Chapter 5 Proof techniques

- direct proof (start from antecedent as assumption, deduce to conclusion; contrapositive included here)
- contradiction proof (show that $P \wedge \neg Q$ (the negation) leads to an impossibility)
- proof by cases (break up antecedent into seperate cases and deduce conclusion in each case)

Def Let $a, b \in \mathbb{Z}$ and $a \neq 0$. Then a *divides* b if (and only if) there exists $n \in \mathbb{Z}$ such that $b = an$.

↓ when mathematicians write definitions they mean "if and only if..." but only write "if..."

When a divides b, we write this as $a \mid b$.

Ex $5 \mid 15$ because $\exists\, n \in \mathbb{Z}$ such that $5 \cdot n = 15$ (namely $n = 3$).

Theorem Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$. If $a \mid b$ and $a \mid c$ then $a \mid (b+c)$.

Proof outline: Assume: • $a, b, c \in \mathbb{Z}$, $a \neq 0$

• $a \mid b$, $a \mid c$

Goal: show $a \mid (b+c)$, which means showing

$\exists\ n \in \mathbb{Z}$ such that $b+c = an$.

Proof Let $a, b, c \in \mathbb{Z}$ such that $a \neq 0$, $a \mid b$, and $a \mid c$. Since $a \mid b$, there exists $j \in \mathbb{Z}$ such that $b = aj$. Likewise, since $a \mid c$, there exists $k \in \mathbb{Z}$ such that $c = ak$.

Therefore

$$\begin{aligned} b+c &= aj + ak \\ &= a(j+k). \end{aligned}$$

Thus since $n = j+k \in \mathbb{Z}$ and $b+c = an$, we have that $a \mid b+c$.

Theorem The number $\sqrt{2}$ is not rational.

Proof Our proof will proceed by contradiction. That is, we assume $\sqrt{2}$ is rational. Thus, $\sqrt{2} = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ with $b \neq 0$, where $\frac{a}{b}$ is a simplified fraction so that a and b have no common factors.

This implies $2 = \left(\frac{a}{b}\right)^2 = \frac{a^2}{b^2}$, and so $a^2 = 2b^2$.

Therefore a^2 is even, which implies a is even (*).

Since a is even, there exists $n \in \mathbb{Z}$ such that $a = 2n$.

That means $b^2 = \frac{1}{2}a^2 = \frac{1}{2}(2n^2) = 2n^2$, which implies b^2 is even and in turn b is even. Thus there exists $m \in \mathbb{Z}$ such that $b = 2m$. However, this is a contradiction because $\frac{a}{b}$ was supposed to be a simplified fraction where a and b have no common factors.

(*) When writing proofs, each step should be clear. The implication a^2 even $\Rightarrow$ a even is not immediately obvious, so I want you to prove it and add it to your proof. What counts as "clear" or "immediate" evolves and requires you to think about your audience. We aim for our readers to understand each step.

Problem 1. Let $a, b, c \in \mathbb{Z}$ with $a, b \neq 0$. Prove that if $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof Let $a, b, c \in \mathbb{Z}$ with $a, b \neq 0$ such that $a \mid b$ and $b \mid c$.

We aim to show that $a \mid c$ by showing there exists $k \in \mathbb{Z}$ such that $ak = c$. Since $a \mid b$, there exists $n \in \mathbb{Z}$ such that $an = b$ and since $b \mid c$, there exists $m \in \mathbb{Z}$ such that $bm = c$. Observe that

$$\begin{aligned} c &= bm \\ &= (an)m \\ &= a(nm). \end{aligned}$$

Therefore, since $k = nm \in \mathbb{Z}$, we have shown $a \mid c$.

Problem 2. Give a proof by contradiction of the following statement. "There is not a smallest positive rational number."

Proof Suppose by way of contradiction that there is a smallest positive rational number q. Therefore, $q = \frac{a}{b}$ for some positive integers a, b such that $q \leq x$ for any positive rational x. Observe that $p = \frac{a}{b+1}$ is a positive rational. Therefore $q \leq p$ and so $\frac{a}{b} \leq \frac{a}{b+1}$.

This implies $\frac{a(b+1)}{b(b+1)} - \frac{ab}{b(b+1)} \leq 0$, which implies.

$\frac{1}{b(b+1)} \leq 0$. However this is a contradiction since $b > 0$.