Logic and Proof Chapter 21 Exercises

Lyle Kopnicky

March 6, 2019

1. Show that addition for the integers, as defined in Section 21.2, is commutative and associative.

   Proof. Recall that the relation $\equiv$ is defined on $\mathbb{N} \times \mathbb{N}$ by $(m, n) \equiv (m', n')$ if and only if $m + n' = m' + n$.

   First we will prove commutativity. Suppose we have integers $[(m_1, n_1)]$ and $[(m_2, n_2)]$.

   Then $[(m_1, n_1)] + [(m_2, n_2)] = [(m_1 + m_2, n_1 + n_2)]$. Commuting the terms, $[(m_2, n_2)]+[(m_1, n_1)] = [(m_2+m_1, n_2+n_1)]$. By commutativity of addition on natural numbers, we have that $m_1 + m_2 = m_2 + m + 1$ and $n_1 + n_2 = n_2 + n_1$, so their equivalence classes must be the same, as well.

   Now we will prove associativity. Again, we just base the proof on the associativity of addition on the natural numbers.

$$\begin{aligned}
&([(m_1, n_1)] + [(m_2, n_2)]) + [(m_3, n_3)] \\
&= [(m_1 + m_2, n_1 + n_2)] + [(m_3, n_3)] \\
&= [((m_1 + m_2) + m_3, (n_1 + n_2) + n_3)] \\
&= [(m_1 + (m_2 + m_3), n_1 + (n_2 + n_3))] \\
&= [(m_1, n_1)] + [(m_2 + m_3, n_2 + n_3)] \\
&= [(m_1, n_1)] + ([(m_2, n_2)] + [(m_3, n_3)])
\end{aligned}$$

2. Show from the construction of the integers in Section 21.2 that $a+0 = a$ for every integer a.

   Proof. For an integer a represented as $[(m, n)]$, we can add zero:

$$[(m, n)] + [(0, 0)] = [(m + 0, n + 0)] = [(m, n)]$$

   Yes, we could have used some other representation of a or of 0, but we've already proven that addition respects the equivalence relation.

3. Define subtraction for the integers by $a - b = a + (-b)$, and show that $a - b + b = a$ for every pair of integers a and b.

   Representing a as $[(m_a, n_a)]$ and b as $[(m_b, n_b)]$, we have

$$\begin{aligned} a - b + b &= a + (-b) + b \\ &= [(m_a, n_a)] + -[(m_b, n_b)] + [(m_b, n_b)] \\ &= [(m_a, n_a)] + [(n_b, m_b)] + [(m_b, n_b)] \\ &= [(m_a + n_b, n_a + m_b)] + [(m_b, n_b)] \\ &= [(m_a + n_b + m_b, n_a + m_b + n_b)] \\ &= [(m_a + (m_b + n_b), n_a + (m_b + n_b))] \end{aligned}$$

   To show that the last line is equal to a, we use the equivalence relation. Since we have:

$$m_a + (m_b + n_b) + n_a = m_a + n_a + (m_b + n_b)$$

   we can rewrite this as the equivalence:

$$[(m_a + (m_b + n_b), n_a + (m_b + n_b))] \equiv [(m_a, n_a)].$$

4. Define multiplication for the integers, by first defining it on the underlying representation and then showing that the operation respects the equivalence relation.

   Def. Since $[(m, n)]$ represents $m - n$, we can think of $[(m_1, n_1)] \times [(m_2, n_2)]$ as $(m_1 - n_1)(m_2 - n_2)$. The ms are both positive and thus will end up in the left of the resulting pair, along with the ns, which are both negative. The terms of opposite sign will produce negative numbers, and thus will end up on the right side of the pair.

   Thus we can define multiplication $[(m_1, n_1)] \times [(m_2, n_2)]$ to be

$$[(m_1 m_2 + n_1 n_2, m_1 n_2 + n_1 m_2)].$$

   Proof. Now to show that this definition respects the equivalence relation. Suppose that $(m_1, n_1) \equiv (m_1', n_1')$ and $(m_2, n_2) \equiv (m_2', n_2')$. Then we must show that $(m_1 m_2 + n_1 n_2, m_1 n_2 + n_1 m_2) \equiv (m_1' m_2' + n_1' n_2', m_1' n_2' + n_1' m_2')$.

   The first equivalence gives us:

$$m_1 + n_1' = m_1' + n_1, \tag{1}$$

and the second gives us

$$m_2 + n'_2 = m'_2 + n_2. \tag{2}$$

The third one, which we're trying to prove, expands to:

$$\begin{aligned} &m_1m_2 + n_1n_2 + m'_1n'_2 + n'_1m'_2 \\ &= m'_1m'_2 + n'_1n'_2 + m_1n_2 + n_1m_2 \end{aligned} \tag{3}$$

We can use (1) and (2) as follows: We know that some number multiplied by the left side of (1) is equal to the same number multiplied by the right side of (1). The same holds for (2), or any equation. Here we carefully choose some factors to multiply by the one side of (1) on the left side of the equation, and by the other side of (1) on the other side of the equation. And the same with (2).[1]

$$\begin{aligned} &m_2(m_1 + n'_1) + n_2(m'_1 + n_1) + m'_1(m_2 + n'_2) + n'_1(m'_2 + n_2) \\ =&m_2(m'_1 + n_1) + n_2(m_1 + n'_1) + m'_1(m'_2 + n_2) + n'_1(m_2 + n'_2) \end{aligned}$$

We can transform that by expanding the multiplications using the distributive law for natural numbers:

$$\begin{aligned} &m_2m_1 + m_2n'_1 + n_2m'_1 + n_2n_1 + m'_1m_2 + m'_1n'_2 + n'_1m'_2 + n'_1n_2 \\ =&m_2m'_1 + m_2n_1 + n_2m_1 + n_2n'_1 + m'_1m'_2 + m'_1n_2 + n'_1m_2 + n'_1n'_2. \end{aligned}$$

Then reorder each term using commutativity so that the subscripts are always in increasing order:

$$\begin{aligned} &m_1m_2 + n'_1m_2 + m'_1n_2 + n_1n_2 + m'_1m_2 + m'_1n'_2 + n'_1m'_2 + n'_1n_2 \\ =&m'_1m_2 + n_1m_2 + m_1n_2 + n'_1n_2 + m'_1m'_2 + m'_1n_2 + n'_1m_2 + n'_1n'_2. \end{aligned}$$

Finally, we can cancel out terms that appear on both sides of the equation. Specifically, all the terms that have one factor with a prime and the other factor without a prime cancel out:

$$\begin{aligned} &m_1m_2 + n_1n_2 + m'_1n'_2 + n'_1m'_2 \\ =&n_1m_2 + m_1n_2 + m'_1m'_2 + n'_1n'_2 \end{aligned}$$

Compare this to (3). It's the same except for rearranging the terms on the right side. Thus, we have proven that our definition for multiplication of integers respects the equivalence relation.

[1] I got some help from `https://www.math.wustl.edu/~freiwald/310integers.pdf`.

5. Show that every Cauchy sequence is bounded: that is, if $(q_i)_{i\in\mathbb{N}}$ is Cauchy, there is some rational M such that $|q_i| \leq M$ for all i. Hint: try letting $\varepsilon = 1$.

   Proof. For reference, the definition of a Cauchy sequence: A sequence of rational numbers $(q_i)_{i\in\mathbb{N}}$ is *Cauchy* if for every rational number $\varepsilon > 0$, there is some natural number $N \in \mathbb{N}$ such that for all $i, j \geq N$, we have that $|q_i - q_j| < \varepsilon$.

   Choose $\varepsilon = 1$. Then there is some natural number N such that for all $i, j \geq N$, $|q_i - q_j| < \varepsilon$. Let m be the maximum value of $|q_i|$ for $i \leq N$. Then we can choose M to be $m + 1$.

   Why? For any $i \leq N$, this is true by how we constructed m. For $i > N$, we have from the definition of Cauchy sequence that $|q_i - q_N| < \varepsilon$. We know from the construction of m that $|q_N| \leq m$. Then we have:

$$\begin{aligned}
|q_i| &\leq |q_N| + |q_i - q_N| && \text{(triangle inequality)} \\
&\leq m + |q_i - q_N| && \text{(substitution)} \\
&< m + \epsilon && \text{(substitution)} \\
&= m + 1 && \text{(substitution)} \\
&= M && \text{(substitution)}
\end{aligned}$$

   So, by transitivity, $|q_i| \leq M$.

6. Let $p = (p_i)_{i\in\mathbb{N}}$ and $q = (q_i)_{i\in\mathbb{N}}$ be Cauchy sequences. Define $p + q = (p_i + q_i)_{i\in\mathbb{N}}$ and $pq = (p_i q_i)_{i\in\mathbb{N}}$.

   a. Show that $p+q$ is Cauchy. That is, for arbitrary $\varepsilon > 0$, show that there exists an N such that for all $i, j \geq N$, $|(p_i+q_i)-(p_j+q_j)| < \varepsilon$.

      Proof. Assume we are given an arbitrary ε. Since p is Cauchy, there is an N_p such that for all $i, j \geq N_p$, $|p_i - p_j| < \varepsilon/2$. Since q is Cauchy, there is an N_q such that for all $i, j \geq N_q$, $|q_i - q_j| < \varepsilon/2$. Then choose $N = \max(N_p, N_q)$. Since $N \geq N_p$, we have that for all $i, j \geq N$, $|p_i - p_j| < \varepsilon/2$. Likewise, since $N \geq N_q$, we have for all $i, j \geq N$ that $|q_i - q_j| < \varepsilon/2$.
      Combining these, we have for all $i, j \geq N$ that $|p_i - p_j| + |q_i - q_j| < \varepsilon$. The triangle inequality tells us that $|(p_i + q_i) - (p_j + q_j)| \leq |p_i - p_j| + |q_i - q_j|$. Transitively, we get $|(p_i + q_i) - (p_j + q_j)| < \varepsilon$.

   b. Show that pq is Cauchy. In addition to the triangle inequality, you will find the previous exercise useful.

Proof. Assume we are given an arbitrary ε. Since p is Cauchy, there is an N_p such that for all $i, j \geq N_p$, $|p_i - p_j| < \varepsilon$. Since q is Cauchy, there is an N_q such that for all $i, j \geq N_q$, $|q_i - q_j| < 1$.

Then choose $N = \max N_p, N_q$. Since $N \geq N_p$, we have that for all $i, j \geq N$, $|p_i - p_j| < \varepsilon$. Likewise, since $N \geq N_q$, we have for all $i, j \geq N$ that $|q_i - q_j| < 1$.

Combining these, we have for all $i, j \geq N$ that $|p_i - p_j||q_i - q_j| < \epsilon$. It's a straightforward case analysis on negative versus positive factors to show that $|(p_i - p_j)(q_i - q_j)| < \epsilon$.

7. These two parts show that addition of Cauchy sequences respects equivalence.

   a. Show that if p, p', q are Cauchy sequences and $p \equiv p'$, then $p + q \equiv p' + q$.

   Proof. Since $p \equiv p'$, we have that for every rational number $\varepsilon > 0$, there is some natural number N such that for all $i \geq N$, we have that $|p_i - p'_i| < \varepsilon$.

   Since for all $i \geq N$, $q_i - q_i = 0$, we have that $|p_i - p'_i + q_i - q_i| < \varepsilon$. We can rearrange those terms to get $|(p_i + q_i) - (p'_i + q_i)| < \varepsilon$. And that's what we need, to show that $p + q \equiv p' + q$.

   b. Using the first part of this problem, show that if p, p', q, q' are Cauchy sequences, $p \equiv p'$, and $q \equiv q'$, then $p + q \equiv p' + q'$. You can use the fact that addition on the real numbers is commutative.

   Proof. From the first part of the problem, $p \equiv p'$ implies that $p + q \equiv p' + q$. And $q \equiv q'$ implies that $q + p' \equiv q' + p'$.

   Now let's prove a lemma that addition of Cauchy sequences is commutative. For any two Cauchy sequences p and q, we have $p + q = (p_i + q_i)_{i \in \mathbb{N}}$. Since addition of rational numbers is commutative, we can also write the sum as $(q_i + p_i)_{i \in \mathbb{N}} = q + p$.

   Therefore we can write $q + p'$ as $p' + q$, and $q' + p'$ as $p' + q'$. By transitivity of the equivalence relation, we get $p + q \equiv p' + q \equiv p' + q'$.

8. Show that if (A_1, B_1) and (A_2, B_2) are Dedekind cuts, then $(A_1, B_1) + (A_2, B_2)$ is also a Dedekind cut.

   Proof. As a reminder, the definition given in the book for a Dedekind cut is a pair of sets of rational numbers (A, B) such that:

- Every rational number q is in either A or B.
- Each $a \in A$ is less than every $b \in B$.
- There is no greatest element of A.
- A and B are both nonempty.

Addition is defined by:

$$\begin{aligned}&(A_1, B_1) + (A_2, B_2) = \\ &(\{a_1 + a_2 \mid a_1 \in A_1, a_2 \in A_2\}, \\ &\ \{b_1 + b_2 \mid b_1 \in B_1, b_2 \in B_2\}).\end{aligned} \tag{4}$$

It turns out that this sum does not necessarily produce a Dedekind cut! For a counterexample, take:

$$\begin{aligned}A_1 &= \{x \in \mathbb{Q} \mid x < 0 \wedge x^2 > 2\}, \\ B_1 &= \{x \in \mathbb{Q} \mid x > 0 \vee x^2 < 2\}, \\ A_2 &= \{x \in \mathbb{Q} \mid x < 0 \vee x^2 < 2\}, \\ B_2 &= \{x \in \mathbb{Q} \mid x > 0 \wedge x^2 > 2\}.\end{aligned}$$

Since there is no rational number x such that $x^2 = 2$, A_1 and B_1 are complements, and A_2 and B_2 are complements, as required.

Intuitively, (A_1, B_1) represents the real number $-\sqrt{2}$, and (A_2, B_2) represents $\sqrt{2}$. Add them together, and you should get 0.

The problem is that, in the sum, 0 should appear in set B, but it does not. The set A will contain all rationals less than 0, and the set B will contain all the rationals greater than 0. But that violates the rule that all rationals should appear in either set A or set B.

Can we fix the definition of addition? Sure. One way is to define the left set A of the sum as before, but define the right set B to be the complement in $\mathbb{Q}$ of A. Then let's check the four required properties for the sum.

The first property, that every rational number q is in A or B, is true by definition of the complement.

One lemma we can prove is that in any Dedekind cut, for every element a of the left set A, every rational number $q < a$ is also in A. To see why this is so, imagine that q were not in A. Then, by the first rule of Dedekind cuts, it would have to be in the right set, B. But the second

rule tells us that each $a \in A$ is less than every $b \in B$. Yet q, in B, would be less than a, a contradiction.

To show that each $a \in A$ is less than every $b \in B$, imagine that for some $a \in A$ and $b \in B$, we had $a \geq b$. We can rule out $a = b$, because B is the complement of A. So that leaves us with $a > b$. Now choose any $a_1 \in A_1$ and $a_2 \in B_2$ such that $a_1 + a_2 = a$. Then we can choose a value $a_1' = a_1 - (a - b)$, which is less than a_1, so by the lemma above, must also be in A_1. Also, $a_1' + a_2 = a_1 - (a - b) + a_2 = a_1 + a_2 - (a - b) = a - (a - b) = b$. Since we have just shown that an element of A_1 plus an element of A_2 equals b, b must be in A. That contradicts our assumption that b was in B.

To show that there is no greatest element of A, suppose there is a greatest element a. According to the definition, there must exist some $a_1 \in A_1$ and $a_2 \in A_2$ that sum to a. But because there is no greatest element in A_1, there exists an $a_1' \in A_1$ such that $a_1' > a_1$. Then $a_1' + a_2 > a_1 + a_2 = a$, yet by the definition of A, $a_1' + a_2$ must be in A. This contradicts our assumption that there is a greatest element of A.

To show that A is nonempty, we need only show that there is some $a_1 \in A_1$ and $a_2 \in A_2$. But we know that because A_1 and A_2 are the left sets of Dedekind cuts.

To show that B is nonempty, we need to show that there is some element $b \in B$ that is not the sum of any $a_1 \in A_1$ and $a_2 \in A_2$. To do this, we just need to choose a $b_1 \in B_1$ and a $b_2 \in B_2$ and add them together to get our b. We can do this because we know that B_1 and B_2 are nonempty. Since any $a_1 \in A$ must be less than b_1, and any $a_2 \in A_2$ must be less than b_2, the sum of $a_1 + a_2$ must be less than b.

Another way we could represent Dedekind cuts is to drop the right set entirely, and just use a single set of rationals, A. The requirements would be that:

- A is nonempty.
- A does not contain all the rationals.
- There is no greatest element of A.
- For every element $a \in A$, every rational $q < a$ is also in A.