Introduction to Mathematical Reasoning Course Notes

Jeffrey Diller
Department of Mathematics
University of Notre Dame
Notre Dame, IN 46555
email: diller.1@nd.edu

January 25, 2012

Abstract

Following are some bare-bones course notes for Math 20630 at Notre Dame. These are not intended to replace a textbook as they include little informal discussion, few examples, and no exercises. Rather, they are intended to bridge the gap between a textbook and my lectures. Despite the skeletal nature of the work, I'd like to see it improved and would welcome any comments and suggestions to that end.

1 Integer Arithmetic

We begin with the integers, i.e. the numbers

$$\ldots, -2, -1, 0, 1, 2, \ldots$$

that you get by starting with zero and proceeding forward or backward in increments of one. We use the boldface letter $\mathbf{Z}$ to denote the set of all integers. Arithmetic with integers is something you've been familiar with for years. It's as likely as not that you can't remember *not* knowing how to add or multiply two integers together. Nevertheless, since you learned these things at an early age, you might never have given them much further thought. We do this now. All the facts about multiplication and division of integers proceed from eight basic rules, which in higher mathspeak are known as the (brace yourself) *axioms for a commutative ring with unit.* We'll just call them the *axioms for arithmetic.*

Concerning addition we have four axioms.

A1 (Commutative law for addition) for all $x, y \in \mathbf{Z}$, $x + y = y + x$.

A2 (Associative law for addition) for all $x, y, z \in \mathbf{Z}$, $(x + y) + z = x + (y + z)$.

A3 (Existence of an additive identity) there is an element $0 \in \mathbf{Z}$ such that for all $x \in \mathbf{Z}$, $x + 0 = x$.

A4 (Existence of additive inverses) for each $x \in \mathbf{Z}$ there is an element $-x \in \mathbf{Z}$ such that $x + (-x) = 0$.

And for multiplication we have three axioms, analogous to the first three for addition.

M1 (Commutative law for multiplication) for all $x, y \in \mathbf{Z}$, $x \cdot y = y \cdot x$.

M2 (Associative law for multiplication) for all $x, y, z \in \mathbf{Z}$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

M3 (Existence of a multiplicative identity) there exists an element $1 \in \mathbf{Z}$ different from 0 and such that for all $x \in \mathbf{Z}$, $x \cdot 1 = x$.

There is a single axiom that relates multiplication and addition.

D (Distributive Law) For all $x, y, z \in \mathbf{Z}$, $x \cdot (y + z) = x \cdot y + x \cdot z$.

And finally, there is an axiom guaraneteeing that the integers consist of more than just the number 0.

N (Non-triviality) $0 \neq 1$.

Of course, there are lots of familiar facts about arithmetic that didn't make it into the list above. We'll get to those shortly. Before proceeding, though, we comment about another omission you might have noticed: subtraction and division are absent from the above list. Subtraction isn't mentioned because it's not really an independent operation. When we write '$a - b$', it's really just shorthand for '$a + (-b)$' (see A4 above). Hence from a logical point of view, there's no need for a separate discussion of subtraction. Division is a more complicated thing, since properly speaking division isn't an operation at all when it comes to integers. Nevertheless, we'll spend much time discussing division later. For now, we skip this thorny issue.

Other facts about arithmetic needn't be stated as axioms. Rather, they can be *deduced* logically from the axioms given above. Here, we present two examples of this, leaving several others to you as exercises.

Proposition 1.1 *For every $x \in \mathbf{Z}$, we have $0 \cdot x = x \cdot 0 = 0$.*

Proof. Let $x \in \mathbf{Z}$ be given. Then

$$\begin{aligned} x \cdot 0 + x \cdot 0 &= x \cdot (0+0) && \text{(by AM)} \\ &= x \cdot 0 && \text{(by A3).} \end{aligned}$$

By axiom A4 there is an additive inverse $-(x \cdot 0)$ for $x \cdot 0$. Using this inverse, we resume where we left off.

$$\begin{array}{lrcll} & x \cdot 0 + x \cdot 0 &=& x \cdot 0 & \\ \Rightarrow & (x \cdot 0 + x \cdot 0) + -(x \cdot 0) &=& x \cdot 0 + -(x \cdot 0) & \text{(because addition is well-defined)} \\ \Rightarrow & x \cdot 0 + (x \cdot 0 + -(x \cdot 0)) &=& x \cdot 0 + -(x \cdot 0) & \text{(by A2)} \\ \Rightarrow & x \cdot 0 + 0 &=& 0 & \text{(by A4)} \\ \Rightarrow & x \cdot 0 &=& 0 & \text{(by A3)} \\ \Rightarrow & 0 \cdot x &=& 0 & \text{(by A1).} \end{array}$$

So $x \cdot 0 = 0 \cdot x = 0$, as claimed. □

The next proposition requires a definition.

Definition 1.2 *We say that $y \in \mathbf{Z}$ is an* additive idenitity *if for all integers $x \in \mathbf{Z}$, we have $x + y = x$.*

Observe that by axiom A3, the integer 0 is an additive identity. However, the axiom doesn't preclude the possibility that there might be some other additive identity in $\mathbf{Z}$. After all, if a number can have two square roots, or a person can have three children...

Proposition 1.3 *The additive identity in $\mathbf{Z}$ is unique.*

Proof. Suppose that $y, z \in \mathbf{Z}$ are both additive identities. Then on the one hand

$$y + z = y,$$

because that's what it means for z to be an additive identity. On the other hand,

$$\begin{aligned} y + z &= z + y && \text{(A1).} \\ &= z && \text{(because } y \text{ is an additive identity).} \end{aligned}$$

Comparing the results of our two computations, we conclude that $y = z$. Thus there is only one additive idenitity in $\mathbf{Z}$. $\square$

Here are some other facts that can be deduced from the ring axioms. Note that once you prove a fact it can then be used to help prove other facts.

Proposition 1.4 *The following statements are true (for any integers $x, y, z \in \mathbf{Z}$).*

1. *If $x + z = y + z$ then $x = y$.*
2. *The additive inverse of x is unique.*
3. *The multiplicative identity is unique.*
4. $-(-x) = x$.
5. $(-1)x = -x$.
6. $(-x)y = -(xy)$.
7. $(-x)(-y) = xy$.

Note that proving the second and third items requires you to have definitions for *additive inverse* and *multiplicative idenitity*

2 Order in the Integers

Besides adding and multiplying integers, one can also compare them with each other, saying which is larger and which is smaller. For instance $0 < 1$, but $-1 < 0$. Such comparison is called an 'order relation.' As with arithmetic, it turns out that all the various facts about order on the integers boil down to a few fundamental rules. These are the following

O1 (Trichotomy) For any $x, y \in \mathbf{Z}$, exactly one of the following is true: $x < y$, $y < x$, or $y = x$.

O2 (Transitivity) For any $x, y, z \in \mathbf{Z}$, the relations $x < y$ and $y < z$ imply that $x < z$.

O3 (Compatibility with addition) For any $x, y, z \in \mathbf{Z}$, the relation $x < y$ implies that $x + z < y + z$.

O4 (Compatibility with multiplication) For any $x, y \in \mathbf{Z}$, $0 < x$ and $0 < y$ imply that $0 < xy$.

The following propostion sums up some important consequences of these axioms

Proposition 2.1 *For any $x, y, z \in \mathbf{Z}$, the following are true.*

1. $0 < x$ *implies that* $-x < 0$ *and* $x < 0$ *implies that* $0 < -x$.
2. $0 < x, y$ *imply that* $0 < x + y$.
3. $0 < x$ *and* $y < 0$ *imply that* $xy < 0$.
4. $x < 0$ *and* $y < 0$ *imply that* $0 < xy$.
5. $0 < 1$.
6. $x < y$ *and* $0 < z$ *implies that* $xz < yz$.
7. $xy = 0$ *implies that either* $x = 0$ *or* $y = 0$.
8. $xz = yz$ *and* $z \neq 0$ *imply that* $x = y$.

Somewhat remarkably, the last two conclusions in this proposition do not even refer to order directly. However, one must rely on the trichotomy axiom for order to prove them! As before, we will not prove all these consequences of the axioms. Rather let us make examples of a couple of them, leaving you the reader the pleasure of proving the rest.
Proof. We prove items 3 and 5, in each case assuming that the preceding items have all been shown to be true.

Let $y < 0$ and $0 < x$. Then

$$\begin{array}{rrcll} & y & < & 0 & \text{(assumption)} \\ \Rightarrow & 0 & < & -y & \text{(item 1)} \\ \Rightarrow & 0 & < & (-y)x & \text{(O4 and assumption on } x) \\ \Rightarrow & 0 & < & -(yx) & \text{(item 4 in Proposition 1.4)} \\ \Rightarrow & yx & < & 0 & \text{(item 1 again)} \\ \Rightarrow & xy & < & 0 & \text{(M1)} \end{array}$$

This proves item 3.

To prove item 5, we apply the trichotomy axiom: either $0 < 1$, $1 < 0$ or $1 = 0$. The last possibility is ruled out by the addendum to axiom M3 for arithmetic.

Now assume that $1 < 0$. If this is so, then item 4 tells us that $0 < 1 \cdot 1$. But $1 \cdot 1 = 1$ by M3. Hence $0 < 1$, contradicting our assumption. The only remaining possibility is $0 < 1$, which is what we wanted to prove. $\square$

The proof of item 5 is an example of *proof by contradiction.* The idea is that we look at want we want to prove, assume the opposite of this is true instead, and then reason ourselves into a logical pickle, all for the sake of concluding that the thing we want to be true really is true. It's sort of like following the driving directions your friend suggests and getting hopelessly lost just to make clear that the directions stink. Needless to say, in ordinary social situations outside of math, proofs by contradiction should be employed with a certain tact and sensitivity.

Thus far we have carefully phrased all our statements concerning order so that only the symbols '$<$' and '$=$' are used, avoiding things like '$>$' and '$\leq$'. However, there is no harm in using these latter symbols if one remembers that things can always be translated back to $<$ and $=$—for instance, that '$x >= y$' is shorthand for '$y < x$ or $y = x$'.

3 The Well-Ordering Principle

Up until now, we have done nothing with integers that we couldn't also have done with rational numbers or real numbers. Indeed, if you think about it, you could go back through the previous sections, substituting 'real number' for 'integer', and all the arguments would be as true as they were before. This is because real numbers also satisfy the axioms given for arithmetic and order. Hence any fact deduced solely from those axioms will be a fact about real numbers just as surely as it is a fact about integers. What we need now is a new axiom, one that will separate the integers from all other kinds of numbers. To state this axiom, we need to single out an important subset of the integers.

Definition 3.1 *A* natural number *is any integer larger than or equal to zero. The set of all natural numbers is denoted* $\mathbf{N}$*.*

Note specifically, that we count 0 among the natural numbers. If we want to refer to the set of all positive integers, we will write '$\mathbf{Z}^+$'. The axiom that distinguishes integers from other sorts of numbers is

The Well-Ordering Principle. *Any non-empty subset of the natural numbers has a smallest element.*

One can perhaps see more clearly how the well-ordering principle distinguishes integers from rational and real numbers from one of its consequences.

Proposition 3.2 *There is no* $n \in \mathbf{Z}$ *such that* $0 < n < 1$*.*

Equivalently, one can say that 1 is the smallest positive integer.

Proof. Assume, in order to obtain a contradiction, that such an integer exists. Then the set $S := \{n \in \mathbf{Z} : 0 < n < 1\}$ is a non-empty set of natural numbers. Hence there is a smallest element of S, which we denote m. But since $m > 0$, we can multiplying the inequalities $0 < m$ and $m < 1$ by m to obtain $0 < m^2$ and $m^2 < m$. From the transitivity axiom 02, we infer $m^2 < 1$ and thus see that m^2 is an element of S smaller than m. This contradicts the fact that m is the smallest element and belies our initial assumption. Hence there is no integer between 0 and 1. $\square$

By contrast there are many rational and real numbers between 0 and 1, and in fact, if one changes the definition of S in the previous proof to include. say, all *rational* numbers between 0 and 1, then S is very far from non-empty (e.g. $1/2 \in S$) and the argument of the proof shows that S has no smallest element. Hence subsets of the non-negative rational (and similarly real) numbers need *not* have smallest elements.

In order to give further applications of the well-ordering principle, we make a couple of further definitions.

Definition 3.3 *Given* $a, b \in \mathbf{Z}$*, we say that* b divides a *if there is a third integer* c *such that* $a = bc$*. Alternatively, we say that* b is a factor of a *or* a is a multiple of b*. In any case, we will write '*$b|a$*' to indicate that* b *divides* a*.*

So for instance $4|12$ but $4 \not| 15$. Observe that for any integer n, we have that both 1 and n divide n simply because $n = 1 \cdot n$. We will say that a factor of n is non-trivial if it is not equal to 1 or n.

Proposition 3.4 *If $a \geq 0$, $b \geq 1$ are integers and a is a non-trivial factor of b, then $1 < a < b$.*

Proof. By assumption, we have $ac = b$ for some $c \in \mathbf{Z}$. Neither a nor c is 0, since this would imply $b = 0$. Thus $a > 0$ and therefore also $c > 0$, since a is a natural number and $b = ac$ is positive. Indeed from Proposition 3.2 and $a \neq 0$ we see that $c \geq 1$ and $a > 1$. Thus $b = ac \geq a \cdot 1 = a$. Since $b \neq a$, we conclude that $a < b$, as asserted. □

Definition 3.5 *A* factorization *of a non-zero integer $b \in \mathbf{Z}$ is a collection $a_1, \ldots, a_k \in \mathbf{Z}$ such that $b = a_1 \ldots a_k$.*

So for instance $4 \cdot 4 \cdot 2$ is a factorization of 32; as is $2 \cdot 2 \cdot 2 \cdot 4$, or for that matter $32 \cdot 1$.

Definition 3.6 *An integer $p > 1$ is called* prime *if p and 1 are the only natural numbers that divide p.*

Note that we will call a factorization of a positive integer n *prime* if all factors included are prime numbers. Our next direct use of the well-ordering principle will be

Theorem 3.7 *Let $n > 1$ be an integer. Then n admits a prime factorization, and in particular n has at least one prime factor.*

Proof. Assume the theorem fails. Then the set S of integers larger than 1 that do not admit prime factorizations is non-empty. By the well-ordering principle, it has a smallest element n. Note that n is not prime, since then n admits the prime factorization $n = n$. Hence n has a non-trivial factor m. That is, $n = mk$ for some other non-trivial factor $k \in \mathbf{N}$. From Proposition 3.4, we infer $1 < m, k < n$. In particular, since n is the *smallest* beyond 1 without a prime factorization, we infer that there are prime numbers $p_1 \ldots p_i$ and $q_1, \ldots q_j$ such that $m = p_1 \ldots p_i$ and $k = q_1 \ldots q_j$. It follows that n admits the prime factorization $n = p_1 \ldots p_i q_1 \ldots q_j$, which contradicts the fact that no such factorization exists. It follows that the set S is non-empty and the theorem is true. □

Changing direction somewhat, we give another application of the well-ordering principle. We pointed out earlier that there is no operation of 'division' for integers, since x/y need not be an integer even if x and y are. However, as the next result indicates, there is a substitute for division: 'division with remainder'. It is the first result we have encountered that really deserves the title 'theorem', and we will use it frequently.

Theorem 3.8 (The Division Algorithm) *Given integers $a \geq 0$ and $b > 0$, there exist unique integers $q, r \in \mathbf{N}$ with the following properties*

- $a = bq + r$.
- $0 \leq r \leq b - 1$.

For example, taking $a = 15$ and $b = 4$, as above, we have $15 = 3 \cdot 4 + 3$. The name 'Division *Algorithm*' is a little misleading, since it does not actually tell one *how* to find the quotient q and remainder r in the conclusion. However, the name is pretty well entrenched in the mathematical literature, so we will continue to use it. Note also that Theorem 3.8 remains true if we assume only that a and b are integers such that $b \neq 0$. That is, one or both of a and b can be negative. Because the proof is cleaner, we content ourselves with the version given here.
Proof. We first prove that integers r and q with the desired properties exist. Let [1]

$$S = \{t \in \mathbf{N} : t = a - bs \text{ for some } s \in \mathbf{Z}\}.$$

Note that S is non-empty because e.g. $t = a - b \cdot 0 = a$ is an element of S. By the well-ordering principle then, S has a smallest element $r \in \mathbf{N}$. Since $r \in S$, we have $r = a - bq$ for some $q \in \mathbf{Z}$. That is, $a = bq + r$. Moreover, because $r = a - bq$ is the *smallest* element of S, it follows that $r - b = a - b(q + 1)$ is not in S. Hence $r - b < 0$. Since $r \in \mathbf{N}$, we conclude that $0 \leq r < b$. This concludes the existence portion of the proof.

Now we prove that r and q are unique. Suppose that r', q' is another pair of integers satisfying the two conclusions of the theorem. Let us say for argument's sake that $r' \geq r$. Then we have

$$\begin{aligned} bq + r &= bq' + r' \\ \Rightarrow b(q' - q) &= r' - r. \end{aligned}$$

That is, $r - r'$ is an integer multiple of b. On the other hand, since $0 \leq r' \leq r < b$, it follows that $0 \leq r - r' \leq b - 1$. The only integer multiple of b between 0 and $b - 1$ is 0, so it must be that $r = r'$. Since $b \neq 0$, it follows that $q = q'$, too. Hence q and r are unique. ☐

We conclude this section with a small but useful observation. The well-ordering principle can be restated in a more flexible fashion using the following terminology.

Definition 3.9 *A number $m \in \mathbf{Z}$ is said to be a* lower bound *for a set $S \subset \mathbf{Z}$ if $m \leq x$ for all $x \in S$. If such an m exists, then S is said to be* bounded below*. Likewise, $M \in \mathbf{Z}$ is an* upper bound *for S if $M \geq x$ for every $x \in S$, and if such an M exists, then S is said to be* bounded above.

Proposition 3.10 *If $S \subset \mathbf{Z}$ is non-empty and bounded below then it has a smallest element. If S is non-empty and bounded above, then it has a largest element.*

[1] You should stop and think about the definition of S til you understand what it's saying—it helps to work out a specific example with specific values for a and b.

The well-ordering principle is a special case of this statement because any set of natural numbers is bounded below by 0.

Proof. Suppose that $S \subset \mathbf{Z}$ is non-empty and bounded below by an integer m. Then $x - m \geq 0$ for every $x \in S$. Hence the set

$$T := \{x - m \in \mathbf{Z} : x \in S\}$$

is a non-empty set of natural numbers and therefore has a smallest element t_0. It follows that there is an element $x_0 \in S$ such that $t_0 = x_0 - m$.

Moreover, if $x \in S$ is any other element, then $x - m \in T$, so $t_0 = x_0 - m \leq x - m$. Hence $x_0 \leq x$. Since $x \in S$ was arbitrary, we conclude that x_0 is the smallest element of S.

The case where S is bounded above is similar and left as an exercise. $\square$

4 Base b expansions of integers

Definition 4.1 *Let $b \geq 2$ and $n \geq 1$ be natural numbers. A* base b expansion *(or b-ary* expansion *for n is a an expression*

$$d_k d_{k-1} \ldots d_1 d_0$$

where the digits *d_j, $j = 0, \ldots, k$, are integers satisfying*

- $0 \leq d_j \leq b-1$;
- $d_k \neq 0$;
- $n = \sum_{j=0}^{k} d_j b^j$;

We extend the notion of b-ary expansions to non-positive integers as follows. The integer 0 is its own b-ary expansion, and the b-ary expansion of a negative integer n is a b-ary expansion for $|n|$ with a minus sign in front of it.

Theorem 4.2 *Given integers $b \geq 2$ and n, there is a unique b-ary expansion for n.*

Proof. We assume without loss of generality that $n \geq 1$. First we address the existence of a b-ary expansion, letting

$$S = \{n \in \mathbf{Z}^+ : n \text{ does not have a } b\text{-ary expansion}\}.$$

Assume in order to reach a contradiction that S is not empty. Then by the well-ordering principle S has a smallest element m. Observe that $m \neq 1, \ldots, b-1$ since these numbers will be their own b-ary expansions and will therefore not be elements of S. Using the division algorithm, we are able to write

$$m = bq + r$$

where $q \geq 1$ and r are as in the conclusion of Theorem 3.8. Since $b \geq 2$ and $r \geq 0$, it follows that

$$m \geq bq > q.$$

Hence q is an element of $\mathbf{Z}^+$ not belonging to S and must have a b-ary expansion:

$$q = d_k d_{k-1} \ldots d_0.$$

Thus

$$m = b \sum_{j=0}^{k} d_j b^j + r = d_k b^{k+1} + d_{k-1} b^k + \cdots + d_0 b + r.$$

But since $0 \leq r \leq b-1$, this means that $d_k d_{k-1} \ldots d_0 r$ is a b-ary expansion for m, contradicting the assumption that $m \in S$. It follows that S is empty: every positive integer has a b-ary expansion.

Now we address the issue of uniqueness. Suppose, in order to obtain a contradiction again, that there is a number $n \in \mathbf{N}$ with two different b-ary expansions. That is [2],

$$d_k b^k + \dots d_1 b + d_0 = n = d'_k b^k + \cdots + d'_1 b + d'_0, \tag{1}$$

where $d_j \neq d'_j$ for at least one j. Let $j = \ell$ be the smallest index where the digits differ; say for argument's sake that $d_\ell > d'_\ell$. Then $d_j = d'_j$ for $j < \ell$, so the last ℓ terms on the left side of (1) cancel the last ℓ terms on the left, giving us

$$d_k b^k + \cdots + d_\ell b^\ell = d'_k b^k + \cdots + d'_\ell b^\ell$$

From this, we can cancel a common factor of b^ℓ and isolate the ℓth terms.

$$d_\ell - d'_\ell = (d'_k - d_k) b^{k-\ell} + \cdots + (d'_{\ell+1} - d_{\ell+1}) b.$$

Since $0 \leq d'_\ell < d_\ell \leq b - 1$, the left side is between 1 and $b - 1$. On the other hand, b divides the right side. Since b cannot divide numbers between 1 and $b - 1$, we have reached a contradiction. We conclude that the b-ary expansion of n is unique. $\square$

[2] Actually, the two expansions might have different numbers of digits, but if this is the case we add leading zeroes to the shorter expansion so that both have the same number of digits. Technically, this violates the second condition in Definition 4.1, but it does not affect the validity of the present argument.

5 Divisibility

In order to present an example in the previous section, we introduced the notion of *divisibility*. In this section, we make a thorough study of divisibility. First we collect some basic results.

Proposition 5.1 *Let $a, b, c \in \mathbf{Z}$ be given.*

1. *If $a|b$ and $b|c$, then $a|c$.*
2. *If $b \neq 0$ and $a|b$, then $|a| \leq |b|$.*
3. *If $a|b$ and $b|a$, then $b = \pm a$.*

Proof. We prove only the first item here, leaving proofs of the remaining items as exercises. If $a|b$ and $b|c$, then by definition, there are integers k, ℓ such that $ak = b$ and $b\ell = c$. Therefore $a(k\ell) = c$, which means that $a|c$. □

Definition 5.2 *Let $a, b \in \mathbf{Z}$ be integers, at least one of which is not 0. The* greatest common divisor $\gcd(a, b)$ *of a and b is the largest natural number n such that $n|a$ and $n|b$.*

The first thing to point out about greatest common divisors is that they exist. The set of all natural numbers dividing both a and b is non-empty because it contains, for instance, the number 1. It is also bounded above: if, for instance, $a \neq 0$ then conclusion 2 in Proposition 5.1 tells us that a number dividing a cannot be larger than $|a|$. Hence by Proposition 3.10, there is a *largest* natural number dividing both a and b.

The significance of the next definition and might seem a little mysterious if you've never seen it before, but it's really very important.

Definition 5.3 *An integer combination of two numbers $a, b \in \mathbf{Z}$ is an integer of the form $ma + nb$, where m, n are also integers.*

For example, 2 is an integer combination of 3 and 5, because $4 \cdot 3 + (-2) \cdot 5 = 2$. Here are a couple of basic but quite useful observations about integer combinations.

Proposition 5.4 *For any $a, b, c, d \in \mathbf{Z}$, the following are true.*

1. *If $c|a$ and $c|b$, then c divides every integer combination of a and b.*
2. *If c and d are integer combinations of a and b, then every integer combination of c and d is also an integer combination of a and b.*

Proof. If $c|a$ and $c|b$, then $a = a'c$ and $b = b'c$ for some $a', b' \in \mathbf{Z}$. Therefore, if $k = ma + nb$ is an integer combination of a and b, we have

$$k = m(a'c) + n(b'c) = c(ma' + nb').$$

Thus c divides k, and the first conclusion is proved.

If $c = ma + nb$ and $d = ra + sb$ are integer combinations of a and b and $k = ic + jd$ is an integer combination of c and d, then

$$k = i(ma + nb) + j(ra + sb) = (im + jr)a + (in + js)b.$$

Thus k is also an integer combination of a and b, and the second conclusion is proved. $\square$

Later on, we'll encounter what's traditionally called the *fundamental theorem of arithmetic*, but if tradition hadn't already spoken for the name, I'd want to apply it to the next result.

Theorem 5.5 *Let a and b be integers not both equal to 0. Then $\gcd(a, b)$ is an integer combination of a and b.*

Proof. Let

$$S = \{k \in \mathbf{Z}^+ : k \text{ is and integer combination of } a \text{ and } b\}$$

Since at least one of the two integers a and b is non-zero, we have $a \cdot a + b \cdot b = a^2 + b^2 \geq 1$. Therefore $a^2 + b^2 \in S$, and our set is non-empty. By the well-ordering principle, S has a smallest element $g \geq 1$. By definition of S, $g = ma + nb$ for some $m, n \in \mathbf{Z}$. I claim that $g = \gcd(a, b)$.

To see that my claim is true, note that since g is an integer combination of a and b, and since $\gcd(a, b)$ divides both a and b, conclusion 1 of Proposition 5.4 implies that $\gcd(a, b)$ divides g. In particular, conclusion 2 of Proposition 5.1 tells us that $\gcd(a, b) \leq g$.

It remains to show that $g \leq \gcd(a, b)$. Since $\gcd(a, b)$ is the *largest* common factor of a and b, it will suffice just to show that $g|a$ and $g|b$. Taking a, for example, we apply the division algorithm to write

$$a = g \cdot q + r$$

where $0 \leq r < g$. Now $r = a \cdot 1 + (-q) \cdot g$ is an integer combination of a and g, so conclusion 2 of Proposition 5.4 implies that r is an integer combination of a and b. On the other hand, g is supposed to be the smallest positive integer combination of a and b. It follows that $r = 0$. Thus $a = g \cdot q$ and we see that $g|a$.

The same argument shows that $g|b$. Thus $g \leq \gcd(a, b)$, as desired. Combining our inequalities, we conclude that $g = \gcd(a, b)$. $\square$

Corollary 5.6 *If $a, b \in \mathbf{Z}$ are not both zero and $c \in \mathbf{Z}$ divides both a and b, then $c | \gcd(a, b)$.*

Proof. By Theorem 5.5, $\gcd(a, b)$ is an integer combination of a and b. Thus by conclusion 1 of Proposition 5.4, $c | \gcd(a, b)$. $\square$

Definition 5.7 *Two non-zero integers a and b are* relatively prime *if* $\gcd(a, b) = 1$.

Corollary 5.8 *If a, b, and c are integers, such that a and b are relatively prime and $a|bc$, then $a|c$.*

Proof. Since $a|bc$, we have $k \in \mathbf{Z}$ such that $bc = ak$. Since $\gcd(a,b) = 1$, we have from Theorem 5.5 that

$$1 = ma + nb$$

for some $m, n \in \mathbf{Z}$. Thus

$$c = mac + nbc = mac + nak = a(mc + nk).$$

Hence $a|c$. □

Corollary 5.9 *If $a, b \in \mathbf{Z}$ are not both zero, then $a/\gcd(a,b)$ and $b/\gcd(a,b)$ are relatively prime integers.*

Proof. Since $\gcd(a,b)$ divides both a and b, there exist $a', b' \in \mathbf{Z}$ such that $a = a' \gcd(a,b)$ and $b = b' \gcd(a,b)$. By Theorem 5.5, there also exist $m, n \in \mathbf{Z}$ such that

$$\gcd(a,b) = ma + nb.$$

Cancelling out the common factor of $\gcd(a,b)$ from the three terms in this equation, we find

$$1 = ma' + nb'.$$

Hence by conclusion 2 of Proposition 5.4, any common factor of a' and b' must also divide 1. It follows then from conclusion 2 of Proposition 5.1 that the only positive integer dividing a' and b' is 1 itself. That is, $a' = a/\gcd(a,b)$ and $b' = b/\gcd(a,b)$ are relatively prime. □

Now let us return to consider prime numbers again. The first result is a relatively straightforward consequence of Corollary 5.8.

Corollary 5.10 *If a, b, c are integers such that a is prime and $a|bc$, then $a|b$ or $a|c$.*

Proof. Exercise. □

Remark 5.11 *The previous corollary extends to products of more than two integers. That is,*

if a is prime and $a|n_1 \cdot \cdots \cdot n_k$, then a must divide one of the n_j.

To see that this is so, note that by the previous corollary $a|n_1$ or $a|(n_2 \cdot \cdots \cdot n_k)$. In the latter case, $a|n_2$ or $a|(n_3 \cdot \cdots \cdot n_k$. Continuing in this fashion, we eventually find that $a|n_1$ or $a|n_2$ or $a|n_3$ or ... or $a|n_k$.

Theorem 5.12 (Fundamental Theorem of Arithmetic) *Every integer $n \geq 2$ has a prime factorization, and this factorization is unique up to order.*

The phrase 'unique up to order' means, for example, that $2 \cdot 3$ is the only prime factorization of 6, as long as you count this to be the same as $3 \cdot 2$.

Proof. Theorem 3.7 already tells us that n has at least one prime factorization. So here we need to show that there isn't a second one. Suppose in order to reach a contradiction that n has two different prime factorizations

$$p_1 \cdot \dots \cdot p_k = n = q_1 \cdot \dots \cdot q_\ell.$$

By cancelling out terms that appear on both sides, we can assume that $p_i \neq q_j$ for any i, j. However, the above equation implies that $p_1 | q_1 \cdot \dots \cdot q_\ell$. So from Corollary 5.10, we see that $p_1 | q_j$ for some j. Since p_1 and q_j are both prime, it follows that $p_1 = q_j$. This contradicts the fact that p_1 is different from all the q_j's. Hence n does not have two different prime factorizations. We conclude that prime factorizations are unique. □

The next theorem is due to Euclid and is an amazing instance of the power of 'proof by contradiction'.

Theorem 5.13 *There are infinitely many prime numbers*

Proof. Suppose to the contrary that there are finitely many prime numbers $p_1, \dots, p_k$. Consider the number

$$n := 1 + p_1 \cdot p_2 \cdot \dots \cdot p_k.$$

Since $n > 1$, there exists a prime number p which divides n. By our initial assumption $p = p_j$ for some j. However, from the previous equation, it's clear that

$$n = p_j \cdot q + 1,$$

where q is the product of all the prime numbers besides p_j. So on the one hand, n is evenly divisible by p_j, but on the other hand dividing n by p_j leaves remainder 1. This is impossible. We conclude that there are infinitely many prime numbers. □

6 Sets and relations

A *set*, which is nothing more than a collection of objects, is one of the most basic notions in mathematics. The objects belonging to the set are called its *elements*. We write '$x \in A$' to indicate that x is an element of A.

The most basic of all sets is the *empty set* $\emptyset$. That is, $\emptyset$ is the unique set which contains no elements. The following definition presents a variety of other basic terminology connected with sets.

Definition 6.1 *Let A and B be sets.*

- *The* union *of A and B is the set*
$$A \cup B := \{x : x \in A \text{ or } x \in B\}.$$
- *The* intersection *of A and B is the set*
$$A \cap B := \{x : x \in A \text{ and } x \in B\}.$$
- *The* difference *between A and B is the set*
$$A - B := \{x \in A : x \notin B\}.$$
- *B is a* subset *of A if every element of B is also an element of A. When B is a subset of A, we call $A - B$ the* complement *of B in A, and when the set A can be understood from context, we write B^c for $A - B$.*
- *We say that A is a* subset *of B if for every $x \in A$, we also have $x \in B$. In this case, we write $A \subset B$.*
- *We say that $A = B$ if $A \subset B$ and $B \subset A$.*
- *We say that A and B are* disjoint *if $A \cap B = \emptyset$.*

Many assertions in mathematics boil down to statements about the relationship between two sets. For instance, the assertion *the solutions of $x^2 = 1$ are 1 and -1* can be rephrased as an equality between two sets

$$\{x \in \mathbf{R} : x^2 = 1\} = \{-1, 1\}.$$

Proving that two sets are equal, or that one is a subset of another is therefore an important skill. Fortunately, it's not a difficult one as long as you remember what you're up to. Let us give an example here.

Proposition 6.2 *For any sets A, B, C, we have*

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

Before beginning, we point out the basic strategy. By definition, showing two sets are equal means showing that one is a subset of the other and vice versa. And to show that one set is a subset of another, we must show that any element in the first is an element of the second.

Proof. To show that the left set is a subset of the right, let $x \in A \cap (B \cup C)$ be given. Then on the one hand $x \in A$, and on the other hand $x \in B$ or $x \in C$. If $x \in B$, then it follows that $x \in A \cap B$. Likewise, if $x \in C$, then it follows that $x \in A \cap C$. Hence $x \in (A \cap B) \cup (A \cap C)$. This proves

$$A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C).$$

To show the right set is a subset of the left set, let $x \in (A \cap B) \cup (A \cap C)$ be given. Then either $x \in A \cap B$ or $x \in A \cap C$. If $x \in A \cap B$, then $x \in A$ and $x \in B$, so certainly $x \in B \cup C$, too. Hence $x \in A \cap (B \cup C)$. If, on the other hand, $x \in A \cap C$, then we similarly see that $x \in A \cap (B \cup C)$. So in either case, we see that $x \in A \cap (B \cup C)$. This proves

$$(A \cap B) \cup (A \cap C) \subset A \cap (B \cup C).$$

Putting the results together, we conclude that

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

□

There is one other way to combine two sets. In some sense, it's the *largest* possible way to combine two sets.

Definition 6.3 *The* cartesion product *of two sets A and B is the set*

$$A \times B := \{(a, b) : a \in A, b \in B\}$$

comprising all ordered pairs whose first element lies in A and whose second element lies in B.

So if A is the set of all U.S. presidents and B is the set of all species of trees, then $(\text{Woodrow Wilson}, \text{weeping willow})$ is an example of an element of $A \times B$. Any kind of 'connection' between the elements of A set with the elements of B can be described as a subset of $A \times B$.

Definition 6.4 *A subset $R \subset A \times B$ is called a* relation *from A to B. If $A = B$, then we say simply that R is a relation on A.*

So if A is the set of all readers of these notes and B is the set of all flavors of ice cream, then

$$R = \{(a, b) \in A \times B : a \text{ likes } b\text{-flavored ice cream}\}$$

is a relation from A to B. One element in R is $(\text{Diller}, \text{strawberry})$. This is not the only element in R, since the author of these notes enjoys several flavors of ice cream. However, (Diller, Chunky Monkey) is certainly not in R, even though it is a well-documented element of $A \times B$.

An example of a relation on $\mathbf{Z}$ is the *order* relation

$$R = \{(a, b) \in \mathbf{Z} \times \mathbf{Z} : a < b\}.$$

So $a < b$ means exactly the same thing as $(a, b) \in R$. In fact, one often writes aRb ('a is related to b') instead of $(a, b) \in R$ ('(a, b) belongs to R'), but keep in mind that the two pieces of notation mean exactly the same thing. Concerning the example in the previous paragraph, I might equally well have said *Diller R strawberry* (or better yet, *Diller ♡ strawberry*!)

Definition 6.5 *A relation R on a set A is called*

- Reflexive *if xRx for every $x \in A$;*
- Symmetric *if xRy implies yRx for every $x, y \in A$;*
- Transitive *if xRy and yRz imply that xRz for every $x, y, z \in A$.*

We call R an equivalence relation *if R enjoys all three of these properties.*

So the order relation $<$ is transitive but not symmetric or reflexive. In particular, it is not an equivalence relation. Consider on the other hand the following relation on the set A of all people

$$R = \{(x, y) \in A \times A : x \text{ and } y \text{ have the same gender}\}.$$

Then R is certainly reflexive, symmetric, and (OK there are exceptions here, but not many) transitive. Hence R is an equivalence relation. More generally and speaking loosely, an equivalence relation on a set A is a relation that ties together elements that have some property in common.

Definition 6.6 *Let R be an equivalence relation on a set A and $x \in A$ be any element. The* equivalence class of *x is the set*

$$[x] = \{y \in A : xRy\}.$$

In the preceding example, there are only two different equivalence classes: the set of all men, and the set of all women.

Theorem 6.7 *Let R be an equivalence relation on a set A. Then each $x \in A$ belongs to its own equivalence class $[x]$, and if $y \in A$ is another element, we have either*

- *xRy, in which case $[x] = [y]$; or*
- *R does not relate x and y, in which case $[x] \cap [y] = \emptyset$.*

Proof. Let $x \in A$ be given. Then xRx because R is reflexive. Hence $x \in [x]$.

Now let $y \in A$ be another element. Suppose first that xRy. I must show that $[x] = [y]$. To do this, let $z \in [y]$ be any element. Then yRz by definition of equivalence class. Since R is transitive and we are assuming that xRy, it follows that xRz. Hence $z \in [x]$. This proves that $[y] \subset [x]$. To prove that $[x] \subset [y]$, I note that by symmetry of R, xRy implies that yRx. So if $z \in [y]$, I can repeat the previous argument with the roles of x and y reversed, to conclude that $[x] \subset [y]$. I conclude that $[x] = [y]$.

It remains to consider the case where x and y are not related by R. In this case, I must show that $[x] \cap [y] = \emptyset$. Suppose in order to get a contradiction that $z \in [x] \cap [y]$. Then by definition of equivalence class, xRz and yRz. Since R is symmetric, it follows that zRy, and since R is transitive it further follows that xRy, contradicting the fact that x and y are not related. I conclude that there is no element z in $[x] \cap [y]$. $\square$

7 Congruences

Systems of linear congruences can be solved in much the same way as other systems of equations: solve the first, plug the solution into the second and solve that, etc. Since this is generally a laborious thing to do, it's good to have a criterion that tells us in advance that the procedure will succeed. The following theorem is the best-known result along these lines.

Theorem 7.1 (Chinese Remainder Theorem) *Let $m_1, \ldots, m_k \geq 2$ be integers such that $\gcd(m_i, m_j) = 1$ whenever $i \neq j$. Then for any $a_1, \ldots, a_k \in \mathbf{Z}$ the system of congruences*

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \\ &\vdots \\ x &\equiv a_k \mod m_k \end{aligned}$$

has a unique solution modulo $m_1 \ldots m_k$.

In other words, the system has a solution $x = x_0$ and any other solution is obtained by adding an integer multiple of $m_1 \ldots m_k$ to x_0.

Lemma 7.2 *Let $m_1, \ldots, m_k$ be as in Theorem 7.1. Then*

$$\gcd(m_j, m_1 \ldots m_{j-1}) = 1$$

for each j between 2 and k.

Proof. Suppose the assertion is not true for some j: there is $k > 1$ such that $k | m_j$ and $k | m_1 \ldots m_{j-1}$. Replacing k with a prime factor of k if necessary, we may assume that k is prime. Thus $k | m_1 \ldots m_{j-1}$ implies (see Remark 5.11) that $k | m_i$ for some i between 1 and $j-1$. But since $k | m_j$, too, we see that $\gcd(m_i, m_j) \geq k$. This contradicts the hypothesis in Theorem 7.1 that $\gcd(m_i, m_j) = 1$. We conclude that $\gcd(m_j, m_1 \ldots m_{j-1}) = 1$. □

Lemma 7.3 *Theorem 7.1 is true in the case $k = 2$*

Proof. By definition of congruence, $x \in \mathbf{Z}$ satisfies $x \equiv a_1 \mod m_1$ if and only if $x = a_1 + km_1$ for some $k \in \mathbf{Z}$. Thus x also satisfies $x \equiv a_2 \mod m_2$ if and only if $m_1 k \equiv a_2 - a_1 \mod m_1$. We are given that $\gcd(m_1, m_2) = 1$, so it follows that m_1 has a multiplicative inverse n modulo m_2. Multiplying the last congruence by n gives

$$k \equiv n m_1 k \equiv n(a_2 - a_1) \mod m_2,$$

which holds if and only if $k = n(a_2 - a_1) + m_2 \ell$ for some $\ell \in \mathbf{Z}$. Plugging this back into the formula for x, we find that a solution of both congruences is an integer of the form

$$x = a_1 + m_1 n(a_2 - a_1) + m_1 m_2 \ell$$

for some $\ell \in \mathbf{Z}$. In other words, the pair of congruences has the unique solution

$$x \equiv a_1 + m_1 n(a_2 - a_1) \mod m_1 m_2.$$

□

Proof of Theorem 7.1. Lemma 7.3 tells us that there is an integer x_2 such that x satisfies the first two congruences if and only if $x \equiv x_2 \mod m_1 m_2$. Thus x satisfies the first three congruences if and only if

$$x \equiv x_2 \mod m_1 m_2 \text{ and } x \equiv a_3 \mod m_3. \tag{2}$$

According to Lemma 7.2, we have $\gcd(m_1 m_2, m_3) = 1$. Hence we can apply Lemma 7.3 again to find $x_3 \in \mathbf{Z}$ such that x satisfies 2 if and only if $x \equiv x_3 \mod m_1 m_2 m_3$. This proves the theorem when there are three congruences. Continuing in this fashion, we find an integer x_k such that x satisfies all k congruences if and only if

$$x \equiv x_k \mod m_1 \dots m_k.$$

□

8 Rational numbers

Theorem 8.1 *The following is an equivalence relation on* $\mathbf{Z} \times \mathbf{Z}_+$*:* $(a, b) \sim (c, d)$ *if and only if* $ad - bc = 0$*.*

Proof. To see that the relation is reflexive, note that $ab - ba = 0$. Hence $(a, b) \sim (a, b)$.

To see that the relation is symmetric, suppose that $(a, b) \sim (c, d)$. Then $ad - bc = 0$, which is the same as saying $cb - da = 0$. Thus $(c, d) \sim (a, b)$.

To see that the relation is transitive, suppose $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$. Then $ad - bc = cf - de = 0$. That is, $ad = bc$ and $cf = de$. Multiplying the first equation by f and the second by b, I find that

$$adf = bcf = bde.$$

Since $d \in \mathbf{Z}_+$, I know that $d \neq 0$. Hence I can cancel the d from the left and right sides, and I am left with $af = be$. That is, $(a, b) \sim (e, f)$.

I conclude that $\sim$ is an equivalence relation. □

While the equivalence relation in this theorem might look a little strange, it's origin becomes much clearer with the introduction of some 'new' notation.

Definition 8.2 *The* $\sim$*-equivalence class of* $(a, b) \in \mathbf{Z} \times \mathbf{Z}_+$*, is denoted* $\frac{a}{b}$ *and called a* rational number*. The set of all rational numbers is denote by* $\mathbf{Q}$*.*

So the equivalence $(a, b) \sim (c, d)$ is exactly the same as the (more familiar looking) equation $\frac{a}{b} = \frac{c}{d}$. The idea here is to develop rational numbers from the ground up, using integers as a starting point and setting aside the things we already 'know' about rationals. In particular, we'll keep using the $(a, b) \sim (c, d)$ notation for the next page or so in order to avoid the trap of inadvertantly assuming things about rationals that we haven't yet proven. However, as you read, you should keep in mind what's 'really going on' at each point, not forgetting that we're only verifying truths you've accepted without question for most of your life. Soon enough, we'll revert to writing rational numbers the in familiar form $\frac{a}{b}$.

Our next result says that any rational number can be uniquely expressed in lowest terms by cancelling common factors from the 'numerator' and 'denominator'.

Theorem 8.3 *For any pair* $(a, b) \in \mathbf{Z} \times \mathbf{Z}_+$*, there is a unique pair* $(a', b') \in \mathbf{Z} \times \mathbf{Z}_+$ *such that* $\gcd(a', b') = 1$ *and* $(a, b) \sim (a', b')$*. Moreover,* $(a, b) = (ka', kb')$ *for some* $k \in \mathbf{Z}_+$*.*

Proof. Let $k = \gcd(a, b)$. Then $a = a'k$ and $b = b'k$ for some $a' \in \mathbf{Z}$ and $b' \in \mathbf{Z}_+$. Since $k \gcd(a', b') = \gcd(ka', kb') = \gcd(a, b) = k$, it follows that $\gcd(a', b') = 1$. Also, $ab' - ba' = ka'b' - kb'a' = 0$. Hence $(a, b) \sim (a', b')$.

It remains to show that the pair (a', b') is unique. Suppose $(a'', b'') \in \mathbf{Z} \times \mathbf{Z}_+$ is another pair of relatively prime integers equivalent to (a, b). Then by transitivity $(a'', b'') \sim (a', b')$. In other words,

$$a''b' = b''a'.$$

From this, I see in particular that $b'|b''a'$. Since b' and a' are relatively prime, it follows that $b'|b''$. Therefore $b'' = \ell b'$ for some $\ell \in \mathbf{Z}_+$. Plugging this into the previous equation, I get

$$a''b' = \ell b'a'.$$

Since $b' \in \mathbf{Z}_+$ is not equal to 0, I can cancel it and get $a'' = \ell b'$. Thus ℓ divides both a'' and b''. Since $\gcd(a'', b'') = 1$, it follows that $\ell = 1$. I conclude that $b'' = \ell b' = b'$ and $a'' = \ell a' = a'$. That is, $(a', b') \in \mathbf{Z} \times \mathbf{Z}_+$ is the only relatively prime pair equivalent to (a, b). $\square$

Now we discuss arithmetic for rational numbers, working first with just ordered pairs. Given two pairs $(a, b), (c, d) \in \mathbf{Z} \times \mathbf{Z}_+$ we define operations $+$ and $\cdot$ according to the formulas

$$\begin{aligned} (a, b) + (c, d) &:= (ad + bc, bd) \\ (a, b) \cdot (c, d) &:= (ac, bd). \end{aligned}$$

The formula for addition might seem a little weird, but it's really not: just think for a second about what you get when you compute $\frac{a}{b} + \frac{c}{d}$ the way you were taught to do it in elementary school.

We will say that $(a, b) < (c, d)$ if and only if $ad < bc$. Note that we rely on the assumption that b and d are positive in this definition!

The important thing about the definitions of $+$, $\cdot$ and $\leq$ from a logical standpoint is that they 'respect' the equivalence relation $\sim$. For instance, the sums

$$\frac{4}{8} + \frac{-8}{12} \text{ and } \frac{3}{6} + \frac{-2}{3}.$$

look quite different, but they should give the same answer if addition of rational numbers is to be meaningful. To put it another way, the sum of two rational numbers should be *independent* of the particular way we choose to represent the numbers. The following theorem addresses this issue.

Theorem 8.4 *Suppose that $(a, b) \sim (a', b')$ and $(c, d) \sim (c', d')$. Then*

1. $(a, b) + (c, d) \sim (a', b') + (c', d')$;
2. $(a, b) \cdot (c, d) \sim (a', b') \cdot (c', d')$;
3. $(a, b) < (c, d)$ *if and only if* $(a', b') < (c', d')$.

Proof. We'll prove the second and third conclusions, leaving the proof of the first to you.

The assumption that $(a, b) \sim (a', b')$ implies $ab' = a'b$, and similarly $(c, d) \sim (c', d')$ implies $cd' = c'd$. Hence,

$$acb'd' - bda'c' = (ab')(cd') - (a'b)(c'd) = 0,$$

from which we conclude that $(ac, bd) \sim (a'c', b'd')$. That is, $(a, b) \cdot (c, d) \sim (a', b') \cdot (c', d')$, so the second conclusion is true.

Now if $(a,b) < (c,d)$, then $ad < bc$. Multiplying this by b', d', we obtain $(ab')(dd') < (bb')(cd')$. Using $(a,b) \sim (a',b')$ and $(c,d) \sim (c',d')$ again, we deduce

$$(a'b)(dd') < (bb')(c'd).$$

Since b and d are positive integers, we may cancel them both, arriving at $a'd' < b'c'$. That is, $(a',b') < (c',d')$. This proves the third conclusion. $\square$

Corollary 8.5 *The following definitions are unambiguous for any rational numbers $\frac{a}{b}, \frac{c}{d} \in$ **Q**.*

- $\frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd}$.
- $\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}$.
- $\frac{a}{b} < \frac{c}{d}$ *if and only if* $ad < bc$.

Theorem 8.6 *All the axioms for arithmetic and order from sections 1 and 2 hold for rational numbers as well as integers.*

Proof. It would take several pages to verify *all* the axioms. I'll make an example of two of them here, and leave the rest to you.

First I'll prove that axiom A3 is true: there exists an additive identity in **Q**. Indeed, I claim that $\frac{0}{1}$ is an additive identity. To see that this is so, observe that for any other rational number $\frac{a}{b}$, I have

$$\frac{a}{b} + \frac{0}{1} = \frac{a \cdot 1 + b \cdot 0}{b \cdot 1} = \frac{a}{b}.$$

Hence $\frac{0}{1}$ is an additive identity.

Next I'll prove that axiom O3 holds. Suppose that $\frac{a}{b}, \frac{c}{d}, \frac{e}{f}$ are rational numbers such that $\frac{a}{b} < \frac{c}{d}$. That is, $ad < bc$. I need to verify that $\frac{a}{b} + \frac{e}{f} < \frac{c}{d} + \frac{e}{f}$, i.e. that

$$\frac{af+be}{bf} = \frac{cf+de}{df}.$$

To do this, I compute

$$(af+be)(df) - (bf)(cf+de) = f^2(ad-bc) < 0$$

since $f^2 > 0$ and $ad < bc$. Thus $\frac{a}{b} + \frac{e}{f} < \frac{c}{d} + \frac{e}{f}$, as I hoped. Axiom O3 is proved. $\square$

Observe that since all the axioms from Sections 1 and 2 hold for rational numbers, so do all the things that we proved from the axioms in those sections.

Despite the similarity to integers, there are two important ways in which arithmetic and order are different for rational numbers. First of all, it is almost always possible to *divide* one rational number by another.

Proposition 8.7 *Every non-zero rational number has a unique multiplicative inverse.*

Proof. Suppose that $\frac{a}{b} \in \mathbf{Q}$ is not equal to $0 := \frac{0}{1}$. That is, $a \neq 0$. Then

$$\frac{a}{b} \cdot \frac{b}{a} = \frac{1}{1}.$$

Hence $\frac{b}{a}$ is a multiplicative inverse for $\frac{a}{b}$. If $x \in \mathbf{Q}$ is another multiplicative inverse, then we have

$$x = x \cdot 1 = x \cdot \frac{a}{b}\frac{b}{a} = 1 \cdot \frac{b}{a} = \frac{b}{a}.$$

Hence the multiplicative inverse of $\frac{a}{b}$ is unique. □

Existence of multiplicative inverses makes algebra much easier for rational numbers. For instance, if $a, b \in \mathbf{Q}$, the equation

$$ax = b$$

has a solution $x \in \mathbf{Q}$ as long as $a \neq 0$. This is definitely *not* true if we replace $\mathbf{Q}$ by $\mathbf{Z}$.

Existence of multiplicative inverses also implies the so-called *density property* for rational numbers.

Proposition 8.8 *If $x, y \in \mathbf{Q}$ are rational numbers with $x < y$, then there exists $z \in \mathbf{Q}$ such that $x < z < y$.*

Proof. Observe that $2x = x + x < x + y < y + y = 2y$. Multiplying through by 2^{-1}, we obtain

$$x < 2^{-1}(x + y) < y.$$

Hence $z = 2^{-1}(x + y)$ satisfies the conclusion of the theorem.

Not everything is better for rational numbers, however: the well-ordering principle fails.

Proposition 8.9 *The set $\{x \in \mathbf{Q} : x > 0\}$ has no smallest element.*

Proof. Call the set S. Suppose, in order to get a contradiction, that x is the smallest element in S. Then $x \neq 0$ by definition of S. The density property therefore gives us $z \in \mathbf{Q}$ such that $0 < z < x$. In particular, $z \in S$. This contradicts the fact that x was the *smallest* element in S. We conclude that S has no smallest element. □

Finally, we point out one other deficiency of $\mathbf{Q}$. This one deeply troubled the Greeks who discovered it.

Theorem 8.10 *There is no $x \in \mathbf{Q}$ such that $x^2 = 2$.*

Proof. Suppose, to get a contradiction, that the assertion is false: there is a rational number $\frac{a}{b}$ such that

$$\frac{a^2}{b^2} = \frac{2}{1}.$$

By Theorem 8.3, we can assume that $\gcd(a, b) = 1$. Thus

$$a^2 = 2b^2.$$

In particular, $2|a \cdot a$. Since 2 is prime, it follows from Corollary 5.10 that $2|a$. Thus $a = 2k$ for some $k \in \mathbf{Z}$. Plugging this into the previous equation and cancelling a factor of 2 gives

$$2a^2 = b^2.$$

Thus $2|b^2$, which further implies that $2|b$. But if 2 divides both a and b, we see that a and b are not relatively prime. Having reached a contradiction, we conclude that there is no $x \in \mathbf{Q}$ such that $x^2 = 2$. $\square$

9 Real numbers: completeness

In previous sections we have discussed integers and rational numbers at some length. Now we turn to real numbers. The set of all real numbers is usually denoted with the boldface $\mathbf{R}$. It includes both integers and rational numbers; that is, $\mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R}$. However, $\mathbf{R}$ is strictly larger than even $\mathbf{Q}$. A real number that does not belong to $\mathbf{Q}$ is called *irrational*.

Among the various important subsets of $\mathbf{R}$, *intervals* should be mentioned immediately. These come in various flavors. There are

- *open intervals* $(a, b) := \{x \in \mathbf{R} : a < x < b\}$
- *closed intervals* $[a, b] := \{x \in \mathbf{R} : a \leq x \leq b\}$
- 'half-open' intervals $(a, b]$ or $[a, b)$.

Note that we occasionally use $+\infty$ and $-\infty$ as the right and left endpoints, respectively, of open and half-open intervals. This should be understood to mean that the endpoint question doesn't exist. For instance $[4, \infty)$ is the set of all real numbers larger than or equal to 4.

But what exactly is a real number? One might say that it's something that can be expressed as an infinite decimal expansion; something like

$$3.141592654\ldots$$

for instance. As answers go, this isn't half bad, but it requires a lot of qualification and elaboration before one can turn it into a logically water-tight definition of 'real number.' In fact, it's rather difficult to say precisely *what* one means by the term 'real number.' Therefore we will do here as we did earlier with integers. Rather than try to say what real numbers 'are,' we will content ourselves with tackling the more practical question of how real numbers behave—i.e. what the rules are for arithmetic and order. In this section, we will be especially concerned to compare and contrast the behavior of real numbers with that of their nearest relatives, rational numbers.

As with rational numbers, the real numbers constitute an *ordered field*: arithemetic and order of real numbers satisfy all the axioms from section 1 and the additional assertion (see Proposition 8.7).

M4 Every non-zero real number has a multiplicative inverse.

In particular, *division* is a (mostly) legitimate operation for real numbers. As a consequence of the axioms, one can appropriate arguments used for rational numbers to show that real numbers enjoy the density property (see Proposition 8.8 and its proof) but fail to obey the well-ordering principle (see Proposition 8.9).

So why, if real numbers turn out to behave pretty much like rational numbers, do we not just content ourselves with rational numbers and leave the rest to posterity to bother with? Would it make any difference? After all, as various state legislatures are said to have noticed, it's a little easier to think about, say, $22/7$ than it is to cope with $3.141592654\ldots$.

Of course, we already began to see at the end of Section 8 that it does make a difference. Positive rational numbers don't necessarily have rational square roots. But the deficiency inherent in rational numbers is actually much deeper that this. Identifying the real problem requires a definition or two.

Definition 9.1 *A set $S \subset \mathbf{R}$ is* bounded above *if there is a number $M \in \mathbf{R}$ such that $x \leq M$ for all $x \in S$. The number M is called an* upper bound *for S.*

Take for example the open interval $S = (0, 1)$. Clearly, 1 is an upper bound for S. So, for that matter, is 75, or $1,000,000$. If, on the other hand, S is the set of all prime numbers, then S has no upper bound. Given any $M \in \mathbf{R}$, we can always find a prime number that exceeds M. The moral here is that a set of real numbers needn't have an upper bound, but if it has one, then it actually has a great many upper bounds. Nevertheless, as the example $(0, 1)$ suggests, not all upper bounds are created equal.

Definition 9.2 *An upper bound M for a set S is called the* least upper bound *(or* supremum*) of S, if M is no larger than any other upper bound for S. We denote the least upper bound for S, provided it exists, by* $\sup S$.

We leave it to you the reader to define *lower bound* and *greatest lower bound* (also called *infimum*) for a set of real numbers. As the wording of Definition 9.2 suggests, least upper bounds are unique if they exist.

Proposition 9.3 *A set $S \subset \mathbf{R}$ has at most one least upper bound.*

Proof. Suppose that x_1, x_2 are both least upper bounds for S. Then since x_1 is a *least* upper bound and x_2 is an upper bound, it follows that $x_1 \leq x_2$. The same argument shows that $x_2 \leq x_1$, too. Hence $x_1 = x_2$, and we conclude that S can't have more than least upper bound. □

Existence of least upper bounds is the thing that separates $\mathbf{R}$ from $\mathbf{Q}$.

Completeness Axiom. *A set $S \subset \mathbf{R}$ that is non-empty and bounded above has a least upper bound.*

For instance, the set
$$S = \{t \in \mathbf{R} : t^2 \leq 2\}$$
is non-empty (exercise: name one real number in S). It's bounded above by e.g. 1.5, because numbers $t > 1.5$ satisfy $t^2 > (1.5)^2 > 2$ and therefore do not belong to S. So by the completeness axiom, S has a least upper bound x. It seems at least plausible that $x^2 = 2$, and we will prove later that this is indeed the case, but let's just take it on faith right now.

Now what if we forget about real numbers and only consider rational numbers? Then our set becomes
$$S' = \{t \in \mathbf{Q} : t^2 \leq 2\}.$$

As before S' is non-empty (name one rational number in S) and bounded above by 1.5 which is a rational number. However, S' *has no least upper bound.* But wait, you say, it does. The number x above is still the least upper bound for S'. However, $x^2 = 2$ so by Theorem 8.10, x is not a rational number. Therein lies the rub: for the duration of this paragraph, we've erased all memory of irrational numbers, so as far as we're concerned the number x no longer exists. In summary, S' has an upper bound but not a least upper bound. In the place we'd like that least upper bound to be, the set $\mathbf{Q}$ has only a hole. This is why we bother with real numbers.

To see another instance of this phenomena, consider the set

$$T = \{t \in \mathbf{R} : t \text{ is smaller than the circumference of a circle of radius } 1\}.$$

This set also has a least upper bound (what is it?), but only if we allow for irrational numbers. The problem in both these examples is that the set $\mathbf{Q}$ is riddled with holes. Everywhere we'd normally expect to find an irrational number, the set $\mathbf{Q}$ has a yawning gap that only a bona fide real number can fill.

Let us consider the completeness axiom from another point of view by comparing it with a variant of the well-ordering principle (see Proposition 3.10): *Every non-empty subset of* $\mathbf{Z}$ *that is bounded above has a largest element.* The largest element in a set is often called its *maximum.* Note that a maximum is automatically a least upper bound, but not vice versa: 1 is the maximum and least upper bound of $[0, 1]$, but it is only the least upper bound of $(0, 1)$. Hence the well-ordering principle can be regarded as a particularly strong version of the completeness axiom, and one might imagine that the completeness axiom will play for $\mathbf{R}$ somewhat the same role that the well-ordering principle did for $\mathbf{Z}$. This is certainly true, but it requires a little more care to put the completeness axiom to work. Let us close this section by using completeness to derive an 'obvious' fact, call the *archimedean property*, about $\mathbf{R}$.

Proposition 9.4 *Given any $x, y \in \mathbf{R}$ with $x > 0$, there exists $n \in \mathbf{N}$ such that $nx > y$.*

Proof. Suppose, in order to reach a contradiction, that $x > 0$ and y are real numbers such that $nx \leq y$ for all $n \in \mathbf{N}$. Then y is an upper bound for the non-empty set

$$S = \{nx : n \in \mathbf{N}\}.$$

By the completeness axiom, the least upper bound $z = \sup S$ exists. In particular, $z - x < z$ is not an upper bound for S. So there exists $n \in \mathbf{N}$ such that $nx > z - x$. Adding 1 to n, we find

$$(n + 1)x > z - x + x = z.$$

But $(n+1)x \in S$, too, so we see that z is not actually an upper bound for S: a contradiction. □

10 Sequences of real numbers: convergence

Real numbers are very slippery creatures. Most cannot be pinned down exactly. For instance we cannot write down $\sqrt{2}$ precisely as a decimal number. We can only say things like $\sqrt{2} = 1.414\ldots$, giving a few digits and suggesting with our $\ldots$ that we could give more digits if we'd already had dinner and our favorite show weren't about to start. Since in most cases, we can only *approximate* the real numbers we find, it is essential to have a firm logical foundation for approximation. It turns out to be rather tricky to get the details of this just right. Historically, it took centuries to do it. Isaac Newton and the calculus gave approximation center stage in mathematics, but the logical foundations for Newton's ideas weren't completed until the work of Weierstrass in the latter half of the 19th century.

10.1 Absolute values and distance

In order to discuss approximation, it is crucial to have some notion of 'distance' in hand. That is, it is important to be able to tell how far an approximation is from the thing it is approximating. Measuring the distance between real numbers is accomplished using the *absolute value function* $|\cdot| : \mathbf{R} \to \mathbf{R}$, which is given by

$$|x| := \begin{cases} x & \text{if} \quad x \geq 0 \\ -x & \text{if} \quad x < 0. \end{cases}$$

The next result summarizes the most important properties of absolute values.

Proposition 10.1 *Given $x, y \in \mathbf{R}$, we have*

1. $|x| \geq 0$, *and* $|x| = 0$ *if and only if* $x = 0$;
2. $|x| = |-x|$;
3. $|xy| = |x||y|$;
4. $|x + y| \leq |x| + |y|$.
5. $||x| - |y|| \leq |x - y|$.

The fourth assertion in this proposition is known as the *triangle inequaltity*, and it will play a prominent role in our work.

Proof. The first three assertions are readily verified, and we leave the proof of the final assertion as an exercise. To prove the triangle inequality, we suppose first that x and y are both non-positive. Then $x + y \leq 0$ and

$$|x + y| = -x - y = |x| + |y|$$

Similarly, $|x + y| = |x| + |y|$ if x and y are non-negative. If, on the other hand, x and y have opposite signs—say $x > 0$ and $y < 0$, then

$$|x + y| = ||x| - |y|| = \pm(|x| - |y|) \leq |x| + |y|.$$

The sign in the third term is determined by whether $|x|$ or $|y|$ is larger. In any case, we have shown that $|x+y| \leq |x| + |y|$ regardless of the signs of x and y. $\square$

For our purposes, the distance between two numbers $x, y \in \mathbf{R}$ will be the quantity $|x-y|$. Note that the first, second, and third assertions in Proposition 10.1 translate to the following important facts about distance.

- $|x-y| \geq 0$, and $|x-y| = 0$ if and only if $x = y$.
- $|x-y| = |y-x|$
- $|x-y| \leq |x-z| + |z-y|$ for every $z \in \mathbf{R}$.

10.2 ...into the fray

The key logical construct underlying everything else about approximation is the idea of a *convergent sequence*, and it is this idea (specifically Definition 10.3) that we take up now. Most find it a little tricky to keep straight and use accurately at first, but be persistent. Once you become truly comfortable with it, your future classes in real analysis (i.e. advanced calculus) will be much easier for you.

Definition 10.2 *If S is a set, then a* sequence (x_n) *of elements of S is a function $x : \mathbf{N} \to S$. The values $x_n := x(n)$ are called* terms *of the sequence.*

For example, one might have $S = \mathbf{N}$ and define $x : \mathbf{N} \to S$ by setting $x(n)$ to be the nth prime number. Thus $x_1 = 2$, $x_2 = 3$, $x_3 = 5$, etc, and (x_n) just gives the prime numbers in increasing order. The set S in Definition 10.2 is perfectly arbitrary, and one might want to consider sequences of sets, sequences of chess moves, or sequences of bad movies when the occasion calls for it. However, for the time being, the set S will always be $\mathbf{R}$, and by 'sequence' we will mean 'sequence of real numbers.' Note also that we'll often write down sequences that are missing one or more leading terms. For instance, $(\frac{1}{n})$ doesn't technically make sense when $n = 0$, but for our purposes, that won't matter.

While you shouldn't forget that a sequence is a actually a special kind of function, you'll be well-served most of the time to think of a sequence less formally as a neverending list of terms. For example $(\frac{1}{n})$ is just $\frac{1}{1}, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots$. Indeed, whenever you're confused about the definition of a particular sequence, you should reach for some scrap paper and try to write down the first five or so terms of the sequence.

Memorize the first half of the following definition word for word, repeat it to yourself in spare moments, and think about what it's saying every night as you drift off to sleep. Imagine that well-armed but mathematically challenged aliens will descend on the planet at the end of this term and threaten to destroy humanity unless you personally explain this definition to them.

Definition 10.3 *A sequence (x_n) is said to* converge *to a number $L \in \mathbf{R}$ if for every $\epsilon > 0$ there exists $N \in \mathbf{N}$ such that $n \geq N$ implies that $|x_n - L| < \epsilon$.*

We call L the limit *of (x_n) and write $\lim x_n = L$ or, less formally, $x_n \to L$. If (x_n) does not converge to any real number L, then we say that (x_n) diverges.*

The following examples show how this definition gets used.

Example 10.4 *The sequence $(\frac{1}{n})$ converges to 0.*

Proof. Let $\epsilon > 0$ be given. By the Archimedean principle, we can find a number $N \in \mathbf{N}$ such that $N = N \cdot 1 > 1/\epsilon$. Then if $n \geq N$, we have

$$\left|\frac{1}{n} - 0\right| = \frac{1}{n} \leq \frac{1}{N} < \frac{1}{1/\epsilon} = \epsilon.$$

Therefore $\lim \frac{1}{n} = 0$. □

The next example is so simple it's confusing.

Example 10.5 *Given $c \in \mathbf{R}$, the constant sequence (c) converges to c.*

Proof. Let $\epsilon > 0$ be given. Take $N = 0$. Then if $n \geq N$, and $x_n = c$ is the nth term in the sequence, we have

$$|x_n - c| = |c - c| = 0 < \epsilon.$$

Therefore, $\lim c = c$. □

Let's try something a bit more representative.

Example 10.6 $\lim \frac{n}{3n-2} = \frac{1}{3}$.

Proof. Let $\epsilon > 0$ be given. Let $N \in \mathbf{N}$ be some number greater than $\frac{2}{9\epsilon} + \frac{2}{3}$ (Note that in particular $N \geq 1$). Then if $n \geq N$, we have

$$\begin{aligned} \left|\frac{n}{3n-2} - \frac{1}{3}\right| &= \left|\frac{2}{9n-6}\right| \\ &= \frac{2}{9n-6} \\ &\leq \frac{2}{9N-6} \\ &< \frac{2}{9(2/3 + 2/9\epsilon) - 6} \\ &= \epsilon. \end{aligned}$$

□

The reader should be aware that in the preceding proof we did not arrive at our choice of N by luck or magic. Before starting the proof, we solved the inequality $|x_n - \frac{1}{3}| < \epsilon$ for n, making the solution our choice of N.

The reader should also take care to see that when we use $<$ or $\leq$ signs, the inequality really holds. For instance, when we replaced n by N, which is *smaller* than n, then the value of the entire expression really did increase. Many beginners (and not a few seasoned veterans) are tempted to make mistakes of convenience when working with inequalities, incorrectly saying that one expression is smaller than another because they want it to be so, rather than because it is.

Finally, we point out that in order to keep the presentation moving, we often omit a little algebraic calculation in our work. The first $=$ in the above proof is a good example of this practice. While it does help control the clutter, it also means that you will find yourself needing to fill in some of the missing computations as you read. Keep a pencil and paper handy for this purpose.

Example 10.7 *The sequence* $((-1)^n)$ *diverges.*

Proof. Suppose, in order to reach a contradiction, that $\lim(-1)^n = L$. Take $\epsilon = 1$, for instance. By definition of convergence, there exists $N \in \mathbf{N}$ such that $n \geq N$ implies that $|(-1)^n - L| < 1$. In particular, if $n \geq N$ is an even integer, then

$$|(-1)^n - L| = |1 - L| < 1.$$

Thus L lies in the interval $(0, 2)$. Likewise, if $n \geq N$ is odd, we have

$$|(-1)^n - L| = |-1 - L| < 1.$$

Hence L also lies in the interval $(-2, 0)$. But $(0, 2) \cap (-2, 0) = \emptyset$, so the limit L does not exist, and the sequence diverges. $\square$

Intuitively, the problem in the previous example is that the sequence $((-1)^n)$ wants to have two limits: -1 and 1. The next result says that this sort of simultaneous possession/consumption of cake is impossible.

Theorem 10.8 *A sequence has no more than one limit.*

Proof. Suppose that (x_n) has two limits A and B. Then for any $\epsilon > 0$, there exists $N_1 \in \mathbf{N}$ such that $n \geq N_1$ implies that

$$|x_n - A| < \epsilon,$$

and $n \geq N_2$ implies that

$$|x_n - B| < \epsilon.$$

Therefore, if n is larger than both N_1 and N_2, we see that

$$|A - B| = |(A - x_n) + (x_n - B)| \leq |x_n - A| + |x_n - B| < 2\epsilon.$$

However, $\epsilon > 0$ was arbitrary here, so we have in effect shown that $|A - B|$ is smaller than *any* positive number. This implies that $|A - B| = 0$, i.e. $A = B$. We conclude that a sequence has at most one limit. $\square$

An important point concerning the definition of convergent sequence is that one can always ignore finitely many of the terms. When checking, for instance, to see if some sequence converges to π, it is completely irrelevant if the first 600 terms are all equal to -10^{10}. What matters is that *after some point* the terms become close to π.

11 Three useful theorems about limits

After a few tries at using the definition of convergence to prove that some sequence converges, almost anyone will be left with the nagging sense that life is very precious and short and that there must be some quicker, more convenient way to dispose of such problems. In this section, we do our best to validate that sentiment. There are at least three standard ways to get around using the definition of convergence. None of them, by itself, is foolproof, but taken together, these three methods will suffice to address most garden variety convergence problems.

Theorem 11.1 *Let (x_n) and (y_n) be sequences converging to real numbers A and B, respectively. Then*

1. $\lim(x_n + y_n) = A + B$;
2. $\lim x_n y_n = AB$;
3. $\lim(x_n - y_n) = A - B$;
4. *if $B \neq 0$, then $\lim x_n/y_n = A/B$.*

Proof. We will prove the first three of these assertions, leaving the third as an exercise for you, the reader.

To prove the first assertion, let $\epsilon > 0$ be given. Since $\lim x_n = A$, there exists $N_1 \in \mathbf{N}$ such that $n \geq N_1$ implies $|x_n - A| < \epsilon/2$. Likewise, there exists $N_2 \in \mathbf{N}$ such that $n \geq N_2$ implies $|y_n - B| < \epsilon/2$. Therefore, if we set $N = \max\{N_1, N_2\}$, then $n \geq N$ implies that

$$|(x_n + y_n) - (A + B)| = |(x_n - A) + (y_n - B)| \leq |x_n - A| + |y_n - B| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon.$$

The '$\leq$' is the triangle inequality, and the '$<$' comes from the fact that if $n \geq N$, then $n \geq N_1$ and $n \geq N_2$. In any case, we conclude that $\lim(x_n + y_n) = A + B$.

To prove the second assertion, we again let $\epsilon > 0$ be given. Since $\lim x_n = A$, there exists $N_1 \in \mathbf{N}$ such that $n \geq N_1$ implies $|x_n - A| < \min\{\epsilon/2|B|, 1\}$. Similarly, there exists $N_2 \in \mathbf{N}$ such that $n \geq N_2$ implies $|y_n - B| < \epsilon/(2|A| + 2)$. If we take $N = \max\{N_1, N_2\}$, and $n \geq N$, then first of all

$$|x_n| = |x_n - A + A| \leq |x_n - A| + |A| \leq 1 + |A|.$$

Moreover,

$$\begin{aligned}
|x_n y_n - AB| &= |x_n y_n - x_n B + x_n B - AB| \\
&\leq |x_n y_n - x_n B| + |x_n B - AB| \\
&= |x_n||y_n - B| + |B||x_n - B| \\
&< (1 + |A|)\frac{\epsilon}{2|A| + 2} + \frac{|B|\epsilon}{2|B|} \\
&= \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon.
\end{aligned}$$

To see that third assertion holds, note that

$$\lim(x_n - y_n) = \lim x_n + \lim(-y_n) = \lim x_n + (\lim -1)(\lim y_n) = \lim x_n - \lim y_n.$$

The first equality holds because of the first assertion in this theorem, the second holds because of the second assertion in this theorem, and the third holds because of Example 10.5. $\square$

Example 11.2 *Let us show using Theorem 11.1 that* $\lim \frac{(n+1)^3}{2n^3+n} = \frac{1}{2}$. *We have*

$$\begin{aligned}\lim \frac{(n+1)^3}{2n^3+n} &= \lim \frac{n^3}{n^3}\frac{(1+\frac{1}{n})^3}{2+\frac{1}{n^2}} = \lim \frac{(1+\frac{1}{n})^3}{2+\frac{1}{n^2}} = \frac{\lim(1+\frac{1}{n})^3}{\lim(2+\frac{1}{n^2})} = \frac{(\lim 1 + \lim \frac{1}{n})^3}{\lim 2 + \lim \frac{1}{n^2}} \\ &= \frac{(1+\lim \frac{1}{n})^3}{2+(\lim \frac{1}{n})^2} = \frac{(1+0)^3}{2+0} = \frac{1}{2}\end{aligned}$$

The first two equalities are just algebra. The third relies on the fourth assertion in Theorem 11.1. The fourth uses the second assertion in Theorem 11.1 in the numerator and the first assertion in Theorem 11.1 in both numerator and denominator. The fifth equality relies in the denominator on the second assertion in Theorem 11.1, and it uses Example 10.5 in both numerator and denominator. The sixth equality follows from Example 10.4.

Definition 11.3 *A sequence* (x_n) *is said to be* bounded *if there is a number* $M \in \mathbf{R}$ *such that* $|x_n| \leq M$ *for all* $n \in \mathbf{N}$.

Proposition 11.4 *A convergent sequence is bounded.*

Proof. Suppose that (x_n) converges to L. Taking $\epsilon = 1$, we then have $N \in \mathbf{N}$ such that $n \geq N$ implies that $|x_n - L| < 1$. In particular, if $n \geq N$, then

$$|x_n| = |x_n - L + L| \leq |x_n - L| + |L| < 1 + |L|.$$

Moreover, since there are only finitely many indices n smaller than N, it follows that there is a number $K \in \mathbf{R}$ such that $|x_n| \leq K$ when $n < N$.

Therefore, if $M = \max\{K, 1+|L|\}$, we can conclude that $|x_n| \leq M$ for *all* $n \in \mathbf{N}$. That is, (x_n) is bounded. $\square$

Example 11.5 *Here and below, we will consider the sequence* (r^n) *for various real numbers* r. *For now, let us suppose that* $|r| > 1$. *I claim then (and it's that* (r^n) *is unbounded. In light of Proposition 11.4, it follows that* (r^n) *diverges (i.e. if convergent sequences are bounded then unbounded sequences diverge).*

Now my claim that (r^n) *is unbounded when* $|r| > 1$ *is intuitively pretty clear. However, technically, it needs justifying. This can be accomplished in much the same way we proved the Archimedean Property. Specifically, I suppose in order to reach a contradiction that* (r^n) *is bounded. That is, there is* $M \in \mathbf{R}$ *such that* $|r|^n \leq M$ *for all* $n \in \mathbf{N}$. *By the Completeness*

Axiom then, I can choose a least *upper bound m for the set $\{|r|^n : n \in \mathbf{N}\}$. Since $|r| > 1$, I have that $m/|r| < m$ and therefore that $|r^n| > m/|r|$ for some $n \in \mathbf{N}$. But then $|r^{n+1}| > m$, contradicting the fact that m is an upper bound for the powers of $|r|$. It follows that (r^n) is unbounded.* □

It is *not* true that a bounded sequence converges. For instance $((-1)^n)$ is bounded by 1, but we showed in the previous section that it does not converge. However, with a little additional information, boundedness of a sequence does sometimes imply its convergence.

Definition 11.6 *A sequence (x_n) is said to be* increasing *if $x_n \le x_{n+1}$ for all $n \in \mathbf{N}$. Similarly, (x_n) is said to be* decreasing *if $x_n \ge x_{n+1}$ for all $n \in \mathbf{N}$. Increasing and decreasing sequences are said to be* monotone*.*

Theorem 11.7 (Monotone Convergence Theorem) *A bounded monotone sequence converges.*

Proof. Let (x_n) be a bounded monotone sequence. Without loss of generality, we may assume that x_n is increasing. By the Completeness Axiom for $\mathbf{R}$, boundedness of (x_n) implies that there is a *least* upper bound L for the terms x_n. We will show that $\lim x_n = L$.

To do this, let $\epsilon > 0$ be given. On the one hand, we have that $x_n \le L$ for all $n \in \mathbf{N}$ because L is an upper bound for (x_n). On the other hand, since L is the *smallest* such upper bound, we know that $x_N > L - \epsilon$ for some $N \in \mathbf{N}$. Moreover, since (x_n) is increasing, we see additionally that $x_n \ge L - \epsilon$ for every $n \ge N$.

To summarize, we now see that $n \ge N$ implies that

$$L - \epsilon < x_n \le L < L + \epsilon.$$

In other words, $|x_n - L| < \epsilon$.

This proves that (x_n) converges to L. □

In order to apply this theorem, we prove a useful, albeit relatively minor, auxiliary result.

Lemma 11.8 *Suppose that (x_n) is a sequence with $\lim x_n = L$. Then $\lim x_{n+1} = L$, too.*

In other words, shifting the index by one in a sequence does not affect its limit.

Proof. Given $\epsilon > 0$, the hypothesis that $x_n \to L$ gives us a natural number N such that $n \ge N$ implies $|x_n - L| < \epsilon$. But if $n \ge N$, then $n + 1 \ge N$, too. Hence $n \ge N$ implies also that $|x_{n+1} - L| < \epsilon$. This proves $\lim x_{n+1} = L$. □

Example 11.9 *Let us again consider the sequence (r^n), this time for $0 \le r \le 1$. Then we have for all n that*

$$0 \le r^{n+1} = r \cdot r^n \le r^n < 1.$$

That is, the sequence is decreasing and bounded below by 0. By the Bounded Convergence Theorem, we conclude that (r^n) converges to some number $L \in \mathbf{R}$. Moreover, the previous lemma and the second assertion in Theorem 11.1 tell us that

$$L = \lim r^{n+1} = (\lim r)(\lim r^n) = rL.$$

That is, $L(1-r) = 0$. Thus either $r = 1$, in which case $\lim r^n = \lim 1 = 1$, or $\lim r^n = L = 0$.

Theorem 11.10 (Squeeze Theorem) *Let $(a_n), (b_n), (c_n)$ be sequences whose terms satisfy $a_n \leq b_n \leq c_n$ for all $n \in \mathbf{N}$. If (a_n) and (c_n) converge to $L \in \mathbf{R}$, then so does (b_n).*

Proof. Let $\epsilon > 0$ be given. Since $\lim a_n = L$, we have $N_1 \in \mathbf{N}$ such that $|a_n - L| < \epsilon$ whenever $n \geq N_1$. Similarly, we $N_2 \in \mathbf{N}$ such that $|b_n - L| < \epsilon$ whenever $n \geq N_2$. So if we take $N = \max N_1, N_2$, then for any $n \geq N$, we have

$$-\epsilon < a_n - L \leq b_n - L \leq c_n - L < \epsilon.$$

In other words $|b_n - L| < \epsilon$. We conclude that $\lim b_n = L$. $\square$

Example 11.11 *Returning once more to the sequence (r^n), we suppose that $-1 < r < 0$. Then since $0 < |r| < 1$ and*

$$-|r|^n < r^n < |r|^n$$

for all $n \in \mathbf{N}$, the Squeeze Theorem tells us that

$$0 = -\lim |r|^n \lim -|r|^n = \lim r^n = \lim |r|^n = 0.$$

Note that if we put all our examples together, we arrive at the following handy fact.

Proposition 11.12 *The sequence (r^n)*

- *diverges if $r \leq -1$ or $r > 1$;*
- *converges to 1 if $r = 1$; and*
- *converges to 0 if $-1 < r < 1$.*

12 Representing real numbers

Definition 12.1 *Let $b > 1$ be an integer. A* base b *(or* b-ary*) expansion is an expression*

$$d_k d_{k-1} \dots d_1 d_0 . d_{-1} d_{-2} \dots \tag{3}$$

where for each $j \leq k$, the digit d_j *is an integer in the range $\{0, \dots, b-1\}$. By convention, the leading index k is always taken to be non-negative; if $k > 0$, then one requires that the leading digit d_k be non-zero.*

For instance $3.141592654\dots$ is a familiar base 10 expansion. A typical base 2 expansion would be something like $10100.0010011100\dots$. Note that for the sake of simplicity we do not allow a leading minus sign in our expansions. So technically, we'll only be talking about b-ary expansions of *non-negative* real numbers. Our first and principal goal is to explain carefully how b-ary expansions correspond to real numbers and vice versa.

Given a base b expansion 3, $d_k \dots d_1 d_0 . d_{-1} d_{-2} \dots$, we associate a sequence $(x_n)_{n \in \mathbf{N}}$ of real numbers as follows. The *nth b-ary approximation* of the expansion is the real number

$$x_n =:= \sum_{j=-n}^{k} d_j b^j.$$

We write

$$x_n = d_k \dots d_0 . d_{-1} \dots d_{-n}$$

for short. So, for the base 10 expansion $3.14159265\dots$, we have

$$x_3 = 3.141 = 3 + 1 \cdot 10^{-1} + 4 \cdot 10^{-2} + 1 \cdot 10^{-3} = \frac{3141}{1000}.$$

Proposition 12.2 *We have for all $n \in \mathbf{N}$ that $0 \leq x_n \leq b^{k+1} - b^{-n}$*

Proof. Let us recall the formula for a geometric sum: if $r \neq 1$ is a real number and $m > \ell$ are integers, then

$$\sum_{j=\ell}^{m} r^j = \frac{r^{m+1} - r^\ell}{r - 1}.$$

Since $0 \leq d_j \leq b - 1$ for each j, we have

$$0 \leq x_n = \sum_{j=-n}^{k} d_j b^j \leq \sum_{j=-n}^{k} (b-1) b^j = (b-1) \frac{b^{k+1} - b^{-n}}{b-1} = b^{k+1} - b^{-n}.$$

$\square$

The next result tells us that we can identify each b-ary expansion with a non-negative real number.

Theorem 12.3 *The sequence* (x_n) *converges to a limit* $x \in \mathbf{R}$ *satisfying* $0 \leq x \leq b^{k+1}$.

Proof. Observe that $x_{n+1} - x_n = d_{-(n+1)} b^{-(n+1)} \geq 0$. Therefore (x_n) is increasing. Proposition 12.2 tells us that (x_n) is bounded. Therefore, by the Bounded Convergence Theorem, we find that (x_n) converges. The limit $x \in \mathbf{R}$ is the least upper bound of the terms x_n, and since all terms lie between 0 and b^{k+1}, we have $0 \leq x \leq b^{k+1}$. □

From now on, we will simply write

$$x = d_k \dots d_0.d_{-1} \dots$$

to indicate that we indentify the real number $x = \lim x_n$ with the b-ary expansion on the right. For example, the repeating 5-ary expansion $2.2222\dots$ is identified with the real number

$$x = \lim x_n = \lim_{n\to\infty} \sum_{j=-n}^{0} 2 \cdot 5^j = \lim_{n\to\infty} 2 \sum_{j=0}^{n} 5^{-j} = 2 \lim \frac{1-5^{-n+1}}{1-5^{-1}} = 2 \cdot \frac{1}{1-\frac{1}{5}} = \frac{5}{2}.$$

That is $2.2222 \dots = \frac{5}{2}$.

Having shown that each b-ary expansion gives rise to a real number, we must now show that each real number comes from some b-ary expansion. To do this, it helps to make a couple of observations about arithmetic of b-ary expansions.

Proposition 12.4 *Suppose in base* b *that* $x = d_k \dots d_0.d_{-1} \dots$ *and Then for any* $\ell \in \mathbf{Z}$, *we have* $b^\ell \cdot x = e_{k+\ell} \dots e_0.e_{-1} \dots$ *where* $e_{j+\ell} = d_j$ *for each* $j \leq k$.

In other words, one gets the b-ary expansion for $b^\ell x$ by shifting the decimal point ℓ places to the right in the b-ary expansion for x. So in base 10, for example, we have

$$10^5 \cdot 3.141592654 \dots = 314159.2654 \dots$$

Proof. We have

$$\begin{aligned} b^\ell x &= b^\ell \lim_{n\to\infty} d_k \dots d_0.d_{-1} \dots d_{-n} \\ &= b^\ell \lim_{n\to\infty} \sum_{j=-n}^{k} d_j b^j = \lim_{n\to\infty} \sum_{j=-n}^{k} d_j b^{j+\ell} = \lim_{n\to\infty} \sum_{j=-n+\ell}^{k+\ell} d_{j-\ell} b^j \\ &= \lim_{n\to\infty} d_k \dots d_{-\ell}.d_{-\ell-1} \dots d_{-n} = d_k \dots d_{-\ell}.d_{-\ell-1} \dots \end{aligned}$$

which is what we needed to show. □

Theorem 12.5 *Let* $b \in \mathbf{N} - \{1\}$ *be a given base. Then any real number* $x \in [0, \infty)$ *has a base* b *expansion.*

Proof. Since $b > 1$, we have that $x/b^\ell \in [0, 1)$ for some $\ell \in \mathbf{N}$. Moreover, if we can show that x/b^ℓ has a b-ary expansion $0.d_{-1}d_{-2}\dots$, then it follows from Proposition 12.4 that $x = d_{-1}\dots d_{-\ell}.d_{-\ell-1}\dots$. Therefore, we can assume without loss of generality that $x \in [0, 1)$.

For each $n \in \mathbf{N} \cup \{0\}$ we set

$$m_n = \max\{m \in \mathbf{N} : \text{ and } m \leq b^n x\}, \quad d_{-n} = m_n - bm_{n-1}.$$

We will show that the numbers d_{-n} are the digits in a b-ary expansion for x.

First we show that the value of d_{-n} is appropriate. Since $x < 1$, $m_0 = 0$. For $n \geq 1$, we have

$$m_n \leq b^n x < m_n + 1, \tag{4}$$

the latter inequality following from the fact that m_n is the *largest* integer not exceeding $b^n x$. Similarly, $m_{n-1} \leq b^{n-1}x < m_{n-1} + 1$. In particular, bm_{n-1} is an integer not exceeding $b^n x$, so it follows that $bm_{n-1} \leq m_n$. Putting these inequalities together, we deduce

$$0 \leq m_n - bm_{n-1} < b^n x - bm_{n-1} = b(b^{n-1}x - m_{n-1}) \leq b \cdot 1 = b.$$

That is, $m_n - bm_{n-1} = d_{-n} \in \{0, 1, \dots, b-1\}$ for every $n \in \mathbf{N}$.

Next we show that $x_n := m_n/b^n$ is the nth approximant of the expansion

$$0.d_{-1}d_{-2}\dots$$

Applying the definition of m_n and d_n repeatedly, we obtain

$$\begin{aligned} m_n &= bm_{n-1} + d_{-n} = b(bm_{n-2} + d_{-n+1}) + d_{-n} \\ &= b^2 m_{n-2} + bd_{-n+1} + d_{-n} = \dots \\ &= b^n m_0 + b^{n-1}d_{-1} + b^{n-2}d_{-2} + \cdots + bd_{-n+1} + d_{-n} \\ &= b^{n-1}d_{-1} + b^{n-2}d_{-2} + \cdots + bd_{-n+1} + d_{-n} \end{aligned}$$

since $m_n = 0$. Therefore

$$x_n = \frac{m_n}{d^n} = 0.d_{-1}d_{-2}\dots d_{-n+1}d_{-n}$$

as claimed.

Finally, the inequality (4) further implies

$$x - \frac{1}{b^n} < \frac{m_n}{b^n} \leq x.$$

So by the Squeeze Theorem,

$$x = \lim \frac{m_n}{b^n} = 0.d_{-1}d_{-2}\dots$$

□

It turns out that b-ary expansions are not always unique. For instance, in base 10,

$$1 = 1.000\cdots = 0.9999999\dots$$

One can see that the second expansion really does represent 1 by directly computing the sequence of approximants and then evaluating the limit. Alternatively, one can apply Proposition 12.4: if $x = 0.9999\ldots$, then we have

$$10 \cdot x = 9.99999\cdots = 9 + x$$

Solving for x gives $x = 1$. It turns out that a real number x has more than one b-ary expansion if and only if it has a *terminating expansion*; i.e. one for which there is an index N such that $d_n = 0$ for all $n \leq N$. Moreover, if x has a terminating expansion, then it has exactly one other expansion (what is it?). We will not prove these things here. Instead, we turn to the subject of b-ary expansions of rational numbers.

Definition 12.6 *A b-ary expansion $x = d_k \ldots d_0.d_{-1}\ldots$ is* repeating *if there exist $m \in \mathbf{Z}$ and $r \in \mathbf{Z}_+$ such that for all $j \leq m$, $d_j = d_{j-r}$. In this case, we write*

$$x = d_k \ldots d_0.d_{-1}\ldots\overline{d_m \ldots d_{m-r}},$$

and we call r the period *of the expansion.*

For example, in base 8

$$26.74\overline{543} := 26.74543543543543\ldots$$

is repeating with period $r = 3$ starting at digit $m = -3$. The real number associated to a repeating expansion is rational and can always be computed by using Proposition 12.4 as we did with $0.\overline{9}$ above. For instance, if $x = 26.74\overline{543}$, then

$$8^5x - 8^2x = 2674543.\overline{543} - 2674.\overline{543} = 2674543 - 2674.$$

However, one must take some care at this point, because the integers on the right are in expressed in base 8, whereas we are implicitly working in base 10 on the left. Since base 10 is more familiar, we resolve the problem by converting to base 10 on the right.

$$32704x = (8^5-8^2)x = 2\cdot8^6+6\cdot8^5+7\cdot8^4+(4-2)\cdot8^3+(5-6)\cdot8^2+(4-7)\cdot8+(3-4) = 750503.$$

Therefore, $x = \frac{750503}{32704}$, which (believe it or not) is in lowest terms.

It is also true that every rational number has a repeating b-ary expansion. To see why this is so, we will compute the base 7 expansion of $\frac{2}{5}$. Since $\frac{2}{5} \leq 1$, we have

$$\frac{2}{5} = 0.d_{-1}d_{-2}d_{-3}\ldots.$$

Multiplying by 7 gives

$$2 + \frac{4}{5} = 7 \cdot \frac{2}{5} = d_{-1}.d_{-2}\ldots d_{-3}$$

The portion of the expansion to the right of the decimal point is smaller than 1, so we must have $2 = d_{-1}$ and $\frac{4}{5} = 0.d_{-2}d_{-3}\ldots$ Mutliplying by 7 again, we find

$$5 + \frac{3}{5} = 7 \cdot \frac{4}{5} = d_{-2}.d_{-3}d_{-4}\ldots$$

Therefore $d_{-2} = 5$. Continuing in this fashion, we obtain

$$\begin{aligned} 6 + \frac{1}{5} &= d_{-3}.d_{-4}d_{-5}\cdots \Rightarrow d_{-3} = 6. \\ 1 + \frac{2}{5} &= d_{-4}.d_{-5}d_{-6}\cdots \Rightarrow d_{-4} = 1. \end{aligned}$$

At this point, we also notice that

$$\frac{2}{5} = 0.d_{-5}d_{-6}\cdots = 0.d_{-1}d_{-2}\ldots$$

so $d_{-5} = d_{-1}$, $d_{-6} = d_{-2}$, and so on. That is, the base 7 expansion of $\frac{2}{5}$ repeats with period 4. We conclude that

$$\frac{2}{5} = 0.\overline{2561}$$

The ideas used in the previous two examples can be codified to prove

Theorem 12.7 *A real number $x \geq 0$ has a repeating b-ary expansion if and only if x is rational.*

Proof. If $x = d_k \ldots d_0.d_{-1}\ldots$ repeats with period r beginning at digit m, then as in the previous example, we have

$$b^{j-m}x - b^{-m}x = (d_k \ldots d_{-m-1})_b.$$

In particular, we have $sx = t$ where $s, t \in \mathbf{N}$. Hence x is rational.

Now suppose that $\frac{s}{t} > 0$ is a rational number. We will show that $\frac{s}{t}$ has a repeating b-ary expansion. If $\frac{s}{t}$ has a terminating (and therefore repeating) expansion, then we are done, so we may assume that $\frac{s}{t}$ does not have a terminating expansion. In particular, we can assume that $t \geq 2$ (why?).

Consider the integers $b^j s \mod t$, $j \in \mathbf{N}$. Since every integer is congruent to one of the integers $0, 1, \ldots, t-1$ modulo t, we must have

$$b^{j_1}s \equiv b^{j_2} \mod t$$

for some $j_2 > j_1$. In particular, t divides $(b^{j_2} - b^{j_1})s$. Therefore, if the b-ary expansion of $\frac{s}{t}$ is $d_k \ldots d_0.d_{-1}\ldots$, then

$$d_k \ldots d_{-j_2}.d_{-j_2-1}d_{j_2-2}\cdots - d_k \ldots d_{-j_1}.d_{j_1-1}d_{j_1-2}\cdots = (b^{j_1} - b^{j_1})\frac{s}{t} = *.0000\cdots \in \mathbf{N}.$$

It follows (from uniqueness of non-terminating expansions) that $d_{-j_2-1} = d_{-j_1-1}$, $d_{-j_2-2} = d_{j_1-2}$ and so on. That is, the b-ary expansion of $\frac{s}{t}$ begins repeating with period $j_2 - j_1$ by (at least) the $-j_1$th digit.

13 Subsequences

We saw earlier that the sequence $((-1)^n)_{n\in\mathbf{N}}$ diverges. However, it is intuitively clear that in some weaker sense this sequence 'converges' to both 1 and -1. The notion of 'subsequence' is designed to give some credence to this intuition.

Definition 13.1 *Let $(x_n)_{n\in\mathbf{N}}$ be a sequence of real numbers and $(n_k)_{k\in\mathbf{N}}$ a strictly increasing sequence of natural numbers. Then the sequence $(x_{n_k})_{k\in\mathbf{N}}$ is called a* subsequence *of (x_n).*

So for example, taking $n_k = 2k$ shows us that the constant sequence $((-1)^2k) = (1)$ is a subsequence of $((-1)^n)$. Similarly, taking $n_k = 2k+1$ shows that the constant sequence (-1) is also a subsequence of $((-1)^n)$. The first subsequence converges to 1 and the second to -1. We call these numbers 'accumulation points' of $((-1)^n)$.

Definition 13.2 *If (x_n) is a subsequence and (x_{n_k}) is a subsequence converging to $L \in \mathbf{R}$, then we call L an* accumulation point *(or* limit point*) of (x_n).*

Returning to another familiar example, we consider $(\frac{1}{n})$. Taking $n = 2^k$ shows us that $(\frac{1}{2^k})$ is a subsequence. Note that in this case, both the sequence and the subsequence converge to 0. This is as one would expect.

Proposition 13.3 *If (x_n) converges to $L \in \mathbf{R}$, then so does every subsequence of (x_n).*

Proof. Let $(x_{n_k})_{k\in\mathbf{N}}$ be a subsequence. Note that since the indices (n_k) are strictly increasing (i.e. $n_k < n_{k+1}$ for every $k \in \mathbf{N}$), it follows that $n_k > k$ for all $k \in \mathbf{N}$. This can be proven inductively, and we leave the details as an exercise for the reader.

To show that $\lim x_{n_k} = L$, we let $\epsilon > 0$ be given. Since $\lim x_n = L$, we have $N \in \mathbf{N}$ such that $n \geq N$ implies $|x_n - L| < \epsilon$. Moreover, if $k \geq N$, we have from the previous paragraph that $n_k \geq N$. So $k \geq N$ implies $|x_{n_k} - L| < \epsilon$. Therefore $\lim x_{n_k} = L$. □

The utility of subsequences is that they are more flexible than sequences in many situations. That is, even when a given sequence doesn't converge, one can often choose a convergent subsequence. Recall for instance that a bounded sequence needn't converge. However, the next result shows that a bounded sequence always has a convergent subsequence.

Theorem 13.4 (Bolzano-Weierstrass Theorem) *Every bounded sequence has an accumulation point.*

Proof. Let (x_n) be a bounded sequence–say $|x_n| \leq M$ for every $n \in \mathbf{N}$. First we will define a sequence of closed intervals $[a_k, b_k]$, $k \in \mathbf{N}$ with the following properties:

- $[a_k, b_k]$ contains infinitely many terms of the sequence (x_n).
- $[a_{k+1}, b_{k+1}] \subset [a_k, b_k]$;
- $b_k - a_k = \frac{2M}{2^k}$.

Indeed we define our intervals 'recursively'. We take $[a_0, b_0] = [-M, M]$. Then we set $[a_1, b_1]$ equal to whichever half $[a_0, 0], [0, b_0]$ contains infinitely many terms of (x_n). If both halves contain infinitely many terms of (x_n), then we arbitrarily choose the left half (it doesn't matter). We then continue this process ad nauseum: given $[a_0, b_0], [a_1, b_1], \dots, [a_k, b_k]$, we split $[a_k, b_k]$ into two halves of equal length and let $[a_{k+1}, b_{k+1}]$ be a half that contains infinitely many points of (x_n). One can check without much trouble that the resulting intervals satisfy all three of the criteria we laid out above.

Observe that since $[a_{k+1}, b_{k+1}] \subset [a_k, b_k]$ for all $k \in \mathbf{N}$, it follows that (a_k) is inreasing and (b_k) is decreasing. Moreover, $|a_k|, |b_k| \leq M$ for all $k \in \mathbf{N}$. Therefore, the Bounded Convergence Theorem tells us that $\lim a_k = A$ and $\lim b_k = B$ for some $A, B \in \mathbf{R}$. In fact, we have

$$B - A = \lim b_k - a_k = \lim \frac{2M}{2^k} = 0,$$

so $A = B$.

Finally, we choose the indices n_k for our subsequence. We let $n_0 = 0$. Since $[a_1, b_1]$ contains infinitely many terms of (x_n), we can choose $n_1 > n_0$ to so that $x_{n_1} \in [a_1, b_1]$. We then proceed by iterating this process. Having chosen $n_0 < \cdots < n_k$, we take advantage of the fact that $[a_{k+1}, b_{k+1}]$ contains infinitely many terms of (x_n) to choose $n_{k+1} > n_k$ so that $x_{n_{k+1}} \in [a_{k+1}, b_{k+1}]$.

The end result is a subsequence (x_{n_k}) of (x_n) satisfying

$$a_k \leq x_{n_k} \leq b_k \text{ for all } k \in \mathbf{N}.$$

Since $\lim a_k = \lim b_k = A$, the squeeze theorem implies that $\lim x_{n_k} = A$. In particular (x_n) has an accumulation point. □

In closing, we consider an example that illustrates the point that sequences can behave *much* more wildly than our favorite whipping boy $\{(-1)^n\}$. Recall that the rational numbers and the natural numbers have the same cardinality. That is, there is a bijective function $f : \mathbf{N} \to \mathbf{Q}$. So letting $x_n = f(n)$ for every $n \in \mathbf{N}$, we obtain a sequence (x_n) and claim that *every real number is a limit point of* (x_n).

To prove the claim, let us fix a real number $L \in \mathbf{R}$. To prove that L is a limit point of (x_n), we must find a subsequence $(x_{n_k}) \subset (x_n)$ converging to L. We do this as follows. Let y_1 be a rational number between $L-1$ and L. Such a number exists by the density property. In fact (and this will be important in what follows), there are actually infinitely many such rational numbers. For now we just pick one and continue. Because f is surjective, we have $y_1 = f(n_1)$ for some $n_1 \in \mathbf{N}$.

Now we pick a rational number $y_2 \in (L - 1/2, L)$. Again, we have $y_2 = f(n_2)$ for some $n_2 \in \mathbf{N}$. Moreover, we can assume that $n_2 > n_1$; in other words we can assume that $y_2 \neq f(0), f(1), \dots f(n_1)$. This is because there are infinitely many rational numbers between $L-1/2$ and L, whereas only finitely many of them are accounted for by $f(0), f(1), \dots, f(n_1)$.

We then construct the rest of our subsequence in the same manner. Having chosen $y_1 = f(n_1) \in (L-1, L)$, $y_2 = f(n_2) \in (L-1/2, L)$, $\dots y_k = f(n_k) \in (L-1/k, L)$ with $n_1 \leq n_2 \leq \cdots \leq n_k$, we choose a rational number $y_{k+1} \in (L - \frac{1}{k+1}, L)$ different from $f(0), f(1), \dots, f(n_k)$. Then $y_{k+1} = f(n_{k+1})$ for some $n_{k+1} > n_k$.

The result is that $(y_k) = (f(n_k)) = (x_{n_k})_{k\in\mathbf{N}}$ is a subsequence of (x_n) satisfying $L-1/k < x_{n_k} < L$ for every $k \in \mathbf{N}$. Since $L = \lim L - 1/k = \lim L$, the Squeeze Theorem tells us that $L = \lim x_{n_k}$. That is, L is a limit point of (x_n).

Since L was an arbitrary real number, we conclude that *every* real number is a limit point of (x_n).

14 A Bit About Continuity

To wrap up our discussion of real numbers, we briefly consider the notion of a continuous function. The reader should be aware that there is a good deal more to say about this subject than we will mention here. Any undergraduate course in 'analysis' (i.e. advanced calculus) would go into more depth about continuity. However, our abrieviated discussion of continuity will allow us to state two important theorems about continuous functions and then end where we began with real numbers: with a statement about nth roots.

Definition 14.1 *Let $S \subset \mathbf{R}$ be a set and $f : S \to \mathbf{R}$ a function. We say that f is* continuous at $a \in S$ *if for every sequence (x_n) in S such that $x_n \to a$, we have*

$$\lim f(x_n) = f(a).$$

If f is continuous at every point of S, we say that f is continuous on S.

In other words, f is continous if you can 'move limits inside f'.

Example 14.2 *Every polynomial $P(x) = c_k x^k + c_{k-1}x^{k-1} + \cdots + c_1 x + c_0$ with coefficients $c_0, \ldots, c_k \in \mathbf{R}$ is continuous on $\mathbf{R}$. This follows from Theorem 11.1: if $x_n \to a$, then*

$$\begin{aligned} \lim P(x_n) &= \lim(c_k x_n^k + c_{k-1}x_n^{k-1} + \cdots + c_1 x_n + c_0 \\ &= \lim(c_k x_n^k) + \lim(c_{k-1}x_n^{k-1} + \cdots + \lim c_1 x_n + \lim c_0 \\ &= (\lim c_k)(\lim x_n)^k + (\lim c_{k-1})(\lim x_n)^{k-1} + (\lim c_1)(\lim x_n) + \lim c_0 \\ &= c_k a^k + c_{k-1}a^{k-1} + \ldots c_1 a + c_0 = P(a). \end{aligned}$$

Using the same kind of argument, one can also show that every rational function (i.e. quotient $P(x)/Q(x)$ of polynomials) is continuous on its domain (i.e. where the denominator is non-zero).

Example 14.3 *The function $f : \mathbf{R} \to \mathbf{R}$ given by*

$$f(x) = \begin{cases} 1 & \text{if } x \geq 0 \\ -1 & \text{if } x < 0 \end{cases}$$

is not continuous at 0. To see this, consider the sequence $(-1/n)$. This sequence converges to 0. However,

$$\lim f(-1/n) = \lim -1 = -1 \neq 1 = f(0)$$

contrary to the definition of continuity.

Theorem 14.4 *Let $f : [a, b] \to \mathbf{R}$ be continuous on the closed interval $[a, b]$. Then there are points $x_{min}, x_{max} \in [a, b]$ such that*

$$f(x_{min}) \leq f(x) \leq f(x_{max})$$

for every $x \in [a, b]$.

In other words, a continuous function on a closed interval has a maximum and a minimum value.

Proof. We will prove the existence of x_{max}. The proof for x_{min} is similar. We define a sequence of points $x_n \in [a, b]$ in one of two ways, depending on whether the range $f([a, b]) \subset \mathbf{R}$ is bounded above.

If the range is not bounded above, then for each $n \in \mathbf{N}$ we can choose $x_n \in [a, b]$ so that $f(x_n) \geq n$.

If the range is bounded above, then by the completeness axiom, the least upper bound $M := \sup f([a, b])$ exists. In this case, we can find for each $n \in \mathbf{N}$ a point $x_n \in [a, b]$ such that $f(x_n) \geq M - \frac{1}{n}$.

In either case, we get a sequence (x_n) inside the closed interval $[a, b]$, so the Bolzano-Weierstrass Theorem tells us that we can find a subsequence $(x_{n_k})_{k \in \mathbf{N}} \subset (x_n)$ converging to some point $x_{max} \in [a, b]$. Since f is continous, we see that

$$\lim_{k \to \infty} f(x_{n_k}) = f(x_{max}).$$

However, if the range of f is unbounded, then we also have that $|f(x_{n_k})| \geq n_k$ for every $k \in \mathbf{N}$. Since $n_k \to \infty$ and $k \to \infty$. This implies that the sequence of values $(f(x_{n_k}))_{k \in \mathbf{N}}$ is unbounded and (by Proposition 11.4) must diverge. This contradicts $\lim_{k \to \infty} f(x_{n_k}) = f(x_{max})$, so we conclude that the range of f is actually bounded.

This means that we are in the second case: $M - \frac{1}{n_k} \leq f(x_{n_k}) \leq M$ for every $k \in \mathbf{N}$. Since $M = \lim M = \lim M - \frac{1}{n_k}$, the Squeeze Theorem implies that

$$M = \lim f(x_{n_k}) = f(x_{max}).$$

Since M is an upper bound for the range of f, we have that $f(x) \leq f(x_{max})$ for every $x \in [a, b]$. □

Theorem 14.5 (Intermediate Value Theorem) *Let $f : [a, b] \to \mathbf{R}$ be a continuous function. Suppose that y is a number between $f(a)$ and $f(b)$. Then there exists $x \in [a, b]$ such that $f(x) = y$.*

To prove this, we need

Lemma 14.6 *Suppose that (x_n) is a convergent sequence such that $x_n \leq C$ for every $n \in \mathbf{N}$. Then $\lim x_n \leq C$.*

Proof. Exercise. □

Proof of the Intermediate Value Theorem. Suppose for argument's sake that $f(a) \leq f(b)$ (the opposite case is handled similarly). Then the set

$$S := \{x \in [a, b] : f(x) \leq y\}$$

contains a, and is bounded above by b. By the completeness axiom, it therefore has a least upper bound $x \in [a, b]$. For the moment, let us assume that $a < x < b$. We will deal later with the possibility that $x = a$ or $x = b$.

We define two sequences $(a_n), (b_n)$ converging to x as follows. For every $n \in \mathbf{N}$ we let $b_n \in [a, b]$ be a number satisfying $x < b_n \leq x + 1/n$. Similarly, we let $a_n \in S$ be a number satisfying $x - 1/n \leq a_n \leq x$. Note that we can choose a_n this way because x is the least upper bound for S. All told, we have

$$x - \frac{1}{n} \leq a_n \leq x < b_n \leq x + \frac{1}{n}.$$

So by the Squeeze Theorem $\lim a_n = \lim b_n = x$. Moreover, since f is continuous and $b_n \notin S$ for any $n \in \mathbf{N}$, we have

$$f(x) = \lim f(b_n) \geq y.$$

Likewise, since $a_n \in S$ for every $n \in \mathbf{N}$, continuity further tells us that

$$f(x) = \lim f(a_n) \leq y.$$

Putting the two inequalities together, we get $f(x) = y$, and the theorem is proved.

It remains to discuss the possibility that, for instance, $x = b$. In this case, we define the sequence (a_n) as above and find again that $f(b) = \lim f(a_n) \leq y$. But $f(b) \geq y$ by hypothesis, so we conclude that $f(b) = y$. The case $x = a$ is handled similarly. $\square$

Corollary 14.7 *Given any $n \in \mathbf{Z}_+$ and $y \in [0, \infty)$, there exists a unique $x \in [0, \infty)$ such that $x^n = y$.*

Proof. Let $f : [0, \infty) \to \mathbf{R}$ be given by $f(x) = x^n$. In particular, f is a polynomial and therefore continuous on $[0, \infty)$.

Suppose first that $y \leq 1$. Then

$$f(0) = 0 \leq y \leq 1 = f(1).$$

Therefore, by the Intermediate Value Theorem there is a number $x \in [0, 1]$ such that $x^n = f(x) = y$.

Suppose instead that $y \geq 1$. Then since $n \geq 1$, we have $f(1) = 1 \leq y \leq y^n = f(y)$. Therefore, by the Intermediate Value Theorem again, there exists $x \in [1, y]$ such that $x^n = f(x) = y$. This proves that every non-negative real number has a non-negative nth root.

Now suppose that some $y \in [0, \infty)$ has two non-negative nth roots x_1 and x_2. Then $x_1^n = x_2^n$. Now we have either $x_1 < x_2$, $x_1 > x_2$, or $x_1 = x_2$. If $x_1 < x_2$, then $n \geq 1$ implies $x_1^n < x_2^n$, which cannot be. Similarly, $x_2 < x_1$ implies $x_2^n < x_1^n$. Therefore, the only possibility is $x_1 = x_2$. This proves that non-negative nth roots are unique. $\square$

15 The Fundamental Theorem of Algebra

The main goal of this section is to prove

Theorem 15.1 (Fundamental Theorem of Algebra) *Every non-constant polynomial has a complex root.*

The proof relies on two basic facts that we will not prove here. However, it should be emphasized that we have already proved these things in the setting of *real* numbers and the proofs in the complex case are completely parallel. What is lacking is theory of convergence sequences of complex numbers, and as it turns out, this theory proceeds readily from the things we have done for sequences of real numbers.

Proposition 15.2 *Every polynomial $P : \mathbf{C} \to \mathbf{C}$ with complex coefficients is a continuous function.*

Theorem 15.3 *If $D = \{z \in \mathbf{C} : |z| \leq R\}$ is a closed disk, and $f : D \to \mathbf{C}$ is a continuous function, then there exists $z_0, z_1 \in D$ such that $|f(z_0)|$ is minimal and $|f(z_1)|$ is maximal—i.e. $|f(z_0)| \leq |f(z)| \leq |f(z_1)|$ for every $z \in D$.*

Taking these two facts for granted, we now proceed by fixing a polynomial $P(z) = a_n z^n + \cdots + a_0$ with coefficients $a_j \in \mathbf{C}$ and $a_n \neq 0$.

Lemma 15.4 *There exists $R > 0$ such that $|z| > R$ implies $|P(z)| \geq |P(0)|$.*

The proof of this lemma is a little messy, but it is essentially just using the fact that for $|z|$ large enough, the leading term $a_n z^n$ in $P(z)$ is much larger than all of the others put together.

Proof. Note that if $|z| \geq 1$, we have

$$\begin{aligned} |P(z)| &\geq |a_n z^n| - \left| \sum_{j=0}^{n-1} a_j z^{n-1} \right| \\ &\geq |a_n||z|^n - \sum_{j=0}^{n-1} |a_j||z|^j \\ &\geq |a_n||z|^n - |z|^{n-1} \sum_{j=0}^{n-1} |a_j| \\ &= |z|^{n-1}(|a_n||z| - \sum_{j=0}^{n-1} |a_j|). \end{aligned}$$

The first two inequalities follow from the triangle inequality. The third inequality is where the assumption $|z| \geq 1$ is used. If we further assume that

$$|z| \geq |a_n|^{-1} \left(|a_0| + \sum_{j=0}^{n-1} |a_j| \right),$$

then we can continue the previous estimate as follows.

$$|P(z)| \geq |z|^{n-1}(|a_0| + \sum_{j=0}^{n-1} |a_j| - \sum_{j=0}^{n-1} |a_j|) = |z|^{n-1}|a_0| \geq |a_0|.$$

Since $P(0) = a_0$, this proves that $|P(z)| \geq |P(0)|$ whenever

$$|z| \geq R := \max\left\{1, |a_n|^{-1}\left(|a_0| + \sum_{j=0}^{n-1} |a_j|\right)\right\}.$$

□

Corollary 15.5 *There exists $z_0 \in \mathbf{C}$ such that $|P(z_0)| \leq |P(z)|$ for all $z \in \mathbf{C}$.*

Proof. Let R be as in the Lemma 15.4 and let $D = \{z \in \mathbf{C} : |z| \leq R\}$. By Theorem 15.3, there exists $z_0 \in D$ such that $|P(z_0)| \leq |P(z)|$ for all $z \in D$. Since $0 \in D$, Lemma 15.4 tells us that

$$|P(z_0)| \leq |P(0)| \leq |P(z)|$$

for all $z \notin D$, too. Since $\mathbf{C} = D \cup (\mathbf{C} - D)$, we conclude that $|P(z_0)| \leq |P(z)|$ for all $z \in \mathbf{C}$. □

Proof of Fundamental Theorem of Algebra. Suppose, in order to get a contradiction, that the polynomial $P(z)$ has degree $n \geq 1$ but no roots. Let z_0, as in Corollary 15.5, be the point where $|P(z)|$ is minimal. Then $Q(z) := P(z + z_0)$ is also a degree n polynomial with no roots, and $|Q(z)|$ achieves its minimum value at $z = 0$. Since $Q(0) \neq 0$, we have

$$Q(z) = c_0 + c_k z^k + c_{k+1} z^{k+1} + \ldots c_n z^n$$

where $c_0 \neq 0$ and $k \leq n$ is the smallest *positive* index such that $c_k \neq 0$. In other words

$$Q(z) = c_0 + c_k z^k + z^{k+1} R(z)$$

for some polynomial R. Let $w \in \mathbf{C}$ satisfy $w^k = -c_0/c_k$ and M be the maximum value of $|R(z)|$ among points z with $|z| \leq |w|$. Then for $r < 1$ we have

$$|Q(rw)| = |c_0 + c_k r^k w^k + r^{k+1} w^{k+1} R(rw)| = |c_0(1-r^k) + r^{k+1} w^{k+1} R(rw)| \leq |c_0|(1-r^k) + M r^{k+1} |w|^{k+1}.$$

And if we further assume that $0 < r < \frac{|c_0|}{2M|w|^{k+1}}$, we find

$$|Q(rw)| \leq |c_0|(1 - r^k) + Mr \cdot r^k |w|^{k+1} \leq |c_0|(1 - r^k) + |c_0|\frac{r^k}{2} = |c_0|(1 - r^k/2) < |c_0|.$$

This contradicts the fact that $|Q(0)| = |c_0|$ is the minimum value of $|Q(z)|$. Therefore Q has a root after all, and so does the original polynomial P. □

16 Cardinality

We learn the following principle when we are quite young: one can determine whether two different sets contain the same number of objects by pairing each object in the first set with an object in the second; if there are no objects left over in either set, then the sets are the same size. Most of us first employed the set of fingers on our hands as the benchmark for sizing up other sets. Later on, we learned to abstract the pairing game somewhat and use (subsets of) $\mathbf{N}$ as our standard yardstick. It was Cantor's simple but revolutionary idea to extend the whole 'comparing by pairing' idea to permit comparison of sizes for infinite sets. The fundamental notion is as follows.

Definition 16.1 *We say that two sets A* have the same cardinality *if there exists a bijection $f : A \to B$. For short, we write $\#A = \#B$. More generally, we say that $\#A \leq \#B$ if there exists an injective function $f : A \to B$.*

Since a bijection and its inverse are both injective functions, it follows that $\#A = \#B$ implies $\#A \leq \#B$ and $\#B \leq \#A$. The notation suggests that the converse should also be true: if $\#A \leq \#B$ and $\#B \leq \#A$, then $\#A = \#B$. However, that is not always so obvious. For instance. the functions $f : (-1, 1) \to [-1, 1]$ given by $f(x) = x$ and $g : [-1, 1] \to (-1, 1)$ given by $g(y) = y/2$ are both injective. Hence $\#(-1, 1) \leq \#[-1, 1]$ and $\#[-1, 1] \leq \#(-1, 1)$. But it's not so clear whether there exists an actual bijection $h : (-1, 1) \to [-1, 1]$. In fact, there is. With a some ingenuity you can even give a formula for the function in this case. More generally, though, the Schroeder-Bernstein Theorem says that having an injection in either direction *always* implies that there's a bijection.

Theorem 16.2 (Schroeder-Bernstein, also Cantor) *Suppose that A and B are sets and that there exist injective functions $f : A \to B$ and $g : B \to A$. Then there is a bijection $h : A \to B$.*

So $\#A \leq \#B$ and $\#B \leq \#A$ imply that $\#A = \#B$ after all. The proof of this is amazingly short, but without elaboration it is also amazingly difficult to grasp. Here I drag the argument out a bit by tying it to a more familiar conundrum. Which came first: the chicken or the egg? Hopefully this makes it a little easier to understand.

Let's call the elements of A 'eggs' and those of B 'chickens'. If $b = f(a)$, then we'll say that b 'hatched from a', and if $a = g(b)$, we'll say that 'a was laid by b' (which sort of implies that all chickens are hens here, but this is what happens when you ruin a nice analogy by thinking too hard about it). Since f and g are injective, we know that no chicken hatches from more than one egg; nor is any egg laid by two different chickens. On the other hand, neither f nor g are assumed to be surjective: there might be 'unhatched' chickens (i.e. those in $B - f(A)$) and 'unlaid' eggs (i.e. those in $A - f(B)$).

Observe that each chicken and egg has an 'ancestory': for instance, if $a_0 \in A$ is an egg laid by $b_0 \in B$, and b_0 is hatched from $a_1 \in A$ and a_1 is laid by $b_1 \in B$, then the last few generations in the ancestory of a_0 are a_0, b_0, a_1, b_1. Now the ancestory of a_0 can be quite short. For instance, if a_0 is an unlaid egg, then the entire ancestory of a_0 consists of the single generation 'a_0'. More generally, if somewhere in the ancestory of a_0, we encounter an unlaid egg a_n, then the family tree stops there: and the full ancestory of a_0 is the finite sequence

$$a_0, b_0, a_1, b_1, \ldots, a_{n-1}, b_{n-1}, a_n.$$

In other words, $a_0 = g(f(g(f(\ldots g(f(a_n))\ldots))))$. We let $A_{egg} \subset A$ consist of those eggs whose ancestors begins with an unlaid egg.

Similarly, it could happen that the chicken came first: if we meet an unhatched chicken as we descend through the generations preceding a_0, then the full ancestory of is $a_0, b_0, \ldots, b_{n-1}, a_{n-1}, b_n$, where the unhatched chicken $b_n \in B$ is the ultimate progenitor. We let $A_{chicken}$ denote the set of eggs whose ancestors begins with an unhatched chicken.

A final possibility is that there is no 'first' ancestor: as we go back through the generations preceding a_0, we never encounter an unhatched chicken or an unlaid egg, and the ancestory of a_0 is then infinite $a_0, b_0, a_1, b_1, a_2, b_2, \ldots$. I should point out here that an ancestory might be infinite by being periodic: e.g. it could be that a_0 is laid by b_0 which hatches from a_1 which is laid by b_1 which hatches from a_0. So the ancestory $a_0, b_0, a_1, b_1, a_0, b_0, a_1, b_1, \ldots$ is infinite with period two[3]. Regardless, let us denote the set of all eggs with infinite ancestories by $A_{infinite}$.

This exhausts the possibilities for ancestories of eggs: we have $A = A_{egg} \cup A_{chicken} \cup A_{infinite}$, where the three subsets on the right are mutually disjoint. We have a corresponding partition-by-ancestory $B = B_{egg} \cup B_{chicken} \cup B_{infinite}$ of chickens.

Now we note that if $b = f(a)$ is the chicken that hatches from an egg $a \in A_{egg}$, then the ancestory of b looks like $b, a, b_0, a_1, b_1, \ldots, a_n$ and therefore also begins with an egg. This shows that $f(A_{egg}) \subset B_{egg}$. Similarly $f(A_{chicken}) \subset B_{chicken}$, $f(A_{infinite}) \subset B_{infinite}$, $g(B_{egg}) \subset A_{egg}$, and so on. Moreover, since every $b \in B_{egg}$ has at least one egg among its ancestors, we see that $f(A_{egg}) = B_{egg}$. As f is injective by hypothesis, it follows that f sends A_{egg} onto B_{egg} bijectively[4]. We likewise have that $g : B_{chicken} \to A_{chicken}$ and $f : A_{infinite} \to B_{infinite}$ are bijective.

Putting all this information together, we see now that we can define a bijection $h : A \to B$ as follows:

$$h(a) = \begin{cases} f(a) & \text{if} \quad a \in A_{egg} \text{ or } a \in A_{infinite} \\ g^{-1}(b) & \text{if} \quad a \in A_{chicken} \end{cases}$$

Then h is well-defined because the sets A_{egg}, $A_{infinite}$ and $A_{chicken}$ form a partition of A and because $g : B_{chicken} \to A_{chicken}$ is invertible. And h is bijective because $A_{egg}, A_{infinite}, A_{chicken}$ are sent bijectively (by f, f, and g^{-1}, respectively) onto the sets $B_{egg}, B_{infinite}, B_{chicken}$ which partition B. This completes the proof of the Schroeder-Bernstein Theorem. The issue of whether chickens or eggs came first remains open. □

[3]evidently, time travel is possible in the chicken and egg universes we are considering!

[4]note that by definition unhatched eggs belong to A_{egg} but not $g(B_{egg})$; so $g : B_{egg} \to A_{egg}$ is not necessarily surjective.

Glossary of notation

$\forall$ for every

$\exists$ there exists

$\exists!$ there exists unique

$\Box$ end of proof (alternatively, 'QED')

$\Rightarrow$ implies

$:=$ is defined to be equal to

$\mathbf{Z}$ set of integers $\ldots, -2, -1, 0, 1, 2, \ldots$

$\mathbf{N}$ set of non-negative integers $0, 1, 2, \ldots$

$\mathbf{Z}_+$ set of positive integers $1, 2, \ldots$

$\mathbf{Q}$ set of rational numbers

$\mathbf{R}$ set of real numbers

$a|b$ the integer a divides the integer b

$\in$ is an element of; e.g. '$3.2 \in \mathbf{R}$' means that 3.2 is an element of $\mathbf{R}$.

$\sum_{j=m}^{n} a_j$ $a_m + \cdots + a_n$

$\emptyset$ the empty set

$A \times B$ cartesian product of the sets A and B

xRy x is related to y by R

$[x]$ equivalence class of x

$\equiv \mod m$ congruent modulo m

$f : A \to B$ f is a function from A to B

$\#A$ cardinality of A

$\sup S$ least upper bound, or supremum, of a set $S \subset \mathbf{R}$

$\inf S$ greatest lower bound, or infimum, of a set $S \subset \mathbf{R}$

(x_n) sequence $x_0, x_1, x_2, \ldots$

$\lim x_n$ limit of the sequence (x_n)