# CS1231 Chapter 3

# Proofs

## 3.1 Mathematical theories

**Terminology 3.1.1.** A *definition* is a description of what a (newly introduced) piece of terminology or notation exactly means and does not mean.

**Definition 3.1.2.** (1) An integer is *even* if it is $2x$ for some integer $x$.

(2) An integer is *odd* if it is $2x + 1$ for some integer $x$.

**Example 3.1.3.** (1) The integer 0 is even because $0 = 2 \times 0$, where 0 is an integer.

(2) The integer $-1231$ is odd because $-1231 = 2 \times (-616) + 1$, where $-616$ is an integer.

**Definition 3.1.4.** (1) An *alphabet* is a set of symbols.

(2) A *string* over an alphabet $\Gamma$ is a finite sequence of symbols from $\Gamma$.

(3) The set of all strings over an alphabet $\Gamma$ is denoted $\Gamma^*$.

(4) The *length* of a string is the number of symbols the string has (including repetition).

**Example 3.1.5.** Let $\Gamma$ be the set that consists precisely of the symbols $\mathrm{A}, \mathrm{B}, \dots, \mathrm{Z}, 0, 1, 2, \dots, 9$, and let $\Phi$ be the set that consists precisely of the symbols $\mathrm{A}, \mathrm{B}, \dots, \mathrm{Z}, \mathrm{a}, \mathrm{b}, \dots, \mathrm{z}$.

(1) $\Gamma$ and $\Phi$ are alphabets.

(2) CS1231 is a string over $\Gamma$, but it is not a string over $\Phi$.

(3) $\mathrm{CS1231} \in \Gamma^*$, but $\mathrm{CS1231} \notin \Phi^*$.

(4) The length of the string CS1231 is 6.

**Terminology 3.1.6.** *Axioms* are propositions that are taken (without proof) to be true in a theory, to specify which objects the theory is about.

**Note 3.1.7.** Even for the same mathematical theory, one may choose different (but equivalent) axioms in different contexts.

**Terminology 3.1.8.** In mathematics, a *proof* of a proposition is a carefully reasoned argument, which may invoke definitions, axioms and previously established propositions, for convincing the reader/audience that the proposition is true beyond doubt.

| | | |
|---|---|---|
| **$\mathbb{R}$ includes $\mathbb{Q}$** | $\forall x \in \mathbb{Q}$ | $x \in \mathbb{R}.$ |
| **$\mathbb{Q}$ includes $\mathbb{Z}$** | $\forall x \in \mathbb{Z}$ | $x \in \mathbb{Q}.$ |
| **$\mathbb{Z}$ includes $\mathbb{N}$** | $\forall x \in \mathbb{N}$ | $x \in \mathbb{Z}.$ |
| **Closure of $\mathbb{R}$ under $+$** | $\forall x, y \in \mathbb{R}$ | $x + y \in \mathbb{R}.$ |
| **Closure of $\mathbb{R}$ under negatives** | $\forall x \in \mathbb{R}$ | $-x \in \mathbb{R}.$ |
| **Definition of $-$** | $\forall x, y \in \mathbb{R}$ | $x - y = x + (-y).$ |
| **Closure of $\mathbb{R}$ under $\times$** | $\forall x, y \in \mathbb{R}$ | $x \cdot y \in \mathbb{R}.$ |
| **Closure of $\mathbb{R}$ under reciprocals** | $\forall x \in \mathbb{R}$ | $\Big(x \neq 0 \to \dfrac{1}{x} \in \mathbb{R}\Big).$ |
| **Definition of $/$** | $\forall x, y \in \mathbb{R}$ | $\Big(y \neq 0 \to \dfrac{x}{y} = x \cdot \dfrac{1}{y}\Big).$ |
| **Naturality of $0$** | | $0 \in \mathbb{N}.$ |
| **Closure of $\mathbb{N}$ under $+1$** | $\forall x \in \mathbb{N}$ | $x + 1 \in \mathbb{N}.$ |
| **Induction** | Every set of natural numbers that contains 0 and is closed under the successor function must contain all natural numbers, i.e., for every set $A$ of natural numbers,<br>$0 \in A \wedge (\forall x \in A \;\; x + 1 \in A) \to \forall x \in \mathbb{N} \;\; x \in A.$ | |
| **Definition of $\mathbb{Z}$** | $\forall x \in \mathbb{R}$ | $(x \in \mathbb{Z} \leftrightarrow x \in \mathbb{N} \vee -x \in \mathbb{N}).$ |
| **Definition of $\mathbb{Q}$** | $\forall x \in \mathbb{R}$ | $\Big(x \in \mathbb{Q} \leftrightarrow \exists y, z \in \mathbb{Z} \;\; \Big(z \neq 0 \wedge x = \dfrac{y}{z}\Big)\Big).$ |
| **Associativity of $+$** | $\forall x, y, z \in \mathbb{R}$ | $(x + y) + z = x + (y + z).$ |
| **Associativity of $\cdot$** | $\forall x, y, z \in \mathbb{R}$ | $(x \cdot y) \cdot z = x \cdot (y \cdot z).$ |
| **Identity for $+$** | $\forall x \in \mathbb{R}$ | $x + 0 = x.$ |
| **Identity for $\cdot$** | $\forall x \in \mathbb{R}$ | $x \cdot 1 = x.$ |
| **Inverse for $+$** | $\forall x \in \mathbb{R}$ | $x + (-x) = 0.$ |
| **Inverse for $\cdot$** | $\forall x \in \mathbb{R}$ | $\Big(x \neq 0 \to x \cdot \dfrac{1}{x} = 1\Big).$ |
| **Commutativity of $+$** | $\forall x, y \in \mathbb{R}$ | $x + y = y + x.$ |
| **Commutativity of $\cdot$** | $\forall x, y \in \mathbb{R}$ | $x \cdot y = y \cdot x.$ |
| **Distributivity of $\cdot$ over $+$** | $\forall x, y, z \in \mathbb{R}$ | $x \cdot (y + z) = (x \cdot y) + (x \cdot z).$ |
| **Irreflexivity of $<$** | $\forall x \in \mathbb{R}$ | $x \not< x.$ |
| **Trichotomy** | $\forall x, y \in \mathbb{R}$ | $(x < y \vee x = y \vee y < x).$ |
| **Transitivity of $<$** | $\forall x, y, z \in \mathbb{R}$ | $(x < y \wedge y < z \to x < z).$ |
| **$+$ respects $<$** | $\forall x, y, z \in \mathbb{R}$ | $(x < y \to x + z < y + z).$ |
| **Closure of $\mathbb{R}^+$ under $\cdot$** | $\forall x, y \in \mathbb{R}$ | $(x > 0 \wedge y > 0 \to x \cdot y > 0).$ |
| **Completeness** | Every nonempty set of real numbers that has an upper bound in $\mathbb{R}$ must have a smallest upper bound in $\mathbb{R}$, i.e., for every nonempty set $A$ of real numbers,<br>$\exists b \in \mathbb{R} \;\; \forall x \in A \;\; x < b$<br>$\to \exists b^* \in \mathbb{R} \;\; \big(\forall x \in A \;\; x < b^*$<br>$\wedge \forall b \in \mathbb{R} \;\; \big((\forall x \in A \;\; x < b) \to b^* \leqslant b\big)\big).$ | |

Table 3.1: A list of axioms for $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$

**Notation 3.1.9.** The end of a proof is often marked by □. Some authors use ■, ⊣, or QED. Here QED stands for *quod erat demonstrandum*, which means "which was to be demonstrated" in Latin.

**Terminology 3.1.10.** One *(logically) deduces* or *infers* a proposition $q$ from propositions $p_1, p_2, \ldots, p_n$ if the forms of $p_1, p_2, \ldots, p_n, q$ alone (without involving the subject matter) guarantee that $q$ is true whenever $p_1, p_2, \ldots, p_n$ are all true.

**Example 3.1.11** (*modus ponens*)**.** Let $p, q$ be propositions. From $p \to q$ and $p$, one can deduce $q$.

**Justification.** As one can see from the following truth table, the only situation when $p \to q$ and $p$ are both true is when $q$ is also true.

| $p$ | $q$ | $p \to q$ |
|---|---|---|
| T | T | T |
| T | F | F |
| F | T | T |
| F | F | T |

□

**Exercise 3.1.12.** Let $p, q$ be propositions. From $p \to q$ and $\neg p$, can one deduce $\neg q$ in general? ✎ 3a

Nope, one cannot deduce ¬q from ¬p as ¬q can be T or F

**Example 3.1.13** (universal instantiation)**.** Let $P(x)$ be a sentence and $z$ be an object. From $\forall x\ P(x)$, one can deduce $P(z)$.

**Justification.** This follows directly from Definition 2.2.1(3), in which we defined exactly when $\forall x\ P(x)$ is true. □

**Example 3.1.14** (transitivity of the conditional)**.** Let $p, q, r$ be propositions. From $p \to q$ and $q \to r$, one can deduce $p \to r$.

**Justification.** This is based on the tautology from Tutorial Exercise 1.5. □

**Example 3.1.15** (transitivity of the biconditional)**.** Let $p, q, r$ be propositions. From $p \leftrightarrow q$ and $q \leftrightarrow r$, one can deduce $p \leftrightarrow r$.

**Justification.** This is based on Tutorial Exercise 1.4 and the transitivity of the conditional. □

**Note 3.1.16.** Typically, a proof in mathematics consists of a number of steps. Each step either comes from the definitions, the axioms or previously established propositions, or is deduced logically from the previous steps.

**Notation 3.1.17.** In a proof, one sometimes write $\therefore\ p$ in the case when $p$ is a proposition to indicate that $p$ is deduced logically from the immediately preceding step(s). One may read $\therefore$ as "therefore".

**Notation 3.1.18.** Like in Theorem 2.3.1 and Theorem 2.4.9, many proofs use the transitivity of the biconditional in the form

$$\begin{array}{r}
p_1 \leftrightarrow p_2. \\
p_2 \leftrightarrow p_3. \\
\vdots \\
p_{n-1} \leftrightarrow p_n. \\
\therefore\ p_1 \leftrightarrow p_n.
\end{array}$$

One may write this more succinctly as

$$\begin{aligned} p_1 &\Leftrightarrow p_2 \\ &\Leftrightarrow p_3 \\ &\vdots \\ &\Leftrightarrow p_n. \end{aligned}$$

Similarly, one may write a proof of the form

$$\begin{aligned} p_1 &\to p_2. \\ p_2 &\to p_3. \\ &\vdots \\ p_{n-1} &\to p_n. \\ \therefore\ p_1 &\to p_n. \end{aligned}$$

more succinctly as

$$\begin{aligned} p_1 &\Rightarrow p_2 \\ &\Rightarrow p_3 \\ &\vdots \\ &\Rightarrow p_n. \end{aligned}$$

Exercise : prove
(p ↔ q) ↔ r =/= p ↔ (q↔r)

**Note 3.1.19.** (1) One may use $\Leftrightarrow$ and $\Rightarrow$ for $\leftrightarrow$ and $\to$ respectively, but not vice versa, because their meanings are essentially the same between two propositions.

(2) In fact, it is common practice to use $\Leftrightarrow$ and $\Rightarrow$ exclusively in mathematical contexts where logic is not the subject matter. We will follow this common practice.

**Terminology 3.1.20.** (1) A *theorem* is a proposition that has a proof and is often of considerable significance (in the particular context).

(2) A *proposition* sometimes refers to a proposition in the sense of Definition 1.1.1 that has a proof and is of medium significance (in the particular context).

(3) A *lemma* is a proposition that has a proof and helps in the proofs of other propositions, but on its own is of little significance (in the particular context).

(4) A *corollary* is a proposition that can be deduced easily from other previously established propositions.

## 3.2 Proof techniques

**Technique 3.2.1.** To prove $\exists x\ P(x)$, where $P(x)$ is a sentence, produce a witness, i.e., an object $z$ for which $P(z)$ is true.

**Justification.** This is based on Note 2.2.5(4). □

**Proposition 3.2.2.** Some even integer $n$ satisfies $n^2 = 2n$.

| | | |
|---|---|---|
| **Base clause for exp** | $\forall x \in \mathbb{R}$ | $x^0 = 1.$ |
| **Recursion clause for exp** | $\forall x \in \mathbb{R}\ \forall y \in \mathbb{N}$ | $x^{y+1} = x^y \cdot x.$ |
| **Definition of $\leqslant$** | $\forall x, y \in \mathbb{R}$ | $(x \leqslant y \leftrightarrow x < y \vee x = y).$ |
| **Closure of $\mathbb{Z}$ under $+$** | $\forall x, y \in \mathbb{Z}$ | $x + y \in \mathbb{Z}.$ |
| **Closure of $\mathbb{Z}$ under $-$** | $\forall x, y \in \mathbb{Z}$ | $x - y \in \mathbb{Z}.$ |
| **Closure of $\mathbb{Z}$ under $\times$** | $\forall x, y \in \mathbb{Z}$ | $x \cdot y \in \mathbb{Z}.$ |
| **Closure of $\mathbb{Q}$ under $+$** | $\forall x, y \in \mathbb{Q}$ | $x + y \in \mathbb{Q}.$ |
| **Closure of $\mathbb{Q}$ under $-$** | $\forall x, y \in \mathbb{Q}$ | $x - y \in \mathbb{Q}.$ |
| **Closure of $\mathbb{Q}$ under $\times$** | $\forall x, y \in \mathbb{Q}$ | $x \cdot y \in \mathbb{Q}.$ |
| **Closure of $\mathbb{Q}$ under $/$** | $\forall x, y \in \mathbb{Q}$ | $\left(y \neq 0 \to \frac{x}{y} \in \mathbb{Q}\right).$ |
| $\mathbb{N} = \mathbb{Z}_{\geqslant 0}$ | $\forall x \in \mathbb{R}$ | $(x \in \mathbb{N} \leftrightarrow x \in \mathbb{Z} \wedge x \geqslant 0)$ |
| **Discreteness of $\mathbb{N}$** | $\forall x \in \mathbb{N}$ | $(x > 0 \to x \geqslant 1).$ |
| **Cancellation Law for $+$** | $\forall x, y_1, y_2 \in \mathbb{R}$ | $(x + y_1 = x + y_2 \to y_1 = y_2).$ |
| **Differences** | $\forall x, z \in \mathbb{R}$ | $x + (z - x) = z.$ |
| **Differences and negatives** | $\forall x, z \in \mathbb{R}$ | $z - x = z + (-x).$ |
| **Double negatives** | $\forall x \in \mathbb{R}$ | $-(-x) = x.$ |
| **Distributivity of $\cdot$ over $-$** | $\forall x, y, z \in \mathbb{R}$ | $x \cdot (y - z) = (x \cdot y) - (x \cdot z).$ |
| **Annihilator for $\times$** | $\forall x \in \mathbb{R}$ | $x \cdot 0 = 0.$ |
| **Cancellation Law for $\cdot$** | $\forall x, y_1, y_2 \in \mathbb{R}$ | $(x \neq 0 \wedge x \cdot y_1 = x \cdot y_2 \to y_1 = y_2).$ |
| **Quotients** | $\forall x, z \in \mathbb{R}$ | $\left(x \neq 0 \to x \cdot \frac{z}{x} = z\right).$ |
| **Double reciprocals** | $\forall x \in \mathbb{R}$ | $\left(x \neq 0 \to \frac{1}{1/x} = x\right).$ |
| **Zero divisors** | $\forall x, y \in \mathbb{R}$ | $(x \cdot y = 0 \to x = 0 \vee y = 0).$ |
| **Products and negatives** | $\forall x, y \in \mathbb{R}$ | $\big((-x) \cdot y = x \cdot (-y) \ \wedge\ x \cdot (-y) = -(x \cdot y)\big).$ |
| | $\forall x, y \in \mathbb{R}$ | $(-x) \cdot (-y) = x \cdot y.$ |
| **Quotients and negatives** | $\forall x, y \in \mathbb{R}$ | $\left(y \neq 0 \to \frac{-x}{y} = \frac{x}{-y} \ \wedge\ \frac{x}{-y} = -\frac{x}{y}\right).$ |
| | $\forall x, y \in \mathbb{R}$ | $\left(y \neq 0 \to \frac{-x}{-y} = \frac{x}{y}\right).$ |
| **Fraction equivalence** | $\forall x, y, z \in \mathbb{R}$ | $\left(y \neq 0 \wedge z \neq 0 \to \frac{x}{y} = \frac{x \cdot z}{y \cdot z}\right).$ |
| **Fraction addition** | $\forall u, v, x, y \in \mathbb{R}$ | $\left(v \neq 0 \wedge y \neq 0 \to \frac{u}{v} + \frac{x}{y} = \frac{u \cdot y + v \cdot x}{v \cdot y}\right).$ |
| **Fraction multiplication** | $\forall u, v, x, y \in \mathbb{R}$ | $\left(v \neq 0 \wedge y \neq 0 \to \frac{u}{v} \cdot \frac{x}{y} = \frac{u \cdot x}{v \cdot y}\right).$ |
| **Fraction division** | $\forall u, v, x, y \in \mathbb{R}$ | $\left(v \neq 0 \wedge x \neq 0 \wedge y \neq 0 \to \frac{u/v}{x/y} = \frac{u \cdot y}{v \cdot x}\right).$ |
| **Closure of $\mathbb{R}^+$ under $+$** | $\forall x, y \in \mathbb{R}$ | $(x > 0 \wedge y > 0 \to x + y > 0).$ |
| **Positivity of negatives** | $\forall x \in \mathbb{R}$ | $\big((x > 0 \vee x = 0 \vee -x > 0) \ \wedge\ \neg(x > 0 \wedge -x > 0)\big).$ |
| | $\forall x \in \mathbb{R}$ | $(x < 0 \to -x > 0).$ |
| **Positivity of one** | | $1 > 0.$ |
| **Positivity of products** | $\forall x, y \in \mathbb{R}$ | $\big(x \cdot y > 0 \to (x > 0 \wedge y > 0) \vee (x < 0 \wedge y < 0)\big).$ |
| **Positivity of squares** | $\forall x \in \mathbb{R}$ | $(x \neq 0 \to x^2 > 0).$ |
| **Positivity and $<$** | $\forall x, y \in \mathbb{R}$ | $(x < y \leftrightarrow y - x > 0).$ |
| **$+$ respects $<$** | $\forall u, v, x, y \in \mathbb{R}$ | $(u < v \wedge x < y \to u + x < v + y).$ |
| **Negatives and $<$** | $\forall x, y \in \mathbb{R}$ | $(x < y \to -y < -x).$ |
| **$\cdot$ and $<$** | $\forall x, y, z \in \mathbb{R}$ | $(x < y \wedge z > 0 \to x \cdot z < y \cdot z).$ |
| | $\forall x, y, z \in \mathbb{R}$ | $(x < y \wedge z < 0 \to x \cdot z > y \cdot z).$ |
| | $\forall u, v, x, y \in \mathbb{R}$ | $(u > 0 \wedge x > 0 \wedge u < v \wedge x < y \to u \cdot x > 0 \wedge u \cdot x < v \cdot y).$ |
| **Strict trichotomy** | $\forall x, y \in \mathbb{R}$ | $\big(\neg(x < y \wedge x = y) \wedge \neg(x = y \ \wedge\ y < x) \wedge \neg(y < x \wedge x < y)\big).$ |
| **Archimedean property of $\mathbb{R}$** | $\forall x \in \mathbb{R}\ \exists y \in \mathbb{N}$ | $y > x.$ |

Table 3.2: Some properties of $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ bootstrapped from the axioms

**Proof.** The integer 2 is even because $2 = 2 \times 1$ where 1 is an integer. Also $2^2 = 4 = 2 \times 2$. □

**Technique 3.2.3.** One way to prove $p \to q$, where $p, q$ are propositions, is to assume $p$ is true, then prove (from this assumption) that $q$ must also be true.

**Proposition 3.2.4.** The square of any even integer is even.

**Proof.** We want to prove that if $n$ is an even integer, then $n^2$ is an even integer.

Let $n$ be an even integer. Use the definition of even integers to find an integer $x$ such that $n = 2x$. Then $n^2 = (2x)^2 = 2(2x^2)$, where $2x^2$ is an integer. So $n^2$ is even by the definition of even integers. □

**Convention 3.2.5.** In proofs, when there is no risk of ambiguity, it is sometimes convenient and instructive to use the same letter for both a variable and an object to be substituted into that variable.

**Exercise 3.2.6.** Let $n$ be an integer. Prove that ✎ 3b

(1) if $n$ is even, then $-n$ is even;

(2) if $n$ is odd, then $-n$ is odd.

**Technique 3.2.7** (proof by contraposition)**.** One way to prove $p \to q$, where $p, q$ are propositions, is to assume $q$ is false, then prove (from this assumption) that $p$ must also be false.

**Justification.** This is based on the equivalence of a conditional proposition $p \to q$ and its contrapositive $\neg q \to \neg p$ from Theorem 1.4.12(1). □

**Proposition 3.2.8.** Any integer whose square is even must itself be even.

**Proof.** We want to prove that for every integer $n$, if $n^2$ is even, then $n$ is even. We will prove instead the contrapositive, that for every integer $n$, if $n$ is not even, then $n^2$ is not even.

Let $n$ be an integer that is not even. Then $n$ is odd. Use the definition of odd integers to find an integer $x$ such that $n = 2x+1$. Then $n^2 = (2x+1)^2 = 4x^2+4x+1 = 2(x^2+2x)+1$, where $x^2+2x$ is an integer. So $n^2$ is odd by the definition of odd integers. This implies $n^2$ is not even, as required. □

**Technique 3.2.9.** One way to prove $p \leftrightarrow q$, where $p, q$ are propositions, is to prove both $p \to q$ and $q \to p$.

**Justification.** This is based on the equivalence of $p \leftrightarrow q$ and $(p \to q) \wedge (q \to p)$ from Tutorial Exercise 1.4. □

**Corollary 3.2.10.** An integer is even if and only if its square is even.

**Proof.** The "←" part is given by Proposition 3.2.8. The "→" part is given by Proposition 3.2.4. □

**Technique 3.2.11** (splitting into cases)**.** One way to prove a proposition $r$ is to first find two propositions $p$ and $q$ such that either $p$ or $q$ is true, and then prove $r$ from each of $p$ and $q$.

**Justification.** This is based on the tautology $(p \vee q) \wedge (p \to r) \wedge (q \to r) \to r$ from Extra Exercise 1.8. □

**Proposition 3.2.12.** If $n$ is an integer, then $n(n+1)$ is even.

**Proof.** We split into two cases.

**Case 1: suppose $n$ is even.** Use the definition of even integers to find an integer $x$ such that $n = 2x$. Then $n(n+1) = (2x)(2x+1) = 2(x(2x+1))$, where $x(2x+1)$ is an integer. So $n(n+1)$ is even.

**Case 2: suppose $n$ is odd.** Use the definition of odd integers to find an integer $x$ such that $n = 2x+1$. Then $n(n+1) = (2x+1)((2x+1)+1) = 2((2x+1)(x+1))$, where $(2x+1)(x+1)$ is an integer. So $n(n+1)$ is even.

So $n(n+1)$ is even in all cases. □

**Remark 3.2.13.** One can split into more than two cases in a proof, say $p_1, p_2, \ldots, p_n$ where each $p_i$ is a proposition, but one must make sure that these $p_i$'s cover all possibilities, i.e., that $p_1 \vee p_2 \vee \cdots \vee p_n$ must be true.

**Note 3.2.14.**

(1) We used implicitly in the proof of Proposition 3.2.12 that every integer is either even or odd, i.e., Proposition 3.2.21.

(2) In addition to Proposition 3.2.21, we used implicitly in the proof of Proposition 3.2.8 that no integer is both even and odd, i.e., Proposition 3.2.17.

(3) Formally Propositions 3.2.17 and 3.2.21 should appear before Propositions 3.2.12 and 3.2.8, and we should not use Propositions 3.2.12 and 3.2.8 in our proofs of Propositions 3.2.17 and 3.2.21.

**Exercise 3.2.15.** Identify where we used Propositions 3.2.17 and 3.2.21 in our proof of Proposition 3.2.8. ✎ 3c

**Technique 3.2.16** (proof by contradiction, also known as *reductio ad absurdum*)**.** One way to prove a proposition $p$ is to assume that $p$ is false, then prove (from this assumption) a contradiction.

**Justification.** This is based on the tautology $(\neg p \to c) \to p$, where $c$ is a contradiction, from Extra Exercise 1.9. □

**Proposition 3.2.17.** No integer is both even and odd.

**Proof.** Suppose some integer, say $n$, is both even and odd. Use the definition of even and odd integers to find integers $x, y$ such that $n = 2x$ and $n = 2y+1$. As $x$ and $y$ are both integers, so is $x - y$, but

$$x - y = \frac{n}{2} - \frac{n-1}{2} = \frac{1}{2},$$

which is not an integer. So we have a contradiction. It follows that no integer can be both even and odd. □

**Exercise 3.2.18** (extra)**.** We used in the proof of Proposition 3.2.17 that $1/2$ is not an integer. Try to prove this from the axioms in Table 3.1 and the properties in Table 3.2. Here you may define $1/2$ to be the (unique) real number $x$ satisfying $2x = 1$. ✎ 3d

**Technique 3.2.19** (Mathematical Induction (MI))**.** Let $b$ be an integer and $P(n)$ be a predicate over $\mathbb{Z}_{\geqslant b}$. To prove that $\forall n \in \mathbb{Z}_{\geqslant b}\ \ P(n)$ is true, it suffices to:

**(base step)** show that $P(b)$ is true; and

**(induction step)** show that $\forall k \in \mathbb{Z}_{\geqslant b}\ \ \big(P(k) \rightarrow P(k+1)\big)$ is true.

Induction hypothesis

**Justification.** The two steps ensure the following are true:

$$\begin{array}{ll}
P(b) & \text{by the base step;} \\
P(b) \rightarrow P(b+1) & \text{by the induction step with } k = b; \\
P(b+1) \rightarrow P(b+2) & \text{by the induction step with } k = b+1; \\
P(b+2) \rightarrow P(b+3) & \text{by the induction step with } k = b+2; \\
\quad\vdots &
\end{array}$$

We deduce that $P(b), P(b+1), P(b+2), \ldots$ are all true by a series of modus ponens. □

**Terminology 3.2.20.** In the induction step, we assume we have an integer $k \geqslant b$ such that $P(k)$ is true, and then show $P(k+1)$ using this assumption. In this process, the assumption that $P(k)$ is true is called the *induction hypothesis*.

**Proposition 3.2.21.** Every integer is either even or odd.

**Proof.** In view of Exercise 3.2.6, it suffices to show that every non-negative integer is either even or odd. We prove this by MI. Let $P(n)$ be the predicate "$n$ is either even or odd" over $\mathbb{Z}_{\geqslant 0}$.

**(Base step)** We know $0 = 2 \times 0$, where 0 is an integer. So 0 is even. Thus $P(0)$ is true.

**(Induction step)** Let $k$ be a non-negative integer such that $P(k)$ is true, i.e., that $k$ is either even or odd. If $k$ is even, say $k = 2x$ where $x$ is an integer, then $k+1 = 2x+1$, which is odd. If $k$ is odd, say $k = 2x+1$ where $x$ is an integer, then $k+1 = 2x+2 = 2(x+1)$, which is even. So $k+1$ is either even or odd in all cases. This shows $P(k+1)$ is true.

Hence $\forall n \in \mathbb{Z}_{\geqslant 0}\ \ P(n)$ is true by MI. □

**Terminology 3.2.22.** We call the proof above an induction *on* $n$ because $n$ is the active variable in it.

**Technique 3.2.23** (Strong Mathematical Induction (Strong MI))**.** Let $b$ be an integer and $P(n)$ be a predicate over $\mathbb{Z}_{\geqslant b}$. To prove that $\forall n \in \mathbb{Z}_{\geqslant b}\ \ P(n)$ is true, it suffices to choose some integer $c \geqslant b$ and:

**(base step)** show that $P(b), P(b+1), \ldots, P(c)$ are true;

**(induction step)** show that

$$\forall k \in \mathbb{Z}_{\geqslant c}\ \ \big(P(b) \wedge P(b+1) \wedge \cdots \wedge P(k) \rightarrow P(k+1)\big)$$

is true.

**Justification.** The two steps ensure the following are true:

Everything behind implies that the next is true

$$\begin{aligned}
&P(b) \land P(b+1) \land \cdots \land P(c) \\
&\qquad\qquad\qquad\qquad \text{by the base step;} \\
&P(b) \land P(b+1) \land \cdots \land P(c) \to P(c+1) \\
&\qquad\qquad\qquad\qquad \text{by the induction step with } k = c; \\
&P(b) \land P(b+1) \land \cdots \land P(c) \land P(c+1) \to P(c+2) \\
&\qquad\qquad\qquad\qquad \text{by the induction step with } k = c+1; \\
&P(b) \land P(b+1) \land \cdots \land P(c) \land P(c+1) \land P(c+2) \to P(c+3) \\
&\qquad\qquad\qquad\qquad \text{by the induction step with } k = c+2; \\
&\qquad\quad \vdots
\end{aligned}$$

We deduce that $P(b), P(b+1), P(b+2), P(b+3), \ldots$ are all true by a series of modus ponens. □

**Proposition 3.2.24.** For every positive integer $n$, there exist a non-negative integer $a$ and an odd integer $b$ such that $n = 2^a b$.

**Proof.** Let $P(n)$ be the predicate "there exist a non-negative integer $a$ and an odd integer $b$ such that $n = 2^a b$" over $\mathbb{Z}_{\geqslant 1}$.

**(Base step)** $P(1)$ is true because $1 = 2^0 \times 1$, where 0 is a non-negative integer and 1 is an odd integer.

**(Induction step)** Let $k$ be a positive integer such that $P(1), P(2), \ldots, P(k)$ are all true. Proposition 3.2.21 tells us that $k+1$ is either even or odd.

**Case 1: suppose $k+1$ is even.** Use the definition of even integers to find an integer $x$ such that $k+1 = 2x$. As $k \geqslant 1$,

$$x = \frac{k+1}{2} \geqslant \frac{1+1}{2} = 1 \quad \text{and} \quad 2k = k+k \geqslant k+1 = 2x.$$

Thus $1 \leqslant x \leqslant k$ and so $P(x)$ is true by the induction hypothesis. Find a non-negative integer $a$ and an odd integer $b$ such that $x = 2^a b$. Then $k+1 = 2x = 2(2^a b) = 2^{a+1} b$, where $a+1$ is a non-negative integer.

**Case 2: suppose $k+1$ is odd.** Then $k+1 = 2^0(k+1)$, where 0 is a non-negative integer.

So $P(k+1)$ is true in all cases.

Hence $\forall n \in \mathbb{Z}_{\geqslant 1}\ \ P(n)$ is true by Strong MI. □

**Exercise 3.2.25** (extra)**.** In Strong MI, one can actually allow $c = b - 1$. How may one make sense of this? ✎ 3e

**Definition 3.2.26.** Let $P(x)$ be a sentence. Then "there exists a unique $x$ such that $P(x)$", sometimes denoted $\exists! x\ P(x)$, means the conjunction of the two propositions below.

**(existence)** "There is at least one $x$ such that $P(x)$", or symbolically $\exists x\ P(x)$.

**(uniqueness)** "There is at most one $x$ such that $P(x)$", or symbolically

$$\forall x_1, x_2\ \big(P(x_1) \land P(x_2) \to x_1 = x_2\big).$$

∀m,n ∈Z (odd(m) ∧ odd(n)) →∃! a ∈Z (m^2 + n^2 = 4a+2))

**Proposition 3.2.27.** For all odd numbers $m, n$, there exists a unique integer $a$ such that $m^2 + n^2 = 4a + 2$.

**Proof.** (Existence) Use the definition of odd numbers to find integers $x, y$ such that $m = 2x+1$ and $n = 2y+1$. Then $m^2+n^2 = (2x+1)^2+(2y+1)^2 = 4x^2+4x+1+4y^2+4y+1 = 4(x^2+x+y^2+y)+2$, where $x^2+x+y^2+y$ is an integer.

(Uniqueness) Suppose $a_1, a_2$ are integers such that $m^2+n^2 = 4a_1+2$ and $m^2+n^2 = 4a_2+2$. Then $4a_1+2 = 4a_2+2$. Subtract 2 from both sides, then divide both sides by 4. Then we see that $a_1 = a_2$. □

**Exercise 3.2.28.** Prove that the $a$ and the $b$ from Proposition 3.2.24 are unique, i.e., if $a_1, a_2$ are non-negative integers and $b_1, b_2$ are odd integers such that $2^{a_1}b_1 = 2^{a_2}b_2$, then $a_1 = a_2$ and $b_1 = b_2$. ✏ 3f

**Remark 3.2.29.** In professional mathematical discourse, one may start a proof for Exercise 3.2.28 by assuming $a_1 \leqslant a_2$ *without loss of generality* because the case when $a_2 \leqslant a_1$ can be handled in exactly the same way by suitably renaming the numbers. In this module, we suggest that students avoid making such assumptions: write out the proof in full, even if it involves repeating some steps. The reason is that, at this level, many students still cannot tell when one can make an assumption without loss of generality, and when not.

## Tutorial exercises

An asterisk (*) indicates a more challenging exercise.

3.1. Someone tries to prove that $x^2 \geqslant 0$ for all real numbers $x$ as follows.

> Suppose not. Then $x^2 < 0$ for all real numbers $x$. However, we know 1 is a real number and $1^2 = 1 \geqslant 0$. This is a contradiction. So $x^2 \geqslant 0$ for all real numbers $x$.

What is wrong with this attempt?

3.2. Consider the proposition "there is a real number $x$ such that $x^2 + 9 = 6x$."

(a) Someone tries to prove this proposition as follows.

> Let $x$ be a real number such that $x^2+9 = 6x$. Then $x^2 - 6x + 9 = 0$. This implies $(x-3)^2 = 0$. Thus $x - 3 = 0$ and so $x = 3$.

What is wrong with this attempt?

(b) Give a correct proof of this proposition.

3.3.* In this exercise, we establish an equivalent formulation of the notion of symmetry from Exercise 2.1.

Let $P(x, y)$ be a predicate on a set $A$. Prove that the following are equivalent.

(a) $\forall x, y \in A \ \ \big(P(x,y) \rightarrow P(y,x)\big)$.

(b) $\forall x, y \in A \ \ \big((P(x,y) \wedge P(y,x)) \vee (\neg P(x,y) \wedge \neg P(y,x))\big)$.

What techniques did you use in your proof? Indicate where you used them.

## Extra exercises

3.4. Someone tries to prove that $x^2 - 6x + 7 > 0$ for all real numbers $x$ as follows.

> Real numbers are negative, zero, or positive. We consider these three cases separately.
>
> - If $x < 0$, say $x = -1$, then $x^2-6x+7 = (-1)^2-6\times(-1)+7 = 1+6+7 = 14 > 0$.
> - If $x = 0$, then $x^2 - 6x + 7 = 0^2 - 6 \times 0 + 7 = 7 > 0$.
> - If $x > 0$, say $x = 1$, then $x^2 - 6x+7 = 1^2 - 6\times 1+7 = 1-6+7 = 2 > 0$.
>
> Since $x^2 - 6x + 7 > 0$ in all the cases, the proposition is proved.

What is wrong with this attempt?

3.5.* Prove that, for all integers $m$ and $n$, if $m^2 + n^2 = k^2$ for some integer $k$, then $m$ and $n$ cannot be both odd.

(Hint: You may find many propositions proved in this chapter useful.)