Terence Tao Analysis I (Ch. 2 - 5): Outline

Franklin She

January 2024

Contents

1 Natural numbers

1.1 The Peano axioms

Remark. Tao wants us to set aside everything we know about the natural numbers (counting, adding, multiplying, algebra) and start from scratch.

Axiom 1.1. *0 is a natural number.*

Axiom 1.2. *If n is a natural number, then $n++$ is a natural number.*

Definition 1.3. We define 1 to be the number $0++$, 2 to be the number $(0++)++$, and so forth.

Axiom 1.4. 0 *is not the successor of any natural number; i.e., we have $n++ \neq 0$ for every natural number n.*

Remark. This prevents us from having a cycle of natural numbers. E.g. We can prove that $4 \neq 0$ by noting that $4 = 3++ \neq 0$.

Axiom 1.5. *Different natural numbers must have different successors; i.e., if n, m are natural numbers and $n \neq m$, then $n++ \neq m++$. The contrapositive is also useful.*

Axiom 1.6. *Principal of mathematical induction. Let $P(n)$ be any property pertaining to a natural number n. Suppose that $P(0)$ is true, and suppose that whenever $P(n)$ is true, $P(n++)$ is also true. Then $P(n)$ is true for every natural number n.*

Assumption 1.7. *(Informal) There exists a number system $\mathbb{N}$, the natural numbers, that satisfies the Peano axioms.*

Remark. Our definition of the natural numbers is axiomatic rather than constructive. We do not describe what the natural numbers are, but describe the properties they have and what you can do with them. This is how mathematics works, treating objects abstractly, caring only about what properties the objects have, not what the objects are or what they mean.

Proposition 1.8. *(Recursive definitions). Suppose for each natural number n, we have some function $f_n : \mathbb{N} \to \mathbb{N}$. Let c be a natural number. Then we can assign a unique natural number a_n to each natural number n, such that $a_0 = c$ and $a_{n++} = f_n(a_n)$ for each natural number n. For example,*

$$a_3 = f_2(f_1(f_0(c))).$$

Remark. This is proved by induction using Axiom 1.4 for the base case and Axiom 1.5 for the recursive case.

1.2 Addition

Definition 1.9. (Addition of natural numbers). Let m be a natural number. To add 0 to m, we define $0 + m := m$. Now suppose inductively that we have defined how to add n to m. Then we can add $n++$ to m by defining $(n++) + m := (n + m)++$. For example,

$$2+3 = (1++)+3 = (1+3)++ = ((0++)+3)++ = ((0+3)++)++ = (3++)++ = 4++ = 5.$$

Lemma 1.10. *(1) For any natural number n, we have $n + 0 = n$. (2) For any natural numbers n, m, we have $n + (m++) = (n + m)++$. Proven easily by induction.*

Proposition 1.11. *(Addition is commutative). For any natural numbers n, m, we have $n+m = m + n$.*

Proof. We prove this by induction on n. The base case $n = 0$ is trivial. Now suppose inductively that we have proven the claim for n. Then

$$(n++) + m = (n + m)++ = (m + n)++.$$

□

Proposition 1.12. *(Addition is associative). For any natural numbers n, m, k, we have $(n + m) + k = n + (m + k)$. Proved similarly by induction.*

Proposition 1.13. *(Cancellation law). Let a, b, c be natural numbers. Then $a + b = a + c$ implies $b = c$. Proved similarly by induction.*

Definition 1.14. (Positive natural numbers). A natural number n is said to be positive iff $n \neq 0$.

Proposition 1.15. *If a is positive and b is a natural number, then $a + b$ is positive. Proved by induction.*

Definition 1.16. (Ordering of the natural numbers). Let n, m be natural numbers. We say that n is less than or equal to m, and write $n \leq m$, iff we have $n = m + a$ for some natural number a. We say that n is strictly less than m, and write $n < m$, iff $n \leq m$ and $n \neq m$.

Proposition 1.17. *(Basic properties of order for natural numbers). Let a, b, c be natural numbers. Then*

1. *(Reflexivity). $a \leq a$.*
2. *(Transitivity). If $a \leq b$ and $b \leq c$, then $a \leq c$.*
3. *(Anti-symmetry). If $a \leq b$ and $b \leq a$, then $a = b$.*
4. *(Addition preserves order). If $a \leq b$, then $a + c \leq b + c$.*
5. *$a < b$ iff $a++ \leq b$.*
6. *$a < b$ iff $b = a + c$ for some positive natural number c.*

Proof. (1) through (4) are easy. (5) and (6) use contradiction for strict inequality. □

Proposition 1.18. *(Trichotomy of order for natural numbers). Let a, b be natural numbers. Then exactly one of the following statements is true: $a < b$, $a = b$, or $b < a$.*

Proposition 1.19. *(Strong principle of induction). Let m_0 be a natural number, and let $P(m)$ be a property pertaining to an arbitrary natural number m. Suppose that for each $m \geq m_0$, we have the following implication: if $P(m')$ is true for all natural numbers $m_0 \leq m' < m$, then $P(m)$ is also true. (In particular, this means that $P(m_0)$ is true, since in this case the hypothesis is vacuous.) Then we can conclude that $P(m)$ is true for all natural numbers $m \geq m_0$.*

Proof. Skipped. Hint from Tao: define $Q(n)$ to be the property that $P(m)$ is true for all $m_0 \leq m < n$. □

1.3 Multiplication

Remark. Just as addition is the iterated increment operation, multiplication is iterated addition.

Definition 1.20. (Multiplication of natural numbers). Let m be a natural number. To multiple zero to m, we define $0 \times m := 0$. Now suppose inductively that we have defined how to multiply n to m. Then we can multiply $n++$ to m by defining $(n++) \times m := (n \times m) + m$

Lemma 1.21. *(Multiplication is commutative). For any natural numbers n, m, we have $n \times m = m \times n$. Proved by induction.*

Lemma 1.22. *(Positive natural numbers have no zero divisors). Let n, m be natural numbers. Then $n \times m = 0$ iff at least one of n, m is equal to zero.*

Proof. ($\Longrightarrow$) Prove the contrapositive. Suppose $n \neq 0$ and $m \neq 0$. Then $n = a++$ and $m = b++$ for some natural numbers a, b. Then

$$n \times m = (a++) \times (b++) = (a \times b) + a + b + 1.$$

So $n \times m$ is positive. ($\Longleftarrow$) Trivial. □

Proposition 1.23. *(Distributive law). For any natural numbers a, b, c, we have $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$.*

Proof. Since multiplication is commutative, it suffices to prove the first identity. We prove this by induction on c. The base case $c = 0$ is trivial. Now suppose inductively that we have proven the claim for c.

$$\begin{aligned} a(b + (c++)) &= a((b + c)++) \\ &= a(b + c) + a \\ &= ab + ac + a \\ &= ab + a(c++) \end{aligned}$$

.

□

Proposition 1.24. *(Multiplication is associative). For any natural numbers a, b, c, we have $(ab)c = a(bc)$. Proved by induction.*

Proposition 1.25. *(Multiplication preserves order). Let a, b, c be natural numbers. Then $a < b$ implies $ac < bc$.*

Proof. Since $a < b$, we have $b = a + d$ for some positive natural number d. Then

$$bc = (a + d)c = ac + dc.$$

Since dc is positive, we have $ac < bc$. □

Corollary 1.26. *(Cancellation law). Let a, b, c be natural numbers. Then $ac = bc$ and $c \neq 0$ implies $a = b$.*

Proof. By trichotomy of order, we have $a < b$ or $a = b$ or $b < a$. If $a < b$, then $ac < bc$, a contradiction. If $b < a$, then $bc < ac$, a contradiction. So $a = b$. □

Proposition 1.27. *(Euclidean algorithm). Let n be a natural number, and let q be a positive natural number. Then there exists natural numbers m, r such that $0 \leq r < q$ and $n = mq + r$.*

Remark. In other words, we can divide n by q and get a quotient m and remainder r.

Proof. Let us fix q and induct on n. The base case n is solved when we take $m = 0$ and $r = n$. Now suppose inductively that we have solved the claim for n. Then $n = mq + r$ for some natural numbers m, r with $0 \leq r < q$. For the recursive case, we have two cases. TO BE CONTINUED. □

Definition 1.28. (Exponentiation for natural numbers). Let m be a natural number. To raise m to the power zero, we define $m^0 := 1$. Now suppose inductively that we have defined m^n. Then we can define $m^{n++} := m^n \times m$.

Remark. Just like one uses the increment operation to recursively define addition, and addition to recursively define multiplication, one can use multiplication to recursively define exponentiation.

2 Set theory

2.1 Fundamentals

Definition 2.1. (Informal) We define a set A to be any unordered collection of objects. If x is an object, we say $x \in A$, otherwise, $x \notin A$.

Axiom 2.2. *(Sets are objects). If A is a set, then A is also an object.*

Remark. There is a special case of set theory called "pure set theory" in which all objects are sets. The number 0 is identified with the empty set $\emptyset = \{\}$, the number 1 as $\{0\} = \{\{\}\}$, the number 2 as $\{0, 1\} = \{\{\}, \{\{\}\}\}$, and so on.

Definition 2.3. (Equality of sets). Two sets A, B are equal iff every element of A is an element of B, and vice versa.

Axiom 2.4. *(Empty set). There exists a set $\emptyset$, also denoted as $\{\}$ such that for every object x, we have $x \notin \emptyset$.*

Lemma 2.5. *(Single choice). Let A be a non-empty set. Then there exists an object x such that $x \in A$.*

Proof. We prove by contradiction. Suppose that for every object x, we have $x \notin A$. Then $A = \emptyset$, a contradiction. □

Axiom 2.6. *(Singleton sets and pair sets). If a is an object, then there exists a set $\{a\}$ such that for every object x, we have $x \in \{a\}$ iff $x = a$. Furthermore, if a, b are objects, then there exists a set $\{a, b\}$ such that for every object x, we have $x \in \{a, b\}$ iff $x = a$ or $x = b$; we refer to this set as the pair set formed by a and b.*

Axiom 2.7. *(Pairwise union). Given any two sets A, B, there exists a set $A \cup B$, called the union of A and B, such that for every object x, we have $x \in A \cup B$ iff $x \in A$ or $x \in B$.*

Lemma 2.8. *(Union is commutative and associative). Let A, B, C be sets. Then $A \cup B = B \cup A$ and $(A \cup B) \cup C = A \cup (B \cup C)$. Simple proof.*

Definition 2.9. (Subsets). Let A, B be sets. We say that A is a subset of B, and write $A \subseteq B$, iff every element of A is also an element of B. We say that A is a proper subset of B, denoted $A \subset B$ if $A \subseteq B$ and $A \neq B$.

Proposition 2.10. *(Sets are partially ordered by set inclusion). Let A, B, C be sets. If $A \subseteq B$ and $B \subseteq C$ (also hold for $\subset$). If $A \subseteq B$ and $B \subseteq A$, then $A = B$.*

Remark. Given two distinct sets, it is not in general true that one of them is a subset of the other. Take the set of even natural numbers and the set of odd natural numbers. Neither set is a subset of the other. This is why we say that sets are only partially ordered.

Axiom 2.11. *(Axiom of specification). Let A be a set, and for each $x \in A$, let $P(x)$ be a property pertaining to x (i.e., $P(x)$ is either a true statement or a false statement). Then there exists a set $\{x \in A : P(x) \text{ is true}\}$, such that for every object y,*

$$y \in \{x \in A : P(x) \text{ is true}\} \iff (y \in A \text{ and } P(y) \text{ is true}).$$

Definition 2.12. (Intersections). The intersection of two sets A, B, denoted $A \cap B$, is defined to be the set

$$A \cap B := \{x \in A : x \in B\}.$$

Also, for all objects x,

$$x \in A \cap B \iff x \in A \text{ and } x \in B.$$

Definition 2.13. (Empty intersection). We say that two sets A, B are disjoint iff $A \cap B = \emptyset$.

Definition 2.14. (Difference sets). Given two sets A, B, we define the difference set $A \setminus B$ to be the set

$$A \setminus B := \{x \in A : x \notin B\}.$$

Proposition 2.15. *(Sets form a boolean algebra). Let A, B, C be sets, and let X be a set containing A, B, C as subsets.*

1. *(Minimal element). $A \cup \emptyset = A$ and $A \cap \emptyset = \emptyset$.*
2. *(Maximal element). $A \cup X = X$ and $A \cap X = A$.*
3. *(Identity). $A \cup A = A$ and $A \cap A = A$.*
4. *(Commutativity). $A \cup B = B \cup A$ and $A \cap B = B \cap A$.*
5. *(Associativity). $(A \cup B) \cup C = A \cup (B \cup C)$ and $(A \cap B) \cap C = A \cap (B \cap C)$.*
6. *(Distributivity). $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ and $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.*
7. *(Partition). $A \cup (X \setminus A) = X$ and $A \cap (X \setminus A) = \emptyset$.*
8. *(De Morgan laws). $X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B)$ and $X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B)$.*

Proof. TODO. □

Axiom 2.16. *(Replacement). Let A be a set. For any object $x \in A$, and any object y, suppose we have a statement $P(x, y)$ pertaining to x and y, such that for each $x \in A$ there is at most one y for which $P(x, y)$ is true. Then there exists a set $\{y : P(x, y) \text{ is true for some } x \in A\}$, such that for any object z,*

$$z \in \{y : P(x, y) \text{ is true for some } x \in A\} \iff P(x, z) \text{ is true for some } x \in A.$$

Definition 2.17. (Infinity). There exists a set $\mathbb{N}$, whose elements are called natural numbers, as well as an object $0 \in \mathbb{N}$, and an object $n++ \in \mathbb{N}$ assigned to every natural number $n \in \mathbb{N}$, such that the Peano axioms are satisfied.

Remark. Tao remarks that this is a more formal version of the definition of the natural numbers in the previous chapter. I am not sure exactly why.

2.2 Russell's paradox

Axiom 2.18. *(Universal specification). (Dangerous!) Suppose for every object x, we have a statement $P(x)$ pertaining to x (i.e., $P(x)$ is either a true statement or a false statement). Then there exists a set $\{x : P(x)$ is true$\}$, such that for every object y,*

$$y \in \{x : P(x) \text{ is true}\} \iff P(y) \text{ is true}.$$

Remark. This axiom asserts that every property corresponds to a set. It also implies most of the axioms in the previous section. This axiom cannot be included into set theory because of the following logical contradiction.

Remark. Discovered by Betrand Russell (1872 - 1970) in 1901. The paradox runs as follows. Let $P(x)$ be the statement

$$P(x) \iff x \text{ is a set and } x \notin x.$$

Using the axiom of universal specification, we can form the set

$$R := \{x : P(x) \text{ is true}\} = \{x : x \text{ is a set and } x \notin x\}.$$

Now we ask the question: is $R \in R$? If $R \in R$, then by the definition of P, we have $R \notin R$. If $R \notin R$, then by the definition of P, we have $R \in R$. This is a contradiction.

Axiom 2.19. *(Regularity). If A is a non-empty set, then there exists at least one element x of A which is either not a set, or is disjoint from A.*

Remark. This axiom is also known as the axiom of foundation and ensures absurdities such as Russell's paradox do not occur. However, it is pretty unintuitive, and never needed for analysis. It is necessary for more advanced set theory.

2.3 Functions

Definition 2.20. (Functions). Let X, Y be sets. A function f from X to Y, denoted $f : X \to Y$, is defined to be a set of ordered pairs (x, y) with $x \in X$ and $y \in Y$, such that every element of X appears in exactly one ordered pair. We write $f(x)$ for the unique y such that $(x, y) \in f$. We call X the domain of f and Y the range of f. We write $f : X \to Y$ to indicate that f is a function from X to Y.

Definition 2.21. (Equality of functions). Two functions $f : X \to Y$ and $g : X \to Y$ are equal iff $f(x) = g(x)$ for all $x \in X$.

Definition 2.22. (Composition). Let $f : X \to Y$ and $g : Y \to Z$ be functions. Then we can define the composition $g \circ f : X \to Z$ of f and g to be the function from X to Z defined by the formula

$$(g \circ f)(x) := g(f(x)).$$

Lemma 2.23. *(Composition is associative). Let $f : X \to Y$, $g : Y \to Z$, and $h : Z \to W$ be functions. Then $h \circ (g \circ f) = (h \circ g) \circ f$.*

Proof. Proved by the definition of composition and equality of functions. □

Definition 2.24. (One-to-one functions). Let $f : X \to Y$ be a function. We say that f is one-to-one, or injective, iff $f(x) = f(y)$ implies $x = y$ for all $x, y \in X$.

Definition 2.25. (Onto functions). Let $f: X \to Y$ be a function. We say that f is onto, or surjective, iff $f(X) = Y$. That is, for every $y \in Y$, there exists $x \in X$ such that $f(x) = y$.

Definition 2.26. (Bijections). Let $f: X \to Y$ be a function. We say that f is a bijection iff f is both one-to-one and onto.

Definition 2.27. (Identity functions). Let X be a set. We define the identity function $\mathrm{id}_X: X \to X$ to be the function $\mathrm{id}_X(x) := x$.

Definition 2.28. (Inverse functions). Let $f: X \to Y$ be a function. We say that f is invertible iff there exists a function $g: Y \to X$ such that $g \circ f = \mathrm{id}_X$ and $f \circ g = \mathrm{id}_Y$. We call g the inverse of f, and denote it by f^{-1}.

Remark. If f is invertible, then f is a bijection. The converse is also true.

2.4 Images and inverse images

Definition 2.29. (Images of sets). If $f: X \to Y$ is a function, and E is a set in X, we define the image $f(E)$ of E under f to be the set

$$f(E) := \{f(x): x \in E\}.$$

This set is a subset of Y. $f(E)$ is also called the forward image of E under f.

Definition 2.30. (Inverse images). If U is a subset of Y, we define the inverse image $f^{-1}(U)$ of U under f to be the set

$$f^{-1}(U) := \{x \in X: f(x) \in U\}.$$

$f^{-1}(U)$ is also called the backwards images of U under f.

Definition 2.31. (Power set axiom). Let X and Y be sets. Then there exists a set Y^X, called the power set of X into Y, which consists of all the functions from X to Y, thus

$$f \in Y^X \iff f: X \to Y.$$

Lemma 2.32. *Let X be a set. Then the set*

$$\{Y: Y \text{ is a subset of } X\}.$$

is a set.

Proof. TODO. Exercise 3.4.6. □

Axiom 2.33. *(Union). Let A be a set, all of whose elements are themselves sets. Then there exists a set $\bigcup A$, called the union of A, which consists of all the elements which belong to at least one element of A, thus*

$$x \in \bigcup A \iff x \in Y \text{ for some } Y \in A.$$

Remark. We can similarly form intersections of families of sets.

2.5 Cartesian products

Definition 2.34. (Ordered pair). If x and y are any objects (possibly equal), we define the ordered pair (x, y) to be a new object. Two ordered pairs (x, y) and (x', y') are equal if and only if the following holds:

$$x = x' \text{ and } y = y'.$$

Definition 2.35. (Cartesian product). If X and Y are sets, we define the Cartesian product $X \times Y$ to be the set of all ordered pairs (x, y) with $x \in X$ and $y \in Y$, thus

$$X \times Y := \{(x, y) : x \in X \text{ and } y \in Y\}.$$

or equivalently,

$$(x, y) \in X \times Y \iff x \in X \text{ and } y \in Y.$$

Definition 2.36. (Ordered n-tuple and n-fold Cartesian product). If n is a natural number, we define an ordered n-tuple to be a function from the set $\{1, \ldots, n\}$ of natural numbers from 1 to n to some set X. We denote this ordered n-tuple by $(x_1, \ldots, x_n)$ or $(x_i)_{1 \leq i \leq n}$. Two ordered n-tuples are equal if and only if they agree at every index. We define the n-fold Cartesian product $X_1 \times \cdots \times X_n$ to be the set of all ordered n-tuples $(x_1, \ldots, x_n)$ with $x_i \in X_i$ for each $i = 1, \ldots, n$, thus

$$X_1 \times \cdots \times X_n := \{(x_1, \ldots, x_n) : x_i \in X_i \text{ for each } i = 1, \ldots, n\}.$$

Remark. Any ordered n-tuple $(x_1, \ldots, x_n)$ is also called an ordered sequence of n elements or a finite sequence.

Lemma 2.37. *(Finite choice). Let $n \geq 1$ be a natural number, and for each natural number $1 \leq i \leq n$, let X_i be a non-empty set. Then the Cartesian product $X_1 \times \cdots \times X_n$ is non-empty.*

Proof. We can prove this via induction on n. The claim is vacuously true with $n = 0$, and when $n = 1$ the claim follows from the single choice lemma. □

Remark. The infinite choice lemma requires an additional axiom, the axiom of choice.

2.6 Cardinality of sets

Remark. Tao remarks how defining the natural numbers axiomatically via the Peano axioms treats natural numbers like ordinals (First, Second, Third) rather than cardinals (One, Two Three). Cardinality of sets notes that the natural numbers can be used to count the cardinality of sets, as long as the set is finite.

Definition 2.38. (Equal cardinality). Two sets X and Y have equal cardinality iff there exists a bijection $f : X \to Y$.

Proposition 2.39. *(Equal cardinality is commutative and transitive). Let X, Y, Z be sets. If X and Y have equal cardinality, then Y and X have equal cardinality. If X and Y have equal cardinality, and Y and Z have equal cardinality, then X and Z have equal cardinality.*

Proof. Proved by the definition of equal cardinality. □

Definition 2.40. (Cardinality n). Let n be a natural number. A set X is said to have cardinality n iff it has equal cardinality to $\{1, \ldots, n\}$. We write $|X| = n$ to denote the fact that X has cardinality n and we also say that X has n elements.

Proposition 2.41. *(Uniqueness of cardinality). Let X be a set with cardinality n. Then n is unique. That is, if m is a natural number such that X has cardinality m, then $n = m$.*

This proposition needs to following lemma to be proved.

Lemma 2.42. *Suppose that $n \geq 1$ and that X is a set with cardinality n. Then there exists an element $x \in X$ such that $X \setminus \{x\}$ has cardinality $n - 1$.*

Proof. Proof idea. We find the bijection from $X \setminus \{x\}$ to $\{1, \ldots, n-1\}$ by taking the bijection from X to $\{1, \ldots, n\}$, call it $f(y)$ and defining a $g(y) = f(y) - 1$ if $f(y) > f(x)$. Intuitively these are the elements "after" the x that was removed, and we shift them down by 1. □

Proof. (of uniqueness of cardinality). We induct on n. For $n = 0$, the claim is true because X must be empty. Now suppose the proposition is already proven for some n. To prove true for $n++$, suppose for contradiction that X has cardinality $n++$ and m, where $n++ \neq m$. By the above lemma, we have that set $X \setminus \{x\}$ has cardinality n and $m - 1$. By the inductive hypothesis, $n = m - 1$, which implies that $n++ = m$, a contradiction. □

Definition 2.43. (Finite sets). A set is finite iff it has cardinality n for some natural number n. A set is infinite iff it is not finite.

Theorem 2.44. *The set of natural numbers $\mathbb{N}$ is infinite.*

Proof. Suppose for contradiction that $\mathbb{N}$ is finite. Then $\mathbb{N}$ has some cardinality n. By the previous lemma, there exists an element $x \in \mathbb{N}$ such that $\mathbb{N} \setminus \{x\}$ has cardinality $n - 1$. But $\mathbb{N} \setminus \{x\}$ is a subset of $\mathbb{N}$, so it has cardinality at most n. This is a contradiction. □

Remark. One can use similar arguments to show that any unbounded set is infinite. However, it is possible for some sets to be "more" infinite than others.

Proposition 2.45. *(Cardinal arithmetic).*

1. *Let X be a finite set, and let $x \notin X$ be an object. Then $X \cup \{x\}$ is finite and $|X \cup \{x\}| = |X| + 1$.*
2. *Let X and Y be finite sets. Then $X \cup Y$ is finite and $|X \cup Y| \leq |X| + |Y|$. If X and Y are disjoint, then $|X \cup Y| = |X| + |Y|$.*
3. *Let X be a finite set and let Y be a subset of X. Then Y is finite and $|Y| \leq |X|$. If Y is also infinite, then $|Y| < |X|$. If $Y \neq X$, then $|Y| < |X|$.*
4. *If X is a finite set and $f : X \to Y$ is a function. Then $f(X)$ is finite and $|f(X)| \leq |X|$. If f is one-to-one, then $|f(X)| = |X|$.*
5. *Let X and Y be finite sets. Then $X \times Y$ is finite and $|X \times Y| = |X| \times |Y|$.*
6. *Let X and Y be finite sets. Then Y^X is finite and $|Y^X| = |Y|^{|X|}$.*

Proof. TODO. □

Remark. This proposition suggests cardinality is a form of arithmetic, distinct from the Peano arithmetic.

3 Integers and rationals

3.1 Integers

Remark. Tao chooses to define integers by subtracting two natural numbers.

Definition 3.1. (Integers). An integer is an expression of the form $a - b$ where a, b are natural numbers. Two integers are considered to be equal $a - b = c - d$ iff $a + d = c + b$. We let $\mathbb{Z}$ denote the set of all integers.

Remark. We have to check if integer equality is a legitimate notion of equality by verifying the reflexive, symmetric, and transitive and substitution axioms.

Definition 3.2. The sum of two integers $(a - b) + (c - d)$ is defined by the formula

$$(a - b) + (c - d) := (a + c) - (b + d).$$

The product of two integers $(a - b)(c - d)$ is defined by the formula

$$(a - b)(c - d) := (ac + bd) - (ad + bc).$$

Lemma 3.3. *(Addition and multiplication are well-defined). The sum and product of two integers are integers and equal inputs give equal outputs.*

Definition 3.4. (Negation of integers) If $a-b$ is an integer, we define its negation $-(a-b)$ by the formula

$$-(a - b) := (b - a).$$

In particular, we define $-a := 0 - a$ for any positive natural number a.

Lemma 3.5. *(Trichotomy of integers). Let x be an integer. Then exactly one of the following three statements is true: x is positive, x is zero, or x is negative.*

Proof. Proof idea. By definition, $x = a - b$ for some natural numbers a, b. Then x is positive if $a > b$, zero if $a = b$, and negative if $a < b$. To show that no more than one hold at a time, we assume each pair and reach a contradiction. □

Remark. Tao comments why we didn't just use this lemma to define the integers. The reason is that if we did so, the rules for adding and multiplying would split into many different cases, e.g., negative times positive equals negative. To verify all the properties would end up being much messier.

Proposition 3.6. *(Laws of algebra for integers). Let x, y, z be integers. Then*

1. *(Additive commutativity). $x + y = y + x$ and $xy = yx$.*
2. *(Additive associativity). $(x + y) + z = x + (y + z)$ and $(xy)z = x(yz)$.*
3. *(Additive identity). $x + 0 = x$.*
4. *(Additive inverse). $x + (-x) = 0$.*
5. *(Multiplicative commutativity). $xy = yx$.*
6. *(Multiplicative associativity). $(xy)z = x(yz)$.*

7. *(Multiplicative identity).* $x \times 1 = x$.

8. *(Distributivity 1).* $x(y+z) = xy + xz$.

9. *(Distributivity 2).* $(y+z)x = yx + zx$.

Remark. The above set of nine identities assert that the integers form a commutative ring.

Proof. These are proven by the definition of integer and the use of algebra of the natural numbers. □

Definition 3.7. (Subtraction). If x, y are integers, we define $x - y$ to be $x + (-y)$.

Proposition 3.8. *(Integers have no zero divisors). Let x, y be integers. If $xy = 0$, then $x = 0$ or $y = 0$.*

Proof. Suppose for contradiction that $x \neq 0$ and $y \neq 0$. Then $x = a - b$ and $y = c - d$ for some positive natural numbers a, b, c, d. Then $xy = (a-b)(c-d) = ac + bd - ad - bc$. Since a, b, c, d are positive, we have $ac, bd, ad, bc > 0$. So $ac + bd - ad - bc > 0$, a contradiction. □

Corollary 3.9. *(Cancellation law). Let x, y, z be integers. If $x \neq 0$ and $xy = xz$, then $y = z$.*

Proof. If $y \neq z$, then $y - z \neq 0$. Then $x(y-z) = xy - xz = 0$, a contradiction. □

Definition 3.10. (Ordering of the integers.) Let x, y be integers. We say that x is greater than or equal to y, and write $x \geq y$ or $y \leq x$ iff we have $x = y + a$ for some natural number a. We say that x is strictly greater than y, and write $x > y$ or $y < x$ iff $x \geq y$ and $x \neq y$.

Lemma 3.11. *(Properties of order). Let a, b, c be integers.*

1. *$a > b$ iff $a - b$ is positive.*

2. *(Addition preserves order). If $a > b$, then $a + c > b + c$.*

3. *(Positive multiplication preserves order). If $a > b$ and c is positive, then $ac > bc$.*

4. *(Negation reverses order). $a > b$ iff $-a < -b$.*

5. *(Order is transitive). If $a > b$ and $b > c$, then $a > c$.*

6. *(Order trichotomy). Exactly one of the following statements is true: $a > b$, $a = b$, or $a < b$.*

Proof. TODO. □

3.2 Rationals

Definition 3.12. (Rationals). A rational number is an expression of the form a/b where a, b are integers and b is positive. Two rational numbers a/b and c/d are considered to be equal iff $ad = bc$. We let $\mathbb{Q}$ denote the set of all rational numbers.

Remark. Again, we have to check if rational equality is a legitimate notion of equality by verifying the reflexive, symmetric, and transitive and substitution axioms.

Definition 3.13. (Sum of rationals). If a/b and c/d are rational numbers, we define their sum $(a/b) + (c/d)$ by the formula

$$(a/b) + (c/d) := (ad + bc)/(bd).$$

their product

$$(a/b)(c/d) := (ac)/(bd).$$

and their negation

$$-(a/b) := (-a)/b.$$

Lemma 3.14. *(Sum, product, and negation are well-defined). The sum, product, and negation of two rational numbers are rational numbers and equal inputs give equal outputs.*

Proof. Proof idea. We show that supposing $a/b = a'/b'$ and $c/d = c'/d'$, then $(ad + bc)/(bd) = (a'd' + b'c')/(b'd')$ and $(ac)/(bd) = (a'c')/(b'd')$. We also show that $(-a)/b = (-a')/b'$. □

Proposition 3.15. *(Laws of algebra for rationals). Let x, y, z be rational numbers. Then*

1. *(Additive commutativity). $x + y = y + x$ and $xy = yx$.*
2. *(Additive associativity). $(x + y) + z = x + (y + z)$ and $(xy)z = x(yz)$.*
3. *(Additive identity). $x + 0 = x$.*
4. *(Additive inverse). $x + (-x) = 0$.*
5. *(Multiplicative commutativity). $xy = yx$.*
6. *(Multiplicative associativity). $(xy)z = x(yz)$.*
7. *(Multiplicative identity). $x \times 1 = x$.*
8. *(Distributivity 1). $x(y + z) = xy + xz$.*
9. *(Distributivity 2). $(y + z)x = yx + zx$.*
10. *(Multiplicative inverse). If $x \neq 0$, then $1/x$ is also a rational number and $x(1/x) = 1$.*

Remark. The above set of ten identities assert that the rationals $\mathbb{Q}$ form a field.

Proof. Proved by the definition of rational number and the use of algebra of the integers. □

Definition 3.16. (Quotient of rationals). If x, y are rational numbers, we define x/y to be $x \times (1/y)$.

Definition 3.17. (Positive and negative rationals). A rational number x is positive iff $x = a/b$ for some positive integers a, b. It is negative iff $x = -y$ for some positive rational y.

Lemma 3.18. *(Trichotomy of rationals). Let x be a rational number. Then exactly one of the following three statements is true: x is positive, x is zero, or x is negative.*

Proof. Similar to the proof of the trichotomy of integers. (I think.) □

Definition 3.19. (Ordering of the rationals). Let x, y be rational numbers. We say that $x > y$ iff $x - y$ is positive. We say that $x \geq y$ iff $x > y$ or $x = y$. We say that $x < y$ iff $x - y$ is a negative, and similarly define $x \leq y$.

Proposition 3.20. *(Basic properties of order on the rationals). Let x, y, z be rational numbers. Then*

1. *(Order trichotomy). Exactly one of the following statements is true: $x > y$, $x = y$, or $x < y$.*
2. *(Order antisymmetry). If $x > y$, then $y < x$.*
3. *(Order transitivity). If $x > y$ and $y > z$, then $x > z$.*
4. *(Addition preserves order). If $x > y$, then $x + z > y + z$.*
5. *(Positive multiplication preserves order). If $x > y$ and z is positive, then $xz > yz$.*

Proof. TODO. □

3.3 Absolute value and exponentiation

Definition 3.21. (Absolute value). Let x be a rational number. If x is positive, then the absolute value of x is defined as $|x| := x$. If x is negative, then $|x| := -x$. If x is zero, then $|x| := 0$.

Definition 3.22. (Distance). Let x, y be rational numbers. We define the distance between x and y to be $|x - y|$. Distance is sometimes denoted as $d(x, y)$.

Proposition 3.23. *(Basic properties of absolute value and distance). Let x, y, z be rational numbers. Then*

1. *(Non-degeneracy of absolute value). $|x| \geq 0$ and $|x| = 0$ iff $x = 0$.*
2. *(Triangle inequality for absolute value). $|x + y| \leq |x| + |y|$.*
3. *$-y \leq x \leq y$ iff $y \geq |x|$. In particular, $-|x| \leq x \leq |x|$.*
4. *(Multiplicative identity for absolute value). $|xy| = |x||y|$. In particular, $|x^n| = |x|^n$ for any natural number n.*
5. *(Non-degeneracy of distance). $d(x, y) \geq 0$ and $d(x, y) = 0$ iff $x = y$.*
6. *(Symmetry of distance). $d(x, y) = d(y, x)$.*
7. *(Triangle inequality for distance). $d(x, z) \leq d(x, y) + d(y, z)$.*

Proof. TODO. □

Definition 3.24. (ϵ-closeness). Let x, y be rational numbers, and let ϵ be a positive rational number. We say that x is ϵ-close to y iff $d(x, y) \leq \epsilon$.

Remark. Tao remarks that this definition is not standard in mathematics textbooks, but we plan to use it as "scaffolding" to construct more important notions of limit (and of Cauchy sequences) and discard the notion of ϵ-close.

Proposition 3.25. *Let x, y, z, w be rational numbers and let ϵ, γ be positive rational numbers. Then*

1. *$x = y$ iff x is ϵ-close to y.*
2. *If x is ϵ-close to y, then y is ϵ-close to x.*
3. *If x is ϵ-close to y and y is γ-close to z, then x is $(\epsilon + \gamma)$-close to z.*
4. *If x and y are ϵ-close, and z and w are γ-close, then $x + z$ and $y + w$ are $(\epsilon + \gamma)$-close, and $x - z$ and $y - w$ are $(\epsilon + \gamma)$-close.*
5. *If x and y are ϵ-close, they are also ϵ'-close for any $\epsilon' > \epsilon$.*
6. *There are a few more, but I'm not going to write them down. See page 88 of Tao.*

Definition 3.26. (Exponentiation to a natural number). Let x be a rational number. To raise x to the power 0, we define $x^0 := 1$. To raise x to the power $n + 1$, we define $x^{n+1} := x^n \times x$.

Proposition 3.27. *(Properties of exponentiation, I). Let x, y be rational numbers and let m, n be natural numbers. Then*

1. *$x^m x^n = x^{m+n}$, $(x^m)^n = x^{mn}$, and $(xy)^n = x^n y^n$.*
2. *Suppose $n > 0$. Then $x^n = 0$ iff $x = 0$.*
3. *If $x \geq y \geq 0$, then $x^n \geq y^n \geq 0$. If $x > y \geq 0$ and $n > 0$, then $x^n > y^n \geq 0$*
4. *$|x^n| = |x|^n$.*

Proof. TODO. □

Definition 3.28. (Exponentiation to a negative number). Let x be a non-zero rational number. Then for any negative integer $-n$, we define $x^{-n} := 1/x^n$.

3.4 Gaps in the rational numbers

Proposition 3.29. *(Interspersing of integers by rationals). Let x be a rational number. Then there exists an integer n such that $n \leq x < n + 1$. In fact, this integer is unique. In particular, there exists a natural number N such that $N > x$ (i.e., there is no such thing as a rational number which is larger than all the natural numbers).*

Remark. The integer n for which $n \leq x < n + 1$ is called the integer part of x, and is denoted $\lfloor x \rfloor$. The natural number N for which $N > x$ is called the ceiling of x, and is denoted $\lceil x \rceil$.

Proof. TODO. □

Proposition 3.30. *(Interspersing of rationals by integers). If x and y are rational numbers with $x < y$, then there exists an integer n such that $x < n < y$.*

Proof. Proof idea. We set $n := (x + y)/2$. □

Proposition 3.31. *There does not exist any rational number x such that $x^2 = 2$.*

Proof. TODO. See page 91 of Tao. □

Proposition 3.32. *For every rational number $\epsilon > 0$, there exists a non-negative rational number x such that $x^2 < 2 < (x + \epsilon)^2$.*

Proof. TODO. □

Remark. This proposition indicates that while the set of rationals does not actually have $\sqrt{2}$, we can get as close as we wish to $\sqrt{2}$. This is how Tao decides to construct the real numbers in the next chapter. There is another way, via "Dedekind cuts", but it is not pursued here.

4 Real numbers

Remark. So far, we constructed three number systems, the natural numbers $\mathbb{N}$, the integers $\mathbb{Z}$, and the rationals $\mathbb{Q}$. Natural numbers were defined using the Peano axioms and were used to recursively define addition and multiplication. Integers were constructed by taking formal differences of natural numbers. Rationals were constructed by taking formal quotients of the integers.

Real numbers are needed for geometry and by extension, calculus. They are constructed by taking limits of rational numbers. This is a very general and useful procedure, that of completing one metric space to form another.

4.1 Cauchy sequences

Definition 4.1. (Sequences). Let m be an integer. A sequence $(a_n)_{n=m}^{\infty}$ of rational numbers is a function from the set $\{n \in \mathbb{Z} : n \geq m\}$ of integers from m to ∞ to the rationals. We denote the value of this function at n by a_n. More informally, a sequence $(a_n)_{n=m}^{\infty}$ of rational numbers is a collection of rationals $a_m, a_{m+1}, a_{m+2}, \ldots$.

Definition 4.2. (ϵ-steadiness). Let $\epsilon > 0$. A sequence $(a_n)_{n=m}^{\infty}$ of rational numbers is said to be ϵ-steady iff each pair a_j, a_k of sequence elements is ϵ-close for every natural number j, k.

Definition 4.3. (Eventual ϵ-steadiness). Let $\epsilon > 0$. A sequence $(a_n)_{n=m}^{\infty}$ of rational numbers is said to be eventually ϵ-steady iff there exists a natural number N such that the sequence $(a_n)_{n=N}^{\infty}$ is ϵ-steady.

Definition 4.4. (Cauchy sequences). A sequence $(a_n)_{n=m}^{\infty}$ of rational numbers is said to be Cauchy iff it is eventually ϵ-steady for every rational number $\epsilon > 0$.

Proposition 4.5. *The sequence defined by $a_n := 1/n$ is a Cauchy sequence.*

Proof. We want to find $N \geq 1$ such that the sequence $a_N, a_{N+1}, \ldots$ is ϵ-steady. That is to say, find N where

$$|1/j - 1/k| \leq \epsilon \text{ for every } j, k \geq N.$$

Because $j, k \geq N$, we know that $0 < 1/j, 1/k \leq 1/N$. This also means that $|1/j - 1/k| \leq 1/N$. So it is sufficient to show that $1/N < \epsilon$, or in other words $N > 1/\epsilon$. We can construct such a N by Proposition 3.29 (Interspersing of integers by rationals), specifically that there exists a natural number N such that $N > x$, where x is a rational number. □

Remark. Verifying from first principles that a sequence is a Cauchy sequence requires thinking in reverse, working out what conditions on N would suffice to force the sequence to be ϵ-steady and then finding such an N.

Definition 4.6. (Bounded sequences). Let $M \geq 0$ be rational. A finite sequence is bounded by M iff $|a_i| \leq M$ for every i. An infinite sequence is bounded by M iff $|a_i| \leq M$ for all $i \geq 1$. A sequence is said to be bounded iff it is bounded by M for some rational $M \geq 0$.

4.2 Equivalent Cauchy sequences

4.3 The construction of the real numbers

4.4 Ordering the reals

4.5 The least upper bound property

4.6 Real exponentiation, part 1