

- (1) Let V be the collection of polynomials with coefficients in \mathbb{Q} in the variable s of degree at most 5. Prove that V is a vector space over \mathbb{Q} of dimension 6 with basis $\{1, x, x^2, x^3, x^4, x^5\}$. Prove that $\{1, 1+x, 1+x+x^2, 1+x+x^2+x^3, 1+x+x^2+x^3+x^4, 1+x+x^2+x^3+x^4+x^5\}$ is a basis for V as well.

Proof. We know that the polynomials with degree at most 5 form a commutative ring under addition. Let

$$p(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5$$

and

$$q(x) = b_0 + b_1x + b_2x^2 + b_3x^3 + b_4x^4 + b_5x^5$$

where $a_i \in \mathbb{Q}$ and $b_i \in \mathbb{Q}$ for all $0 \leq i \leq 5$. Let $m, n \in \mathbb{Q}$. First we will show that $(m+n)p(x) = mp(x) + np(x)$. We have

$$\begin{aligned} (m+n)p(x) &= (m+n)a_0 + (m+n)a_1x + (m+n)a_2x^2 + (m+n)a_3x^3 \\ &\quad + (m+n)a_4x^4 + (m+n)a_5x^5 \\ &= ma_0 + na_0 + ma_1x + na_1x + ma_2x^2 + na_2x^2 + ma_3x^3 + na_3x^3 \\ &\quad + ma_4x^4 + na_4x^4 + ma_5x^5 + na_5x^5 \\ &= ma_0 + ma_1x + ma_2x^2 + ma_3x^3 + ma_4x^4 + ma_5x^5 + na_0 + na_1x \\ &\quad + na_2x^2 + na_3x^3 + na_4x^4 + na_5x^5 \\ &= mp(x) + np(x). \end{aligned}$$

So the first distributive law holds. The next distributive law is $m(p(x) + q(x)) = mp(x) + mq(x)$. We have

$$\begin{aligned} m(p(x) + q(x)) &= m(a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5 + b_0 + b_1x \\ &\quad + b_2x^2 + b_3x^3 + b_4x^4 + b_5x^5) \\ &= ma_0 + ma_1x + ma_2x^2 + ma_3x^3 + ma_4x^4 + ma_5x^5 + mb_0 \\ &\quad + mb_1x + mb_2x^2 + mb_3x^3 + mb_4x^4 + mb_5x^5 \\ &= mp(x) + mq(x). \end{aligned}$$

So the second distributive law holds. Now we only need to show that $(mn)p(x) = m(np(x))$. We have

$$\begin{aligned} (mn)p(x) &= (mn)a_0 + (mn)a_1x + (mn)a_2x^2 + (mn)a_3x^3 + (mn)a_4x^4 + (mn)a_5x^5 \\ &= m(na_0) + m(na_1x) + m(na_2x^2) + m(na_3x^3) + m(na_4x^4) + m(na_5x^5) \\ &= m(na_0 + na_1x + na_2x^2 + na_3x^3 + na_4x^4 + na_5x^5) \\ &= m(np(x)). \end{aligned}$$

Thus this is a vector space over \mathbb{Q} . Let $p(x) \in V$. Then $p(x)$ is a polynomial of degree at most 5. So there exists $a_i \in \mathbb{Q}$ for $0 \leq i \leq 5$ such that

$$p(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5$$

by definition of a polynomial of degree at most 5. It is easy to see that this is a linear combination of $\{1, x, x^2, x^3, x^4, x^5\}$. Thus this set spans V . Consider

$$b_01 + b_1x + b_2x^2 + b_3x^3 + b_4x^4 + b_5x^5 = 0.$$

where $b_i \in \mathbb{Q}$. Thus we have a polynomial equal to the zero polynomial. By definition of the zero polynomial, $b_i = 0$ for all i . Hence this set is linearly independent, and thus a basis for B . Since V is a vector space and we have a basis of degree 6, V has dimension 6.

Once again, we will let $p(x) \in V$ such that

$$p(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5.$$

We let $b_5 = a_5$ and $b_i = a_i - a_{i+1}$ for all $0 \leq i \leq 4$. Then we have

$$\begin{aligned} p(x) &= a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5 \\ &= (b_0 + b_1 + b_2 + b_3 + b_4 + b_5) + (b_1 + b_2 + b_3 + b_4 + b_5)x \\ &\quad + (b_2 + b_3 + b_4 + b_5)x^2 + (b_3 + b_4 + b_5)x^3 + (b_4 + b_5)x^4 + b_5x^5 \\ &= b_0(1) + b_1(1 + x) + b_2(1 + x + x^2) + b_3(1 + x + x^2 + x^3) \\ &\quad + b_4(1 + x + x^2 + x^3 + x^4) + b_5(1 + x + x^2 + x^3 + x^4 + x^5). \end{aligned}$$

Hence $p(x)$ can be written as a linear combination of the set $\{1, 1 + x, 1 + x + x^2, 1 + x + x^2 + x^3, 1 + x + x^2 + x^3 + x^4, 1 + x + x^2 + x^3 + x^4 + x^5\}$. So this set spans V .

Now suppose we have

$$\begin{aligned} a_0(1) + a_1(1 + x) + a_2(1 + x + x^2) + a_3(1 + x + x^2 + x^3) \\ + a_4(1 + x + x^2 + x^3 + x^4) + a_5(1 + x + x^2 + x^3 + x^4 + x^5) = 0. \end{aligned}$$

Rearranging terms gives

$$\begin{aligned} (a_0 + a_1 + a_2 + a_3 + a_4 + a_5) + (a_1 + a_2 + a_3 + a_4 + a_5)x \\ + (a_2 + a_3 + a_4 + a_5)x^2 + (a_3 + a_4 + a_5)x^3 + (a_4 + a_5)x^4 + a_5x^5 = 0. \end{aligned}$$

By definition of the zero polynomial, all of the coefficients must be zero. So the coefficient of x^5 must be zero. Hence $a_5 = 0$. Similarly, $0 = a_4 + a_5 = a_4 + 0$. So $a_4 = 0$. Similarly, we get that $a_i = 0$ for all i , Hence this set is linearly independent. Thus this is a basis for V . \square

- (2) In class we proved the theorem: $\dim(V) = \dim(W) + \dim(V/W)$ where w is a subspace of V , and deduced the corollary: if $f : V \rightarrow W$ then $\dim(V) = \dim(\ker(f)) + \dim(\text{Im}(f))$. Prove this in reverse, that is, prove (without appeal to the theorem

above) theorem: that if $f : V \rightarrow W$ then $\dim(V) = \dim(\ker(f)) + \dim(\text{Im}(f))$ and deduce corollary: if $W \leq V$ then $\dim(V) = \dim(W) + \dim(V/W)$.

Proof. Suppose that $f : V \rightarrow W$ is a linear transformation. Since $\ker f$ is a subspace of V , $\ker f$ has a basis $X = \{l_1, l_2, \dots, l_m\}$ which can be extended to form a basis of V , $Y = \{l_1, l_2, \dots, l_m, v_{m+1}, \dots, v_n\}$. Since $l_i \in \ker f$ for all $i \leq m$, $f(l_i) = 0$ for all $i \leq m$. Also, $f(v_i) \in \text{image}(f)$ and $f(v_i) \neq 0$ for all $i > m$, since $v_i \in V$ and v_i is not an element of $\ker(f)$. We now show that $Z = \{f(v_{m+1}), \dots, f(v_n)\}$ is a basis for $\text{image}(f)$. To show that Z spans $\text{image}(f)$, let $w \in \text{image}(f)$. Thus, there exists some $v \in V$ such that $f(v) = w$. Since Y forms a basis for V ,

$$v = x_1 l_1 + x_2 l_2 + \dots + x_m l_m + x_{m+1} v_{m+1} + \dots + x_n v_n$$

for some scalars x_1, x_2, \dots, x_n . By substitution,

$$\begin{aligned} w &= f(v) = f(x_1 l_1 + x_2 l_2 + \dots + x_m l_m + x_{m+1} v_{m+1} + \dots + x_n v_n) \\ &= x_1 f(l_1) + x_2 f(l_2) + \dots + x_m f(l_m) + x_{m+1} f(v_{m+1}) + \dots + x_n f(v_n) \\ &= x_{m+1} f(v_{m+1}) + \dots + x_n f(v_n) \end{aligned}$$

Thus, w can be written as a linear combination of the vectors in Z . So Z spans $\text{image}(f)$. To show that Z is linearly independent, suppose that

$$x_{m+1} f(v_{m+1}) + \dots + x_n f(v_n) = 0$$

for some scalars x_{m+1}, \dots, x_n . Since f is a linear transformation,

$$x_{m+1} f(v_{m+1}) + \dots + x_n f(v_n) = f(x_{m+1} v_{m+1} + \dots + x_n v_n)$$

Thus, $x_{m+1} v_{m+1} + \dots + x_n v_n \in \ker(f)$, so

$$x_{m+1} v_{m+1} + \dots + x_n v_n = x_1 l_1 + x_2 l_2 + \dots + x_m l_m$$

for some scalars x_1, x_2, \dots, x_m , since X is a basis for $\ker(f)$. Rearranging the equation, we see that

$$-x_1 l_1 - x_2 l_2 - \dots - x_m l_m + x_{m+1} v_{m+1} + \dots + x_n v_n = 0$$

Since Y is linearly independent, this implies that $-x_1 = -x_2 = \dots = -x_m = x_{m+1} = \dots = x_n = 0$. Thus, $x_{m+1} = \dots = x_n = 0$, so Z is linearly independent. Therefore Z is a basis for $\text{image}(f)$. Since $\dim(\ker(f))$ is the number of vectors in X , $\dim(\text{image}(f))$ is the number of vectors in Z , and $\dim(V)$ is the number of vectors in Y , it follows that $\dim(V) = \dim(\ker(f)) + \dim(\text{image}(f))$. In the case where $V \leq W$, consider the natural projection map $\pi : V \rightarrow V/W$. This is a linear transformation with the properties that $\ker(\pi) = W$ and $\text{image}(\pi) = V/W$. Thus, $\dim(V) = \dim(W) + \dim(V/W)$ by substitution. \square

- (3) Let V be a vector space over a field k and let $f : V \rightarrow V$ be a linear transformation. A non-zero vector $v \in V$ such that $f(v) = \lambda v$ for some constant $\lambda \in k$ is called an *eigenvector* with *eigenvalue* λ . Prove that for a fixed $\lambda \in k$ the collection of eigenvectors of f with eigenvalue λ (together with $\vec{0}$) forms a subspace of V .

Proof. Let N be the collection of eigenvectors of f with eigenvalue λ , together with $\vec{0}$. Since $\vec{0} \in N$, we know that $N \neq \emptyset$. Let $x, y \in N$. Then we know that $f(x) = \lambda x$ and $f(y) = \lambda y$. Let $\alpha \in k$. Then we have

$$\begin{aligned} f(x + \alpha y) &= f(x) + \alpha f(y) \\ &= \lambda x + \alpha \lambda y \\ &= \lambda x + \lambda \alpha y \\ &= \lambda(x + \alpha y). \end{aligned}$$

Thus $x + \alpha y \in N$. Hence N is a subspace of V . □

- (4) Let ϕ be a linear transformation from a finite dimensional vector space V to itself (i.e. $\phi : V \rightarrow V$). Prove that there is an integer m such that $\ker(\phi^m) \cap \text{image}(\phi^m) = \{0\}$.

Proof. Let $x \in \ker(\phi^i)$ for some $i > 0$. Then $\phi^i(x) = 0$. Since ϕ is a linear transformation, $\phi(0) = 0$. Thus, $\phi^{i+1}(x) = \phi(\phi^i(x)) = \phi^i(0) = 0$. So $x \in \ker(\phi^{i+1})$. Therefore $\ker(\phi^i) \subseteq \ker(\phi^{i+1})$ for all $i > 0$. Now, let $x \in \text{image}(\phi^i)$. Then there exists a $v \in V$ such that $\phi^i(v) = x$. Also, $\phi^i(v) = \phi^{i-1}(\phi(v)) = x$. Since $\phi(v) \in V$ and $\phi^{i-1}(\phi(v)) = x$, it follows that $x \in \text{image}(\phi^{i-1})$. Thus, $\text{image}(\phi^i) \subseteq \text{image}(\phi^{i+1})$ for all $i > 1$. We now have the following scenario:

$$\ker(\phi) \subseteq \ker(\phi^2) \subseteq \dots \subseteq \ker(\phi^i) \subseteq \ker(\phi^{i+1}) \subseteq \dots$$

and

$$\text{image}(\phi) \supseteq \text{image}(\phi^2) \supseteq \dots \supseteq \text{image}(\phi^{i-1}) \supseteq \text{image}(\phi^i) \supseteq \dots$$

We also know that $\ker(\phi^i)$ and $\text{image}(\phi^i)$ are subspaces of V for all $i > 0$. Since V is a finite vector space, and a subspace of a finite vector space always has dimension less than or equal to the dimension of the original vector space, there must exist some m such that $\ker(\phi^m)$ is of largest size and $\text{image}(\phi^m)$ is of smallest size. Thus, for all $k > m$, $\ker(\phi^m) = \ker(\phi^k)$ and $\text{image}(\phi^m) = \text{image}(\phi^k)$. Consider $k = 2m$. Suppose that $x \in \ker(\phi^m) \cap \text{image}(\phi^m)$. This means that there exists some $v \in V$ such that $\phi^m(v) = x$ and that $\phi^m(x) = 0$. Notice that $\phi^{2m}(v) = \phi^m(\phi^m(v)) = \phi^m(x) = 0$. Thus, $v \in \ker(\phi^{2m})$. Since $\ker(\phi^{2m}) = \ker(\phi^m)$, $v \in \ker(\phi^m)$. Thus, $x = \phi^m(v) = 0$. Therefore $\ker(\phi^m) \cap \text{image}(\phi^m) = \{0\}$. □

- (5) Let V be the vector space of polynomials with coefficients in \mathbb{Q} in the variable x of degree at most 5. Determine the transition matrix from the basis $\{1, x, x^2, x^3, x^4, x^5\}$ to the basis $\{1, 1+x, 1+x+x^2, 1+x+x^2+x^3, 1+x+x^2+x^3+x^4, 1+x+x^2+x^3+x^4+x^5\}$.

Proof. Consider the matrix

$$\begin{pmatrix} 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Suppose $p(x) \in V$ is written as a linear combination of the basis $\{1, x, x^2, x^3, x^4, x^5\}$. Then

$$p(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5$$

where $a_i \in \mathbb{Q}$. Applying this transition matrix gives

$$\begin{pmatrix} 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \end{pmatrix} = \begin{pmatrix} a_0 - a_1 \\ a_1 - a_2 \\ a_2 - a_3 \\ a_3 - a_4 \\ a_4 - a_5 \\ a_5 \end{pmatrix}$$

So we now have

$$\begin{aligned} & (a_0 - a_1) + (a_1 - a_2)(1 + x) + (a_2 - a_3)(1 + x + x^2) + (a_3 - a_4)(1 + x + x^2 + x^3) \\ & \quad + (a_4 - a_5)(1 + x + x^2 + x^3 + x^4) + a_5(1 + x + x^2 + x^3 + x^4 + x^5) \\ & = (a_0 - a_1 + a_1 - a_2 + a_2 - a_3 + a_3 - a_4 + a_4 - a_5 + a_5) + (a_1 - a_2 + a_2 - a_3 + a_3 \\ & \quad - a_4 + a_4 - a_5 + a_5)x + (a_2 - a_3 + a_3 - a_4 + a_4 - a_5 + a_5)x^2 + (a_3 - a_4 \\ & \quad + a_4 - a_5 + a_5)x^3 + (a_4 - a_5 + a_5)x^4 + a_5x^5 \\ & = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5. \end{aligned}$$

So we get $p(x)$ written in terms of the other basis. Thus this is the transition matrix from the basis $\{1, x, x^2, x^3, x^4, x^5\}$ to the basis $\{1, 1 + x, 1 + x + x^2, 1 + x + x^2 + x^3, 1 + x + x^2 + x^3 + x^4, 1 + x + x^2 + x^3 + x^4 + x^5\}$. \square

- (6) Let V be the vector space of polynomials with coefficients in \mathbb{Q} in the variable x of degree at most 5. Let $d : V \rightarrow V$ be the linear transformation of V to itself given by the usual differentiation of a polynomial with respect to x (i.e. $d(p(x)) = p'(x)$). Determine the matrix of d with respect to the two bases for V given in the previous problem.

Proof. With respect to the first basis $(\{1, x, x^2, x^3, x^4, x^5\})$, Consider the matrix

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Suppose $p(x) \in V$ is written as a linear combination of the basis $\{1, x, x^2, x^3, x^4, x^5\}$. Then

$$p(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5$$

where $a_i \in \mathbb{Q}$. Applying this derivative matrix gives

$$\begin{pmatrix} 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \end{pmatrix} = \begin{pmatrix} a_1 \\ 2a_2 \\ 3a_3 \\ 4a_4 \\ 5a_5 \\ 0 \end{pmatrix}$$

So we now have $a_1 + 2a_2x + 3a_3x^2 + 4a_4x^3 + 5a_5x^4$, the derivative of $p(x)$. With respect to the other basis $\{1, 1+x, 1+x+x^2, 1+x+x^2+x^3, 1+x+x^2+x^3+x^4, 1+x+x^2+x^3+x^4+x^5\}$, we need only transition from the this basis to the first, apply the derivative matrix, then transition back to the other basis. The following matrix takes us from the second basis to the first:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

To show this, suppose $p(x) \in V$ is written as a linear combination of the basis $\{1, 1+x, 1+x+x^2, 1+x+x^2+x^3, 1+x+x^2+x^3+x^4, 1+x+x^2+x^3+x^4+x^5\}$. Then

$$p(x) = a_0 + a_1(1+x) + a_2(1+x+x^2) + a_3(1+x+x^2+x^3) + a_4(1+x+x^2+x^3+x^4) + a_5(1+x+x^2+x^3+x^4+x^5)$$

where $a_i \in \mathbb{Q}$. Applying this transition matrix gives

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \end{pmatrix} = \begin{pmatrix} a_0 + a_1 + a_2 + a_3 + a_4 + a_5 \\ a_1 + a_2 + a_3 + a_4 + a_5 \\ a_2 + a_3 + a_4 + a_5 \\ a_3 + a_4 + a_5 \\ a_4 + a_5 \\ a_5 \end{pmatrix}$$

So we now have

$$\begin{aligned} & (a_0 + a_1 + a_2 + a_3 + a_4 + a_5) + (a_1 + a_2 + a_3 + a_4 + a_5)x + (a_2 + a_3 + a_4 + a_5)x^2 + \\ & \quad (a_3 + a_4 + a_5)x^3 + (a_4 + a_5)x^4 + a_5x^5 \\ = & a_0 + a_1 + a_2 + a_3 + a_4 + a_5 + a_1x + a_2x + a_3x + a_4x + a_5x + a_2x^2 + a_3x^2 + a_4x^2 + a_5x^2 + \\ & \quad + a_3x^3 + a_4x^3 + a_5x^3 + a_4x^4 + a_5x^4 + a_5x^5 \\ = & a_0 + a_1(1 + x) + a_2(1 + x + x^2) + a_3(1 + x + x^2 + x^3) \\ & \quad + a_4(1 + x + x^2 + x^4) + a_5(1 + x + x^2 + x^3 + x^4 + x^5) \end{aligned}$$

which was our original polynomial. Combining this matrix with the derivative matrix and the transition matrix from the previous problem, we arrive at our derivative matrix in the second basis:

$$\begin{pmatrix} 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \\ = & \begin{pmatrix} 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 2 & 2 & 2 & 2 \\ 0 & 0 & 0 & 3 & 3 & 3 \\ 0 & 0 & 0 & 0 & 4 & 4 \\ 0 & 0 & 0 & 0 & 0 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 1 & -1 & -1 & -1 & -1 \\ 0 & 0 & 2 & -1 & -1 & -1 \\ 0 & 0 & 0 & 3 & -1 & -1 \\ 0 & 0 & 0 & 0 & 4 & -1 \\ 0 & 0 & 0 & 0 & 0 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

□

- (7) Let R be commutative and let ${}_R M$ be a cyclic left R -module generated by m . Prove that $\text{Ann}_R(M) = \text{Ann}_R(m)$. Conclude that $M \cong R/\text{Ann}_R(M)$.

Proof. Let $x \in \text{Ann}_R(M)$. Then we know that $xn = 0$ for all $n \in M$. Since $m \in M$ we know that $xm = 0$. So $x \in \text{Ann}_R(m)$. Thus $\text{Ann}_R(M) \subseteq \text{Ann}_R(m)$. Let $x \in \text{Ann}_R(m)$. Then we know that $xm = 0$. Since M is cyclic, then all $n \in M$ can be written as rm for some $r \in R$. We have that $x(rm) = r(xm) = 0$. Thus $x \in \text{Ann}_R(M)$. Hence $\text{Ann}_R(M) = \text{Ann}_R(m)$. By a proposition in class, we know that $M \cong R/\text{Ann}_R(m)$. Since $\text{Ann}_R(M) = \text{Ann}_R(m)$, we have that $M \cong R/\text{Ann}_R(M)$ by substitution. □

- (8) Prove that if R is commutative and $M = Rx$ and $N = Ry$ are cyclic left R -modules then $M \cong N$ if and only if $\text{Ann}_R(M) = \text{Ann}_R(N)$.

Proof. (\Rightarrow) Suppose that $M \cong N$. To show $\text{Ann}_R(M) = \text{Ann}_R(N)$, we proceed by double containment. Let $r \in \text{Ann}_R(M)$. Thus, $rm = 0$ for all $m \in M$. Let $n \in N$. Since $M \cong N$, there exists some isomorphism $\varphi: N \rightarrow M$. Consider $\varphi(rn)$. Since φ is an isomorphism, $\varphi(rn) = r(\varphi(n))$. Since $\varphi(n) \in M$, $r\varphi(n) = 0$. Thus, $\varphi(rn) = 0$. Since φ is an isomorphism, $\ker(\varphi) = 0$, so $rn = 0$. Thus, $r \in \text{Ann}_R(N)$. Therefore, $\text{Ann}_R(M) \subseteq \text{Ann}_R(N)$. Applying the same argument with M and N interchanged gives us the other containment, $\text{Ann}_R(N) \subseteq \text{Ann}_R(M)$. Thus, $\text{Ann}_R(M) = \text{Ann}_R(N)$.

(\Leftarrow) Suppose that $\text{Ann}_R(M) = \text{Ann}_R(N)$. Since $M = Rm$ and $N = Rn$, we know that $M \cong R/\text{Ann}_R(M)$ and $N \cong R/\text{Ann}_R(N)$, by the previous problem. By Substitution, $N \cong R/\text{Ann}_R(M)$ and $M \cong R/\text{Ann}_R(N)$. Thus $M \cong N$. □

- (9) Let ${}_R M$ be free with basis $\{m_i\}$ and let ${}_R N$ be any R -module. Prove that for any set function $f: \{m_i\} \rightarrow N$ there is a unique R -homomorphism $f': M \rightarrow N$ such that $f'(m_i) = f(m_i)$ for all i .

Proof. Define $f': M \rightarrow N$ as

$$f'(m) = f'(a_1 m_1 + a_2 m_2 + \dots) = a_1 f(m_1) + a_2 f(m_2) + \dots$$

This map is clearly well-defined. To show that this is an R -homomorphism, let $a = a_1m_1 + a_2m_2 + \dots$ and $b = b_1m_1 + b_2m_2 + \dots$ be elements of M and let $r \in R$. Then we have

$$\begin{aligned} f'(a + rb) &= f(a_1m_1 + a_2m_2 + \dots + rb_1m_1 + rb_2m_2 + \dots) \\ &= a_1f(m_1) + a_2f(m_2) + \dots + rb_1f(m_1) + rb_2f(m_2) + \dots \\ &= (a_1f(m_1) + a_2f(m_2) + \dots) + r(b_1f(m_1) + b_2f(m_2) + \dots) \\ &= f'(a) + rf'(b). \end{aligned}$$

Thus this is a homomorphism. Also notice that $f'(m_i) = f(m_i)$ for all i . To show that this is unique, assume that $g' : M \rightarrow N$ and that $g'(m_i) = f(m_i)$. Let $a = a_1m_1 + a_2m_2 + \dots$ be an arbitrary element of M . Then we have

$$f'(a) = a_1f(m_1) + a_2f(m_2) + \dots$$

Since g' is an R -module homomorphism, we know that

$$g'(a) = a_1g'(m_1) + a_2g'(m_2) + \dots$$

However, $g'(m_i) = f(m_i)$. So we have that $g'(a) = f'(a)$. Thus $g' = f'$. Hence f' is unique. \square

(10) Let A be the matrix

$$\begin{pmatrix} -2 & 3 & 0 \\ -3 & 3 & 0 \\ -12 & 12 & 6 \end{pmatrix}$$

over the integers. Find the Smith normal form for A (hint – start by adding column 2 to column 1).

Proof. First, add column 2 to column 1 to get:

$$\begin{pmatrix} 1 & 3 & 0 \\ 0 & 3 & 0 \\ 0 & 12 & 6 \end{pmatrix}$$

Next, subtract 3 times column 1 from column 2:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 12 & 6 \end{pmatrix}$$

Finally, subtract 4 times row 2 from row 3:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 6 \end{pmatrix}$$

And we now have the Smith normal form for A . \square

- (11) Continuing the above problem, find the matrices of P and Q such that QAP is the Smith normal form.

Proof. Define the matrices

$$P = \begin{pmatrix} 1 & -3 & 0 \\ 1 & -2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

and

$$Q = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -4 & 1 \end{pmatrix}.$$

We can see that QAP is given by

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -4 & 1 \end{pmatrix} \begin{pmatrix} -2 & 3 & 0 \\ -3 & 3 & 0 \\ -12 & 12 & 6 \end{pmatrix} \begin{pmatrix} 1 & -3 & 0 \\ 1 & -2 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 6 \end{pmatrix}$$

which is the Smith normal form. □

- (12) Still continuing, if the original basis for G was $\{g_1, g_2, g_3\}$ and the original set of generators for K was $\{k_1, k_2, k_3\}$, find the new basis and set of generators.

Proof. The right hand matrix

$$\begin{pmatrix} 1 & -3 & 0 \\ 1 & -2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

gives us the following relations between the original generators $\{k_1, k_2, k_3\}$ and the new generators $\{l_1, l_2, l_3\}$:

$$l_1 = k_1 + k_2$$

$$l_2 = -3k_1 - 2k_2$$

$$l_3 = k_3$$

Thus, our new generators are $\{k_1 + k_2, -3k_1 - 2k_2, k_3\}$ The left hand matrix

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -4 & 1 \end{pmatrix}$$

gives us the following relations between the original basis $\{g_1, g_2, g_3\}$ and the new basis $\{b_1, b_2, b_3\}$:

$$g_1 = b_1$$

$$g_2 = b_2 - 4b_3$$

$$g_3 = b_3$$

Solving for b_1 , b_2 , and b_3 , we obtain our new basis: $\{g_1, g_2 + 4g_3, g_3\}$.

□