Homework 8 Solutions

2 (a) Let $r \in R$. First assume that $x - r | f(x)$. Then we can write $f(x) = (x-r)q(x)$, and so $f(r) = (r-r)q(r) = 0q(r) = 0$. Now assume that $f(r) = 0$. Then we can write $f(x) = (x-r)q(x) + p(x)$, and $\deg p(x) < \deg(x-r) = 1$, and so $\deg p(x) = 0$, so $p(x) = p$ is a constant. So $f(r) = (r-r)q(r) + p = 0q(r) + p = p$, but $f(r) = 0$, so $p = 0$. Thus, $f(x) = (x-r)q(x)$, and so $x - r | f(x)$.

(b) Let $r_1, \ldots, r_m \in R$ distinct. First assume that $(x - r_1)\ldots(x - r_m)|f(x)$. Then $f(x) = (x-r_1)\ldots(x-r_m)q(x)$, and so $f(r_i) = 0$ for all i. Now assume that $f(r_i) = 0$ for all i. We proceed by induction. The first step was previous part. Now assume that this holds true for $m = k$, and we want to show it for $k+1$. As $f(r_1) = \ldots = f(r_k) = 0$, we have that $f(x) = (x-r_1)\ldots(x-r_k)q(x)$, by hypothesis. However, we also have that $f(r_{k+1}) = 0$, and so $f(r_{k+1}) = (r_{k+1}) - r_1)\ldots(r_{k+1} - r_k)q(r_{k+1}) = 0$. But $r_{k+1} - r_i \neq 0$ for all $1 \leq i \leq k$, and as R is a domain, that means that $q(r_{k+1}) = 0$. By the previous part, $q(x) = (x - r_{k+1})q'(x)$, and so $f(x) = (x - r_1)\ldots(x-r_k)q(x) = (x-r_1)\ldots(x-r_k)(x-r_{k+1})q'(x)$, and so $(x-r_1)\ldots(x-r_{k+1})|f(x)$, as desired.

(c) No. If $R = \mathbb{Z}/4\mathbb{Z}$, then look at $f(x) = x^2$. Then $(x-2) \not| x^2$, but $2^2 = 4 = 0$.

3 (a) Let $f(x)$ be a polynomial of degree n. Assume, for contradiction, that f has $n+1$ roots $a_1, \ldots, a_{n+1}$. Then, by problem 2, f is divisible by $(x-a_1)\ldots(x-a_{n+1}) = g(x)$. So $f(x) = q(x)g(x)$. But $\deg f(x) = n$, $\deg g(x) = n+1$, and $\deg q(x)g(x) = \deg q(x) + \deg g(x)$. Thus, $\deg q(x) = -1$, contradicting divisibility. Thus, $f(x)$ cannot have more than n roots.

(b) Let f, g of degree $< n$ and $a_1, \ldots, a_n \in F$ such that $f(a_i) = g(a_i)$ for all i. Define $h(x) = f(x) - g(x)$. Then $h(a_i) = f(a_i) - g(a_i) = 0$ for all i. Thus, h has at least n roots. However, $\deg h(x) = \deg(f(x) - g(x)) \leq \min\{\deg f(x), \deg g(x)\} < n$, and so $h(x)$ has fewer than n roots, a contraiction.

(c) Let $n = 1$, $f(x) = x$ and $g(x) = -x$. Then $f(0) = 0$, $g(0) = 0$ agree on one number, but they are distinct.

4 (a) Let $(y_1, \ldots, y_m)$ an R-basis of M. Define $f : M \to R^m$ by

$$f(\sum_{i=1}^{m} a_i y_i) = \sum_{i=1}^{m} a_i e_i.$$

We must show that this is a homomorphism, injective, and surjective. To see that it is a homomorphism, set $a = \sum a_i y_i$, $b = \sum b_i y_i$ and $r \in R$:

$$\begin{aligned}
f(a+b) &= f(\sum a_i y_i + \sum b_i y_i) \\
&= f(\sum (a_i + b_i) y_i) \\
&= \sum (a_i + b_i) e_i \\
&= \sum a_i e_i + \sum b_i e_i \\
&= f(\sum a_i y_i) + f(\sum b_i y_i) \\
&= f(a) + f(b) \\
f(ra) &= f(r \sum a_i y_i) \\
&= f(\sum r a_i y_i) \\
&= \sum r a_i e_i \\
&= r \sum a_i e_i \\
&= r f(\sum a_i y_i) \\
&= r f(a)
\end{aligned}$$

Now we must show that it is injective and surjective. Assume that $f(a) = 0$. Then $\sum a_i e_i = 0$, but e_i forms a basis for R^m, and so $a_i = 0$ for all i. Thus, f is injective. To see that it is surjective, let $\sum \alpha_i e_i \in R^m$. This is the image of $\sum \alpha_i y_i \in M$. Thus, surjective, and so f is an isomorphism.

Now start with $f : M \to R^m$ an isomorphism. Then $f^{-1} : R^m \to M$ is also an isomorphism. Let $y_i = f^{-1}(e_i)$. Then $y_1, \ldots, y_m$ is a basis for M. This is because every element of M can be written as $\sum a_i y_i$, because this is $\sum a_i f^{-1}(e_i) = f^{-1}(\sum a_i e_i)$, and f^{-1} is surjective. Similarly, every element can be written uniquely because f^{-1} is injective.

(b) Let $(y_1, \ldots, y_m)$ be an R-basis for M. Let $f_1, \ldots, f_m$ be the dual basis. Then the map $\phi : M \to M^*$ by $\phi(\sum a_i y_i) = \sum a_i f_i$ is an isomorphism. Similarly, if $\phi : M \to M^*$ is an isomorphism, then we can construct a basis as follows: let $y_1 \in M$ be arbitrary and not zero. Then let f_1 be $\phi(y_1)$. Find $y_2 \in \ker f_1$, it is linearly independent from y_2, and set $f_2 = \phi(y_2)$. Continue in this manner, choosing $y_i \in \ker f_1 \cap \ldots \ker f_{i-1}$ until you have a generating set $y_1, \ldots, y_m$. As $f_1, \ldots, f_m$ have $f_i(y_j) = \delta_{ij}$, it is the dual, and so the y_i form a basis, as desired.

5 (a) Let $f_1, f_2, f \in M^*$, $x_1, x_2, x \in M$ and $r \in R$. We first show that ϕ is bilinear.

$$\begin{aligned}
\phi(x, f_1 + f_2) &= (f_1 + f_2)(x) \\
&= f_1(x) + f_2(x) \\
&= \phi(x, f_1) + \phi(x, f_2) \\
\phi(x, rf) &= (rf)(x) \\
&= rf(x) \\
&= r\phi(x, f) \\
&= rf(x) \\
&= f(rx) \\
&= \phi(rx, f) \\
\phi(x_1 + x_2, f) &= f(x_1 + x_2) \\
&= f(x_1) + f(x_2) \\
&= \phi(x_1, f) + \phi(x_2, f)
\end{aligned}$$

Now we must show that ϕ is nondegenerate. As we are in the situation of the previous problem, let $y_1, \ldots, y_m$ a basis for M and $f_1, \ldots, f_m$ the dual basis for M^*. Then let $x = \sum a_i y_i \neq 0$. Then some $a_i \neq 0$. Then $\phi(x, f_i) = f_i(x) = a_i \neq 0$. Similarly, let $f = \sum a_i f_i \neq 0$, then some $a_i \neq 0$, and so $\phi(y_i, f) = f(y_i) = a_i \neq 0$. Thus, ϕ is nondegenerate.

(b) Let X be the set of R bases of M and Y the set of R bases of M^*. We want to show that ϕ induces a map $\bar{\phi} : X \to Y$ which is a bijection. Let $(y_1, \ldots, y_m) \in X$, that is, be a basis for M. Then set f_i be the unique map such that $\phi(y_j, f_i) = \delta_{ij}$. Then the set $(f_1, \ldots, f_m)$ is a basis of M^*, that is, an element of Y. Thus, we have a map $\bar{\phi} : X \to Y$. To see that it is injective, we set $y = (y_1, \ldots, y_m)$ and $x = (x_1, \ldots, x_m)$ in X such that $\bar{\phi}(x) = \bar{\phi}(y)$. Then $(f_1, \ldots, f_m) = (g_1, \ldots, g_m)$ as bases of M^*, that is, for the linear functions on M. So $f_i = g_i$, and so $f_i(x_j) = g_i(x_j) = \delta_{ij}$ and $f_i(y_j) = g_i(y_j) = \delta_{ij}$. So x and y have the same dual basis. Taking the dual of this basis, and referring to a previous problem set, we have that $x = y$. To see that it is surjective, we let $(f_1, \ldots, f_m) \in M^*$, and then take the dual basis in $(M^*)^* \cong M$, and note that $\bar{\phi}$ will map this to $(f_1, \ldots, f_m)$. Thus, we have a bijection.

7 (a) To see that A' is a basis, we note that $|A'| = |A|$, and so it is enough to show that for all $a \in A$, we have $a \in \text{span}A'$. For $i \neq 0$, we

have $X^i = p_i - p_{i-1}$, and for $i = 0$ we have $X^0 = p_0$. Thus, A' is a basis. The transition matrix must take $\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = 1$ to itself, and similarly the other standard basis vectors such that To see that A' is a basis, we note that $|A'| = |A|$, and so it is enough to show that for all $a \in A$, we have $a \in \text{span} A'.e_i \mapsto \begin{pmatrix} 1 \\ \vdots \\ 1 \\ 0 \\ vdots \\ 0 \end{pmatrix}$, with i ones. The matrix which does this is

$$T = \begin{pmatrix} 1 & 1 & \cdots & \cdots & 1 \\ 0 & 1 & \cdots & \cdots & 1 \\ 0 & 0 & 1 & \cdots & 1 \\ \vdots & \cdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

(b) To see that B' is a basis, we note that $|B'| = |B|$, and so it is enough to show that for all $b \in B$, we have $b \in \text{span} B'$. For $i \neq n$, we have $e_i = f_i + f_n$ and for $i = n$, we have $e_n = f_n$, and so B' is a basis. For this, we must send the vector e_i to $f_i = e_i - e_n$, and so the matrix must be

$$S = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & \ddots & \cdots & 0 \\ \vdots & 0 & \cdots & \ddots & 0 \\ -1 & -1 & \cdots & -1 & 1 \end{pmatrix}$$

(c) The matrix of f in bases A and B is the identity. Because A and B are the standard bases for their spaces, and we end up taking the ith standard basis vector to the ith standard basis vector. For the matrix of f in terms of A' and B', we need to do more work. We can do this by noting that our map is $Pol \overset{T}{P} ol \xrightarrow{f} F^n \xrightarrow{S^{-1}} F^n$ by changing basis, performing f, then changing back. This gives the identity map because it is the map from the basis A to the basis B. Thus, we have $S^{-1} \circ f \circ T = \text{id}$. Thus, $f = ST^{-1}$. Computing this gives

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 1 & \cdots & 1 \\ 0 & 0 & \ddots & \cdots & 1 \\ \vdots & 0 & \cdots & 1 & 1 \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}$$