

18.700 - Fall 2006 - Solutions to Problem Set 3

Problem 0.

- (a) Yes, there exists a unique homomorphism A with the required properties, because $\left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \end{pmatrix} \right\}$ is a basis of \mathbb{R}^2 .

$$A \begin{pmatrix} 1 \\ 0 \end{pmatrix} = A \left[\begin{pmatrix} 2 \\ 1 \end{pmatrix} - \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right] = \begin{pmatrix} 1 \\ 1 \end{pmatrix} - \begin{pmatrix} 2 \\ 0 \end{pmatrix} = \begin{pmatrix} -1 \\ 1 \end{pmatrix}$$

$$A \begin{pmatrix} 0 \\ 1 \end{pmatrix} = A \left[\begin{pmatrix} 1 \\ 1 \end{pmatrix} - \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right] = \begin{pmatrix} 2 \\ 0 \end{pmatrix} - \begin{pmatrix} -1 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 \\ -1 \end{pmatrix}$$

so that $A = \begin{pmatrix} -1 & 3 \\ 1 & -1 \\ 1 & -1 \end{pmatrix}$.

- (b) Let \mathcal{B} be a set of generators of V and call $L(\mathcal{B}) = \{L(v) \in W \mid v \in \mathcal{B}\}$.

Notice that $\text{span } L(\mathcal{B}) = L(\text{span } \mathcal{B}) \subseteq \text{Im}(L)$.

Assume that \mathcal{B} is a set of generators, so that $\text{span } L(\mathcal{B}) = \text{Im}(L)$. Hence, $L(\mathcal{B})$ is a set of generators of W if and only if L is surjective.

Now, assume instead that \mathcal{B} is a set of linearly independent vectors. To say that $L(\mathcal{B})$ is not a set of linearly independent vectors is the same as to say that: there exists $a_1, \dots, a_n \in \mathbb{F}$ with some $a_i \neq 0$ and $v_1, \dots, v_n \in \mathcal{B}$ such that $a_1 L(v_1) + \dots + a_n L(v_n) = 0$ in W . This is the same as saying that $a_1 v_1 + \dots + a_n v_n \in \ker L$. Thus, if L is injective, then $a_1 + \dots + a_n = 0$. Vice versa, if L is not injective, then consider $\mathcal{B} = \{v\}$ with $0 \neq v \in \ker(L)$. Then \mathcal{B} is a set of linearly independent vectors in V (because $v \neq 0$), but $L(\mathcal{B}) = \{0\} \subset W$ is not.

The statement about bases can be deduced from the previous two.

Problem 1.

- (a) Call $v_i = t^{i-1}$ for $i = 1, \dots, d+1$, so that $\mathcal{B} = \{v_1, \dots, v_{d+1}\}$.

Then $D(v_k) = D(t^{k-1}) = (k-1)t^{k-2} = (k-1)v_{k-1}$ for $k = 1, \dots, d+1$. Hence,

$$M_{\mathcal{B}}^{\mathcal{B}}(D) = \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 2 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & 3 & \cdots & 0 & 0 \\ 0 & 0 & 0 & 0 & \ddots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & d \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}$$

- (b) If $p(t) \in \mathbb{R}[t]_{\leq d}$, then $D(p) = p'$ is the zero polynomial if and only if $p(t)$ is a constant polynomial, so $\ker(D) = \{\text{constant polynomials}\}$ (sometimes also denoted by $\mathbb{R} \subset \mathbb{R}[t]_{\leq d}$).

The image of D is the span of $\{(k+1)t^k \mid k = 0, \dots, d-1\}$, so that $\text{Im}(D) = \mathbb{R}[t]_{\leq d-1}$.

The homomorphism D is neither injective nor surjective, so for sure it is not invertible.

- (c) Notice that $\bar{n} = \bar{0}$ in \mathbb{Z}/p if and only if n is a multiple of p (by definition).
Hence, $\ker(\tilde{D}) = \text{span}_{\mathbb{Z}/p}\{t^{kp} \mid k \in \mathbb{N}, kp \leq d\}$.
Similarly, the image of \tilde{D} does not contain the monomials of the type t^{kp-1} .
Hence, $\text{Im}(\tilde{D}) = \text{span}_{\mathbb{Z}/p}\{t^n \mid 0 \leq n \leq d-1 \text{ but } n \neq kp-1\}$.

Problem 2.

Call e_1, \dots, e_n the standard basis of \mathbb{F}^n and, for every $k = 1, \dots, n$, define $V_k = \text{span}_{\mathbb{F}}\{e_1, \dots, e_k\} \subseteq \mathbb{F}^n$. Moreover, define $V_0 = \{0\}$.

If $X \subset \mathbb{F}^n$, call $A(X) = \{A(x) \in \mathbb{F}^n \mid x \in X\}$ and $B(X) = \{B(x) \in \mathbb{F}^n \mid x \in X\}$.

- (a) *Proof by hand.*

By definition, $(AB)_{ij} = \sum_{k=1}^n A_{ik}B_{kj}$.

A upper triangular $\implies A_{ik} = 0$ if $k < i$ and B upper triangular $\implies B_{kj} = 0$ if $j < k$.
Hence, $(AB)_{ij}$ can be nonzero only if there exists an integer k such that $j \geq k \geq i$, that is only $j \geq i$, that is AB is upper triangular.

Conceptual proof.

The matrix M corresponding to a homomorphism $M : \mathbb{F}^n \longrightarrow \mathbb{F}^n$ is upper triangular if and only if $M(V_k) \subseteq V_k$ for $k = 1, \dots, n$.

Now, $AB(V_k) = A(B(V_k)) \subseteq A(V_k) \subseteq V_k$, where the first \subseteq depends on the fact that B is upper triangular and the second \subseteq depends on the fact the A is upper triangular.

- (b) *Proof by hand.*

By definition, $(AB)_{ij} = \sum_{k=1}^n A_{ik}B_{kj}$.

A strictly upper triangular $\implies A_{ik} = 0$ if $k \leq i$ and B upper triangular $\implies B_{kj} = 0$ if $j < k$.
Hence, $(AB)_{ij}$ can be nonzero only if there exists an integer k such that $j \geq k > i$, that is only $j > i$, that is AB is strictly upper triangular.

The proof for BA is very similar.

Conceptual proof.

The matrix M corresponding to a homomorphism $M : \mathbb{F}^n \longrightarrow \mathbb{F}^n$ is strictly upper triangular if and only if $M(V_k) \subseteq V_{k-1}$ for $k = 1, \dots, n$.

If A is strictly upper triangular and B is upper triangular, then $AB(V_k) = A(B(V_k)) \subseteq A(V_k) \subseteq V_{k-1}$. Hence, AB is strictly upper triangular.

Similarly, for BA .

- (c) *Conceptual proof.*

As A is strictly upper triangular, $A(V_k) \subseteq V_{k-1}$ for $k = 1, \dots, n$.

$A^n(V) = A^n(V_n) = A^{n-1}(A(V_n)) \subseteq A^{n-1}(V_{n-1}) = A^{n-2}(A(V_{n-1})) \subseteq A^{n-2}(V_{n-2}) \subseteq \dots \subseteq A(V_1) \subseteq V_0 = \{0\}$, so that $A^n = 0$.

If A is upper triangular but not strictly, then there exists an integer $1 \leq i \leq n$ such that $A_{ii} = \lambda_i \neq 0$, that is: $A(e_i) = \lambda_i e_i + v_{i-1}$, for $\lambda_i \neq 0$ and some $v_{i-1} \in V_{i-1}$.

We want to show that $A_{ii}^k = \lambda_i^k$ and so $A^k \neq 0$ for every $k \geq 1$.

Let's proceed by induction on $k \geq 1$.

For $k = 1$, $A_{ii}^1 = A_{ii} = \lambda_i \neq 0$.

Assume the thesis true for A^{k-1} . Then $A^{k-1}(e_i) = \lambda_i^{k-1} e_i + w_{i-1}$, for some $w_{i-1} \in V_{i-1}$.

Hence, $A^k(e_i) = A(A^{k-1}(e_i)) = A(\lambda_i^{k-1} e_i + w_{i-1}) = \lambda_i^{k-1} A(e_i) + A(w_{i-1}) = \lambda_i^{k-1} \lambda_i e_i + A(w_{i-1}) = \lambda_i^k e_i + A(w_{i-1})$. Because A is upper triangular and $w_{i-1} \in V_{i-1}$, the vector $A(w_{i-1}) \in V_{i-1}$, which implies $A_{ii}^k = \lambda_i^k$.

Problem 3.

$AX = 0$ if and only if $\text{Im}(X) \subseteq \ker(A)$, essentially by definition.
Hence, $S_A = \text{hom}_{\mathbb{F}}(\mathbb{F}^k, \ker(A))$, which is a vector space.
If $\dim_{\mathbb{F}} \ker(A) = r$ and $\mathcal{B} = \{v_1, \dots, v_r\}$ is basis of $\ker(A)$, then

$$\begin{array}{ccc} S_A = \text{hom}_{\mathbb{F}}(\mathbb{F}^k, \ker(A)) & \longrightarrow & \text{hom}_{\mathbb{F}}(\mathbb{F}^k, \mathbb{F}^r) \\ L & \xrightarrow{\quad\quad\quad} & M_{\mathcal{B}} \circ L \end{array}$$

is an isomorphism (because $M_{\mathcal{B}} : \ker(A) \rightarrow \mathbb{F}^r$ is an isomorphism).
Hence, $\dim_{\mathbb{F}} S_A = \dim_{\mathbb{F}} \text{hom}_{\mathbb{F}}(\mathbb{F}^k, \ker(A)) = \dim_{\mathbb{F}} \text{hom}_{\mathbb{F}}(\mathbb{F}^k, \mathbb{F}^r) = kr = k \cdot \dim_{\mathbb{F}} \ker(A)$.

Problem 4.

(a) By direct computation,

$$\begin{aligned} \text{ev}_q(v_1) &= \text{ev}_q(1) = 1 = w_1 \\ \text{ev}_q(v_2) &= \text{ev}_q(t+1) = q(s) + 1 = (a_0 + 1) + a_1s + a_2s^2 = (a_0 + 1)w_1 + a_1w_2 + a_2w_3 \\ \text{ev}_q(v_3) &= \text{ev}_q((t+1)^2) = (q(s) + 1)^2 = (a_0 + a_1s + a_2s^2)^2 = \\ &= a_0^2 + 2a_0a_1s + (2a_0a_2 + a_1^2)s^2 + 2a_1a_2s^3 + a_2^2s^4 = \\ &= (a_0^2)w_1 + (2a_0a_1)w_2 + (2a_0a_2 + a_1^2)w_3 + (2a_1a_2)w_4 + (a_2^2)w_5 \end{aligned}$$

$$\text{Hence, } M_{\mathcal{C}}^{\mathcal{B}}(\text{ev}_q) = \begin{pmatrix} 1 & a_0 + 1 & a_0^2 \\ 0 & a_1 & 2a_0a_1 \\ 0 & a_2 & 2a_0a_2 + a_1^2 \\ 0 & 0 & 2a_1a_2 \\ 0 & 0 & a_2^2 \end{pmatrix}$$

(b) $Q_p(t+1) = (t+1)^p = t^p + pt^{p-1} + \dots + pt + 1$, whereas $Q_p(t) + Q_p(1) = t^p + 1$.

Comparing the two and looking for instance at the degree $p-1$, we have that:

if Q_p is a homomorphism, then $Q_p(t+1) = Q_p(t) + Q_p(1)$ and so in particular the coefficient of t^{p-1} in $Q_p(t+1)$ must be zero in \mathbb{F} . As that coefficient is p , this implies that $\text{char}(\mathbb{F}) = p$.
For the second part, $Q_p(t^d) = t^{pd}$, so that a basis for the image of Q_p is given by $\{t^{pd} \mid d \in \mathbb{N}\}$, whereas $\ker(Q_p) = \{0\}$ (so the basis of $\ker(Q_p)$ is the empty set).