITION 58. *Every well-ordered set is similar to a unique ordinal number.*

PROPOSITION 59. *There is no set of all ordinal numbers.*

THEOREM 60 (Zorn's Lemma). *Suppose a partially ordered set P has the property that every chain in P has an upper bound in P . Then there is an element $a \in P$ such that the only upper bound for $\{a\}$ is a .*

THEOREM 61 (Well-Ordering Theorem). *Every set has a well-ordering.*

CHAPTER 3

Cardinality

DEFINITION 62. Two sets A and B are said to have the same *cardinality* (written $|A| = |B|$) if there is a bijection $f : A \rightarrow B$.

A set A has cardinality at most the cardinality of B ($|A| \leq |B|$) if there is an injection $f : A \rightarrow B$.

A set A has cardinality less than the cardinality of B ($|A| < |B|$) if $|A| \leq |B|$ and $|A| \neq |B|$.

THEOREM 63. If $|A| \leq |B|$ and $|B| \leq |A|$ then $|A| = |B|$.

THEOREM 64. For any set A , $|\mathcal{P}(A)| > |A|$.

DEFINITION 65. A *cardinal number* is an ordinal number α such that for any ordinal number β with $|\alpha| = |\beta|$ we have $\alpha \in \beta$.

PROPOSITION 66. For any set S , there is a unique cardinal number α with $|\alpha| = |S|$.

DEFINITION 67. For these sets S and α we define $|S| = \alpha$.

DEFINITION 68. A set A is said to be *finite* $|A| \in \omega$, and *infinite* otherwise.

PROPOSITION 69. A set is infinite if and only if it has the same cardinality as some proper subset.

PROPOSITION 70. Any infinite set S satisfies $\omega \in |S|$.

DEFINITION 71. An infinite set A is said to be *countable* if $|A| = \omega$, and *uncountable* otherwise.

CHAPTER 4

Number Systems

DEFINITION 72. A *binary operation* on A is a function $\cdot : A \times A \rightarrow A$. We usually write $\cdot(a, b) = c$ as $a \cdot b = c$.

It is *associative* if $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for any a, b, c in A .

It is *commutative* if $a \cdot b = b \cdot a$ for any a, b in A .

DEFINITION 73. A *monoid* is an ordered pair (A, \cdot) of a set A and a binary operation \cdot on A such that there exists an element 1 , called the *identity*, such that $a \cdot 1 = 1 \cdot a = a$ for all a .

REMARK 74. There are two main notations for monoid-type structures. These are

- Multiplicative notation, in which the operation is notated $a \cdot b$ or simply ab , and the identity element is 1 ; and
- Additive notation, in which the operation is notated $a + b$ and the identity element is 0 .

DEFINITION 75. A *group* is a monoid (A, \cdot) such that for each element a of A there is an element b of A such that $ab = 1 = ba$.

A group is *abelian* if the operation is commutative.

PROPOSITION 76. If $ab = ba = 1$ and $ac = 1$ or $ca = 1$ then $b = c$.

DEFINITION 77. The element b of A such that $ab = ba = 1$ is called the *inverse* of a . In multiplicative notation, the inverse of a is notated a^{-1} . In additive notation, the inverse of a is notated $-a$.

REMARK 78. We often define $\frac{a}{b} = ab^{-1}$ in multiplicative notation, and $a - b = a + (-b)$ in additive notation.

DEFINITION 79. A *ring* is an ordered triple $(A, +, \cdot)$ such that $(A, +)$ is an abelian group, $(A \setminus \{0\}, \cdot)$ is a monoid, and the *distributive laws* hold:

$$a \cdot (b + c) = ab + ac \quad \text{and} \quad (a + b) \cdot c = ac + bc.$$

It is *commutative* if \cdot is commutative.

It is *ordered* if there is a total order \leq on A satisfying

- if $a \leq b$ then $a + c \leq b + c$, and
- if $0 \leq a$ and $0 \leq b$ then $0 \leq ab$.

DEFINITION 80. A *field* is a commutative ring $(A, +, \cdot)$ such that $(A \setminus \{0\}, \cdot)$ is a group.

An *ordered field* is a field that is also an ordered ring.

DEFINITION 81. In an ordered field \mathbb{F} , the *absolute value* $|a|$ of an element a of \mathbb{F} is a if $0 \leq a$, otherwise $-a$.

PROPOSITION 82. $|a + b| \leq |a| + |b|$.

DEFINITION 83. Let X and Y be similar well-ordered sets, and let A and B be the least elements of X and Y respectively. Assume that all other elements of X and Y are operations on A and B respectively, and let f be the similarity between A and B .

A function $\varphi : A \rightarrow B$ is said to be a *homomorphism* if for every $a, b \in A$ and every $\cdot \in X \setminus \{A\}$ we have

$$\varphi(a \cdot b) = \varphi(a)f(\cdot)\varphi(b).$$

An *isomorphism* is a bijective homomorphism.

If there exists an isomorphism from A to B , then we say A and B are *isomorphic*.

PROPOSITION 84. *The property of being isomorphic is reflexive, symmetric and transitive.*

REMARK 85. We don't say that isomorphism is an equivalence relation, since it would imply there exists a set of all X s.

THEOREM 86. *There exists a unique ordered ring \mathbb{Z} (up to isomorphism) such that $\{x \in \mathbb{Z} : x \geq 0\}$ is well-ordered.*

\mathbb{Z} is commutative.

DEFINITION 87. The *integers*, \mathbb{Z} , are a well-ordered ring. The *non-negative integers* $\mathbb{Z}_{\geq 0}$ are $\{n \in \mathbb{Z} : n \geq 0\}$. The *positive integers* \mathbb{Z}^+ are $\mathbb{Z}_{\geq 0} \setminus \{0\}$.

REMARK 88. We avoid use of the term *natural numbers*, and the symbol \mathbb{N} , since some use them to mean the positive integers and others use them to mean the nonnegative integers.

PROPOSITION 89. $\mathbb{Z}_{\geq 0}$ is similar to ω .

REMARK 90. Thus, we may identify ω with $\mathbb{Z}_{\geq 0}$. In particular, the cardinality of a finite set is a nonnegative integer.

PROPOSITION 91. *Every ordered ring contains a unique subring isomorphic to \mathbb{Z} .*

DEFINITION 92. In $\mathbb{Z} \times \mathbb{Z}^+$, we define the operations

$$(a, b) + (c, d) = (ad + bc, bd), \quad (a, b)(c, d) = (ac, bd).$$

We also define an equivalence relation \sim where $(a, b) \sim (c, d) \iff ad = bc$.

We define the *rational numbers* \mathbb{Q} as the partition of $\mathbb{Z} \times \mathbb{Z}^+$ induced by this equivalence relation, with $[(a, b)] + [(c, d)] = [(ad + bc, ac + bd)]$ and $[(a, b)] \cdot [(c, d)] = [(ac, bd)]$.

PROPOSITION 93. *The relation \sim is an equivalence relation. Moreover, the operations $+$ and \cdot are uniquely defined. With these operations, \mathbb{Q} is a field.*

PROPOSITION 94. *Every ordered field contains a unique subfield isomorphic to \mathbb{Q} .*

DEFINITION 95. A totally ordered set S is *complete* if every nonempty subset that has an upper bound in S has a least upper bound in S .

THEOREM 96. *There exists a unique complete ordered field, up to isomorphism.*

DEFINITION 97. We call this field \mathbb{R} .

DEFINITION 98. We define $\mathbb{Q}_{\geq 0}$, \mathbb{Q}^+ , $\mathbb{R}_{\geq 0}$, \mathbb{R}^+ in an analogous way to $\mathbb{Z}_{\geq 0}$ and \mathbb{Z}^+ .

DEFINITION 99. We define the *complex numbers* \mathbb{C} as \mathbb{R}^2 , with the operations

$$(a, b) + (c, d) = (a + c, b + d), \quad (a, b) \cdot (c, d) = (ac - bd, ad + bc).$$

We usually write (a, b) as $a + bi$. We define the *conjugate* of $a + bi$ to be $\overline{a + bi} = a - bi$.

PROPOSITION 100. *There are unique homomorphisms $\mathbb{Z} \rightarrow \mathbb{Q}$, $\mathbb{Q} \rightarrow \mathbb{R}$ and $\mathbb{Q} \rightarrow \mathbb{C}$. There is also a homomorphism $\mathbb{Z} \rightarrow \mathbb{C}$.*

REMARK 101. Because of this, we usually take $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

PROPOSITION 102. *Let $a \in \mathbb{C}$. Then, $a\bar{a} \in \mathbb{R}_{\geq 0}$.*

PROPOSITION 103. *Let $b \in \mathbb{R}_{\geq 0}$. There exists a unique $x \in \mathbb{R}_{\geq 0}$ such that $x \cdot x = b$.*

DEFINITION 104. We call x the *square root* of b , denoted \sqrt{b} .

We call $\sqrt{a\bar{a}}$ the *modulus* of a , denoted $|a|$.

PROPOSITION 105. $|a + b| \leq |a| + |b|$.

THEOREM 106. $|\mathbb{Z}^+| = |\mathbb{Z}_{\geq 0}| = |\mathbb{Z}| = |\mathbb{Q}| = \omega$, but $|\mathbb{R}| = |\mathbb{C}| = |\mathcal{P}(\omega)|$.

CHAPTER 5

Vector Spaces

DEFINITION 107. Let \mathbb{F} be a field. A *vector space over \mathbb{F}* is an abelian group V (of *vectors*) together with a function $\cdot : \mathbb{F} \times V \rightarrow V$ (*scalar multiplication*) such that

- $a(b\mathbf{v}) = (ab)\mathbf{v}$ (compatible),
- $1\mathbf{v} = \mathbf{v}$ (identity), and
- $a(\mathbf{u} + \mathbf{v}) = a\mathbf{u} + a\mathbf{v}$ and $(a + b)\mathbf{v} = a\mathbf{v} + b\mathbf{v}$ (distributive).

DEFINITION 108. Let S be a subset of V . A *linear combination* of elements of S is a vector of the form

$$\sum_{i=1}^n a_i \mathbf{s}_i,$$

where each \mathbf{s}_i is a distinct element of S .

DEFINITION 109. A subset S of V is *linearly independent* if any linear combination of elements of S that produces $\mathbf{0}$ has all coefficients equal to 0. Otherwise, it is *linearly dependent*.

DEFINITION 110. A *subspace* W of V is a nonempty subset of V which is also a vector space over \mathbb{F} .

PROPOSITION 111. A subset W of V is a subspace iff the following conditions hold:

- W is nonempty;
- W is closed under addition; and
- W is closed under scalar multiplication.

DEFINITION 112. The *span* of a subset S of V is the intersection of all linear subspaces of V that contain S .

PROPOSITION 113. The span of S is the set of linear combinations of elements of S .

DEFINITION 114. A subset S of V is a *basis* if it is linearly independent and its span is V .

THEOREM 115. Assume V has a finite basis. Then, any two bases of V have the same cardinality.

THEOREM 116. If we take the Axiom of Choice, then

- Every vector space V has a basis.
- Any two bases of V have the same cardinality.

DEFINITION 117. The *dimension* of V is the cardinality of a basis of V .

DEFINITION 118. An *inner product space* is a vector space V over a field \mathbb{F} which is either \mathbb{R} or \mathbb{C} , together with a function $\langle \cdot, \cdot \rangle : V \times V \rightarrow \mathbb{F}$ satisfying

- $\langle \mathbf{x}, \mathbf{y} \rangle = \overline{\langle \mathbf{y}, \mathbf{x} \rangle}$ (conjugate symmetry)
- $\langle a\mathbf{x} + b\mathbf{y}, \mathbf{z} \rangle = a\langle \mathbf{x}, \mathbf{z} \rangle + b\langle \mathbf{y}, \mathbf{z} \rangle$ (linearity in the first argument), and
- $\langle \mathbf{x}, \mathbf{x} \rangle = 0 \implies \mathbf{x} = \mathbf{0}$.

DEFINITION 119. Let S be a set, and let $n \in \mathbb{Z}^+$. An *ordered n -tuple* $\{a_i\}_1^n$ of elements of S is a function $f : \{x \in \mathbb{Z}^+ : x \leq n\} \rightarrow S$. We write $a_i = f(i)$ for each positive integer i which is at most n .

DEFINITION 120. For any $n \in \mathbb{Z}^+$, we define \mathbb{R}^n and \mathbb{C}^n to be the set of ordered n -tuples of real and complex numbers respectively, with addition and scalar multiplication defined componentwise.

PROPOSITION 121. \mathbb{C}^n is an inner product space over \mathbb{C} with the inner product

$$\langle a, b \rangle = \sum_{i=1}^n a_i \overline{b_i}.$$

\mathbb{R}^n is an inner product space over \mathbb{R} with the inner product

$$\langle a, b \rangle = \sum_{i=1}^n a_i b_i.$$

DEFINITION 122. A *normed vector space* is a vector space V over \mathbb{R} or \mathbb{C} on which there is a *norm*: a function $\|\cdot\| : V \rightarrow \mathbb{C}$ satisfying

- $\|\mathbf{x}\| \geq 0$,
- $\|\mathbf{x}\| = 0$ implies $\mathbf{x} = \mathbf{0}$,
- $\|a\mathbf{x}\| = |a|\|\mathbf{x}\|$, and
- $\|\mathbf{x} + \mathbf{y}\| \leq \|\mathbf{x}\| + \|\mathbf{y}\|$ (the triangle inequality).

PROPOSITION 123. If V is an inner product space, then $\langle \mathbf{x}, \mathbf{x} \rangle$ is real for all \mathbf{x} . Moreover, $\|\mathbf{x}\| = \sqrt{\langle \mathbf{x}, \mathbf{x} \rangle}$ is a norm on V .

CHAPTER 6

Metric Spaces

DEFINITION 124. A *metric space* is a nonempty set M together with a function $d : M \times M \rightarrow \mathbb{R}$ such that

- $d(x, y) = 0 \iff x = y$,
- $d(x, y) = d(y, x)$ (symmetry),
- $d(x, z) \leq d(x, y) + d(y, z)$ (triangle inequality).

PROPOSITION 125. If (M, d) is a metric space then $d(x, y) > 0$ for any $x \neq y$.

DEFINITION 126. A norm induces a distance, called the *induced metric*, by $d(x, y) = \|y - x\|$.

PROPOSITION 127. Every normed vector space is a metric space with the induced metric.

COROLLARY 128. \mathbb{R}^n and \mathbb{C}^n are metric spaces.

APPENDIX A

Proofs