MA2101S - Linear Algebra II(S) Suggested Solutions

(Semester 2 : AY2014/15)

Written by : Pan Jing Bin
Audited by : Dick Jessen William

Question 1

(a) To prove 'if' :

Let $u_1 + U', u_2 + U' \in U/U'$ such that $u_1 + U' = u_2 + U'$.

Then $u_1 - u_2 \in U'$ so $\alpha(u_1 - u_2) \in V'$. We have

$$\beta(u_1 + U') = \alpha(u_1) + V' = \alpha(u_1) - \alpha(u_1 - u_2) + V' = \alpha(u_2) + V' = \beta(u_2 + U').$$

Thus β is well defined.

To prove 'only if' :

Let $w \in U'$. Then $w + U' = 0_V + U'$. Since β is well-defined:

$$\beta(w + U') = \beta(0_V + U') \to \alpha(w) + V' = 0_V + V'.$$

Thus $\alpha(w) \in V'$ so $\alpha(U') \subseteq V'$.

(b)(i) Let $u + U', v + U' \in U/U'$ and $x, y \in \mathbb{F}$.

$$\begin{aligned}\beta(xu + yv + U') = \alpha(xu + yv) + V' &= x\alpha(u) + y\alpha(v) + V' \text{ (Since } \alpha \text{ is a linear transformation)}\\ &= x\beta(u + U') + y\beta(v + U').\end{aligned}$$

Thus β is linear.

(ii) To prove 'if' :

Let $u + U' \in \ker(\beta)$. Then

$$\beta(u + U') = 0_V + V' \to \alpha(u) \in V'.$$

Thus $u \in \alpha^{-1}(V')$. Since $\alpha^{-1}(V') \subseteq U', u \in U'$ so $u + U' = 0_V + U'$. This means that $\ker(\beta) = \{0_V\}$ so β is injective.

To prove 'only if' :

Let $v \in \alpha^{-1}(V')$. Then $\alpha(v) \in V'$.

$\beta(v + U') = 0_V + V'$ so $v + U' \in \ker(\beta)$. By injectivity of β, $v + U' = 0_V + U'$. Thus $v \in U'$ so $\alpha^{-1}(V') \subseteq U'$.

(iii) To prove 'if' :

Let $w + V' \in V/V'$. Since $\alpha(U) + V' = V$, we can write $w = u + v$ for $u \in \alpha(U), v \in V'$.

$$u \in \alpha(U) \to \exists u' \in U \text{ such that } \alpha(u') = u.$$

$u' + U' \in U/U'$ and $\beta(u' + U') = \alpha(u') + V' = u + V' = w + V'$.

Thus β is surjective.

To prove 'only if' :

$\alpha(U) \subseteq V \wedge V' \subseteq V \to \alpha(U) + V' \subseteq V$. Thus it suffice to prove that $V \subseteq \alpha(U) + V'$.

Let $k \in V$. By surjectivity of β, $\exists k' + U' \in U/U'$ such that $\beta(k' + U') = k + V'$.

$$\alpha(k') + V' = k + V' \to k - \alpha(k') \in V'.$$

Thus we can write: $k = k - \alpha(k') + \alpha(k')$ for $k - \alpha(k') \in V'$ and $\alpha(k') \in \alpha(U)$.

But this means that $k \in \alpha(U) + V'$. Hence $V \subseteq \alpha(U) + V'$.

Question 2

(a) We will only prove that $U_1 = \text{span}(\{u_1, \alpha(u_1), \alpha^2(u_1), ...\})$. The proof for U_2 is similiar.

Obviously $\text{span}(\{u_1, \alpha(u_1), \alpha^2(u_1), ...\}) \subseteq U_1$ since U_1 is α-invariant. Thus it suffice to prove $U_1 \subseteq \text{span}(\{u_1, \alpha(u_1), \alpha^2(u_1), ...\})$. Let $w \in U_1$.

$$\begin{aligned} w &= c_0 v + c_1\alpha(v) + c_2\alpha^2(v) + ... + c_n\alpha^n(v) \quad \text{for some } c_1, c_2, ...c_n \in \mathbb{F} \\ &= c_0(u_1 + u_2) + c_1\alpha(u_1 + u_2) + c_2\alpha^2(u_1 + u_2) + ... + c_n\alpha^n(u_1 + u_2) \\ &= [c_0u_1 + c_1\alpha(u_1) + ... + c_n\alpha^n(u_1)] + [c_0u_2 + c_1\alpha(u_2) + ... + c_n\alpha^n(u_2)]. \end{aligned}$$

Since U_1 and U_2 are α-invariant subspaces:

$$[c_0u_1 + c_1\alpha(u_1) + ... + c_n\alpha^n(u_1)] \in U_1 \wedge [c_0u_2 + c_1\alpha(u_2) + ... + c_n\alpha^n(u_2)] \in U_2.$$

But we can also write: $w = w + 0_V$ for $w \in U_1,\ 0_V \in U_2$. Since $U_1 + U_2$ is a direct sum, we must have:

$$c_0u_1 + c_1\alpha(u_1) + ... + c_n\alpha^n(u_1) = w \ \wedge\ c_0u_2 + c_1\alpha(u_2) + ... + c_n\alpha^n(u_2) = 0_V.$$

Thus $w \in \text{span}(\{u_1, \alpha(u_1), \alpha^2(u_1), ...\})$ so $U_1 \subseteq \text{span}(\{u_1, \alpha(u_1), \alpha^2(u_1), ...\})$.

(b)(i) Similarly, we only prove the case for $i = 1$. Since $V = \text{span}(\{v, \alpha(v), \alpha^2(v), ...\})$, $\exists r(x) \in F[x]$ such that $r(\alpha)(v) = u_1$. If $\deg(r(x)) < \deg(m(x))$, then we are done. If $\deg(r(x)) \geq \deg(m(x))$, then we perform the Euclidean Algorithm:

$r(x) - b(x)m(x) = q_1(x)$ for some $b(x), q_1(x) \in F[x] \wedge \deg(q_1(x)) < \deg(m(x))$

$$\begin{aligned} q_1(\alpha)(v) &= r(\alpha)(v) - b(\alpha)m(\alpha)(v) \\ &= r(\alpha)(v) - 0_V \text{ (By definition of minimial polynomial)} \\ &= u_1. \text{ (As desired)} \end{aligned}$$

(ii) Claim: $(q_1 + q_2)(\alpha) = I_V$.

Proof: Let $\alpha^k(v) \in \{v, \alpha(v), \alpha^2(v), ...\}$

$$\begin{aligned} q_1(\alpha)(v) + q_2(\alpha)(v) &= u_1 + u_2 = v \\ q_1(\alpha)(\alpha^k(v)) + q_2(\alpha)(\alpha^k(v)) &= \alpha^k[q_1(\alpha)(v) + q_2(\alpha)(v)] \\ &= \alpha^k(v). \end{aligned}$$

Since $V = \text{span}(\{v, \alpha(v), \alpha^2(v), ...\})$, and $(q_1 + q_2)(\alpha)(\alpha^k(v)) = \alpha^k(v)\ \forall \alpha^k(v) \in \{v, \alpha(v), \alpha^2(v)...\}$, we conclude that $q_1(\alpha) + q_2(\alpha) = I_V$.

$q_1(x) + q_2(x) - 1$ is a polynomial of degree less than $m(x)$.

But $q_1(\alpha) + q_2(\alpha) - I_V = 0_V$. Thus $q_1(x) + q_2(x) - 1 = 0$. (Otherwise it contradicts the definition of minimal polynomial) Hence we get: $q_1(x) + q_2(x) = 1$.

Note that:

$$q_1(\alpha)(u_1 + u_2) = u_1 + 0_V \to q_1(\alpha)(u_1) + q_1(\alpha)(u_2) = u_1 + 0_V.$$

Recall that $q_1(\alpha)(u_1) \in U_1 \wedge q_2(\alpha)(u_2) \in U_2$ since U_1 and U_2 are α-invariant. By the unique expression property of direct sums, $q_1(\alpha)(u_1) = u_1 \wedge q_1(\alpha)(u_2) = 0_V$.

Then $q_1(\alpha)(q_2(\alpha)(v)) = q_1(\alpha)(u_2) = 0_V$.

(iii) From part(b), we know that $q_1(\alpha)(u_2) = 0_V$.

Since $U_2 = \text{span}(\{u_2, \alpha(u_2), \alpha^2(u_2), ...\})$, $q_1(\alpha)(k) = 0_V \ \forall k \in U_2$

Thus by definition of minimial polynomial, $p_2(x) \mid q_1(x)$. Similarly, $p_1(x) \mid q_2(x)$.

But $\gcd(q_1(x), q_2(x)) = 1$ since $q_1(x) + q_2(x) = 1$. Thus $p_1(x)$ and $p_2(x)$ must be coprime as well.

(c) Let $p_1(x), p_2(x)$ denote the minimal polynomial of α restricted on U_1 and U_2 respectively. Since $f(\alpha)^k(v) = 0$ and $V = \text{span}(\{v, \alpha(v)\alpha^2(v), ...\})$, $f(\alpha)^k(t) = 0 \ \forall t \in V$. By definition of minimial polynomial, $m_\alpha(x) \mid f(x)^k$.

Thus $p_1(x) = f(x)^{k_1} \ \wedge \ p_2(x) = f(x)^{k_2}$ for some $0 \le k_1 \le k, 0 \le k_2 \le k$. If $k_1 > 0 \wedge k_2 > 0$, then $\gcd(p_1(x), p_2(x)) \ne 1$, which contradicts (b)(iii). Hence $k_1 = 0 \vee k_2 = 0$ so $U_1 = \{0\}$ or $U_2 = \{0\}$.

Question 3

(a) For any arbitrary $A \in SL_2(\mathbb{F}_p)$, the first column of A can be any column except the zero column. (Which will result in $\det(A) = 0$) Thus there are $p^2 - 1$ choices for the first column of A.

For the second column of A, consider 2 cases:

Case 1: $a = 0 \ \vee \ c = 0$.

Without loss of generality, assume $a = 0 \wedge c \ne 0$.

Since $ad - bc = 1$, d can be any element while there is only 1 choice for b, which is $-c^{-1}$. Thus there are p choices for the second column of A.

Case 2: $a \ne 0 \wedge c \ne 0$.

Then d can be any element and for each d there is only 1 choice for b, which is $adc^{-1} - c^{-1}$. Similiar to case 1, there are p choices for the second column of A.

To conclude, there are $(p^2 - 1)p = p^3 - p$ elements in $SL_2(\mathbb{F}_p)$.

(b) Let $A \in SL_2(\mathbb{F}_p)$ and consider 2 cases.

Case 1: $c_A(x) = m_A(x)$.

Since $\det(A) = 1, c_A(x) = x^2 + ax + 1$ for some $a \in \mathbb{F}_p$. Then A is similar to R (Rational canonical form):

$$R = \begin{pmatrix} 0 & -1 \\ 1 & -a \end{pmatrix}, \text{ where } C_A(x) = x^2 + ax + 1.$$

There are p choices for a so there are p pairwise non-similar matrices of this form. (Note that changing the value of a will result in a non-similar matrix since the characteristic polynomial of A have changed)

Case 2: $c_A(x) \ne m_A(x)$.

Then $c_A(x) = (x - \lambda)^2$ and $m_A(x) = x - \lambda$ for some $\lambda \in \mathbb{F}_p$.
Since $\det(A) = 1, \lambda^2 = 1$. Note that since $m_A(x)$ has no repeated factors, A is diagonalisable.

If $\mathbb{F}_p$ has characteristic greater than 2, then $\lambda^2 = 1$ have 2 solutions: $\lambda = 1 \vee \lambda = -1$.

Thus there are 2 matrices that A can be similar to: $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$.

If $\mathbb{F}_p$ has characteristic 2, then $\lambda^2 = 1$ have only 1 solution: $\lambda = 1$. (Since $-1 = 1$)

Thus there is only 1 matrix that A can be similar to: $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

In conclusion, there are $p+2$ pairwise non-similar matrices when $\text{char}(\mathbb{F}_p) \neq 2$ and $p+1$ pairwise non-similar matrices when $\text{char}(\mathbb{F}_p) = 2$.

Question 4

(a) Let $(p, q), (r, s)$ denote the index of positively of ϕ and ψ respectively.

Claim 1: $p \leq r$

Proof: Let M_ϕ, M_ψ denote the maximal subspace of V such that $\phi_{|_{M_\phi \times M_\phi}}$ and $\psi_{|_{M_\psi \times M_\psi}}$ are positive definite. Then $\dim(M_\phi) = p \wedge \dim(M_\psi) = r$. Since $\phi(v, v) \leq \psi(v, v)$, $\phi(v, v) > 0 \to \psi(v, v) > 0$.

Thus $M_\phi \subseteq M_\psi$ so we have $\dim(M_\phi) \leq \dim(M_\psi)$ and $p \leq r$.

Claim 2: $q \geq s$

Proof: Let N_ϕ, N_ψ denote the maximal subspace of V such that $\phi_{|_{N_\phi \times N_\phi}}$ and $\psi_{|_{N_\psi \times N_\psi}}$ are negative definite. Then $\dim(N_\phi) = q \wedge \dim(N_\psi) = s$. Since $\phi(v, v) \leq \psi(v, v)$, $\psi(v, v) < 0 \to \phi(v, v) < 0$.

Thus $N_\psi \subseteq N_\phi$ so we have $\dim(N_\phi) \geq \dim(N_\psi)$ and $q \geq s$.

Combining the two claims, we have: $p - q \leq r - s$ so $s_\phi \leq s_\psi$.

(b) Existence: Let $B = \{w_1, w_2, ...w_n\}$ be a basis for W and let C and D be the representing matrix of θ and χ under basis B respectively. (Note that a representing matrix exist since W is finite-dimensional). Since χ is non-degenerate, D is invertible so D^{-1} exists. Choose α to be the linear operator such that:

$$[\alpha]_B = D^{-1}C.$$

Then we have:

$$\theta(x, y) = ([x]_B)^T C[y]_B = ([x]_B)^T DD^{-1}C[y]_B = ([x]_B)^T D[\alpha(y)]_B = \chi(x, \alpha(y)).$$

Uniqueness: Let α_1, α_2 both be linear operators on W such that:

$$\chi(x, \alpha_1(y)) = \chi(x, \alpha_2(y)) = \theta(x, y) \ \forall x, y \in W.$$

Let A_1, A_2 be the standard matrix of α_1 and α_2 under basis B respectively.

$$\forall x, y \in W, \ ([x]_B)^T DA_1[y]_B = ([x]_B)^T DA_2[y]_B$$

This equality holds for all $x, y \in W$, so $DA_1 = DA_2$. Since D is invertible, $A_1 = A_2$. This means that α_1 and α_2 have the same standard matrix under basis B. Thus we conclude that $\alpha_1 = \alpha_2$.