Norwegian University of Science and Technology
Department of Mathematical Sciences

Solutions to exercise set 1

Note that there are several ways to approach the problems, but that only one is presented here. Other solutions may be just as valid!

1 Suppose that, on the contrary, both m and $m+1$ are integer multiples of n. Write $m = an$ and $m+1 = bn$, where $a < b$ are integers. Then

$$1 = (m+1) - m = bn - an = (b-a)n, \tag{1}$$

where

$$(b-a)n \geq 2, \tag{2}$$

since $b - a \geq 1$ and $n \geq 2$. Equations (1) and (2) imply that

$$1 \geq 2,$$

which is a contradiction. Hence $m+1$ is not an integer multiple of n.

2 $\Longrightarrow$ Since n is even, we have $n = 2m$ for an integer m. Then

$$n^2 = 4m^2 = 2\tilde{m}, \quad \tilde{m} = 2m^2,$$

so n^2 is even.

$\Longleftarrow$ We want to prove "*If n^2 is even, then n is even*". It is easier to look at the contrapositive statement (which is logically equivalent!) "*If n is not even, then n^2 is not even*", or "*If n is odd, then n^2 is odd*" instead.
Suppose therefore that n is odd, which means that we can write $n = 2m+1$ for an integer m. Then

$$n^2 = 4m^2 + 4m + 1 = 2\tilde{m} + 1, \quad \tilde{m} = 2m^2 + 2m,$$

so n^2 is odd.

3 We show the two inclusions $(A \cap B)^c \subseteq A^c \cup B^c$ and $(A \cap B)^c \supseteq A^c \cup B^c$ separately.

$\subseteq$ Suppose that $x \in (A \cap B)^c$. Then $x \notin A \cap B$, which implies that $x \notin A$ or $x \notin B$ (keep in mind that "or" can mean that both are true). Thus $x \in A^c$ or $x \in B^c$, meaning that $x \in A^c \cup B^c$. Hence $(A \cap B)^c \subseteq A^c \cup B^c$.

⊇ All the implications in the argument for ⊆ are in fact equivalences (convince yourself of this!) We can therefore run the argument in reverse to conclude that $(A \cap B)^c \supseteq A^c \cup B^c$.

It is often the case that it is simpler to think in one direction first, and then only later check if you can do the argument in the other direction.

4 **a)** The differentiation operator is not injective, because we can change the constant term without changing the derivative. For instance,

$$D(x+1) = D(x+2) = 1.$$

Next, we show that D is surjective. Let therefore

$$q(x) = \sum_{i=0}^{n} b_i x^i \tag{3}$$

be an arbitrary element of $\mathcal{P}$. If we now define p by

$$\begin{aligned} p(x) &= \sum_{i=0}^{n} \frac{b_i}{i+1} x^{i+1} \\ &= \sum_{i=1}^{n+1} \frac{b_{i-1}}{i} x^i, \end{aligned} \tag{4}$$

we see that

$$\begin{aligned} (Dp)(x) &= \sum_{i=1}^{n+1} i \frac{b_{i-1}}{i} x^{i-1} \\ &= \sum_{i=0}^{n} b_i x^i = q(x). \end{aligned} \tag{5}$$

Bonus: As we indicated, the reason why $D\colon \mathcal{P} \to \mathcal{P}$ is not injective is that differentiation "destroys" the information about the constant term. We therefore let $\mathcal{Q}$ be the set of polynomials with no constant term; that is, polynomials of the form

$$p(x) = \sum_{i=1}^{n} a_i x^i$$

for $n = 0, 1, 2, \ldots$ and real numbers a_i. The map $D\colon \mathcal{Q} \to \mathcal{P}$ is still a surjection, since the polynomial p in (4) lies in $\mathcal{Q}$. However, it is now also injective: Suppose that the two polynomials

$$r(x) = \sum_{i=1}^{n} c_i x^i, \quad s(x) = \sum_{i=1}^{n} d_i x^i$$

in $\mathcal{Q}$ are mapped to the same polynomial by D (note that we can use the same n for r and s by padding with coefficients that are zero). Then

$$0 = (Dr)(x) - (Ds)(x) = \sum_{i=1}^{n} i(c_i - d_i) x^{i-1},$$

which implies that $c_i = d_i$ for all i, due to the fundamental theorem of algebra. Hence $r = s$.

b) The integration operator is not surjective, because $(Ip)(x)$ has no constant term for any p. However, it is injective: Suppose that the two polynomials

$$p(x) = \sum_{i=0}^{n} a_i x^i, \quad q(x) = \sum_{i=0}^{n} b_i x^i$$

are mapped to the same polynomial by I. Then

$$0 = (Dp)(x) - (Dq)(x) = \sum_{i=1}^{n} \frac{a_i - b_i}{i+1} x^{i+1},$$

which implies that $a_i = b_i$ for all i (by the fundamental theorem of algebra). Hence $p = q$.

Bonus: The reason why $I \colon \mathcal{P} \to \mathcal{P}$ is not surjective is that it maps to polynomials without constant terms. We should therefore choose $\mathcal{R} = \mathcal{Q}$, which was defined in **a)**. The map $\mathcal{I} \colon \mathcal{P} \to \mathcal{Q}$ is then surjective: If

$$q(x) = \sum_{i=1}^{n} b_i x^i$$

is an arbitrary element of $\mathcal{Q}$, we may define

$$\begin{aligned} p(x) &= \sum_{i=1}^{n} i b_i x^{i-1} \\ &= \sum_{i=0}^{n-1} (i+1) b_{i+1} x^i, \end{aligned}$$

which satisfies

$$\begin{aligned} (Ip)(x) &= \sum_{i=0}^{n-1} \frac{(i+1) b_{i+1}}{i+1} x^{i+1} \\ &= \sum_{i=1}^{n} b_i x^i = q(x). \end{aligned}$$

c) We have in fact (almost) already showed that $D \circ I = \mathrm{id}_{\mathcal{P}}$. The polynomial p defined in (4) is equal to Iq, where q was the arbitrary polynomial in (3), and (5) shows that

$$(D \circ I)(q) = D(Iq) = Dp = q.$$

Hence $D \circ I = \mathrm{id}_{\mathcal{P}}$.

Next, we want to show that $I \circ D \neq \mathrm{id}_{\mathcal{P}}$. From before, we know that constant terms cause trouble. We therefore look at what happens to the polynomial $x + 1$. Indeed

$$\begin{aligned} (I \circ D)(x+1) &= I(D(x+1)) \\ &= I(1) \\ &= x \neq x + 1, \end{aligned}$$

so $I \circ D \neq \mathrm{id}_{\mathcal{P}}$.

Bonus: They are inverses of each other; $D = I^{-1}$ and $I = D^{-1}$. This follows from the identity $D \circ I = id_{\mathcal{P}}$ (which still holds after modifying the domain of D and the codomain of I) and the fact that they are bijections.

5 **a)** First off, the map $g \circ f \colon X \to Z$ is well defined since the domain of $g \colon Y \to Z$ is equal to the codomain of $f \colon X \to Y$.

In order to show that $g \circ f \colon X \to Z$ is surjective, let $z \in Z$. Because g is surjective, there is some $y \in Y$ such that $g(y) = z$; and because f is surjective, there is some $x \in Y$ such that $f(x) = y$. Now

$$(g \circ f)(x) = g(f(x)) = g(y) = z$$

shows that $g \circ f$ is surjective.

Assume that $(g \circ f)(x) = (g \circ f)(y)$, or $g(f(x)) = g(f(y))$. Using the injectivity of g, we conclude that $f(x) = f(y)$, which in turn implies that $x = y$ through the injectivity of f. Hence $g \circ f$ is injective, and thus a bijection.

b) We know that $g \circ f$ is a bijection under the assumption in **a)**. Hence it has an inverse map $(g \circ f)^{-1} \colon Z \to X$, which by definition satisfies the identity

$$(g \circ f) \circ (g \circ f)^{-1} = \mathrm{id}_Z,$$

or

$$g \circ f \circ (g \circ f)^{-1} = \mathrm{id}_Z\,.$$

We will find an expression for $(g \circ f)^{-1}$ by solving this equation. If we compose g^{-1} with each side of the equation, we obtain

$$\begin{aligned}(g^{-1} \circ g) \circ f \circ (g \circ f)^{-1} &= g^{-1} \circ \mathrm{id}_Z \\ \mathrm{id}_Y \circ f \circ (g \circ f)^{-1} &= g^{-1} \\ f \circ (g \circ f)^{-1} &= g^{-1}.\end{aligned}$$

Doing the same thing with f^{-1}, we find

$$\begin{aligned}\mathrm{id}_X \circ (g \circ f)^{-1} &= f^{-1} \circ g^{-1} \\ (g \circ f)^{-1} &= f^{-1} \circ g^{-1},\end{aligned}$$

which is what we wanted to show.

6 When proving something by induction, we need two things:

- The inductive step, where we show that if the statement is true for n, then it is true for $n + 1$ as well.
- The base case, where we show that the statement is true for some $n_0 \in \mathbb{N}$.

If one has both these, then the statement holds for all natural numbers $n \geq n_0$. The problem in the proof given in the problem is that there is no base case. We cannot conclude anything without the base case.