Problem Set 6

Instructions: You are encouraged to work together on these problems, but each student should hand in their own final draft, written in a way that indicates their individual understanding of the solutions. Never submit something for grading that you do not completely understand. You cannot use any resources besides me, your classmates, our course notes, and the textbook.

I will post the .tex code for these problems for you to use if you wish to type your homework. If you prefer not to type, please *write neatly*. As a matter of good proof writing style, please use complete sentences and correct grammar. You may use any result stated or proven in class or in a homework problem, provided you reference it appropriately by either stating the result or stating its name (e.g. the definition of ring or Lagrange's Theorem). Do not refer to theorems by their number in the course notes or textbook.

Problem 1. Let F be a field and consider a monic polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ in $F[x]$ with $n \geqslant 1$.

a) Show that the principal ideal $(f(x))$ is a subspace of the F-vector space $F[x]$.

Proof. First, note that $(f(x))$ is nonempty, since it contains $f(x)$. To show that $(f(x))$ is a subspace we need to check that $(f(x))$ is closed under addition and multiplication by elements of F. This is certainly true as ideals are closed under addition and multiplication by any elements of $F[x]$, and thus in particular closed under multiplication by elements of F. □

b) Show that the set $B = \{\overline{1}, \overline{x}, \ldots, \overline{x^{n-1}}\}$, where $\overline{x^i} = x^i + (f(x))$, is a basis for the quotient F-vector space $F[x]/(f(x))$.

Proof. Let $g(x) \in F[x]$. By the Division Algorithm in $F[x]$, we have $g(x) = f(x)q(x) + r(x)$ where $r(x) = 0$ or $\deg(r) < n$. Since $g(x) - r(x) \in (f(x))$, we deduce that $g(x) + (f(x)) = r(x) + (f(x))$. Since $\deg(r) < n$, it follows that $r(x) + (f(x))$ is in the F-span of B, hence B spans $F[x]/(f(x))$.

Suppose $a_0\overline{1} + a_1\overline{x} + \cdots + a_{n-1}\overline{x^{n-1}} = 0$ in $F[x]/(f(x))$. Then $a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in (f(x))$. But the only polynomial in $(f(x))$ of degree less than n is 0, so $a_0 = \cdots = a_{n-1} = 0$ and thus B is linearly independent. □

c) Consider the linear transformation $l_x \colon F[x]/(f(x)) \to F[x]/(f(x))$ defined by $l_x(v) = \overline{x}v$ for any $v \in F[x]/(f(x))$. Find the matrix representing l_x in the basis B from part b).

Proof. Recall that the columns of $[\lambda_x]_B^B$ are obtained by collecting the coefficients of the expressions for $l_x(b)$ for each $b \in B$ as linear combinations of the elements of B.

$$\begin{aligned}
l_x(\overline{1}) = \overline{x} &= 0 \cdot \overline{1} + 1 \cdot \overline{x} + 0 \cdot \overline{x^2} + \cdots + 0 \cdot \overline{x^{n-1}} \\
l_x(\overline{x}) = \overline{x^2} &= 0 \cdot \overline{1} + 0 \cdot \overline{x} + 1 \cdot \overline{x^2} + \cdots + 0 \cdot \overline{x^{n-1}} \\
&\vdots \\
l_x(\overline{x^{n-2}}) = \overline{x^{n-2}} &= 0 \cdot \overline{1} + 0 \cdot \overline{x} + 0 \cdot \overline{x^2} + \cdots + 1 \cdot \overline{x^{n-1}}
\end{aligned}$$

Finally,

$$l_x(\overline{x^{n-1}}) = -a_0 \cdot \overline{1} - a_1 \cdot \overline{x} - a_2 \cdot \overline{x^2} + \cdots - a_{n-1} \cdot \overline{x^{n-1}}.$$

Thus

$$[\lambda_x]_B^B = \begin{bmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \ddots & 0 & -a_2 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & 1 & -a_{n-1} \end{bmatrix}. \quad \square$$

Problem 2. Let $V = \mathbb{R}^3$ with the standard basis $B = \{e_1, e_2, e_3\}$ and let $t : V \to V$ be the linear transformation represented by the matrix

$$[t]_B^B = \begin{bmatrix} 0 & -1 & 0 \\ -1 & 0 & 3 \\ 0 & 0 & 1 \end{bmatrix}.$$

a) Find the invariant factor decomposition of the $\mathbb{R}[x]$-module V_t.

Answer: From Problem 6 of Problem Set 5, we see that the Smith Normal Form for $xI_3 - A$ is

$$xI_3 - A \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & (x^2-1)(x-1) \end{pmatrix}.$$

The invariant factor decomposition of the $\mathbb{R}[x]$-module V_t is

$$V_t \cong \mathbb{R}[x]/((x^2-1)(x-1)). \quad \square$$

b) Find the characteristic and minimal polynomials of t.

Answer: We showed in class that the characteristic polynomial is the product of all the invariant factors, so $c_t(x) = \det(xI_3 - A) = (x^2-1)(x-1)$. If the invariant factors are $g_1 | \cdots | g_k$, then the minimal polynomial is g_k, so $m_t(x) = (x^2-1)(x-1)$. $\square$

c) Find the rational canonical form of t.

Answer: $RCF(t) = C\left((x^2-1)(x-1)\right) = C(x^3 - x^2 - x + 1) = \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$. $\square$

d) Find the Jordan canonical form of t.

Answer: First notice that the characteristic and minimal polynomial factor completely into linear factors, thus $JCF(t)$ exists. Since

$$V_t \cong \mathbb{R}[x]/\left((x^2-1)(x-1)\right) = \mathbb{R}[x]/\left((x+1)(x-1)^2\right) \cong \mathbb{R}[x]/(x+1) \oplus \mathbb{R}[x]/\left((x-1)^2\right)$$

the elementary divisors of t are $x+1$ and $(x-1)^2$. Thus

$$JCF(t) = J_1(-1) \oplus J_2(1) = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}. \quad \square$$

Problem 3. Let F be a field, let V and W be vector spaces over F, let $a\colon V \to V$ and $b\colon W \to W$ be linear transformations and let V_a and W_b be the $F[x]$-modules they determine.

a) Show that a function $g : V_a \to W_b$ is an $F[x]$-module homomorphism if and only if

(1) $g : V \to W$ is a linear transformation and

(2) $g \circ a = b \circ g$.

Proof. Suppose that F is a field, V, W are vector spaces over F, $a\colon V \to V$ and $b\colon W \to W$ are linear transformations, and $g : V_a \to W_b$ is a function.

($\Rightarrow$): Suppose that g is an $F[x]$-module homomorphism. Then for all $f \in F[x]$ and $v, v' \in V$, we have $g(v+v') = g(v)+g(v')$ and $g(fv) = fg(v)$. Considering the first of these identities together with the second one applied in the particular case where $f \in F$ is a constant polynomial shows that g is also an F-module homomorphism, so (1) holds.

Moreover, using the definition of the $F[x]$-module action on V_a and W_b, we have

$$(g \circ a)(v) = g(a(v)) \overset{V_a \text{ action}}{=} g(x \cdot v) \overset{g \text{ hom}}{=} xg(v) \overset{W_b \text{ action}}{=} b(g(v)) = (b \circ g)(v).$$

Therefore (2) holds.

($\Leftarrow$): Suppose that (1) and (2) hold. Let p be any element of $F[x]$, and let $v, v' \in V_a$. We can write

$$p(x) = f_n x^n + \cdots + f_0 = \sum_{i=0}^{n} f_i x^i$$

for some $n \geqslant 0$ and $f_n, \ldots, f_0 \in F$. Property (2) and induction on i gives $g \circ a^i = b^i \circ g$ for all $i \geqslant 1$; denote this property as (2'). Now we check that g is an $F[x]$-module homomorphism:

$$\begin{aligned} g(v + v') &= g(v) + g(v') \text{ by (1)} \\ g(p(x)v) &= g\left(\left(\sum_{i=0}^{n} f_i x^i\right) v\right) \overset{V_a \text{ action}}{=} g\left(\sum_{i=0}^{n} f_i a^i(v)\right) \overset{(i)}{=} \sum_{i=0}^{n} f_i g(a^i(v))) \\ &\overset{(2')}{=} \sum_{i=0}^{n} f_i b^i(g(v))) \overset{W_b \text{ action}}{=} \sum_{i=0}^{n} f_i x^i g(v) = p(x)g(v). \end{aligned}$$

Hence g is an $F[x]$-module homomorphism. □

b) Suppose that $V = F^m = W$, and let $A, B \in \mathrm{M}_m(F)$ be the matrices representing the linear transformations a and b, respectively, in the standard basis of F^m. Show that there is an $F[x]$-module isomorphism $V_a \cong W_b$ if and only if the matrices A and B are similar.

Proof. Using part (a), a function $g : V_a \to W_b$ is an $F[x]$-module homomorphism if and only if it is F-linear and satisfies $g \circ a = b \circ g$ for some g. We showed in class that there is an isomorphism $\mathrm{Hom}_F(V, W) \cong \mathrm{M}_m(F)$; more precisely, we showed that the linear map $g\colon V_a \to W_b$ is F-linear if and only if, fixing the standard basis of $V_a = W_b = F^m$, g can be represented by a matrix P such that $g(v) = Pv$ for all $v \in V_a$.

Furthermore, g is an isomorphism if and only if P is invertible. If g is an isomorphism, then $g \circ a = b \circ g$ holds and thus $PA = BP \iff B = PAP^{-1}$, so A and B being similar.

Conversely, if A and B being similar, then there exists some invertible matrix P such that $PA = BP \iff B = PAP^{-1}$. The map $g\colon V \to W$ defined by $g(v) = Pv$ is an isomorphism, since P is invertible, and $PA = BP$ implies $g \circ a = b \circ g$. We conclude that g gives an isomorphism $V_a \cong W_b$. □

Problem 4. Let F be a field and n a positive integer. We say an $n \times n$ matrix A with entries in F is **unipotent** if $A - I_n$ is nilpotent, meaning that $(A - I_n)^k = 0$ for some $k \geqslant 1$. For the field $F = \mathbb{Q}$, find (with complete justification) the number of similarity classes of 4×4 unipotent matrices and give an explicit representative for each class.

Proof. We know two $n \times n$ matrices are similar if and only they have the same invariant factors, say $g_1 | \dots | g_s$. We can thus characterize all the similarity classes of unipotent matrices by classifying the possible invariant factors, and the corresponding rational canonical forms provide a representative of each class. If $(A - I_n)^k = 0$ for some $k \geqslant 1$, then A satisfies the polynomial $(x-1)^k$, and thus the minimal polynomial of A must divide $(x-1)^k$. Since the minimal polynomial of A is of degree at most 4, we conclude that the minimal polynomial of A must be $(x-1)^k$ for some $1 \leqslant k \leqslant 4$; in particular, $g_s = (x-1)^k$. Moreover, the characteristic polynomial of A has degree 4 and must divide some power of $(x-1)^k$, and thus $c_A = g_1 \cdots g_s = (x-1)^4$. We must then have the following possibilities:

- The invariant factors of A are $g_1 = g_2 = g_3 = g_4 = x - 1$, so $xI - A$ has Rational Canonical Form I_4.
- The invariant factors of A are $g_1 = g_2 = x - 1$ and $g_3 = (x-1)^2 = x^2 - 2x + 1$, so $xI - A$ has Rational Canonical Form
$$c(x-1) \oplus c(x-1) \oplus c((x-1)^2) = \begin{bmatrix}1\end{bmatrix} \oplus \begin{bmatrix}1\end{bmatrix} \oplus \begin{bmatrix}0 & -1\\ 1 & 2\end{bmatrix} = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & -1\\ 0 & 0 & 1 & 2\end{bmatrix}.$$
- The invariant factors of A are $g_1 = (x-1)^2$ and $g_2 = (x-1)^2 = x^2 - 2x + 1$, so $xI - A$ has Rational Canonical Form
$$c((x-1)^2) \oplus c((x-1)^2) = \begin{bmatrix}0 & -1\\ 1 & 2\end{bmatrix} \oplus \begin{bmatrix}0 & -1\\ 1 & 2\end{bmatrix} = \begin{bmatrix}0 & -1 & 0 & 0\\ 1 & 2 & 0 & 0\\ 0 & 0 & 0 & -1\\ 0 & 0 & 1 & 2\end{bmatrix}.$$
- The invariant factors of A are $g_1 = x - 1$ and $g_2 = (x-1)^3 = x^3 - 3x^2 + 3x - 1$, so $xI - A$ has Rational Canonical Form
$$c(x-1) \oplus c((x-1)^3) = \begin{bmatrix}1\end{bmatrix} \oplus \begin{bmatrix}0 & 0 & 1\\ 1 & 0 & -3\\ 0 & 1 & 3\end{bmatrix} = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 1 & 0 & -3\\ 0 & 0 & 1 & 3\end{bmatrix}.$$
- The invariant factor of A is $g_1 = (x-1)^4 = x^4 - 4x^3 + 6x^2 - 4x + 1$, so $xI - A$ has Rational Canonical Form
$$c((x-1)^4) = \begin{bmatrix}0 & 0 & 0 & -1\\ 1 & 0 & 0 & 4\\ 0 & 1 & 0 & -6\\ 0 & 0 & 1 & 4\end{bmatrix}. \quad \square$$