Problem Set #10 Part B
Official Solutions
Total Points: 51

Inna Zakharevich

(5) 1. We know that if

$$e_i = \sum_{j=1}^{n} a_{ij} f_j \qquad f_i = \sum_{j=1}^{n} b_i j e_j$$

then $A = (a_{ij})$ and $B = (b_{ij})$. Plugging in the definition for f_j into the first sum we see that

$$e_i = \sum_{j=1}^{n} a_{ij} \sum_{k=1}^{n} b_{jk} e_k \Longrightarrow e_i = \sum_{j=1}^{n} \left(\sum_{k=1}^{n} a_{ik} b_{kj} \right) e_j.$$

However, we also know that the e_i are linearly independent; thus we see that

$$\sum_{k=1}^{n} a_{ij} b_{jk} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$$

However, these are also the entries of the matrix AB; thus we see that $AB = \mathrm{Id}$. By plugging in the definition for e_j into the sum for f_i we get that $BA = \mathrm{Id}$.

(9) 2.

(2) (1) Consider a polynomial in V. This will be written as a sum of monomials with x taken to powers from 0 to $n-1$; thus every polynomial is a linear combination of the vectors $\{1, x, \ldots, x^{n-1}\}$, so this is a basis.

The map $f : P(x) \mapsto P(x+1)$ maps any monomial to a polynomial of the same degree. Thus the map will map a polynomial of degree at most $n-1$ to a polynomial of degree at most $n-1$, so it is a map from V to itself. Notice that $f(\lambda P(x)) = \lambda P(x+1) = \lambda f(P(x))$, and $f(P(x)+Q(x)) = P(x+1)+Q(x+1) = f(P(x)) + f(Q(x))$, so we see that the map is linear.

(2) (2) Notice that $f(x^m) = \sum_{i=1}^{m} \binom{m}{i} x^i$, so it follows that the matrix for M in terms of the monomials x^i is $\left(\binom{i-1}{j-1}\right)$, where $\binom{a}{b} = 0$ if $b > a$.

(5) (3) From problem 1 we see that all we need to do is calculate the matrix for the basis $\{x^i\}$ in terms of the basis $\{(x+1)^i\}$. We claim that

$$x^m = \sum_{i=0}^{m} (-1)^{m-i} \binom{m}{i} (x+1)^i.$$

We will do this by calculating algorithmically, and using induction. First note that for any $a > m$, the coefficient of $(x+1)^a$ will be 0. Since $(x+1)^m$ is the only polynomial of degree greater than or equal to m left, we have that the coefficient of $(x+1)^m$ is 1. Now, starting with $(x+1)^m$ we will systematically eliminate the highest-degree monomial (other than x^m); the coefficient of x^a will be the coefficient of this monomial at the $n-a$-th step. We start with $(x+1)^m$; the coefficient of x^{m-1} is m. Thus the coefficient of $(x+1)^{m-1}$ will be $-\binom{m}{m-1}$, as stated. Now suppose that for all of $m-1, \ldots, a$ the coefficients were $(-1)^{m-i}\binom{m}{i}$. Then we claim that the coefficient of x^{a-1} in

$$\sum_{i=0}^{m-a} (-1)^i \binom{m}{m-i} (x+1)^{m-i}$$

is $(-1)^{m-a}\binom{m}{a-1}$. Then we will know that the coefficient of $(x+1)^{a-1}$ will be the negative of that, and we will have shown the result. Indeed, the coefficient is

$$\begin{aligned} \sum_{i=0}^{m-a} (-1)^i \binom{m}{m-i} \binom{m-i}{a-1} &= \binom{m}{a-1} \sum_{i=0}^{m-a} (-1)^i \binom{m-a+1}{i} \\ &= (-1)^{m-a+1} \binom{m}{a-1} \end{aligned}$$

as desired. Thus we have shown the formula for x^m in terms of $(x+1)^i$, so we know that

$$M^{-1} = \left((-1)^{i-j} \binom{i-1}{j-1} \right).$$

(10) 3.

(5) (1) **Solution 1**: We will prove this claim by induction. Clearly if $n = 1$ the set $\{\exp(\alpha_i x)\}$ is linearly independent. Suppose that with $n-1$ distinct α_i the set is linearly independent, but with n it isn't for some α_i. Then we have that for some a_i, $\sum_{i=1}^n a_i \exp(\alpha_i x) = 0$, for all x. Differentiating, we get that $\sum_{i=1}^n a_i \alpha_i \exp(\alpha_i x) = 0$ for all x. Multiplying the first of these by α_1 and subtracting, we get that $\sum_{i=2}^n (\alpha_1 - \alpha_i) a_i \exp(\alpha_i x) = 0$. By the induction hypothesis we know that $(\alpha_1 - \alpha_i) a_i = 0$, and since all of the α_i are distinct this means that $a_i = 0$ for $i \geq 2$. Thus $a_1 = 0$ also, and we have shown that any n are linearly independent, and the claim follows.

Solution 2: Let V be the space of all C^∞ functions from $\mathbf{R}$ to $\mathbf{R}$. We know that differentiation is a linear function on this space. Also, $(\exp(\alpha_i x))' = \alpha_i \exp(\alpha_i x)$, so $\exp(\alpha_i x)$ is an eigenvector of this operator. If the α_i are distinct then the set $\{\exp(\alpha_1 x), \ldots, \exp(\alpha_n x O)\}$ is a set of eigenvectors with different eigenvalues, which we already know is linearly independent.

(5) (2) Without loss of generality we will assume that α_n is the largest α_i. Then for some open interval I containing α_n no other α_i is contained in I. Then we know that for $i < n$ $|x - \alpha_i|$ is differentiable inside I.

Suppose that for some $a_1, \ldots, a_n$ we have $\sum_{i=1}^n a_i |x - \alpha_i| = 0$. Then this is also true inside I. Then the function $\left(\sum_{i=1}^{n-1} a_i |x - \alpha_i|\right)'$ is differentiable and constant in this interval. It should be equal to $-a_n|x - a_n|'$ on the set $I - \{a_n\}$. However, unless $a_n = 0$ $-a_n|x - a_n|'$ is nonconstant on this set. Thus we see that $a_n = 0$. By induction we conclude that all of the coefficients must be 0, and we see that the set is linearly independent.

(10) 4.

(5) (1) Suppose that such a v exists. Thus we have $w = vu$. Suppose that $x \notin \ker w$. Then $vux \neq 0$, so $ux \neq 0$ so $x \notin \ker u$. Thus $\ker u \subseteq \ker v$.

Now suppose that $\ker u \subseteq \ker w$. Let $\{u_1, \ldots, u_n\}$ be a basis for U such that $\{u_1, \ldots, u_m\}$ $(n \geq m)$ is a basis for $\ker u$, and $\{u_1, \ldots, u_{m'}\}$ is a basis for $\ker w$ $(m' \geq m)$ (this is possible because $\ker u \subseteq \ker w$). Consider $uu_1, \ldots, uu_n$. Let $\{v_1, \ldots, v_k\}$ be linearly independent and such that $\{uu_{m+1}, \ldots, uu_n, v_1, \ldots, v_k\}$ contains a basis, and such that $\{uu_i, v_1, \ldots, v_k\}$ is linearly independent for all $i > m$. Then let v be the transformation that sends uu_i to wu_i for $n \leq i > m$ and v_i to 0 for $1 \leq i \leq k$. This transformation will be well-defined unless some $\{uu_{i_1}, \ldots, uu_{i_l}\}$ are not linearly independent for $i_j > m'$. We will show that the set $\{uu_{m'+1}, \ldots, uu_n\}$ is linearly inependent. Suppose that it is not. Then we have a_i such that $\sum_{i=m'+1}^n a_i uu_i = 0$. However, this means that $u\left(\sum_{i=m'+1}^n a_i u_i\right) = 0$, which does not occur unless all of the $a_i = 0$ because we are only looking at vectors outside of the kernel of u. Thus we have a transformation v such that $uv = w$ on a basis for U, so we know that $uv = w$.

(5) (2) Suppose that such a u exists. Then if $x \in \operatorname{im} w$ we know that there is some $y \in U$ such that $wy = x$, so $v(uy) = x$, so $x \in \operatorname{im} v$. Thus $\operatorname{im} w \subseteq \operatorname{im} v$.

Now suppose that $\operatorname{im} w \subseteq \operatorname{im} v$. Let $\{v_1, \ldots, v_n\}$ be a basis for V such that $\{vv_1, \ldots, vv_m\}$ $(m \leq n)$ is a basis for $\operatorname{im} v$, and $\{vv_1, \ldots, vv_l\}$ $(l \leq m)$ is a basis for $\operatorname{im} w$ (this is possible because $\operatorname{im} w \subseteq \operatorname{im} v$). Then let $\{u_1, \ldots, u_{m'}\}$ be a basis for U. Notice that $m' \geq l$ because l is the dimension of $\operatorname{im} w$. Then if we define $uu_i = v_i$ for $1 \leq i \leq l$ and 0 otherwise, we will have $uv = w$.

(17) 5.

(5) (1) Let T be the linear transformation that M represents with a standard basis in K^n. Then T is invertible if and only if M is invertible. Suppose that T is invertible. Then we know that it is a surjection onto a basis of K^n, so rank $T = n$, so rank $M = n$. Now suppose that $\operatorname{rank} M = n$. Then $\operatorname{rank} T = n$. Suppose that $Tx = Ty$. Then $T(x - y) = 0$. Consider a basis for K^n with $x - y$ as the first vector. Then the dimension of the image would be at most $n - 1$ (since the first vector of the basis is mapped to 0) so the rank is at most $n - 1$. Contradiction. Thus such a basis does not exist, so $x = y$. Thus T is injective, and therefore invertible, so M is also invertible.

(5) (2) Suppose that for every $1 \leq k \leq n$ we have that the dimension of the subspace generated by $C_1, \ldots, C_k$ is k. Then in particular this is true for $k = n$ so the rank of M is n. Thus M is invertible, by the first part.

Now suppose that M is invertible. This means that $\{e_i T\}$ is linearly independent. In particular, $\{e_1 T, \ldots, e_k T\}$ is linearly independent for $1 \leq k \leq n$. Note that $e_i T = C_i$, so we see that $C_1, \ldots, C_k$ are linearly independent.

(2) (3) We have n^2 spots in the matrix. Each spot can be filled by one of p elements of $\mathbf{Z}/p\mathbf{Z}$, so there are p^{n^2} such matrices.

(5) (4) We will first show that there are p^k vectors in a k-dimensional subspace of K^n. Let $U \subseteq K^n$ be a k-dimensional subspace. Then we know there exists an invertible matrix M that maps U to the subspace K^k. Since U is bijective and we know that K^k has p^k elements, we see that U contains p^k elements.

Now we will count the number of invertible matrices M. By parts 1 and 2, a matrix M is invertible if and only if the first k rows are linearly independent for all k. Thus we will count the number of such M by counting the number of ways to pick a new vector to add to the matrix. There will be p^{i-1} such vectors, so there are p^{i-1} choices of entries that we can't make in order to make the first i rows linearly independent. Thus there will be $\prod_{i=1}^{n}(p^{n^2} - p^{i-1})$ invertible matrices.