

Number Systems Homework

Real Analysis

Answer Key

1. From well-ordering to induction.

Assume the *well-ordering principle*: every nonempty subset of $\mathbb{N}$ has a least element. Let $P(n)$ be a statement defined for every $n \in \mathbb{N}$, where 1 is the least natural number. Suppose that $P(1)$ is true and that, for every $k \in \mathbb{N}$, if $P(k)$ is true, then $P(k+1)$ is true.

- (a) To prove the principle of mathematical induction, suppose instead that $P(n)$ is false for at least one $n \in \mathbb{N}$, and define

$$F = \{n \in \mathbb{N} : P(n) \text{ is false}\}.$$

Explain why F has a least element m and why $m \neq 1$.

- (b) Explain why $m-1 \in \mathbb{N}$ and why the minimality of m implies that $P(m-1)$ is true.
(c) Use the inductive implication with $k = m-1$ to obtain a contradiction. Conclude that well-ordering implies the principle of mathematical induction.

Solution. If P fails somewhere, then F is nonempty, so well-ordering gives a least element m . Since $P(1)$ is true, $1 \notin F$, and hence $m \neq 1$. Because 1 is the least element of $\mathbb{N}$ and $m \neq 1$, we have $m > 1$, so $m-1 \in \mathbb{N}$. The minimality of m gives $m-1 \notin F$; thus $P(m-1)$ is true. The inductive implication now shows that $P(m)$ is true, contradicting $m \in F$. Therefore F is empty and $P(n)$ is true for every $n \in \mathbb{N}$.

2. Commutativity of multiplication on the natural numbers.

Recall that multiplication on $\mathbb{N}$ is defined recursively by

$$n \cdot 0 = 0, \quad n \cdot S(m) = n \cdot m + n.$$

In this problem, you will use the principle of mathematical induction to prove that multiplication is commutative. You may use the previously established properties of addition.

- (a) Use induction on n to prove that

$$0 \cdot n = 0.$$

- (b) Fix $n \in \mathbb{N}$. Use induction on m to prove the auxiliary identity

$$S(n) \cdot m = n \cdot m + m$$

for every $m \in \mathbb{N}$.

- (c) Fix $n \in \mathbb{N}$. Use induction on m , together with parts (a) and (b), to prove that

$$n \cdot m = m \cdot n$$

for every $m \in \mathbb{N}$.

Solution. For part (a), the base case is $0 \cdot 0 = 0$. If $0 \cdot n = 0$, then

$$0 \cdot S(n) = 0 \cdot n + 0 = 0.$$

Thus $0 \cdot n = 0$ for every $n \in \mathbb{N}$.

For part (b), fix $n \in \mathbb{N}$. When $m = 0$,

$$S(n) \cdot 0 = 0 = n \cdot 0 + 0.$$

Suppose $S(n) \cdot m = n \cdot m + m$. Then, using the recursive definition and the properties of addition,

$$\begin{aligned} S(n) \cdot S(m) &= S(n) \cdot m + S(n) \\ &= (n \cdot m + m) + S(n) \\ &= (n \cdot m + n) + S(m) \\ &= n \cdot S(m) + S(m). \end{aligned}$$

The auxiliary identity follows by induction.

For part (c), fix $n \in \mathbb{N}$ and induct on m . The base case is $n \cdot 0 = 0 = 0 \cdot n$ by part (a). Suppose $n \cdot m = m \cdot n$. Then

$$n \cdot S(m) = n \cdot m + n = m \cdot n + n = S(m) \cdot n,$$

where the final equality follows from part (b). Therefore multiplication on $\mathbb{N}$ is commutative.

3. The rational numbers: operations and order.

Construct $\mathbb{Q}$ from pairs $(a, b) \in \mathbb{Z} \times \mathbb{N}$, where

$$(a, b) \sim (c, d) \iff ad = bc.$$

Define

$$\begin{aligned} [(a, b)] + [(c, d)] &= [(ad + bc, bd)], \\ [(a, b)] [(c, d)] &= [(ac, bd)], \\ [(a, b)] < [(c, d)] &\iff ad < bc. \end{aligned}$$

Suppose $(a, b) \sim (a', b')$ and $(c, d) \sim (c', d')$.

- Prove that rational addition is well-defined.
- Prove that rational multiplication is well-defined.
- Prove that the strict ordering is well-defined. Clearly identify where the fact that $b, b', d, d' \in \mathbb{N}$ are positive is used.
- Let $x = [(a, b)]$ with $a \neq 0$. Prove from the definitions that $x^{-1} = [(b, a)]$ when $a > 0$, and $x^{-1} = [(-b, -a)]$ when $a < 0$. In particular, verify that $xx^{-1} = 1$.

Solution. The hypotheses are $ab' = a'b$ and $cd' = c'd$. For addition, we must show

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

After expanding, this follows by multiplying $ab' = a'b$ by dd' and multiplying $cd' = c'd$ by bb' . For multiplication, multiplying the two equivalences gives $acb'd' = a'c'bd$.

For order, suppose $ad < bc$. Since $bb'dd' > 0$, multiplication by positive integers and substitution using $ab' = a'b$ and $cd' = c'd$ give

$$ad < bc \iff ab'dd' < bb'cd' \iff a'bdd' < bb'c'd \iff a'd' < b'c'.$$

The reverse direction is identical. Positivity ensures that multiplying or cancelling does not reverse the inequality.

If $a > 0$, then (b, a) is an allowed representative and

$$[(a, b)][(b, a)] = [(ab, ab)] = [(1, 1)].$$

If $a < 0$, then $-a > 0$, $(-b, -a)$ is allowed, and

$$[(a, b)][(-b, -a)] = [(-ab, -ab)] = [(1, 1)].$$

Thus the stated elements are multiplicative inverses.

4. The real numbers: Cauchy sequences and well-defined operations.

Let $\mathcal{C}_{\mathbb{Q}}$ be the set of rational Cauchy sequences. For $(x_n), (y_n) \in \mathcal{C}_{\mathbb{Q}}$, define

$$(x_n) \sim (y_n) \iff \text{for every } \varepsilon > 0, \text{ eventually } |x_n - y_n| < \varepsilon.$$

The real numbers are the equivalence classes $[(x_n)]$, with addition and multiplication defined term by term.

- (a) If $(x_n) \sim (x'_n)$ and $(y_n) \sim (y'_n)$, prove that $(x_n + y_n) \sim (x'_n + y'_n)$. Thus, addition on $\mathbb{R}$ is well-defined.
- (b) Under the same hypotheses, prove that $(x_n y_n) \sim (x'_n y'_n)$. You may use the fact that every Cauchy sequence is bounded. Also use the identity

$$x_n y_n - x'_n y'_n = x_n (y_n - y'_n) + y'_n (x_n - x'_n).$$

Thus, multiplication on $\mathbb{R}$ is well-defined.

- (c) Explain why the tempting definition

$$[(x_n)] < [(y_n)] \iff x_n < y_n \text{ eventually}$$

is not well-defined by comparing the equivalent sequences (0) and $(1/n)$. State a corrected definition using an eventual fixed positive separation, and prove that your definition does not depend on the representatives.

Solution. Given $\varepsilon > 0$, eventually $|x_n - x'_n| < \varepsilon/2$ and $|y_n - y'_n| < \varepsilon/2$. Hence

$$|(x_n + y_n) - (x'_n + y'_n)| \leq |x_n - x'_n| + |y_n - y'_n| < \varepsilon.$$

By boundedness, choose $M > 0$ such that $|x_n| \leq M$ and $|y'_n| \leq M$ for every n , increasing M if necessary. Eventually both $|y_n - y'_n| < \varepsilon/(2M)$ and $|x_n - x'_n| < \varepsilon/(2M)$. The given identity and the triangle inequality then yield

$$|x_n y_n - x'_n y'_n| < M \frac{\varepsilon}{2M} + M \frac{\varepsilon}{2M} = \varepsilon.$$

The sequences (0) and $(1/n)$ are equivalent, but $0 < 1/n$ for every n ; replacing $(1/n)$ by the equivalent sequence (0) changes the truth of the proposed relation. A correct definition declares $[(x_n)] < [(y_n)]$ when there are $r \in \mathbb{Q}$, with $r > 0$, and $N \in \mathbb{N}$ such that $y_n - x_n \geq r$ for every $n \geq N$. If $(x_n) \sim (x'_n)$ and $(y_n) \sim (y'_n)$, eventually $|x_n - x'_n| < r/4$ and $|y_n - y'_n| < r/4$. Therefore

$$y'_n - x'_n \geq (y_n - x_n) - |y_n - y'_n| - |x_n - x'_n| > r/2.$$

Thus the corrected relation is independent of the representatives.

5. Completeness and the Archimedean property.

You may now use the least-upper-bound property of $\mathbb{R}$. The *Archimedean property* states that for every $x \in \mathbb{R}$, there is an $n \in \mathbb{N}$ such that $n > x$.

- (a) Suppose, for contradiction, that $\mathbb{N}$ is bounded above in $\mathbb{R}$, and let $s = \sup \mathbb{N}$. Explain why $s - 1$ is not an upper bound for $\mathbb{N}$.
- (b) Choose $n \in \mathbb{N}$ satisfying $n > s - 1$ and use $n + 1 \in \mathbb{N}$ to contradict the fact that s is an upper bound. Conclude that $\mathbb{R}$ has the Archimedean property.
- (c) Prove that for every $\varepsilon > 0$, there is an $n \in \mathbb{N}$ such that $0 < 1/n < \varepsilon$.
- (d) Prove that for every $x \in \mathbb{R}$, there is an $m \in \mathbb{Z}$ such that

$$m - 1 \leq x < m.$$

In particular, $m - 1 \leq x \leq m$. (Choose $N \in \mathbb{N}$ with $N > |x|$ and apply well-ordering to $\{j \in \mathbb{N} : j - N > x\}$.)

Solution. If $s - 1$ were an upper bound, it would be an upper bound smaller than the least upper bound s . Hence some $n \in \mathbb{N}$ satisfies $n > s - 1$. Then $n + 1 > s$, but $n + 1 \in \mathbb{N}$, contradicting that s is an upper bound. Therefore $\mathbb{N}$ is unbounded above, which is the Archimedean property.

Given $\varepsilon > 0$, apply the Archimedean property to $1/\varepsilon$ and choose $n > 1/\varepsilon$. Positivity gives $0 < 1/n < \varepsilon$.

Given $x \in \mathbb{R}$, choose $N \in \mathbb{N}$ with $N > |x|$ and define

$$A = \{j \in \mathbb{N} : j - N > x\}.$$

The Archimedean property makes A nonempty, so let j_0 be its least element and set $m = j_0 - N$. Then $x < m$. If $m - 1 > x$, the preceding natural-number index would also belong to A , contradicting the minimality of j_0 ; the initial-index case is ruled out by $-N < x$. Therefore $m - 1 \leq x < m$, and hence also $m - 1 \leq x \leq m$.

6. **The rational numbers are dense in the real numbers.**

Let $a, b \in \mathbb{R}$ with $a < b$. The goal is to prove that there is a $q \in \mathbb{Q}$ such that $a < q < b$.

(a) Use the Archimedean property to choose $n \in \mathbb{N}$ such that

$$n(b - a) > 1.$$

(b) Apply Problem 5(d) to na to obtain an $m \in \mathbb{Z}$ satisfying

$$m - 1 \leq na < m.$$

Prove that $m < nb$.

(c) Set $q = m/n$. Prove that $a < q < b$, and conclude that $\mathbb{Q}$ is dense in $\mathbb{R}$.

Solution. Choose $n > 1/(b - a)$. Then $n(b - a) > 1$. By Problem 5(d), choose $m \in \mathbb{Z}$ with $m - 1 \leq na < m$. We have

$$m \leq na + 1 < na + n(b - a) = nb.$$

Since $na < m < nb$ and $n > 0$, division by n gives $a < m/n < b$. Thus $q = m/n \in \mathbb{Q}$ lies in (a, b) .