# MATH 258: Homework #9

Jesse Farmer

09 March 2005

1. *Let $A$ be a commutative ring and define $E = \{f \in A[x] \mid \deg f \leq n-1, f\,monic\}$. Let $f_0, \ldots, f_{n-1} \in E$ with $\deg f_i = i$ for $0 \leq i \leq n-1$. Show that $\{f_0, \ldots, f_{n-1}\}$ form a basis for $E$ over $A$, and hence that $E$ is a free $A$-module of rank $n$.*

   We prove this by induction on $n$. It is obviously true for $n = 1$, so assume it for the $n-1$ case. Without loss of generality assume that for $f \in E$ we have $\deg f = n$, since otherwise the $n-1$ case applies. Then we can write
   $$f(x) = x^n + \sum_{i=0}^{n-1} \lambda_i f_i(x)$$
   for some $\lambda_i \in A$. Write $f_n(x) = x^n + a_{n-1} + \cdots + a_0$. Then
   $$f(x) - f_n(x) = \sum_{i=0}^{n-1} (\lambda_i - a_i) f_i(x)$$
   so that
   $$f(x) = \sum_{i=0}^{n-1} (\lambda_i - a_i) f_i(x) + f_n(x)$$
   Since the $\{f_i\}$ are monic they must be linearly independent. This follows since if $\lambda x^k = 0$ for some $k \in \mathbb{N}$ then $\lambda = 0$, so this applies equally well to sums of such components. Therefore $E$ is a free $A$-module of rank $n$.

2. *Let $K$ be a field and $f \in K[x]$ with $\deg f = n > 0$. Show that $V = K[x]/(f \cdot K[x])$ is a vector space of dimension $n$ over $K$.*

   Any quotient of an $A$-module, where $A$ is a ring, field, etc., is always an $A$-module, so we must just verify that the dimension is $n$. Consider the set $\{\bar{1}, \ldots, \bar{x}^{n-1}\}$. Writing $\bar{x}$ as $x$ for now, this set spans since we have the following:
   $$f(x) = \sum_{x=0}^{n} a_i x_i \equiv 0$$
   Hence we can write $x^m = \sum_{i=0}^{m-1} b_i x_i$ for all $m \geq n$. Any $g \in K[x]/(f \cdot K[x])$ can therefore be written as a linear combination of $\{1, \ldots, x^{n-1}\}$ since any power of $x$ greater than $n$ can be successively reduced by using the above equality until it is a polynomial of degree less than $n$.

3. *Let $K$ be a field and $V, V'$ finite-dimensional vector spaces over $K$. Let $f : V \to V'$ be a $K$-linear map. Show that $\dim V = \dim(\ker f) + \dim f(V)$.*

   From class, for any subspace $W$ of a vector space $V$, $\dim V = \dim W + \dim V/W$. By the first isomorphism theorem it follows that $\dim V = \dim \ker f + \dim f(V)$.

4. *Let $K$ be a field and $V, V'$ be finite-dimensional vector spaces over $K$. Suppose that* $\dim V = \dim V' = n$*. Show that for a $K$-linear map $f : V \to V'$ being an isomorphism, being injective, and being surjective are all equivalent.*

   It is sufficient to show that a $K$-linear map is surjective if and only if it is injective. Recall that $\dim V = \dim \ker f + \dim f(V)$. If $f$ is surjective then $f(V) = V'$ and hence $\dim \ker f = 0$. But then $\ker f = 0$ and hence $f$ is injective. Similarly, if $f$ is injective then $\dim f(V) = n$, so that $f(V) \cong V'$ (two finite-dimensional vector spaces are isomorphic if and only if they have the same dimension), and hence $f$ is surjective.

5. *Let $V = K^n$ where $K$ is a field and $(\lambda_1, \dots, \lambda_n) \in K^n$ with not all $\lambda_i = 0$. Define*

$$W = \left\{ (a_1, \dots, a_n) \in K^n \mid \sum_{i=1}^{n} \lambda_i a_i = 0 \right\}$$

   *Show that $W$ is a subspace of $V$. Compute* $\dim W$*.*

   Since the 0-vector is in $W \subset V$, it suffices to check that $x + ky \in W$ for all $x, y \in W$ and $k \in K$. But this is fairly obvious as $x + ky = (x_1 + ky_1, \dots, x_n + ky_n)$ and hence

$$\sum \lambda_i(x_i + ky_i) = \sum \lambda_i x_i + k \sum \lambda_i y_i = 0$$

   Consider $K$ as a one dimensional vector space over itself and define $\varphi : V \to K$ by

$$\varphi(a_1, \dots, a_n) = \sum_{i=1}^{n} \lambda_i a_i$$

   Since not all $\lambda_i$ are zero and $K$ is a field this map is surjective. $\ker \varphi = W$, so that

$$\dim W = \dim V - \dim K = n - 1$$

6. *Let $A$ be a commutative ring and $E$ an $A$-modules. Let $\{e_1, \dots, e_n\}$ generate $E$. Show that $E$ is a free $A$-module with basis $\{e_1, \dots, e_n\}$ if and only if for all $A$-modules $M$ and $x_1, \dots, x_n \in M$ there exists an $A$-linear map $f : E \to M$ such that $f(e_i) = x_i$. Is such an $f$ unique?*

   Let $\{e_1, \dots, e_n\}$ be a basis for $E$ and let $M$ be an $A$-module with $x_1, \dots, x_n \in M$. Define

$$f\left(\sum a_i e_i\right) = \sum a_i x_i$$

   Clearly this satisfies the condition that $f(e_i) = x_i$. It is linear since

$$f(x + y) = f\left(\sum (a_i + b_i)e_i\right) = \sum (a_i + b_i)x_i = \sum a_i x_i + \sum b_i x_i = f(x) + f(y)$$

   and similarly for the ring action on $E$ and $M$. For the converse, let $M = A^n$ and fix the standard basis $\{x_1, \dots, x_n\}$ of $M$, i.e., $x_i$ is 0 in every coordinate except the $i^{th}$ where it is 1. Then any $A$-linear map satisfying $f(e_i) = x_i$ is obviously surjective. To see injectivity, recall that the $\{e_i\}$ generate $E$. Then if $f(x) = f(\lambda_1 e_1 + \cdots + \lambda_n e_n) = 0$ it follows that $\lambda_i e_i = 0$ for every $\lambda_i, e_i$, and hence $x = 0$. Therefore $\ker f = 0$ and $f$ is injective.

7. *Let $A$ be a nonzero commutative ring and $I \subset A$ an ideal. Show that any two elements of $I$ are linearly dependent. Deduce that every nonzero ideal of $A$ is a free $A$-module if and only if $A$ is a principal ideal domain.*

   Let $a = y$ and $b = -x$, then for any $x, y \in I$, $ax + by = 0$ even though $a, b \neq 0$. If $A$ is a PID then every ideal is generated by a single element, and a single element in a PID is always linearly independent. If every nonzero ideal of $A$ is free then, from the first part, every ideal must be generated by one element (since otherwise no set of generators could be a basis).

8. (a) *Let $A$ be an integral domain and $a \in A$. Let $E$ be an $A$-module and define*

$$E(a) = \{x \in E \mid a^r x = 0, \text{ for some } r \geq 0\}$$

*Show that $E(a)$ is a submodule of $E$.*

Since $0 \in E(a)$ for any $a$, $E(a) \neq \emptyset$. Let $x, y \in E(a)$ and $b \in A$, then there exist $r, s \in \mathbb{Z}_+$ such that $a^s x = 0$ and $a^r y = 0$. Therefore

$$a^{r+s}(x + by) = a^{r+s}x + ba^{r+s}y = 0$$

Hence $x + by \in E(a)$ and therefore $E(a)$ is a submodule.

(b) *Let $A$ be as above and let $E$ be a finitely generated torsion module. Show that $Ann(E)$ is a nonzero ideal.*

Ann$(E)$ is an ideal since it is the kernel of the homomorphism from $A$ to the sub-modules of $E$ given by $a \mapsto aE$. Recall that $E$ is a torsion module if $E = \text{tor}(E) = \{x \in E \mid \exists a \in A \text{ s.t. } ax = 0\}$. Assume $E = \langle F \rangle$ where $F$ is finite. Then for every $x \in F$ there exists some nonzero $a_x$ such that $a_x x = 0$. Let

$$a = \prod_{x \in F} a_x$$

Then $a \in \text{Ann}(E)$, since every element of $E$ can be written as an $A$-linear combination of elements of $F$.

9. *Let $A$ be a PID and $E \neq 0$ a finitely generated torsion module. Let $I = Ann(E)$, and, say, $I = Aa$ where*

$$a = \prod_{i=1}^{r} p_i^{m_i}$$

*for $m_i > 0$ and $p_i$ a prime element of $A$ with $Ap_i \neq Ap_j$ for $i \neq j$.*

(a) *Show that the sub-module $E(p_1) + \cdots + E(p_r) = E'$ is a direct sum of the sub-modules $E(p_1), \ldots, E(p_r)$.*

First, it cannot be the case that there exist $p, q$ prime elements such that $p^n x = q^m x = 0$ for $x \neq 0$ since if this were the case then $(p^n - q^m)x = 0$, and hence $p \mid q$ or $q \mid p$, a contradiction. Therefore, since $E$ is a torsion module, it follows that $E(p_i) = \{x \in E \mid p_i^{m_i} x = 0\}$. This is because if $aE = 0$ (as it does, by assumption) then if $x \in E(p_i)$, $p_i^r x = p_i^{m_i} x = 0$ for some $p_i$. But by construction $r \leq m_i$.

This condition, viz., that no two prime distinct elements have powers which annihilate a given element of $E'$, also guarantees that $E'$ is in fact the direct sum of the $E(p_i)$.

(b) *Show that $E = E'$.*

This follows from the Chinese Remainder Theorem by noting that the ideals $p_i^{m_i} A$ are comaximal and that $E/(p_i^{m_i} A)E \cong E(p_i)$ (it is the kernel of the homomorphism defined by $x \mapsto a_i x$ where $a_i = \frac{a}{p_i^{m_1}}$). Therefore

$$E \cong \frac{E}{\{0\}} \cong \frac{E}{(a)E} \cong E(p_1) \times \cdots \times E(p_n)$$

and, from the previous part, the last expression is isomorphic to the direct sum of the $E(p_i)$.

(c) *Show that $E(p_i) = a_i E$, and hence that $p_i^{m_i} E(p_i) = 0$.*

This was essentially shown already, but, since every element $x \in E$ is annihilated by $a$, then it must be annihilated by some prime power dividing $a$. From the first part there is only one such prime, $p_i$, and hence the power to do this is $m_i$. Therefore $E(p_i)$ consists of precisely those elements that are divisible by other primes dividing $a$. By the first part, again, this means that $E(p_i) = a_i E$, and hence $p_i^{m_i} E(p_i) = aE = 0$.

10. *Let $A$ be a commutative ring and $R = A[x]$. Let $E$ be an $A$-module and $\alpha \in End_A(E)$. Show that $E$ acquires an $R$-module structure if, for $x \in E$, we define*

$$f(x) \cdot z = f(\alpha) \cdot z = \sum_{i=1}^{r} a_i \alpha^i(z)$$

*where $f(x) = \sum_{i=1}^{r} a_i x^i$.*

Note that $\alpha^i \in \mathrm{End}_A(E)$ for any $i \in \mathbb{N}$, where this means not "to the power of" but rather "$i$-fold composition." We take addition on $E$ as it is as an $A$-module, and multiplication as defined above. Fix $\alpha \in \mathrm{End}_A(E)$. Let $f, g \in R$ and $z \in E$, then

$$(f+g) \cdot z = \sum (a_i + b_i)\alpha^i(z) = \sum a_i \alpha^i(z) + \sum a_i \alpha^i(z) = f \cdot z + g \cdot z$$

Let $f, g \in R$ and $z \in E$, then

$$f \cdot (g \cdot z) = f \cdot \left( \sum_i b_i \alpha^i(z) \right) = \sum_k a_k \alpha^k \left( \sum_i b_i \alpha^i(z) \right) = \sum_k a_k \sum_i b_i \alpha^{k+i}(z) = \sum_j c_j \alpha^j(z)$$

where $c_j = \sum_l a_l b_{j-l}$. But this last expression is equal to $(fg) \cdot z)$. Now let $y, z \in E$ and $f \in R$, then

$$f \cdot (y+z) = \sum a_i \alpha^i(y+z) = \sum a_i \left( \alpha^i(y) + \alpha^i(z) \right) = \sum a_i \alpha^i(y) + \sum a_i \alpha^i(z) = f \cdot y + f \cdot z$$

That $1 \cdot z = z$ for all $z \in E$ is obvious, and hence $E$ can be extended from an $A$-module to an $A[x]$-module, given some $\alpha \in \mathrm{End}_A(E)$.

11. *Let $A$ be a commutative ring and $E, F$ be $A$-modules. Let $\alpha \in End_A(E)$ and $\beta \in End_A(F)$. Show that an $A$-lienar map $\eta : E \to F$ is an $A[x]$-linear map if $f \circ \alpha = \beta \circ f$.*

Let $E_\alpha$ and $E_\beta$ be as defined in the previous problem. Let $f \in A[x]$ and $z \in E$. Assume $\eta \circ \alpha = \beta \circ \eta$, then

$$\begin{aligned} \eta(f \cdot z) &= \eta \left( \sum a_i \alpha^i(z) \right) \\ &= \sum a_i \eta \left( \alpha^i(z) \right) \\ &= \sum a_i \beta^i \left( \eta(z) \right) \\ &= f \cdot \eta(z) \end{aligned}$$

The additive properties of $\eta$ certainly still hold as a function on $E_\alpha$, so it follows that $\eta$ is an $A[x]$-linear map.