

# MA2101S Homework 3

Qi Ji

A0167793L

12th February 2018

1. Let  $K$  be a *finite* field, and let  $q := |K|$  denote the number of elements in  $K$ . Let  $V$  be a  $K$ -vector space of dimension  $n \geq 1$ .

(a) Show that the number of ordered  $K$ -bases of  $V$  is  $(q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})$ .

**Claim.** Let  $A = \{v_1, \dots, v_r\} \subseteq V$  be a linearly-independent set, then  $|\text{span}(A)| = q^r$ .

*Proof of claim.*  $\text{span}(A)$  is a  $r$ -dimensional  $K$ -subspace of  $V$ , so  $\text{span}(A) \cong K^r$ . Since  $|K^r| = q^r$ ,  $|\text{span}(A)| = q^r$ .  $\square$

*Proof.* Since  $\dim_K V = n$ ,  $V \cong K^n$ . Therefore  $|V| = |K^n| = q^n$ . Now count the number of ways to choose ordered  $K$ -bases of  $V$ , by constructing a linearly independent array, similarly to the proof of existence of basis (for finite-dimensional vector spaces).

- Start by choosing any vector  $v_1 \in V \setminus \{0_V\}$ , by claim,  $|\{0_V\}| = |\text{span}(\emptyset)| = q^0 = 1$ , so  $|V \setminus \{0_V\}| = q^n - 1$ , we have  $(q^n - 1)$  ways to choose  $v_1$ .
- Then choose  $v_2 \in V \setminus \text{span}(\{v_1\})$ . Since  $\text{span}(\{v_1\}) \subseteq V$  and  $|\text{span}(\{v_1\})| = q^1$ ,  $|V \setminus \text{span}(\{v_1\})| = q^n - q$ . There are  $(q^n - q)$  ways to choose  $v_2$ .
- Generally, for  $i \in \{1, \dots, n\}$ , we choose  $v_i \in V \setminus \text{span}(\{v_1, \dots, v_{i-1}\})$ , from claim,

$$|\text{span}(\{v_1, \dots, v_{i-1}\})| = q^{i-1},$$

and as  $\text{span}(\{v_1, \dots, v_{i-1}\}) \subseteq V$ ,  $|V \setminus \text{span}(\{v_1, \dots, v_{i-1}\})| = q^n - q^{i-1}$ , and we have  $(q^n - q^{i-1})$  ways to choose the  $i$ -th vector.

When algorithm halts after  $n$  iterations, by construction, we obtain  $n$  linearly-independent vectors in  $V$ , by well-definedness of dimension,  $(v_1, \dots, v_n)$  is an ordered basis for  $V$ . Then re-examining the algorithm, by multiplication principle of counting, there are

$$\prod_{i=1}^n (q^n - q^{i-1})$$

ways to choose an ordered  $K$ -basis for  $V$ , which evaluates to the expression given.  $\square$

- (b) Deduce that  $(q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})$  is divisible by  $n!$  by determining the number of (unordered)  $K$ -bases of  $V$ .

*Proof.* Let  $a \in \mathbb{N}$  be the number of (unordered)  $K$ -bases for  $V$ . Given an arbitrary unordered basis of  $V$ , there are  $(\dim_K V)! = n!$  ways to arrange them to get ordered bases of  $V$ . Then by multiplication principle,  $a \cdot n! = |\{\text{ordered } K\text{-bases for } V\}|$ , therefore  $n! \mid (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})$ .  $\square$

**2.** Consider the field  $\mathbb{R}$  as a vector space over  $\mathbb{Q}$ . Show that  $\dim_{\mathbb{Q}} \mathbb{R}$  is not finite.

*Proof.* Suppose (for a contradiction)  $\mathbb{R}$  as a  $\mathbb{Q}$ -vector space is finite dimensional, that is  $\exists n \in \mathbb{N}$ .  $\dim_{\mathbb{Q}} \mathbb{R} = n$ , then we have the isomorphism that  $\mathbb{R} \cong \mathbb{Q}^n$ . From elementary set theory, we know  $\mathbb{Q} \cong \mathbb{N}$  and that a finite product of countable sets is countable. We can hence conclude that  $|\mathbb{Q}^n| = \aleph_0$ , but we have  $|\mathbb{R}| = |\mathbb{Q}^n| = \aleph_0$ , which contradicts Cantor's Theorem.  $\square$

**3.** Consider  $\mathbb{C}$  as a 2-dimensional  $\mathbb{R}$ -vector space, and let  $T \in \text{End}_{\mathbb{R}}(\mathbb{C})$  be an  $\mathbb{R}$ -linear operator on  $\mathbb{C}$ . ( $T$  is an  $\mathbb{R}$ -linear map  $\mathbb{C} \rightarrow \mathbb{C}$ .)

- (a) Let  $[T]_{\mathcal{B}} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{M}_2(\mathbb{R})$  denote the matrix over  $\mathbb{R}$  associated to  $T$  with respect to the ordered basis  $\mathcal{B} = (1, i)$  of  $\mathbb{C}$ . Show that  $T$  is  $\mathbb{C}$ -linear if and only if one has  $d = a$  and  $c = -b$  in the entries of  $[T]_{\mathcal{B}}$ .

*Proof.* From definition of  $[T]_{\mathcal{B}}$ ,  $T$  is an  $\mathbb{R}$ -linear map defined on the basis  $\mathcal{B}$  as

$$\begin{aligned} T : \mathbb{C} &\rightarrow \mathbb{C}; \\ 1 &\mapsto a + ci; \\ i &\mapsto b + di. \end{aligned}$$

Suppose  $T$  is  $\mathbb{C}$ -linear, then in particular take  $i \in \mathbb{C}$ ,

$$\begin{aligned} i \cdot T(1) &= T(1 \cdot i) \\ i(a + ci) &= b + di \\ -c + ai &= b + di \end{aligned}$$

Since  $\mathcal{B} = (1, i)$  is an  $\mathbb{R}$ -basis for  $\mathbb{C}$ , by uniqueness of vector representation, we have  $b = -c$  and  $a = d$  in  $\mathbb{R}$ .

Conversely suppose  $a = d$  and  $c = -b$  in  $[T]_{\mathcal{B}}$ , then

$$[T]_{\mathcal{B}} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

which means  $T$  is the  $\mathbb{R}$ -linear map defined on the ordered basis  $\mathcal{B}$  as

$$\begin{aligned} T : \mathbb{C} &\rightarrow \mathbb{C}; \\ 1 &\mapsto a - bi; \\ i &\mapsto b + ai. \end{aligned}$$

Since  $T$  is  $\mathbb{R}$ -linear, then for  $v, w \in \mathbb{C}$ ,  $T(v + w) = T(v) + T(w)$  (linear under vector addition). To show  $T$  is  $\mathbb{C}$ -linear, it remains to show  $T$  is  $\mathbb{C}$ -linear under scalar multiplication, that is for  $v \in \mathbb{C}, r \in \mathbb{C}$ , show that  $r \cdot T(v) = T(r \cdot v)$ . Let  $x_1, x_2, y_1, y_2 \in \mathbb{R}$  such that  $v = x_1 + y_1i$  and  $r = x_2 + y_2i$ . Using  $\mathbb{R}$ -linearity of  $T$ , compute  $r \cdot T(v)$ ,

$$\begin{aligned} r \cdot T(v) &= r(x_1T(1) + y_1T(i)) \\ &= r(x_1(a - bi) + y_1(b + ai)) \\ &= (x_2 + y_2i)((ax_1 + by_1) + (ay_1 - bx_1)i) \\ &= (ax_1x_2 - ay_1y_2 + bx_1y_2 + by_1x_2) \\ &\quad + (ax_1y_2 + ay_1x_2 - bx_1x_2 + by_1y_2)i \end{aligned}$$

Now compute  $T(r \cdot v)$ ,

$$\begin{aligned} r \cdot v &= (x_2 + y_2i)(x_1 + y_1i) \\ &= (x_1x_2 - y_1y_2) + (x_1y_2 + x_2y_1)i \\ T(r \cdot v) &= (x_1x_2 - y_1y_2)T(1) + (x_1y_2 + x_2y_1)T(i) \\ &= (x_1x_2 - y_1y_2)(a - bi) + (x_1y_2 + x_2y_1)(b + ai) \\ &= ax_1x_2 - ay_1y_2 + bx_1y_2 + bx_2y_1 \\ &\quad + (-bx_1x_2 + by_1y_2 + ax_2y_1 + ax_1y_2)i \end{aligned}$$

It can be verified that  $r \cdot T(v) = T(r \cdot v)$ . Hence  $T$  is  $\mathbb{C}$ -linear. □

(b) Show that there exist complex numbers  $\lambda, \mu \in \mathbb{C}$  such that for any  $z \in \mathbb{C}$ , one has

$$T(z) = \lambda z + \mu \bar{z} \quad \text{in } \mathbb{C},$$

and give explicit expressions of  $\lambda$  and  $\mu$  in terms of  $T(1)$  and  $T(i)$ . Deduce that  $T$  is  $\mathbb{C}$ -linear if and only if  $\mu = 0$ .

*Solution.*  $T(1)$  and  $T(i)$  are vectors in  $\mathbb{C}$  determined by  $T$ . Firstly, we solve for  $\lambda, \mu \in \mathbb{C}$  satisfying the following linear system,

$$\left. \begin{aligned} \lambda + \mu &= T(1) \\ \lambda i - \mu i &= T(i) \end{aligned} \right\} \quad (3.1)$$

Solving this system in  $\mathbb{C}$ ,

$$\left( \begin{array}{cc|c} 1 & 1 & T(1) \\ i & -i & T(i) \end{array} \right) \xrightarrow[\text{Elimination}]{\text{Gauss-Jordan}} \left( \begin{array}{cc|c} 1 & 0 & \frac{T(1)-iT(i)}{2} \\ 0 & 1 & \frac{T(1)+iT(i)}{2} \end{array} \right)$$

So we have now a solution to (3.1)

$$\lambda = \frac{T(1) - iT(i)}{2}; \quad \mu = \frac{T(1) + iT(i)}{2}.$$

Since  $T(1), T(i) \in \mathbb{C}$ , we have the existence of  $\lambda, \mu \in \mathbb{C}$  satisfying the system of equations in (3.1). Then for any  $z \in \mathbb{C}$ , by  $\mathbb{R}$ -linearity of  $T$ , let  $a, b \in \mathbb{R}$  such that  $z = a + bi$ ,

$$\begin{aligned} T(z) &= T(a + bi) \\ &= aT(1) + bT(i) \\ &= a(\lambda + \mu) + b(\lambda - \mu)i \\ &= \lambda(a + bi) + \mu(a - bi) \\ &= \lambda z + \mu \bar{z} \end{aligned} \quad \blacksquare$$

Deduce that  $T$  is  $\mathbb{C}$ -linear if and only if  $\mu = 0$ .

*Proof.* Suppose  $T$  is  $\mathbb{C}$ -linear, then

$$\begin{aligned} i \cdot T(i) &= T(i \cdot i) \\ i(\lambda i - \mu i) &= T(-1) = -T(1) \\ -\lambda + \mu &= -\lambda - \mu \\ \mu &= -\mu \\ \mu &= 0 \end{aligned}$$

Conversely suppose  $\mu = 0$ , then we have  $T(z) = \lambda z$ . Since  $T$  is already  $\mathbb{R}$ -linear, it is linear under vector addition. To show  $\mathbb{C}$ -linearity, it remains to show linearity under scalar multiplication. For any  $y, z \in \mathbb{C}$ ,

$$\begin{aligned} y \cdot T(z) &= y \cdot \lambda z \\ &= \lambda \cdot (yz) \\ &= T(yz) \end{aligned}$$

This completes the proof. □

4. Keep the notation as in the previous problem.

(a) Show that  $T$  is an  $\mathbb{R}$ -isomorphism if and only if  $\lambda\bar{\lambda} \neq \mu\bar{\mu}$ .

*Proof.* Suppose  $T$  is an  $\mathbb{R}$ -isomorphism, and suppose (for a contradiction)  $\lambda\bar{\lambda} = \mu\bar{\mu}$ , then

$$\begin{aligned} T(\bar{\lambda}) &= \lambda\bar{\lambda} + \mu\lambda \\ T(\mu) &= \lambda\mu + \mu\bar{\mu} \\ T(\bar{\lambda} - \mu) &= 0 \end{aligned}$$

By injectivity of  $T$ ,  $\bar{\lambda} = \mu$ . Let  $a, b \in \mathbb{R}$  such that

$$\begin{aligned} \lambda &= a + bi \\ \mu &= a - bi \end{aligned}$$

Then from 3 (b),  $T$  sends the basis vectors in  $\mathcal{B} = (1, i)$  to

$$\begin{aligned} T(1) &= \lambda + \mu \\ &= a + bi + a - bi \\ &= 2a \\ T(i) &= (\lambda - \mu)i \\ &= (a + bi - a + bi)i \\ &= -2b \end{aligned}$$

This contradicts with  $T$  being an  $\mathbb{R}$ -isomorphism, as  $T(1)$  and  $T(i)$  are  $\mathbb{R}$ -linearly dependent in  $\mathbb{C}$ . Hence if  $T$  is an  $\mathbb{R}$ -isomorphism,  $\lambda\bar{\lambda} \neq \mu\bar{\mu}$ .

To prove the converse implication, I shall prove the contrapositive. Suppose  $T : \mathbb{C} \rightarrow \mathbb{C}$  is *not* an  $\mathbb{R}$ -isomorphism, then  $\text{rank}(T) < \dim_{\mathbb{R}} \mathbb{C} = 2$ . Then consider the matrix representation of  $T$  with respect to the ordered basis  $\mathcal{B} = (1, i)$  of  $\mathbb{C}$ . Let  $a, b, c, d \in \mathbb{R}$  such that

$$[T]_{\mathcal{B}} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{M}_2(\mathbb{R}).$$

As  $\text{rank}(T) \leq 1$ ,  $T(1)$  and  $T(i)$  are linearly dependent, so  $\exists \alpha, \beta \in \mathbb{R}$ , not all 0, such that

$$\alpha(a + ci) = \beta(b + di) \quad (4.1)$$

Then by uniqueness of vector representation with respect to basis  $\mathcal{B}$ , we have  $\alpha a = \beta b$  and  $\alpha c = \beta d$ , so  $\alpha\beta ad = \alpha\beta bc$ . Then either

$$\alpha\beta = 0 \text{ or } ad = bc. \quad (4.2)$$

From 3 (b), we have explicit expressions for  $\lambda$  and  $\mu$  in terms of  $T(1)$  and  $T(i)$ ,

$$\begin{aligned}\lambda &= \frac{T(1) - iT(i)}{2} \\ &= \frac{(a + ci) - (bi - d)}{2} \\ &= \frac{(a + d) + (c - b)i}{2} \\ \mu &= \frac{T(1) + iT(i)}{2} \\ &= \frac{(a + ci) + (bi - d)}{2} \\ &= \frac{(a - d) + (c + b)i}{2}\end{aligned}$$

Case  $\alpha = 0$ , then from (4.1), as  $\beta \neq 0$ ,  $T(i) = b + di = 0$ , so  $\lambda = \mu = \frac{T(1)}{2}$ , which gives the equality  $\lambda\bar{\lambda} = \mu\bar{\mu}$ . Case  $\beta = 0$ , then similarly from (4.1), because  $\alpha \neq 0$ ,  $T(1) = a + ci = 0$ , then we have  $\lambda = -\mu$ , which gives the equality  $\lambda\bar{\lambda} = \mu\bar{\mu}$ .

Case  $ad = bc$ , proceed to compute  $\lambda\bar{\lambda}$  and  $\mu\bar{\mu}$ , we obtain

$$\begin{aligned}\lambda\bar{\lambda} &= \frac{1}{4} ((a + d)^2 + (c - b)^2) \\ &= \frac{1}{4} (a^2 + 2ad + d^2 + b^2 - 2bc + c^2) \\ \mu\bar{\mu} &= \frac{1}{4} ((a - d)^2 + (c + b)^2) \\ &= \frac{1}{4} (a^2 - 2ad + d^2 + b^2 + 2bc + c^2)\end{aligned}$$

Substituting (4.2) into the expressions above gives us that  $\lambda\bar{\lambda} = \mu\bar{\mu}$ . Taking the contrapositive, we get the implication that that if  $\lambda\bar{\lambda} \neq \mu\bar{\mu}$ ,  $T$  is an  $\mathbb{R}$ -isomorphism.  $\square$

- (b) Show that  $|T(z)| = |z|$  for any  $z \in \mathbb{C}$  (i.e.  $T$  is an isometric isomorphism of normed  $\mathbb{R}$ -vector spaces) if and only if  $\lambda\mu = 0$  and  $|\lambda + \mu| = 1$

*Proof.* Suppose  $|T(z)| = |z|$ , then because of isometric property,  $T$  has a trivial kernel. Recall that  $T$  has property for any  $z \in \mathbb{C}$ ,  $T(z) = \lambda z + \mu \bar{z}$ . In addition, because  $T$  is an endomorphism with a trivial kernel, and  $\mathbb{C}$  is finite-dimensional, by rank-nullity theorem,  $T$  is an isomorphism. Using the isometric property, evaluate  $T(1)$ ,

$$1 = |T(1)| = |\lambda + \mu|.$$

It remains to show that  $\lambda\mu = 0$ .

Now suppose for a contradiction  $\lambda\mu \neq 0$ , that is, both  $\lambda \neq 0$  and  $\mu \neq 0$ . Let  $\alpha, \beta \in (-\pi, \pi]$  such that

$$\begin{aligned}\lambda &= |\lambda| e^{i\alpha} \\ \mu &= |\mu| e^{i\beta}\end{aligned}$$

Let  $z \in \mathbb{C}$  such that  $z = e^{i\theta}$  where  $\theta = \frac{\beta - \alpha}{2}$  (i.e.  $z$  is the number on the unit circle with argument  $\frac{\beta - \alpha}{2}$ ), clear that  $|z| = 1$ , now compute  $T(z)$ ,

$$\begin{aligned}T(z) &= T(e^{i\theta}) \\ &= |\lambda| e^{i\alpha} e^{i\theta} + |\mu| e^{i\beta} e^{-i\theta} \\ &= |\lambda| e^{i(\alpha + \theta)} + |\mu| e^{i(\beta - \theta)} \\ &= |\lambda| e^{i(\alpha + \beta)/2} + |\mu| e^{i(\beta + \alpha)/2}\end{aligned}$$

In triangle inequality, for both numbers non-zero, equality holds if and only if the two numbers have the same argument. Now make use of this result while measuring distance,

$$\begin{aligned}|T(z)| &= ||\lambda| e^{i(\alpha + \beta)/2} + |\mu| e^{i(\beta + \alpha)/2}| \\ 1 &= ||\lambda| e^{i(\alpha + \beta)/2}| + ||\mu| e^{i(\beta + \alpha)/2}| \\ &= |\lambda| + |\mu|\end{aligned}$$

We have  $|\lambda + \mu| = |\lambda| + |\mu| = 1$ , which means  $\text{Arg}(\lambda) = \text{Arg}(\mu) = \alpha = \beta$ . Now take any  $z' = e^{i\phi} \in \mathbb{C}$  where  $\phi$  is not a multiple of  $\pi$ , clear that  $|z'| = 1$ ,

$$\begin{aligned}T(z') &= T(e^{i\phi}) \\ &= |\lambda| e^{i\alpha} e^{i\phi} + |\mu| e^{i\alpha} e^{-i\phi} \\ &= |\lambda| e^{i(\alpha + \phi)} + |\mu| e^{i(\alpha - \phi)}\end{aligned}$$

Now due to our selection of  $z'$ ,

$$\alpha + \phi \neq \alpha - \phi \pmod{(-\pi, \pi]},$$

so  $\text{Arg}(e^{i(\alpha + \phi)}) \neq \text{Arg}(e^{i(\alpha - \phi)})$ , then equality does not hold in triangle inequality, so we have

$$\begin{aligned}|T(z')| = 1 &= ||\lambda| e^{i(\alpha + \phi)} + |\mu| e^{i(\alpha - \phi)}| < ||\lambda| e^{i(\alpha + \phi)}| + ||\mu| e^{i(\alpha - \phi)}| \\ &= ||\lambda| e^{i(\alpha + \phi)} + |\mu| e^{i(\alpha - \phi)}| < |\lambda| + |\mu| = 1\end{aligned}$$

which is a contradiction. Hence  $\lambda\mu = 0$ .

Conversely suppose  $\lambda\mu = 0$  and  $|\lambda + \mu| = 1$ , then  $\lambda = 0$  or  $\mu = 0$ .

Case  $\lambda = 0$ ,  $|\mu| = 1$ , then

$$\begin{aligned}T(z) &= \mu\bar{z} \\|T(z)| &= |\mu\bar{z}| = |z|\end{aligned}$$

Case  $\mu = 0$ ,  $|\lambda| = 1$ , then similarly

$$\begin{aligned}T(z) &= \lambda z \\|T(z)| &= |\lambda z| = |z|\end{aligned}$$

Which completes the proof.

□



5. Let  $K$  be a field and let  $V$  be a  $K$ -vector space. Let  $T \in \text{End}_K(V)$  be a  $K$ -linear endomorphism of  $V$ . Recall that  $T^2 = T \circ T \in \text{End}_K(V)$  denotes the composite of  $T$  with itself.

(a) Show that  $\text{Ker}(T) = \text{Ker}(T^2)$  if and only if  $\text{Ker}(T) \cap \text{Im}(T) = \{0\}$ .

*Proof.* Suppose  $\text{Ker}(T) = \text{Ker}(T^2)$ , then take any  $y \in \text{Ker}(T) \cap \text{Im}(T)$ , then  $\exists x \in V$ .  $T(x) = y$  and  $T(y) = 0$ , therefore  $(T \circ T)(x) = 0$  which means  $x \in \text{Ker}(T^2)$ , then by assumption,  $x \in \text{Ker}(T)$  which means  $y = T(x) = 0$ . Therefore  $\text{Ker}(T) \cap \text{Im}(T) \subseteq \{0\}$ . As the reverse containment is trivial ( $T(0) = 0$ ),  $\text{Ker}(T) \cap \text{Im}(T) = \{0\}$ .

Conversely suppose  $\text{Ker}(T) \cap \text{Im}(T) = \{0\}$ . Trivially, take  $x \in \text{Ker}(T)$ , since  $T(x) = 0$ ,  $T^2(x) = T(T(x)) = T(0) = 0$  which gives us  $\text{Ker}(T) \subseteq \text{Ker}(T^2)$ . On the other hand, take  $x \in \text{Ker}(T^2)$ , so  $T(T(x)) = 0$ . We can now see that  $T(x) \in \text{Ker}(T)$  and  $T(x) \in \text{Im}(T)$ , then  $T(x) \in \text{Ker}(T) \cap \text{Im}(T)$  and by hypothesis,  $T(x) = 0$ , this means  $x \in \text{Ker}(T)$ , therefore  $\text{Ker}(T) \supseteq \text{Ker}(T^2)$ . This completes the proof that  $\text{Ker}(T) = \text{Ker}(T^2)$ .  $\square$

(b) Show that  $\text{Im}(T) = \text{Im}(T^2)$  if and only if  $V = \text{Ker}(T) + \text{Im}(T)$ .

*Proof.* Suppose  $\text{Im}(T) = \text{Im}(T^2)$ , take any arbitrary  $v \in V$ , then clearly  $T(v) \in \text{Im}(T) = \text{Im}(T^2)$ . So  $\exists a \in V$ .  $T^2(a) = T(v)$ . Now by linearity

$$\begin{aligned} T(T(a)) &= T(v) \\ T(v) - T(T(a)) &= 0 \\ T(v - T(a)) &= 0 \\ v - T(a) &\in \text{Ker}(T) \end{aligned}$$

Then  $\exists k \in \text{Ker}(T)$ .  $v - T(a) = k$ , so  $v = k + T(a)$ . Since for any arbitrary  $v \in V$ , there exists  $k \in \text{Ker}(T)$ ,  $T(a) \in \text{Im}(T)$ , such that  $v = k + T(a)$ ,  $V = \text{Ker}(T) + \text{Im}(T)$ .

Conversely suppose  $V = \text{Ker}(T) + \text{Im}(T)$ . Trivially,  $\text{Im}(T) \supseteq \text{Im}(T^2)$ , as take  $y \in \text{Im}(T^2)$ , then  $\exists x \in V$ .  $T^2(x) = y$ , then as  $T(x) \in V$  such that  $T(T(x)) = y$ ,  $y \in \text{Im}(T)$ .

Now take any  $y \in \text{Im}(T)$ , then  $\exists x \in V$ .  $T(x) = y$ . As  $V = \text{Ker}(T) + \text{Im}(T)$ ,  $\exists k \in \text{Ker}(T)$ ,  $v \in V$ .  $x = k + T(v)$ . Then

$$\begin{aligned} y &= T(x) = T(k + T(v)) \\ &= T^2(v) \end{aligned}$$

which implies  $y \in \text{Im}(T^2)$ , so  $\text{Im}(T) \subseteq \text{Im}(T^2)$ . Therefore  $\text{Im}(T) = \text{Im}(T^2)$ .  $\square$

**6.** Let  $K$  be a field and let  $V$  be a  $K$ -vector space, of finite dimension  $n := \dim_K(V)$  over  $K$ . Let  $T \in \text{End}_K(V)$  be a  $K$ -linear endomorphism of  $V$ . Suppose there exists a vector  $v \in V$  such that

$$T(v), T^2(v), \dots, T^n(v) \quad \text{is a basis for } V.$$

Show that

$$v, T(v), \dots, T^{n-1}(v) \quad \text{is also a basis for } V,$$

and that  $T$  is invertible as a  $K$ -linear endomorphism on  $V$ .

*Proof.* Let  $\mathcal{B} := (T(v), T^2(v), \dots, T^n(v))$ , be an ordered basis for  $V$ . Then consider the equation

$$d_1 v + d_2 T(v) + \dots + d_n T^{n-1}(v) = 0 \tag{6.1}$$

where  $d_1, \dots, d_n \in K$ . Then by linearity of  $T$ .

$$\begin{aligned} T(d_1 v + d_2 T(v) + \dots + d_n T^{n-1}(v)) &= T(0) \\ d_1 T(v) + d_2 T^2(v) + \dots + d_n T^n(v) &= 0 \end{aligned}$$

and as  $\mathcal{B}$  is a basis for  $V$ , we have  $d_1 = \dots = d_n = 0$ , so  $\mathcal{C} := (v, T(v), \dots, T^{n-1}(v))$  is a linearly-independent list. Then as  $\text{length}(\mathcal{C}) = \dim_K(V) = n$ , by well-definedness of dimension,  $\mathcal{C}$  is also a (ordered) basis for  $V$ .

To show that  $T$  is invertible, it suffices to define a linear map  $U \in \text{End}_K(V)$  such that  $TU = UT = \text{id}_V$ . Proceed by defining a linear map  $U : V \rightarrow V$  on the basis  $\mathcal{B}$  as

$$\begin{aligned} T(v) &\mapsto v \\ T^2(v) &\mapsto T(v) \\ &\dots \\ T^n(v) &\mapsto T^{n-1}(v) \end{aligned}$$

Then for any  $w \in V$ , as  $\mathcal{C}$  is a basis for  $V$ ,  $\exists c_1, \dots, c_n \in K$  such that

$$\begin{aligned} w &= \sum_{i=1}^n c_i T^{i-1}(v) \\ T(w) &= \sum_{i=1}^n c_i T^i(v) \\ (UT)(w) &= \sum_{i=1}^n c_i T^{i-1}(v) \end{aligned}$$

so  $UT = \text{id}_V$ . Similarly for any  $w \in V$ , as  $\mathcal{B}$  is also a basis for  $V$ ,  $\exists c_0, \dots, c_{n-1} \in K$  such that

$$\begin{aligned} w &= \sum_{i=0}^{n-1} c_i T^{i+1}(v) \\ U(w) &= \sum_{i=0}^{n-1} c_i T^i(v) \\ (TU)(w) &= \sum_{i=0}^{n-1} c_i T^{i+1}(v) \end{aligned}$$

so  $TU = \text{id}_V$ . Therefore  $T$  is invertible. □