MATH1050 Proof-writing Exercise 4 (Answers and selected solutions)

1. **Solution.** *There are two acceptable arguments.*

   Acceptable argument (A).

   Let r be a real number greater than 1. Denote by $P(n)$ the proposition below:

   Suppose $a_1, a_2, \cdots, a_n$ are positive real numbers. Then $\log_r\left(\prod_{j=1}^{n} a_j\right) = \sum_{j=1}^{n} \log_r(a_j)$.

   - Suppose a, b are positive real numbers. Then $\log_r(ab) = \log_r(a) + \log_r(b)$ by ($\sharp$).
     It follows that $P(2)$ is true.
   - Let $k \in \mathbb{N}\backslash\{0, 1\}$. Suppose $P(k)$ is true. We verify that $P(k + 1)$ is true:
     * Suppose $a_1, a_2, \cdots, a_k, a_{k+1}$ are positive real numbers.
       Since $a_1, a_2, \cdots, a_k$ are positive real numbers, $a_1a_2 \cdots a_k$ is a positive real number.
       Then

$$\begin{aligned}
\log_r\left(\prod_{j=1}^{k+1} a_j\right) &= \log_r\left(\left(\prod_{j=1}^{k} a_j\right) \cdot a_{k+1}\right) \\
&= \log_r\left(\prod_{j=1}^{k} a_j\right) + \log_r(a_{k+1}) \qquad \text{(by } (\sharp)\text{)} \\
&= \sum_{j=1}^{k} \log_r(a_j) + \log_r(a_{k+1}) \qquad \text{(by } P(k)\text{)} \\
&= \sum_{j=1}^{k+1} \log_r(a_j)
\end{aligned}$$

       Hence $P(k + 1)$ is true.

   By the Principle of Mathematical Induction, $P(n)$ is true for any positive integer $n \in \mathbb{N}\backslash\{0, 1\}$.

   Acceptable argument (B), but not preferrable.

   Let r be a real number greater than 1. Let $\{a_j\}_{j=1}^{\infty}$ be an infinite sequence of positive real numbers. Denote by $S(n)$ the proposition below:

$$\log_r\left(\prod_{j=1}^{n} a_j\right) = \sum_{j=1}^{n} \log_r(a_j).$$

   - We have $\log_r(a_1a_2) = \log_r(a_1) + \log_r(a_2)$ by ($\sharp$).
     Then $S(2)$ is true.
   - Let $k \in \mathbb{N}\backslash\{0, 1\}$. Suppose $S(k)$ is true. We verify that $S(k + 1)$ is true:
     * Since $a_1, a_2, \cdots, a_k$ are positive real numbers, $a_1a_2 \cdots a_k$ is a positive real number.
       Then

$$\begin{aligned}
\log_r\left(\prod_{j=1}^{k+1} a_j\right) &= \log_r\left(\left(\prod_{j=1}^{k} a_j\right) \cdot a_{k+1}\right) \\
&= \log_r\left(\prod_{j=1}^{k} a_j\right) + \log_r(a_{k+1}) \qquad \text{(by } (\sharp)\text{)} \\
&= \sum_{j=1}^{k} \log_r(a_j) + \log_r(a_{k+1}) \qquad \text{(by } S(k)\text{)} \\
&= \sum_{j=1}^{k+1} \log_r(a_j)
\end{aligned}$$

Hence $S(k+1)$ is true.

By the Principle of Mathematical Induction, $S(n)$ is true for any positive integer $n \in \mathbb{N}\backslash\{0, 1\}$.

2. ——

3. ——

4. **Solution.**

   (a) Let A, B be $(m \times m)$-square matrices with real entries. Suppose A, B are non-singular.

   We verify that AB is non-singular:

   Pick any $\mathbf{x} \in \mathbb{R}^m$. Suppose $AB\mathbf{x} = \mathbf{0}$.
   We have $A(B\mathbf{x}) = \mathbf{0}$. Then, since A is non-singular, $B\mathbf{x} = \mathbf{0}$.
   Then, since B is non-singular, we have $\mathbf{x} = \mathbf{0}$.
   It follows that AB is non-singular.

   (b) i. Let n be an integer greater than 1. Let $A_1, A_2, \cdots, A_n$ be $(m \times m)$-square matrices. Suppose $A_1, A_2, \cdots, A_n$ are non-singular. Then $A_1 A_2 \cdots A_n$ is non-singular.

   ii. Denote by $P(n)$ the proposition below:

   Let $A_1, A_2, \cdots, A_n$ be $(m \times m)$-square matrices. Suppose $A_1, A_2, \cdots, A_n$ are non-singular. Then $A_1 A_2 \cdots A_n$ is non-singular.

   - $P(2)$ is true by the result of part (a).
   - Let k be an integer greater than 1. Suppose $P(k)$ is true.
     We verify that $P(k+1)$ is true:

     Let $A_1, A_2, \cdots, A_k, A_{k+1}$ be $(m \times m)$-square matrix.
     Suppose $A_1, A_2, \cdots, A_k, A_{k+1}$ is non-singular. Write $C = A_1 A_2 \cdots A_k$.
     By $P(k)$, since $A_1, A_2, \cdots, A_k$ are non-singular, the product C is non-singular.
     Note that $A_1 A_2 \cdots A_k A_{k+1} = CA_{k+1}$.
     Then, by the result of part (a), $A_1 A_2 \cdots A_k A_{k+1}$ is non-singular.

   By the Principle of Mathematical Induction, $P(n)$ is true for any integer greater than 1.

   Alternative 'inductive step'.

   - Let k be an integer greater than 1. Suppose $P(k)$ is true.
     We verify that $P(k+1)$ is true:

     Let $A_1, A_2, \cdots, A_k, A_{k+1}$ be $(m \times m)$-square matrix.
     Suppose $A_1, A_2, \cdots, A_k, A_{k+1}$ is non-singular.
     By the result in part (a), since A_k, A_{k+1} are non-singular, $A_k A_{k+1}$ is non-singular.
     $A_1, A_2, \cdots, A_{k-1}, A_k A_{k+1}$ are non-singular. Then by $P(k)$, the product $A_1 A_2 \cdots A_{k-1} A_k A_{k+1}$ is non-singular.

5. (a) **Answer.**

   Let n be an integer greater than 1. For any integer m between 2 and n, the integer m is a prime number or m is a product of at least two prime numbers.

   (b) ——

6. **Solution.**

   [We want to prove this statement: '*Suppose S is a subset of $\mathbb{R}$. Further suppose λ, μ are greatest elements of S. Then $\lambda = \mu$.*']

   Suppose S is a subset of $\mathbb{R}$. Further Suppose λ, μ are greatest element of S.

   By definition of greatest element, we have $x \leq \lambda$ for any $x \in S$. Also by definition of greatest element, $\mu \in S$. Then $\mu \leq \lambda$.

   Modifying the argument above (by interchanging the roles of λ, μ), we have $\lambda \leq \mu$.

   We have $\mu \leq \lambda$ and $\lambda \leq \mu$. Then $\lambda = \mu$.

7. *Comment.*

   The statement to be proved should be formulated as:

- *Let ζ be a complex number. Suppose ζ is neither real nor purely imaginary. Let z be a complex number. Let a, b, c, d be real numbers. Suppose $z = a\zeta + b\overline{\zeta}$ and $z = c\zeta + d\overline{\zeta}$. Then $a = c$ and $b = d$.*

The argument should start in this way:

> Let ζ be a complex number. Suppose ζ is neither real nor purely imaginary.
>
> Pick any complex number z. Let a, b, c, d be real numbers. Suppose $z = a\zeta + b\overline{\zeta}$ and $z = c\zeta + d\overline{\zeta}$.

8. *Comment.*

   The statement to be proved should be formulated as:

   - *Let p be a positive real number, and q be a real number. Suppose $f(x)$ be the cubic polynomial given by $f(x) = x^3 + px + q$.*
     Let v be a real number. Let α, β be real numbers. Suppose '$u = \alpha$', '$u = \beta$' are real solutions of the equation $f(u) = v$ with unknown u.
     Then $\alpha = \beta$.

9. **Solution.**

   > [We want to prove this statement: '*Let I be an interval in $\mathbb{R}$, and $f, g : I \longrightarrow \mathbb{R}$ be functions. Suppose f is strictly increasing on I and g is strictly decreasing on I.*
   > *Let $c, c' \in I$. Suppose $f(c) = g(c)$ and $f(c') = g(c')$. Then $c = c'$.*]

   Let I be an interval in $\mathbb{R}$, and $f, g : I \longrightarrow \mathbb{R}$ be functions. Suppose f is strictly increasing on I and g is strictly decreasing on I.

   Pick any $c, c' \in I$. Suppose $f(c) = g(c)$ and $f(c') = g(c')$. We verify that $c = c'$ by the proof-by-contradiction method:

   - Suppose it were true that $c \neq c'$.
     Without loss of generality, assume $c < c'$.
     Since f is strictly increasing on I, we would have $f(c) < f(c')$.
     Since g is strictly decreasing on I we would have $g(c) > g(c')$.
     Recall that $f(c) = g(c)$ and $f(c') = g(c')$.
     Then $f(c) < f(c') = g(c') < g(c) = f(c)$. Therefore $f(c) < f(c)$. Contradiction arises.

10. **Solution.**

    > [We want to prove this statement: 'For any $\mathbf{v} \in \mathbb{R}^n$, for any $c_1, c_2, \cdots, c_k, d_1, d_2, \cdots, d_k \in \mathbb{R}$, if $\mathbf{v} = c_1\mathbf{u}_1 + c_2\mathbf{u}_2 + \cdots + c_k\mathbf{u}_k$ and $\mathbf{v} = d_1\mathbf{u}_1 + d_2\mathbf{u}_2 + \cdots + d_k\mathbf{u}_k$ then $c_1 = d_1$, $c_2 = d_2$, ... and $c_k = d_k$.']

    Pick any $\mathbf{v} \in \mathbb{R}^n$.
    Let $c_1, c_2, \cdots, c_k, d_1, d_2, \cdots, d_k \in \mathbb{R}$.
    Suppose that $\mathbf{v} = c_1\mathbf{u}_1 + c_2\mathbf{u}_2 + \cdots + c_k\mathbf{u}_k$ and $\mathbf{v} = d_1\mathbf{u}_1 + d_2\mathbf{u}_2 + \cdots + d_k\mathbf{u}_k$.
    Then $c_1\mathbf{u}_1 + c_2\mathbf{u}_2 + \cdots + c_k\mathbf{u}_k = \mathbf{v} = d_1\mathbf{u}_1 + d_2\mathbf{u}_2 + \cdots + d_k\mathbf{u}_k$.
    Therefore $(c_1 - d_1)\mathbf{u}_1 + (c_2 - d_2)\mathbf{u}_2 + \cdots + (c_k - d_k)\mathbf{u}_k = \mathbf{0}$.
    Since $\mathbf{u}_1, \mathbf{u}_2, \cdots, \mathbf{u}_k$ are linearly independent, we have $c_1 - d_1 = c_2 - d_2 = \cdots = c_k - d_k = 0$.
    Then $c_1 = d_1$, $c_2 = d_2$, ..., and $c_k = d_k$.

11. ——