MA2101S - Linear Algebra II (S) Suggested Solutions

(Semester 2, AY2021/2022)

Written by: Timothy Wan
Audited by: Matthew Fan

Question 1

First we show (a) implies (b). Assume (a) holds, and let $w \in \operatorname{im}(\alpha+\beta)$. Then there exists $v \in V$ such that

$$\begin{aligned} v &= (\alpha+\beta)(w) \\ &= \alpha(w) + \beta(w) \\ &\in \operatorname{im}\alpha + \operatorname{im}\beta. \end{aligned}$$

Thus $\operatorname{im}(\alpha+\beta) \subseteq \operatorname{im}\alpha + \operatorname{im}\beta$. To prove equality, we show that their dimensions match. Clearly $\dim\operatorname{im}(\alpha+\beta) \le \dim(\operatorname{im}\alpha + \operatorname{im}\beta)$. The reverse inequality is then given by

$$\begin{aligned} &\dim\operatorname{im}(\alpha+\beta) \\ &= \operatorname{rk}(\alpha+\beta) \\ &= \operatorname{rk}\alpha + \operatorname{rk}\beta && \text{by (a)} \\ &\ge \operatorname{rk}\alpha + \operatorname{rk}\beta - \dim(\operatorname{im}\alpha \cap \operatorname{im}\beta) \\ &= \dim\operatorname{im}\alpha + \dim\operatorname{im}\beta - \dim(\operatorname{im}\alpha \cap \operatorname{im}\beta) \\ &= \dim(\operatorname{im}\alpha + \operatorname{im}\beta) && \text{by the dimension formula.} \end{aligned}$$

This proves our claim of equality. Finally, since the red inequality equalizes if and only if $\dim(\operatorname{im}\alpha \cap \operatorname{im}\beta) = 0$, this forces $\operatorname{im}\alpha \cap \operatorname{im}\beta$ to be the zero space, so the sum $\operatorname{im}\alpha + \operatorname{im}\beta$ is direct, as desired.

Now we show (b) implies (c). Let us assume (b) holds. Since the sum $\operatorname{im}\alpha \oplus \operatorname{im}\beta$ is direct, clearly $\operatorname{im}\alpha \cap \operatorname{im}\beta = \{0\}$; furthermore it is obvious that

$$\operatorname{im}\alpha \subseteq \operatorname{im}\alpha \oplus \operatorname{im}\beta = \operatorname{im}(\alpha+\beta),$$

where the equality is given by (b).

We next assume (c) holds and show (d). Clearly $\operatorname{im}\alpha \cap \operatorname{im}\beta = \{0\}$. It is also clear that $\ker\alpha + \ker\beta \subseteq V$, as both kernels are subspaces of V, so it remains to prove the reverse inclusion. Let $v \in V$. Then we have that $\alpha(v) \in \operatorname{im}\alpha \subseteq \operatorname{im}(\alpha+\beta)$, so there exists some $v' \in V$ such that $\alpha(v) = (\alpha+\beta)(v')$. By linearity it follows that

$$\alpha(v - v') = \beta(v').$$

But the left side of this equation lives in $\operatorname{im}\alpha$, and the right side in $\operatorname{im}\beta$; both sides and hence elements of $\operatorname{im}\alpha \cap \operatorname{im}\beta = \{0\}$, so $\alpha(v - v') = 0 = \beta(v')$, whence $v - v' \in \ker\alpha$ and $v' \in \ker\beta$. We conclude by writing $v = (v - v') + v' \in \ker\alpha + \ker\beta$, then since $v \in V$ is arbitrary, we are done.

Assume now that (d) holds, then clearly $V = \ker\alpha + \ker\beta$. We first show that $\ker(\alpha+\beta) \subseteq \ker\alpha \cap \ker\beta$. Let $v \in \ker(\alpha + \beta)$, then

$$\alpha(v) + \beta(v) = (\alpha + \beta)(v) = 0$$

by definition. Rearranging and applying linearity, we get $\alpha(v) = \beta(-v)$. The left side of this equation live in $\operatorname{im}\alpha$, and the right side in $\operatorname{im}\beta$, so we know both sides of the equation are elements of $\operatorname{im}\alpha + \operatorname{im}\beta = \{0\}$. It follows that $\alpha(v) = \beta(-v) = 0$ so $v \in \ker\alpha$ and $-v \in \ker\beta$ (hence $v \in \ker\beta$). Then $v \in \ker\alpha \cap \ker\beta$ as desired. The reverse inclusion can be deduced as follows: for every $v \in \ker\alpha \cap \ker\beta$, we have $v \in \ker\alpha$ and $v \in \ker\beta$, so

$$(\alpha + \beta)(v) = \alpha(v) + \beta(v) = 0 + 0 = 0,$$

by definition of the kernel, whence $v \in \ker(\alpha + \beta)$ as desired.

Finally to prove that (e) implies (a), assume (e) and note that

$$\begin{aligned}
\operatorname{rk}(\alpha + \beta) &= \dim V - \operatorname{nullity}(\alpha + \beta) && \text{by the rank-nullity theorem} \\
&= \dim V - \dim\ker(\alpha + \beta) \\
&= \dim V - \dim(\ker\alpha \cap \ker\beta) && \text{by (e)} \\
&= \dim V - (\dim\ker\alpha + \dim\ker\beta - \dim V) && \text{by the dimension formula} \\
&= (\dim V - \dim\ker\alpha) + (\dim V - \dim\ker\beta) \\
&= (\dim V - \operatorname{nullity}\alpha) + (\dim V - \operatorname{nullity}\beta) \\
&= \operatorname{rk}\alpha + \operatorname{rk}\beta && \text{by the rank-nullity theorem.}
\end{aligned}$$

■

Question 2

Part (a)

Subpart (i)

Note first that M is clearly non-empty. Suppose that $\beta_1, \beta_2 \in M$ and $\lambda \in F$. Then there exist polynomials $p_1(x), p_2(x) \in F[x]$ such that $\beta_1 = p_1(\alpha)$ and $\beta_2 = p_2(\alpha)$. Then since $p_1 + \lambda p_2 \in F[x]$, it follows that

$$\beta_1 + \lambda\beta_2 = p_1(\alpha) + \lambda p_2(\alpha) = (p_1 + \lambda p_2)(\alpha) \in M,$$

which was what we wanted. $\blacksquare$

Subpart (ii)

Let $d = \deg m_\alpha(x)$, we will show that

$$\mathcal{B} = \{\mathrm{id}_V, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$$

is a basis of M. (The fact that $\dim M = d$ then follows immediately from this.) We first note that $\mathcal{B}$ is independent; indeed, suppose that $\lambda_0, \ldots, \lambda_{d-1}$ so that $\sum_{i=0}^{d-1} \lambda_i \alpha^i = 0_M$. Then $\sum_{i=0}^{d-1} \lambda_i \alpha^i = 0_M$ kills every $v \in V$ so by minimality of $m_\alpha(x)$ we must have either $\sum_{i=0}^{d-1} \lambda_i x^i = 0_{F[x]}$, or $d - 1 = \deg \sum_{i=0}^{d-1} \lambda_i x^i \geq \deg m_\alpha(x) = d$. The latter is clearly impossible, and the former holds if and only if $\lambda_0 = \ldots = \lambda_{d-1} = 0_F$, so independence follows.

To show that $\mathcal{B}$ spans M, let $p(\alpha) \in M$ and note that by the division algorithm, there exists (unique) $q(x), r(x) \in F[x]$ such that $p(x) = q(x)m_\alpha(x) + r(x)$ with $r(x) = 0_{F[x]}$ or $\deg r(x) \leq d$. In either case, we can write

$$r(x) = \sum_{i=0}^{d-1} \lambda_i x^i$$

for some $\lambda_0, \ldots, \lambda_{d-1} \in F$. Now let $v \in V$ be arbitrary, and observe that by definition of the minimal polynomial we have

$$\begin{aligned} p(\alpha)(v) &= (q(\alpha)m_\alpha(\alpha) + r(\alpha))(v) \\ &= q(\alpha)m_\alpha(\alpha)(v) + r(\alpha)(v) \\ &= r(\alpha)(v) \end{aligned}$$

so $p(\alpha) = r(\alpha)$ as linear endomorphisms on V. But this gives us

$$p(\alpha) = r(\alpha) = \sum_{i=0}^{d-1} \lambda_i \alpha^i \in \operatorname{span} \mathcal{B}$$

so we are done. $\blacksquare$

Part (b)

Note that the set $\{\mathrm{id}_V, \beta, \beta^2, \ldots, \beta^{\dim M}\}$ is a subset of M that has more elements than $\dim M$; it must thus be dependent, i.e. there exists $\lambda_0, \ldots, \lambda_{\dim M} \in F$, not all zero, such that

$$\lambda_0 \,\mathrm{id}_V + \lambda_1 \beta + \ldots + \lambda_{\dim M} \beta^{\dim M} = 0_M.$$

Then β satisfies $\sum_{i=0}^{\dim M} \lambda_i x^i$, which clearly has degree less than or equal $\dim M = \deg m_\alpha(x)$ (from (a)(ii)). ■

Part (c)

Suppose first that (ii) holds. Then for any $v \in V$ and $p(x) \in F[x]$ we have

$$p(\alpha)(v) = p(g(\beta))(v) \in \langle v \rangle_\beta \text{ and } p(\beta)(v) = p(f(\alpha))(v) \in \langle v \rangle_\alpha,$$

so clearly $\langle v \rangle_\alpha = \langle v \rangle_\beta$, and (iii) holds.

Now suppose that (iii) holds, then by the given assumption, there exists $v \in V$ such that $p(\alpha)(v) \neq 0_V$ for any proper divisor $p(x)$ of $m_\alpha(x)$. Then clearly $m_{\alpha,v}(x) = m_\alpha(x)$. It follows that

$$\deg m_\beta(x) \geq \deg m_{\beta,v}(x) = \dim \langle v \rangle_\beta = \dim \langle v \rangle_\alpha = \deg m_{\alpha,v}(x) = \deg m_\alpha(x).$$

Reversing the roles of α and β, we get the reverse equality, which proves (i).

It remains to assume (i) holds and show (ii). We start by showing that

$$\mathcal{C} = \{\mathrm{id}_V, \beta, \beta^2, \ldots, \beta^{\deg m_\beta(x)-1}\}$$

is also a basis of M. (The argument is practically copy-pasted from (a)(ii).) Let us define $d = \deg m_\beta(x) = \deg m_\alpha(x) = \dim M$ to simplify notation. We first claim $\mathcal{C}$ is independent; indeed, set $\lambda_0, \ldots, \lambda_{d-1}$ so that $\sum_{i=0}^{d-1} \lambda_i \beta^i = 0_M$. Then $\sum_{i=0}^{d-1} \lambda_i \beta^i = 0_M$ kills every $v \in V$ so by minimality of $m_\beta(x)$ we must have either $\sum_{i=0}^{d-1} \lambda_i x^i = 0_{F[x]}$, or $d - 1 \leq \deg \sum_{i=0}^{d-1} \lambda_i x^i \geq \deg m_\beta(x) = d$. The latter is clearly impossible, and the former holds if and only if $\lambda_0 = \ldots = \lambda_{d-1} = 0_F$, so independence follows.

Since C is a set of $d = \dim M$ vectors that are independent in M, C is a basis of M. Since $\alpha \in M$ we thus have scalars $\mu_0, \ldots, \mu_{d-1}$ such that

$$\alpha = \mu_0 \,\mathrm{id}_V + \mu_1 \beta + \ldots + \mu_{d-1} \beta^{d-1},$$

so setting $g(x) = \sum_{i=0}^{d-1} \mu_i x^i$ proves (ii). ■

Question 3

Part (a)

Suppose first that $p(x) \mid h(x)$, then there exists $g(x) \in F[x]$ such that $p(x)g(x) = h(x)$. Then it follows that

$$h(\alpha)(v') = g(\alpha)p(\alpha)(v') \in \langle v \rangle_\alpha$$

since $p(\alpha)(v') \in \langle v \rangle_\alpha$ by definition and $\langle v \rangle_\alpha$ is α-invariant. Conversely, if $h(\alpha)(v') \in \langle v \rangle_\alpha$, we can apply the division algorithm to get (unique) $q(x), r(x) \in F[x]$ such that $h(x) = q(x)p(x) + r(x)$ with either $r(x) = 0_{F[x]}$ or $\deg r(x) < \deg p(x)$. Then

$$h(\alpha)(v') = q(\alpha)p(\alpha)(v') + r(\alpha)(v'),$$

which we rearrange to get

$$r(\alpha)(v') = h(\alpha)(v') - q(\alpha)p(\alpha)(v') \in \langle v \rangle_\alpha.$$

By minimality of $p(x)$, we must have $\deg r(x) \geq \deg p(x)$, so we are forced to conclude that $r(x) = 0$. Then $h(x) = q(x)p(x)$ so $p(x) \mid h(x)$ as desired. ■

Part (b)

We have $m(\alpha)(v') = 0_V \in \langle v \rangle_\alpha$ by assumption, so by (a) it follows that $p(x) \mid m(a)$. ■

Part (c)

From (b) there exists $g(x) \in F[x]$ such that $g(x)p(x) = m(x)$. Then $g(\alpha)f(\alpha)(v) = g(\alpha)p(\alpha)(v') = m(v') = 0$. By the minimality of $m(x)$, we must have $g(x)p(x) = m(x) \mid g(x)f(x)$, whence $p(x) \mid f(x)$. By the definition of divisibility, there exists $q(x)$ so that $f(x) = p(x)q(x)$ as desired. ■

Part (d)

Subpart (i)

We see that

$$p(\alpha)(v'') = p(\alpha)(v' - q(\alpha)(v)) = p(\alpha)(v') - p(\alpha)q(\alpha)(v) = f(\alpha)(v) - f(\alpha)(v) = 0.$$

■

Subpart (ii)

Let $a(x), b(x) \in F[x]$ be arbitrary. Then

$$\begin{aligned} a(\alpha)(v) + b(\alpha)(v') &= a(\alpha)(v) + b(\alpha)(v + q(\alpha)(v'')) \\ &= a(\alpha)(v) + b(\alpha)(v) + b(\alpha)q(\alpha)(v'') \in \langle v \rangle_\alpha + \langle v'' \rangle_\alpha \end{aligned}$$

and

$$\begin{aligned} a(\alpha)(v) + b(\alpha)(v'') &= a(\alpha)(v) + b(\alpha)(v - q(\alpha)(v')) \\ &= a(\alpha)(v) + b(\alpha)(v) - b(\alpha)q(\alpha)(v') \in \langle v \rangle_\alpha + \langle v' \rangle_\alpha \end{aligned}$$

so that $\langle v \rangle_\alpha + \langle v' \rangle_\alpha = \langle v \rangle_\alpha + \langle v' \rangle_\alpha$. It remains to show that the sum $\langle v \rangle_\alpha + \langle v'' \rangle_\alpha$ is direct. Let $w \in \langle v \rangle_\alpha \cap \langle v'' \rangle_\alpha$, then there exists $a(x), b(x) \in F[x]$ such that

$$a(\alpha)(v) =: w := b(\alpha)(v'') = b(\alpha)(v' - q(\alpha)(v)) = b(\alpha)(v') - b(\alpha)q(\alpha)(v).$$

Rearranging gives $b(\alpha)(v') = (b(\alpha)q(\alpha) + a(\alpha))(v) \in \langle v \rangle_\alpha$, so by (a) we know that $p(x) \mid b(x)$. Let $g(x) \in F[x]$ such that $p(x)g(x) = b(x)$. Then

$$w = b(\alpha)(v'') = g(\alpha)p(\alpha)(v'') = g(\alpha)(0_V) = 0_V,$$

as desired. ■

Question 4

Part (a)

Since ϕ is symmetric and F is of characteristic 2, we have (by brute force expansion)

$$\begin{aligned}\phi(w_1, w_1) &= \phi(\phi(u_1, u_2)v + u_1 + u_2), \phi(u_1, u_2)v + u_1 + u_2)) \\ &= \phi(\phi(u_1, u_2)v, \phi(u_1, u_2)v)) + \phi(u_1, u_1) + \phi(u_2, u_2) \\ &= \phi(u_1, u_2)^2\phi(v, v) + \phi(u_1, u_1) + \phi(u_2, u_2) \\ &= \phi(u_1, u_2)^2\phi(v, v) \neq 0,\end{aligned}$$

$$\begin{aligned}\phi(w_2, w_2) &= \phi(v + \phi(v, v)u_1, v + \phi(v, v)u_1) \\ &= \phi(v, v) + \phi(\phi(v, v)u_1, \phi(v, v)u_1) \\ &= \phi(v, v) + \phi(v, v)^2\phi(u_1, u_1) \\ &= \phi(v, v) \neq 0,\end{aligned}$$

$$\begin{aligned}\phi(w_1, w_2) &= \phi(\phi(u_1, u_2)v + u_1 + u_2), v + \phi(v, v)u_1)) \\ &= \phi(\phi(u_1, u_2)v), v) + \phi(\phi(u_1, u_2)v), \phi(v, v)u_1) + \phi(u_1, v) + \phi(u_1, \phi(v, v)u_1) \\ &+ \phi(u_2, v) + \phi(u_2, \phi(v, v)u_1) \\ &= \phi(u_1, u_2)\phi(v, v) + \phi(u_1, u_2)\phi(v, v)\phi(v, u_1) + \phi(u_1, v) + \phi(v, v)\phi(u_1, u_1) \\ &+ \phi(u_2, v) + \phi(v, v)\phi(u_2, u_1) = 0.\end{aligned}$$

■

Part (b)

Note that ϕ cannot have rank 0 as $\phi(v, v) \neq 0$. If ϕ has rank 1 we are done, so henceforth assume $\operatorname{rk}\phi > 1$. Consider the space $\{v\}^\perp$. If there exists $v' \in \{v\}^\perp$ with $\phi(v', v') \neq 0$ we are also done as v, v' satisfy the required condition. Hence we can also assume that $\phi(v', v') = 0$ for all $v' \in \{v\}^\perp$. It now remains to find some $u, u' \in \{v\}^\perp$ such that $\phi(u, u') \neq 0$, then we can apply the process in (a) to get our desired w_1, w_2. But $\operatorname{span} v$ is non-degenerate (because $\phi(v, v) \neq 0$) so $V = \operatorname{span} v \oplus \{v\}^\perp$. Then by looking at any matrix representation of ϕ with respect to a basis $\{v, \ldots\}$ it is clear that $\phi|_{\{v\}^\perp}$ has nonzero rank. So our desired u_1, u_2 must exist and we are done. ■

Part (c)

We prove the statement via induction on $\operatorname{rk}\phi$.

Suppose first that $\operatorname{rk}\phi = 1$. Let $\mathcal{B}$ be any basis of $\{v\}^\perp$, then it is clear that $B \cup \{v\}$ is an orthogonal basis (because $\operatorname{rk}\phi|_{\operatorname{span}\mathcal{B}} = 0$ clearly.)

Now suppose for some $n \in \mathbb{Z}_{>0}$ that our statement holds for $\operatorname{rk}\phi = n$. Then If $\operatorname{rk}\phi = n + 1 \neq 1$, then from (b) there exist $w_1, w_2 \in V$ so that $\phi(w_1, w_1) \neq 0$, $\phi(w_2, w_2) \neq 0$ and $\phi(w_1, w_2) = 0$. Then $w_1 \in \{w_2\}^\perp$ and $\phi|_{\{w_2\}^\perp}(w_1, w_1) \neq 0$. Furthermore $\operatorname{rk}\phi|_{\{w_2\}^\perp} = n$, so we can invoke the induction hypothesis to get a basis $\mathcal{B}$ of $\{w_2\}^{\perp}$. Then $\mathcal{B} \cup \{w_2\}$ is easily checked to be an orthogonal basis of V, as desired. ■

Question 5

Part (a)

Let $n = \dim V$ and fix a basis $\{v_1, \dots, v_n\}$ of V. Suppose first that α is linear and $\phi_W(\alpha(v), \alpha(v)) = \phi_V(v, v)$ for all $v \in V$. Let $v, v' \in V$. Let $\lambda_1, \dots, \lambda_n, \mu_1, \dots, \mu_n \in \mathbb{R}$ such that $v = \sum_{i=1}^n \lambda_i v_i$ and $v' = \sum_{j=1}^n \mu_j v_j$. Then

$$\begin{aligned}
\phi_V(v, v') &= \phi_V\left(\sum_{i=1}^n \lambda_i v_i, \sum_{j=1}^n \mu_j v_j\right) \\
&= \sum_{i=1}^n \lambda_i \sum_{j=1}^n \mu_j \phi_V\left(v_i, v_j\right) \\
&= \sum_{i=1}^n \lambda_i \sum_{j=1}^n \mu_j \phi_W\left(\alpha(v_i), \alpha(v_j)\right) \\
&= \sum_{i=1}^n \lambda_i \sum_{j=1}^n \mu_j \phi_W\left(\alpha(v_i), \alpha(v_j)\right) \\
&= \phi_W\left(\sum_{i=1}^n \lambda_i \alpha(v_i), \sum_{j=1}^n \mu_i \alpha(v_j)\right) \\
&= \phi_W\left(\alpha\left(\sum_{i=1}^n \lambda_i v_i\right), \alpha\left(\sum_{j=1}^n \mu_j v_j\right)\right) \\
&= \phi_W(\alpha(v), \alpha(v')).
\end{aligned}$$

Conversely if $\phi_W(\alpha(v), \alpha(v')) = \phi_V(v, v')$ for all $v, v' \in V$ then by setting $v = v'$ we see that $\phi_W(\alpha(v), \alpha(v)) = \phi_V(v, v)$ for all $v \in V$. Now let $v, v' \in V$ be arbitrary and $\lambda \in \mathbb{R}$. We claim that $\alpha(v + \lambda v') - \alpha(v) - \lambda\alpha(v') = 0$. Indeed, by fully expanding, we see that

$$\begin{aligned}
&\phi_W(\alpha(v + \lambda v') - \alpha(v) - \lambda\alpha(v'), \alpha(v + \lambda v') - \alpha(v) - \lambda\alpha(v')) \\
&= \phi_W(\alpha(v + \lambda v'), \alpha(v + \lambda v')) + \ldots + \lambda^2 \phi_W(\alpha(v'), \alpha(v')) \\
&= \phi_V(v + \lambda v', v + \lambda v') + \ldots + \lambda^2 \phi_V(v', v') \\
&= \phi_V(v + \lambda v' - v - \lambda v', v + \lambda v' - v - \lambda v') \\
&= \phi(0_V, 0_V) = 0.
\end{aligned}$$

By non-degeneracy of ϕ_W our conclusion follows. ■

Part (b)

From (a) we see that α is linear and $\phi_W(\alpha(v), \alpha(v)) = \phi_V(v, v)$ for all $v \in V$, so it suffices to show that $\ker \alpha = \{0\}$. Let $v \in \ker \alpha$, then $\alpha(v) = 0$. We have $\phi_V(v, v) = \phi_W(\alpha(v), \alpha(v)) = \phi_W(0, 0) = 0$, so by non-degeneracy of ϕ_V we have $v = 0$ as desired. ■