MATH1030 Examples of simple proofs in linear algebra

1. Recall the definition for the notion of Lie products:

   Let P, Q be $(n \times n)$-square matrices with real entries.
   The $(n \times n)$-square matrix $PQ - QP$ is called the Lie product of P, Q, and is denoted by $[P, Q]$.

2. **Statement (1).**
   Suppose A, B, C are $(n \times n)$-square matrices, and β, γ are real numbers. Then $[A, \beta B + \gamma C] = \beta[A, B] + \gamma[A, C]$.
   Proof of Statement (1).

   [Preparation.
   Ask: What is the assumption?
   Answer. '*A, B, C are $(n \times n)$-square matrices, and β, γ are real numbers*'.
   Further ask: What is the (desired) conclusion to be deduced from the assumption?
   Answer. '$[A, \beta B + \gamma C] = \beta[A, B] + \gamma[A, C]$'.]

   Suppose A, B, C are $(n \times n)$-square matrices, and β, γ are real numbers.

   [Reminder: We try to deduce $[A, \beta B + \gamma C] = \beta[A, B] + \gamma[A, C]$.]

   Then

$$\begin{aligned} [A, \beta B + \gamma C] &= A(\beta B + \gamma C) - (\beta B + \gamma C)A \\ &= A(\beta B) + A(\gamma C) - (\beta B)A - (\gamma C)A \\ &= \beta AB + \gamma AC - \beta BA - \gamma CA \\ &= \beta(AB - BA) + \gamma(AC - CA) \\ &= \beta[A, B] + \gamma[A, C] \qquad \square \end{aligned}$$

   Remark. We can similarly deduce these statements below:

   (a) *Suppose A is an $(n \times n)$-square matrix. Then $[A, A] = \mathcal{O}_{n\times n}$.*
   (b) *Suppose A, B are $(n \times n)$-square matrices. Then $[A, B] = -[B, A] = [-B, A] = [B, -A]$.*
   (c) *Suppose A, B, C are $(n\times n)$-square matrices, and α, β are real numbers. Then $[\alpha A+\beta B, C] = \alpha[A, C]+\beta[B, C]$.*
   (d) *Suppose A, B, C are $(n \times n)$-square matrices. Then $[A, [B, C]] + [B, [C, A]] + [C, [A, B]] = \mathcal{O}_{n\times n}$.*

3. Recall the definitions for the notions of symmetric matrix and skew-symmetric matrix.

   Let C be an $(n \times n)$-square matrix.
   (a) *C is said to be symmetric if and only if $C^t = C$.*
   (b) *C is said to be skew-symmetric if and only if $C^t = -C$.*

4. **Statement (2).**
   Let A be an $(n \times n)$-square matrix. Suppose A is symmetric and A is skew-symmetric. Then $A = \mathcal{O}_{n\times n}$.
   Proof of Statement (2).

   [Ask: What is the assumption?
   Answer. '*A is an $(n \times n)$-square matrix. Also, A is symmetric and A is skew-symmetric.*'
   Further ask: What is the (desired) conclusion to be deduced from the assumption?
   Answer. '$A = \mathcal{O}_{n\times n}$'.]

   Let A be an $(n \times n)$-square matrix. Suppose A is symmetric and A is skew-symmetric.

   [Reminder: We try to deduce $A = \mathcal{O}_{n\times n}$.
   Observe: We want to obtain some equality concerned with A. It will be good if we can start with some equality involving A.
   Ask: Does the assumption provide any equality concerned with A?]

   Since A is symmetric, we have $A^t = A$.

   Since A is skew-symmetric, we have $A^t = -A$. Then $A = -A^t$.

   Now we have $2A = A + A = A^t + (-A^t) = A^t - A^t = \mathcal{O}_{n\times n}$.

   Then $A = \frac{1}{2}\mathcal{O}_{n\times n} = \mathcal{O}_{n\times n}$. $\square$

5. Recall the definition for the notion of matrix inverse.

   Let P be an $(n \times n)$-square matrix.

   Suppose Q is a $(n \times n)$-square matrix. Further suppose $QP = I_n$ and $PQ = I_n$. Then we say Q is a matrix inverse of P.

6. **Statement (3).**

   Let A, B, C be $(n \times n)$-square matrices. Suppose each of B, C is a matrix inverse of A. Then $B = C$.

   Proof of Statement (3).

   Let A, B, C be $(n \times n)$-square matrices. Suppose each of B, C is a matrix inverse of A.

   Since B is a matrix inverse of A, we have $BA = I_n$ and $AB = I_n$.

   Since C is a matrix inverse of A, we have $CA = I_n$ and $AC = I_n$.

   [Ask: Can we obtain from, say, '$BA = I_n$', some other equality, with B alone in one side and without B in the other side? Or how about C?]

   We have $BA = I_n$ and $AC = I_n$.

   Then $B = BI_n = B(AC) = (BA)C = I_nC = C$. □

7. Recall the definition for the notion of idempotence.

   Suppose C is an $(n \times n)$-square matrix.
   Then C is said to be idempotent if and only if $C^2 = C$.

   Recall the definition for the notion of invertibility.

   Suppose P is an $(n \times n)$-square matrix.
   Then P is said to be invertible if and only if P has a matrix inverse.

8. **Statement (4).**

   Let A be an $(n \times n)$-square matrix. Suppose $A - I_n$ is idempotent. Then A is invertible.

   Proof of Statement (4).

   [Ask: What is the assumption?
   Answer. '*A is an $(n \times n)$-square matrix. Also, $A - I_n$ is idempotent.*'
   Further ask: What is the (desired) conclusion to be deduced from the assumption?
   Answer. '*A has a matrix inverse.*' But what is it, really? '*There is some $(n \times n)$-square matrix B so that $BA = I_n$ and $AB = I_n$*'.]

   Let A be an $(n \times n)$-square matrix. Suppose $A - I_n$ is idempotent.

   [Reminder: We try to deduce that A is invertible.
   Objective: We try to name an appropriate $(n \times n)$-matrix B for which $BA = I_n$ and $AB = I_n$.
   Ask: What does the assumption tell us about A? Can we extract some equality about A from it?
   Answer: '$(A - I_n)^2 = A - I_n$'.]

   Since $A - I_n$ is idempotent, we have

   $$A - I_n = (A - I_n)^2 = A(A - I_n) - I_n(A - I_n) = \cdots = A^2 - 2A + I_n.$$

   Therefore $\frac{3}{2}A - \frac{1}{2}A^2 = I_n$.

   Hence $(\frac{3}{2}I_n - \frac{1}{2}A)A = I_n$ and $A(\frac{3}{2}I_n - \frac{1}{2}A) = I_n$.

   Then there exists some $(n \times n)$-square matrix B, namely, $B = \frac{3}{2}I_n - \frac{1}{2}A$, such that $BA = I_n$ and $AB = I_n$.

   Therefore A is invertible. □

9. **Statement (5).**

   Let A be an $(n \times n)$-square matrix. Suppose A is idempotent, and A is not the identity matrix. Then there exists some non-zero vector $\mathbf{v}$ in $\mathbb{R}^n$ such that $A\mathbf{v} = \mathbf{0}$.

   Proof of Statement (5).

   Let A be an $(n \times n)$-square matrix. Suppose A is idempotent, and A is not the identity matrix.

[Reminder: We want to deduce that there exists some non-zero vector $\mathbf{v}$ in $\mathbb{R}^n$ such that $A\mathbf{v} = \mathbf{0}$.
Ask: How does such a vector $\mathbf{v}$ arise? Is there some equality with A involved in one side and with only the zero matrix (or zero vector) in the other side?]

Since A is idempotent, $A^2 = A$.

Then $A(A - I_n) = A^2 - A = \mathcal{O}_{n\times n}$.

Since A is not the identity matrix, $A - I_n$ is not the zero matrix. Then there is a non-zero entry somewhere in $A - I_n$, say, in the k-th column.

Denote the k-th column of $A - I_n$ by $\mathbf{v}$. By definition, there is a non-zero entry in $\mathbf{v}$. Then $\mathbf{v}$ is not a zero vector in $\mathbb{R}^n$.

Since $A(A - I_n) = \mathcal{O}_{n\times n}$, we have $A\mathbf{v} = \mathbf{0}$. □

10. Recall the definition for the notion of nilpotence.

Suppose A is a square matrix.
Then A is said to be nilpotent if and only if there is some positive integer p so that $A^p = \mathcal{O}$.

11. **Statement (6).**

Let A be an $(n \times n)$-square matrix. Suppose A is not the zero matrix and A is nilpotent. Then $I_n - A$ is invertible, and there is some positive integer k so that $I_n + A + A^2 + \cdots + A^k$ is a matrix inverse of $I_n - A$.

Proof of Statement (6).

Let A be an $(n \times n)$-square matrix. Suppose A is not the zero matrix and A is nilpotent.

[Preparatory roughwork. Observe that for each positive integer m, the equality

$$(I_n - A)(I_n + A + A^2 + \cdots + A^m) = I_n - A^{m+1}$$

hold regardless of the assumption on A.
Ask: Does the assumption guarantee that the 'right-hand-side' becomes I_n for some appropriate value(s) of m? How?]

Since A is nilpotent, there is some positive integer p so that $A^p = \mathcal{O}$. Since A is not the zero matrix, $p > 1$.

Take $k = p - 1$. Note that k is a positive integer.

Define $B = I_n + A + A^2 + \cdots + A^p$. We have

$$\begin{aligned}(I_n - A)B &= (I_n - A)(I_n + A + A^2 + \cdots + A^k) \\ &= (I_n + A + A^2 + \cdots + A^k) - A(I_n + A + A^2 + \cdots + A^k) \\ &= (I_n + A + A^2 + \cdots + A^k) - (A + A^2 + \cdots + A^k + A^{k+1}) \\ &= I_n - A^{k+1} = I_n - A^p = I_n - \mathcal{O}_{n\times n} = I_n.\end{aligned}$$

Similarly, we also deduce $B(I_n - A) = I_n$.

Then $I_n - A$ is invertible and B is a matrix inverse of A. □

12. **Statement (7).**

Let A, B be $(n \times n)$-square matrices. Suppose $[A, B] = \mathcal{O}_{n\times n}$. Then for any positive integer k, $A^kB = BA^k$.

Proof of Statement (7).

Let A, B be $(n \times n)$-square matrices. Suppose $[A, B] = \mathcal{O}_{n\times n}$.

For each positive integer k, denote by $P(k)$ the proposition $A^kB = BA^k$.

- [We intend to deduce $P(1)$, with the help of $[A, B] = \mathcal{O}_{n\times n}$.]
  Note that $AB - BA = [A, B] = \mathcal{O}_{n\times n}$. Then $AB = BA$.
  Hence $P(1)$ is true.
- Let m be an integer. Suppose $P(m)$ is true.
  [With the assumption $P(m)$ and with the help of $P(1)$ (which has been verified already), we intend to deduce $P(m + 1)$.]
  By $P(1)$, we have $AB = BA$.
  Then $A^{m+1}B = A^m(AB) = A^m(BA) = (A^mB)A$.
  By $P(m)$, we have $A^mB = BA^m$.
  Then $A^{m+1}B = (A^mB)A = (BA^m)A = BA^{m+1}$.
  Therefore $P(m + 1)$ is true.

By the Principle of Mathematical Induction, $P(k)$ is true for any positive integer k. □

13. **Statement (8).**

Let A be an $(n \times n)$-square matrix. Suppose A is nilpotent. Then A is not invertible.

Proof of Statement (8).

Let A be an $(n \times n)$-square matrix. Suppose A is nilpotent.

Further suppose (for the sake of argument for the moment) that A were invertible.

> [We intend to obtain something 'ridiculous wrong' from all of the above. Then we will be forced to concede that under the assumption given in the statement to be proved, it is impossible for it to happen that '*A is invertible.*']

Since A is nilpotent, there is some positive integer p so that $A^p = \mathcal{O}_{n\times n}$.

Since A were invertible, there would be some $(n \times n)$-square matrix B so that $BA = I_n$ and $AB = I_n$.

We have

$$\begin{aligned} B^2A^2 &= B(BA)A = BI_nA = BA = I_n, \\ B^3A^3 &= B(B^2A^2)A = BI_nA = BA = I_n, \\ &\vdots \\ B^pA^p &= B(B^{p-1}A^{p-1})A = BI_nA = BA = I_n \end{aligned}$$

Recall that $A^p = \mathcal{O}_{n\times n}$. Then $I_n = B^pA^p = B^p\mathcal{O}_{n\times n} = \mathcal{O}$.

> [We have obtained something 'ridiculous wrong', namely, '$I_n = \mathcal{O}_{n\times n}$'. This is called a contradiction.

Contradiction arises.

> [So we are forced to concede that under the assumption given in the statement to be proved, it is impossible for it to happen that '*A is invertible.*']

Hence, in the first place, A is not invertible. □

14. **Statement (9).**

Let A be an $(n \times n)$-square matrix. Suppose A is idempotent and A is not the zero matrix. Then A is not nilpotent.

Proof of Statement (9), with the method of proof-by-contradiction.

Let A be an $(n \times n)$-square matrix. Suppose A is idempotent and A is not the zero matrix.

Further suppose (for the sake of argument for this moment) that A were nilpotent.

> [We intend to obtain something 'ridiculous wrong' from all of the above. Then we will be forced to concede that under the assumption given in the statement to be proved, it is impossible for it to happen that '*A is not the zero matrix.*']

Since A is idempotent, we have $A^2 = A$.

Since A was nilpotent, there would be some positive integer p so that $A^p = \mathcal{O}$. Since $A \neq \mathcal{O}_{n\times n}$, we would have $p > 2$.

Then we have

$$\begin{aligned} A^3 &= A^2A = A^2 = A, \\ A^4 &= A^3A = A^3 = A, \\ &\vdots \\ A^p &= A^{p-1}A = \cdots = A. \end{aligned}$$

Recall that $A^p = \mathcal{O}_{n\times n}$. Then $A = A^p = \mathcal{O}_{n\times n}$.

But by assumption, $A \neq \mathcal{O}_{n\times n}$ also.

> [We have obtained something 'ridiculous wrong', namely, '*$A = \mathcal{O}_{n\times n}$ and $A \neq \mathcal{O}_{n\times n}$ simultaneously*'. This is called a contradiction.

Contradiction arises.

> [So we are forced to concede that under the assumption given in the statement to be proved, it is impossible for it to happen that '*A is nilpotent.*']

Hence, in the first place, A is not nilpotent. □