MATH2001 Homework, Part 2

Roman Maksimovich, SID: 21098878

Problem 1. *Let S be a set and $f: A \to B$ a map from A to B. Define $f_S : \mathrm{Hom}(B,S) \to \mathrm{Hom}(A,S)$ given by $\alpha \to \alpha \circ f$.*

(a) *Show that if f is injective, then f_S is surjective for any non-empty S.*

Solution. Assume that f is injective and consider an arbitrary $g \in \mathrm{Hom}(A,S)$. Since S is non-empty, we can also fix an element $s^* \in S$. Define a map $\alpha: B \to S$ as follows:

$$\forall b \in B: \quad \alpha(b) = \begin{cases} g(f^{-1}(b)), \text{ if } b \in f(A), \\ s*, \text{ otherwise} \end{cases}$$

If $b \in f(A)$, the pre-image $f^{-1}(b) \in A$ is unique since f is injective. Now, consider the composition $\alpha \circ f$:

$$\forall a \in A: \quad (\alpha \circ f)(a) = \alpha(f(a)) = g(f^{-1}(f(a))) = g(a),$$

meaning that $g = \alpha \circ f$, or $g = f_S(\alpha)$. Hence, f_S is surjective. ∎

(b) *Show that if f is surjective, then f_S is injecctive for any S.*

Solution. Assume that f is surjective. Consider two functions α_1 and α_2 from $\mathrm{Hom}(B,S)$, such that $f_S(\alpha_1) = f_S(\alpha_2)$ (if $\mathrm{Hom}(B,S)$ is empty, then injectivity is trivial). In other words, we have $\alpha_1 \circ f = \alpha_2 \circ f$. Since f is surjective, there is a function $g: B \to A$ such that

$$\forall b \in B: \quad f(g(b)) = b.$$

Now, let $b \in B$ be arbitrary. We write

$$\alpha_1(b) = \alpha_1(f(g(b))) = \alpha_2(f(g(b))) = \alpha_2(b).$$

Hence, $\alpha_1 = \alpha_2$, and we conclude that f_S is injective. ∎

(c) *Are the converses of the above statements true?*

Solution. No, both converses are false.
For part (a), take $A = \{1,2\}$, $B = \{1\}$, and $S = \{1\}$. We see that $\mathrm{Hom}(A,S)$ and $\mathrm{Hom}(B,S)$ both contain only one element, so f_S is bijective (in particuler, surjective) for any f. Still, the only map $f: A \to B$ is clearly not injective, since $f(1) = f(2) = 1$.
For part (b), take the opposite: $A = \{1\}$, $B = \{1,2\}$, and $S = \{1\}$. The map f_S is again bijective and thus injecctive for any f. However, the map $f: A \to B$, $f(1) = 1$ is not surjective. ∎

Problem 2. *Let $f: X \to Y$ be a function. Define a relation on X given by $x_1 \sim x_2$ if and only if $f(x_1) = f(x_2)$.*

(a) *Show that $\sim$ is an equivalence relation on X.*

Solution.

- **Reflexivity.** $f(x) = f(x) \implies x \sim x$, $\forall x \in X$.
- **Symmetricity.** Trivial, since $f(x) = f(y) \iff f(y) = f(x)$.
- **Transitivity.** Trivial, since if $f(x) = f(y)$ and $f(y) = f(z)$, then $f(x) = f(z)$.

■

(b) *Construct a bijection between the quotient set $X/\sim$ and the image* $\mathrm{Im} f$.

Solution. Consider a class $[x] \in X/\sim$. Define $\overline{f}([x]) = f(x)$. The fuction $\overline{f}$ is well-defined since

$$[x_1] = [x_2] \iff x_1 \sim x_2 \iff f(x_1) = f(x_2),$$

i.e. the image of $[x]$ does not depend on the choice of class representative.
We see that $\overline{f}$ is injective:

$$\overline{f}([x_1]) = \overline{f}([x_2]) \implies f(x_1) = f(x_2) \implies x_1 \sim x_2 \implies [x_1] = [x_2].$$

We also see that $\overline{f}$ is surjective:

$$\forall y \in \mathrm{Im} f: \quad y = f(f^{-1}(y)) = \overline{f}([f^{-1}(y)]),$$

i.e. every element $y \in \mathrm{Im} f$ has a pre-image in the form of $[f^{-1}(y)]$, where $f^{-1}(y)$ is one of the pre-images of y due to f.
Hence, $\overline{f}$ is bijective, and we are done. ■

Problem 3. *For each fixed $n \in \mathbb{Z}$, consider the equivalence relation $a \sim b \iff a - b \equiv n \pmod n$ (or $a - b \equiv 0$ for short). Denote $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\sim$.*

(a) *Show that $\sim$ is an equivalence relation and describe $\mathbb{Z}/n\mathbb{Z}$ with $n = 0, 1, 2$.*

Solution. Reflexivity is trivial: $x - x = 0 \equiv 0 \pmod n$. Symmetricity is also trivial, since if x is a multiple of n, then $-x$ is also a multiple of n, and so

$$a \sim b \implies a - b \equiv 0 \implies b - a \equiv 0 \implies b \sim a.$$

Transitivity is trivial as well, since the sum of multiples of n is a multiple of n, and $a - c = (a - b) + (b - c)$. Hence if $a \sim b$ and $b \sim c$, then $a \sim c$.
If $n = 0$, then $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}$, since no number apart from 0 is a multiple of 0, and all equivalence classes consist of one element.
If $n = 1$, then $\mathbb{Z}/n\mathbb{Z} \cong \{1\}$, since all numbers are multiples of 1, and thus there is only one equivalence class, i.e. $\mathbb{Z}$.
If $n = 2$, then $\mathbb{Z}/n\mathbb{Z} \cong \{1, 2\}$, since there are two equivalence classes: the even and the odd numbers. This is obvious since $a - b \cong 0 \pmod 2$ iff a and b are of the same parity. ■

(b) *Define operations $+$ and $\cdot$ on $\mathbb{Z}/n\mathbb{Z}$ such that the quitient map π satisfies $\pi(a+b) = \pi(a)+\pi(b)$ and $\pi(ab) = \pi(a)\pi(b)$ for all $a, b \in \mathbb{Z}$.*

Solution. Take $[a], [b] \in \mathbb{Z}/n\mathbb{Z}$. Define $[a] + [b] = [a + b]$ and $[a] \cdot [b] = [a \cdot b]$. To prove correctness, we consider $a' \sim a$ and $b' \sim b$. We have $n \mid (a' - a)$ and $n \mid (b' - b)$. Hence

$$n \mid ((a' - a) + (b' - b)) = ((a' + b') - (a + b)),$$

and $(a + b) \sim (a' + b')$. Moreover,

$$n \mid ((a' - a)b' + (b' - b)a) = (a'b' - ab' + ab' - ab) = (a'b' - ab),$$

and so $ab \sim a'b'$. In other words, both addition and multiplication are defined correctly. By definition, we also see that

$$\pi(a + b) = [a + b] = [a] + [b] = \pi(a) + \pi(b)$$

and

$$\pi(ab) = [ab] = [a] \cdot [b] = \pi(a) \cdot \pi(b).$$

∎

Problem 4. *Let* $m, n \in \mathbb{N}$ *such that* $m + n = 0$. *Prove that* $m = n = 0$.

Solution. Consider two cases:

- $n = 0$. Then $m + n = m + 0 = n = 0$, and hence $m = n = 0$.
- $n = S(k)$. Then $m + n = m + S(k) = S(n + k) = 0$, which is impossible due one of Peano's axioms, stating that $S(n) \neq 0$ for all $n \in \mathbb{N}$.

These two cases are exhaustive due to the last axiom. ∎

Problem 5. *Prove that the multiplication operation* $[a, b] \cdot [c, d] := [ac + bd, ad + bc]$ *is well-defined.*

Solution. Let $[a', b'] = [a, b]$ and $[c', d'] = [c, d]$. That means, $a' + b = a + b'$ and $c' + d = c + d'$. Utilizing the commutativity, associativity, and distribution properties of multiplication on $\mathbb{N}$, we have

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

By using a totally similar derivation, we see that $[a, b] \cdot [c', d'] = [a', b'] \cdot [c', d']$.
Hence, by transitivity, $[a, b] \cdot [c, d] = [a', b'] \cdot [c', d']$. ∎

Problem 6. *Prove that the operation* $\cdot$ *(multiplication) on* $\mathbb{Z}$ *satisfies the following properties:*

(a) Distributivity.

Proof. Let $m = [m_1, m_2]$, $n = [n_1, n_2]$, $p = [p_1, p_2]$. We have

$$\begin{gathered}
m \cdot (n + p) = [m_1, m_2] \cdot [n_1 + p_1, n_2 + p_2] = \\
= [m_1(n_1 + p_1) + m_2(n_2 + p_2), m_2(n_1 + p_1) + m_1(n_2 + p_2)] = \\
= [m_1n_1 + m_2n_2 + m_1p_1 + m_2p_2, m_2n_1 + m_1n_2 + m_2p_1 + m_1p_2] = \\
= [m_1n_1 + m_2n_2, m_2n_1 + m_1n_2] + [m_1p_1 + m_2p_2, m_2p_1 + m_1p_2] = \\
= [m_1, m_2] \cdot [n_1, n_2] + [m_1, m_2] \cdot [p_1, p_2] = \\
= m \cdot n + m \cdot p.
\end{gathered}$$

∎

(b) *Associativity.*

Proof. Let $m = [m_1, m_2]$, $n = [n_1, n_2]$, $p = [p_1, p_2]$. We have

$$\begin{gathered}
m \cdot (n \cdot p) = [m_1, m_2] \cdot ([n_1, n_2] \cdot [p_1, p_2]) = \\
= [m_1, m_2] \cdot [n_1p_1 + n_2p_2, n_1p_2 + n_2p_1] = \\
= [m_1(n_1p_1 + n_2p_2) + m_2(n_1p_2 + n_2p_1), m_1(n_1p_2 + n_2p_1) + m_2(n_1p_1 + n_2p_2)] = \\
= [m_1n_1p_1 + m_1n_2p_2 + m_2n_1p_2 + m_2n_2p_1, m_1n_1p_2 + m_1n_2p_1 + m_2n_1p_1 + m_2n_2p_2] = \\
= [(m_1n_1 + m_2n_2)p_1 + (m_1n_2 + m_2n_1)p_2, (m_1n_1 + m_2n_2)p_2 + (m_1n_2 + m_2n_1)p_1] = \\
= [m_1n_1 + m_2n_2, m_1n_2 + m_2n_1] \cdot [p_1, p_2] = \\
= ([m_1, m_2] \cdot [n_1, n_2]) \cdot [p_1, p_2] = \\
= (m \cdot n) \cdot p.
\end{gathered}$$

∎

(c) *Commutativity.*

Proof. Let $m = [m_1, m_2]$, $n = [n_1, n_2]$. We have

$$\begin{gathered}
m \cdot n = [m_1, m_2] \cdot [n_1, n_2] = \\
= [m_1n_1 + m_2n_2, m_1n_2 + m_2n_1] = [n_1m_1 + n_2m_2, n_1m_2 + n_2m_1] = \\
= [n_1, n_2] \cdot [m_1, m_2] = n \cdot m.
\end{gathered}$$

∎

(d) *Multiplicative unit.*

Proof. Let $m = [m_1, m_2]$. Then

$$\begin{gathered}
m \cdot 1 = [m_1, m_2] \cdot [1, 0] = [m_1 \cdot 1 + m_2 \cdot 0, m_1 \cdot 0 + m_2 \cdot 1] = \\
= [m_1, m_2] = m.
\end{gathered}$$

Analogously, $1 \cdot m = m$. Now assume that $e \in \mathbb{Z}$ has the property that $m \cdot e = e \cdot m = m$ for all $m \in \mathbb{Z}$. We simply have $e = e \cdot 1 = 1$, and we are done. ∎

(e) *Cancellation.*

Proof. Let $m = [m_1, m_2]$, $n = [n_1, n_2]$, and $k = [k_1, k_2]$ be such that $m \cdot k = n \cdot k$ and $k_1 \neq k_2$. We have

$$\begin{aligned}
[m_1, m_2] \cdot [k_1, k_2] &= [n_1, n_2] \cdot [k_1, k_2], \\
[m_1 k_1 + m_2 k_2, m_1 k_2 + m_2 k_1] &= [n_1 k_1 + n_2 k_2, n_1 k_2 + n_2 k_1], \\
m_1 k_1 + m_2 k_2 + n_1 k_2 + n_2 k_1 &= n_1 k_1 + n_2 k_2 + m_1 k_2 + m_2 k_1, \\
k_1(m_1 + n_2) + k_2(m_2 + n_1) &= k_1(m_2 + n_1) + k_2(m_1 + n_2).
\end{aligned}$$

Now we will need the following statement:

Lemma. *For any two numbers $a_1, a_2 \in \mathbb{N}$, there is a number $b \in \mathbb{N}$ such that either $a_1 = a_2 + b$ or $a_2 = a_1 + b$.*

Proof. We conduct a proof by induction over a_1.

1. $a_1 = 0$. Then, taking $b = a_2$, we have $a_2 = a_1 + b$.
2. If the statement holds for a_1, it holds for $S(a_1)$. Let $a_2 \in \mathbb{N}$. Then there is a b such that either $a_1 = a_2 + b$ or $a_2 = a_1 + b$. In the first case, take $b' = S(b)$. We have

$$S(a_1) = S(a_2 + b) = a_2 + S(b) = a_2 + b'.$$

   In the second case, we handle two posiibilities:
   - $b = 0$. Then take $b' = 1$, and write

$$S(a_1) = S(a_2) = a_2 + 1 = a_2 + b'.$$

   - $b = S(c),\ c \in \mathbb{N}$. Then take $b' = c$, and write

$$a_2 = a_1 + S(c) = S(a_1) = c = S(a_1) + b',$$

     q.e.d.

■

Now, without loss of generality, assume that $k_1 = k_2 + b$. We have

$$\begin{aligned}
(k_2 + b)(m_1 + n_2) + k_2(m_2 + n_1) &= (k_2 + b)(m_2 + n_1) + k_2(m_1 + n_2), \\
k_2(m_1 + n_2) + b(m_1 + n_2) + k_2(m_2 + n_1) &= k_2(m_2 + n_1) + b(m_2 + n_1) + k_2(m_1 + n_2), \\
b(m_1 + n_2) &= b(m_2 + n_1), \\
m_1 + n_2 &= m_2 + n_1, \\
[m_1, m_2] &= [n_1, n_2],
\end{aligned}$$

q.e.d. ■