

Algebraic Structures II, MAT 574, Homework 9

Part I

Chapter 16

4. If R is a commutative ring, show that the characteristic of $R[x]$ is the same as the characteristic of R .

Proof. Let m be the characteristic of R . Then $m \cdot r = 0$ for every element $r \in R$ (Definition 12.7 in the lecture note.) For every element $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in R[x]$, we get

$$m \cdot f(x) = (ma_n)x^n + (ma_{n-1})x^{n-1} + \cdots + (ma_1)x + (ma_0) = 0x^n + \cdots + 0x + 0 = 0.$$

In order to show that such m is the least positive integer satisfying $mf(x) = 0$ for every element $f(x) \in R[x]$, suppose that there exists a positive integer l such that $lf(x) = 0$ for every element $f(x) \in R[x]$. In particular, for all constant polynomials $g(x) = a_0 \in R[x]$, where $a_0 \in R$, we have $lg(x) = la_0 = 0$ for all $a_0 \in R$. Since m is the characteristic of R , this means that $m \leq l$. □

9. If $\phi : R \rightarrow S$ is a ring homomorphism, define $\bar{\phi} : R[x] \rightarrow S[x]$ by

$$a_n x^n + \cdots + a_1 x + a_0 \mapsto \phi(a_n)x^n + \cdots + \phi(a_1)x + \phi(a_0).$$

Show that $\bar{\phi}$ is a ring homomorphism.

Proof. Let $f(x) = a_n x^n + \cdots + a_1 x + a_0$ and $g(x) = b_m x^m + \cdots + b_1 x + b_0$ be arbitrary elements of $R[x]$. Let $s = \max(n, m)$. Then

$$f(x) + g(x) = (a_s + b_s)x^s + (a_{s-1} + b_{s-1})x^{s-1} + \cdots + (a_1 + b_1)x + a_0 + b_0,$$

where we let $a_i = 0$ for all $i > n$ and $b_j = 0$ for all $j > m$. Therefore

$$\bar{\phi}(f(x) + g(x)) = \phi(a_s + b_s)x^s + \phi(a_{s-1} + b_{s-1})x^{s-1} + \cdots + \phi(a_1 + b_1)x + \phi(a_0 + b_0),$$

where $\phi(a_k + b_k) = \phi(a_k) + \phi(b_k)$ for all $k = 1, \dots, s$ because ϕ is a ring homomorphism. Since $\phi(0) = 0$, we have $\phi(a_i) = 0$ for all $i > n$ and $\phi(b_j) = 0$ for all $j > m$. Therefore

$$\bar{\phi}(f(x) + g(x)) = \bar{\phi}(f(x)) + \bar{\phi}(g(x)).$$

For the multiplication operation, we have

$$f(x)g(x) = c_{m+n}x^{m+n} + c_{m+n-1}x^{m+n-1} + \cdots + c_1x + c_0,$$

where $c_k = a_k b_0 + a_{k-1} b_1 + \cdots + a_1 b_{k-1} + a_0 b_k = \sum_{i=0}^k a_{k-i} b_i$ for each $k = 1, \dots, m+n$. Then since ϕ is a ring homomorphism, we obtain

$$\phi(c_k) = \phi\left(\sum_{i=0}^k a_{k-i} b_i\right) = \sum_{i=0}^k \phi(a_{k-i} b_i) = \sum_{i=0}^k \phi(a_{k-i}) \phi(b_i).$$

Hence

$$\overline{\phi}(f(x)g(x)) = \sum_{k=0}^{m+n} \phi(c_k) x^k = \sum_{k=0}^{m+n} \left(\sum_{i=0}^k \phi(a_{k-i}) \phi(b_i) \right) x^k = \overline{\phi}(f(x)) \overline{\phi}(g(x)).$$

□

10. If the rings R and S are isomorphic, show that $R[x]$ and $S[x]$ are isomorphic.

Proof. Let $\phi : R \rightarrow S$ be an isomorphism. Let $\overline{\phi} : R[x] \rightarrow S[x]$ be the map such that $\overline{\phi}(f(x)) = \sum_{i=0}^n \phi(a_i) x^i$ for every element $f(x) = \sum_{i=0}^n a_i x^i \in R[x]$. Then by Problem 9, this map $\overline{\phi}(x)$ is a ring homomorphism. We claim that $\overline{\phi}$ is an isomorphism if ϕ is an isomorphism. In order to show that $\overline{\phi}$ is one-to-one, we compute the kernel of $\overline{\phi}$:

$$\begin{aligned} \ker(\overline{\phi}) &= \left\{ f(x) = \sum_{i=0}^n a_i x^i \in R[x] \mid \overline{\phi}(f(x)) = \sum_{i=0}^n \phi(a_i) x^i = 0 \right\} \\ &= \left\{ f(x) = \sum_{i=0}^n a_i x^i \in R[x] \mid \phi(a_i) = 0 \text{ for all } i \right\} \\ &= \left\{ f(x) = \sum_{i=0}^n a_i x^i \in R[x] \mid a_i \in \ker \phi \text{ for all } i \right\}. \end{aligned}$$

Hence if ϕ is one-to-one, then $\ker \phi = 0$ so that $\ker(\overline{\phi}) = 0$.

In order to show that $\bar{\phi}$ is onto, let $g(x) = \sum_{i=0}^m s_i x^i \in S[x]$. Then for each i , since $s_i \in S$ and ϕ is onto, there exists $r_i \in R$ such that $\phi(r_i) = s_i$. Let $f(x) = \sum_{i=0}^m r_i x^i \in R[x]$. Then

$$\bar{\phi}(f(x)) = \sum_{i=0}^m \phi(r_i) x^i = \sum_{i=0}^m s_i x^i = g(x).$$

□

11. Let $f(x) = x^3 + 2x + 4$ and $g(x) = 3x + 2$ in $\mathbb{Z}_5[x]$. Determine the quotient and remainder upon dividing $f(x)$ by $g(x)$.

Proof.

$$f(x) = (2x^2 + 2x + 1)g(x) + 2.$$

□

22. Prove that $\mathbb{Z}[x]$ is not a principal ideal domain.

Proof. As a counterexample, let I be the ideal of all polynomials in $\mathbb{Z}[x]$ that have a constant term in $2\mathbb{Z}$. We show that the ideal I is not a principal ideal. In other words, we show that there is no $g(x) \in \mathbb{Z}[x]$ such that $I = (g(x))$.

Suppose there is $g(x) \in \mathbb{Z}[x]$ such that $I = (g(x))$. Since all the even-constant polynomials $c(x) = 2n$ in $\mathbb{Z}[x]$ are in I , we have $c(x) = k(x)g(x)$ for $k(x) \in \mathbb{Z}[x]$. Since \mathbb{Z} is an integral domain, by Corollary 16.5 in the lecture note, $0 = \deg(c(x)) = \deg(k(x)) + \deg(g(x))$ so that $g(x) = 2m$ is a constant polynomial. Consider

$$f(x) = mx + 2.$$

Then $f(x) \in I$ so that $f(x) = h(x)g(x)$ for some $h(x) \in \mathbb{Z}[x]$. Again, since \mathbb{Z} is an integral domain, by Corollary 16.5 in the lecture note, $1 = \deg(f(x)) = \deg(h(x)) + \deg(g(x)) = \deg(h(x))$ so that $h(x) = \alpha x + \beta$, where $\alpha, \beta \in \mathbb{Z}$. Therefore $f(x) = h(x)g(x)$ implies that

$$mx + 2 = (\alpha x + \beta)(2m) = 2m\alpha x + 2m\beta.$$

Therefore $m = 2m\alpha$ or $\alpha = \frac{1}{2}$ (since $m \neq 0$), which is a contradiction because $\alpha \in \mathbb{Z}$. □

31. For every prime p , show that

$$x^{p-1} - 1 = (x-1)(x-2)\cdots[x-(p-1)]$$

in $\mathbb{Z}_p[x]$.

Proof. First we claim that $a^{p-1} = 1$ in \mathbb{Z}_p for every nonzero element $a \in \mathbb{Z}_p$. For every prime p , \mathbb{Z}_p is a field (Corollary 13.14 in the lecture note). In particular, the set \mathbb{Z}_p^* of nonzero elements form a group under multiplication (Remark 13.12 in the lecture note). Hence for every nonzero element $a \in (\mathbb{Z}_p^*, \cdot)$, the order of a divides the order of group (\mathbb{Z}_p^*, \cdot) , which is $p-1$ (Lagrange Theorem, Theorem R.13 in the lecture note). Therefore $a^{p-1} = 1$ in \mathbb{Z}_p .

Let $f(x) = x^{p-1} - 1$ in $\mathbb{Z}_p[x]$. Then by the above claim every nonzero element $a \in \mathbb{Z}_p$ is a zero of $f(x)$. Therefore by Corollary 16.11 in the lecture note, $x-a$ divides $f(x)$ for every nonzero element $a \in \mathbb{Z}_p$. Hence

$$f(x) = (x-1)(x-2)\cdots(x-(p-1))g(x)$$

for some $g(x) \in \mathbb{Z}_p[x]$. Since \mathbb{Z}_p is a domain, by Corollary 16.5, we can compare the degrees:

$$p-1 = \deg(f(x)) = \deg(x-1) + \deg(x-2) + \cdots + \deg(x-(p-1)) + \deg(g(x)) = p-1 + \deg(g(x)),$$

which shows that $g(x) = c$ for some constant c . Moreover this $c = 1$ because the leading coefficient of $f(x)$ is 1. \square

36. If I is an ideal of a ring R , prove that $I[x]$ is an ideal of $R[x]$.

Proof. Recall that $I[x] = \left\{ \sum_{i=0}^n a_i x^i \in R[x] \mid a_i \in I \right\}$. Use Theorem 14.3 in the lecture

note. Let $f(x) = \sum_{i=0}^n a_i x^i$ and $g(x) = \sum_{i=0}^m b_i x^i$ be elements of $I[x]$. Let $s = \max(n, m)$. Then

$$f(x) - g(x) = (a_s - b_s)x^s + (a_{s-1} - b_{s-1})x^{s-1} + \cdots + (a_1 - b_1)x + a_0 - b_0,$$

where we let $a_i = 0$ for all $i > n$ and $b_j = 0$ for all $j > m$. Since for every i , $a_i - b_i \in I$, we get $f(x) - g(x) \in I[x]$.

Let $h(x) = \sum_{i=0}^l d_i x^i \in R[x]$ and $f(x) = \sum_{i=0}^n a_i x^i \in I[x]$. Then

$$h(x)f(x) = c_{l+n}x^{l+n} + c_{l+n-1}x^{l+n-1} + \cdots + c_1x + c_0,$$

where $c_k = d_k a_0 + d_{k-1} a_1 + \cdots + d_1 a_{k-1} + d_0 a_k = \sum_{i=0}^k d_{k-i} a_i$ for each $k = 1, \dots, l+n$. Since $a_i \in I$ for all i , we have $c_k = \sum_{i=0}^k d_{k-i} a_i \in I$, or $h(x)f(x) \in I[x]$. \square

38. Let R be a commutative ring with unity. if I is a prime ideal of R , prove that $I[x]$ is a prime ideal of $R[x]$.

Proof. Let $\phi : R \rightarrow R/I$ be the natural ring homomorphism, i.e., $\phi(r) = r + I$. Then by Problem 9, the induced map $\bar{\phi} : R[x] \rightarrow (R/I)[x]$ is a ring homomorphism. Recall that

$$\bar{\phi}(a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0) = (a_n + I)x^n + (a_{n-1} + I)x^{n-1} + \cdots + (a_1 + I)x + (a_0 + I).$$

It is clear that this map $\bar{\phi}$ is onto. Now we claim that $\ker(\bar{\phi}) = I[x]$.

$$\begin{aligned} \ker(\bar{\phi}) &= \left\{ f(x) = \sum_{i=0}^n a_i x^i \in R[x] \mid \bar{\phi}(f(x)) = \sum_{i=0}^n \phi(a_i) x^i = 0 \right\} \\ &= \left\{ f(x) = \sum_{i=0}^n a_i x^i \in R[x] \mid \phi(a_i) = a_i + I = I \text{ for all } i \right\} \\ &= \left\{ f(x) = \sum_{i=0}^n a_i x^i \in R[x] \mid a_i \in I \text{ for all } i \right\} \\ &= I[x] \end{aligned}$$

Hence by Theorem 15.8 in the lecture note, $R[x]/I[x]$ is isomorphic to $(R/I)[x]$. Since I is a prime ideal of R , the factor ring R/I is a domain. Then by Theorem 16.3 in the lecture note, $(R/I)[x]$ is a domain. Hence by the isomorphism, $R[x]/I[x]$ is a domain, which proves that $I[x]$ is a prime ideal. \square

Part II

1. Let $\phi : R \rightarrow S$ be a ring homomorphism. Define $\bar{\phi} : R[x] \rightarrow S[x]$ by

$$a_n x^n + \cdots + a_1 x + a_0 \mapsto \phi(a_n) x^n + \cdots + \phi(a_1) x + \phi(a_0).$$

Prove that ϕ is one-to-one if and only if $\bar{\phi}$ is one-to-one.

Proof. We claim that $\ker(\bar{\phi}) = (\ker(\phi))[x]$. Recall that in Problem 10, we showed that

$$\begin{aligned} \ker(\bar{\phi}) &= \left\{ f(x) = \sum_{i=0}^n a_i x^i \in R[x] \mid \bar{\phi}(f(x)) = \sum_{i=0}^n \phi(a_i) x^i = 0 \right\} \\ &= \left\{ f(x) = \sum_{i=0}^n a_i x^i \in R[x] \mid \phi(a_i) = 0 \text{ for all } i \right\} \\ &= \left\{ f(x) = \sum_{i=0}^n a_i x^i \in R[x] \mid a_i \in \ker \phi \text{ for all } i \right\} \\ &= (\ker(\phi))[x]. \end{aligned}$$

Hence $\ker(\bar{\phi}) = 0$ if and only if $\ker(\phi) = 0$. □

2. Let R and S be commutative rings. Let $\phi : R \rightarrow S$ be a ring homomorphism and α an element of S . Define $\zeta_\alpha : R[x] \rightarrow S$ by

$$a_n x^n + \cdots + a_1 x + a_0 \mapsto \phi(a_n) \alpha^n + \cdots + \phi(a_1) \alpha + \phi(a_0).$$

Prove that ζ_α is a ring homomorphism.

(This map ζ_α is called an *evaluation homomorphism* at α with respect to ϕ .)

Proof. Let $f(x) = a_n x^n + \cdots + a_1 x + a_0$ and $g(x) = b_m x^m + \cdots + b_1 x + b_0$ be arbitrary elements of $R[x]$. Let $s = \max(n, m)$. Then

$$f(x) + g(x) = (a_s + b_s) x^s + (a_{s-1} + b_{s-1}) x^{s-1} + \cdots + (a_1 + b_1) x + a_0 + b_0,$$

where we let $a_i = 0$ for all $i > n$ and $b_j = 0$ for all $j > m$. Therefore

$$\zeta_\alpha(f(x) + g(x)) = \phi(a_s + b_s) \alpha^s + \phi(a_{s-1} + b_{s-1}) \alpha^{s-1} + \cdots + \phi(a_1 + b_1) \alpha + \phi(a_0 + b_0),$$

where $\phi(a_k + b_k) = \phi(a_k) + \phi(b_k)$ for all $k = 1, \dots, s$ because ϕ is a ring homomorphism. Since $\phi(0) = 0$, we have $\phi(a_i) = 0$ for all $i > n$ and $\phi(b_j) = 0$ for all $j > m$. Therefore

$$\zeta_\alpha(f(x) + g(x)) = \zeta_\alpha(f(x)) + \zeta_\alpha(g(x)).$$

For the multiplication operation, we have

$$f(x)g(x) = c_{m+n}x^{m+n} + c_{m+n-1}x^{m+n-1} + \dots + c_1x + c_0,$$

where $c_k = a_k b_0 + a_{k-1} b_1 + \dots + a_1 b_{k-1} + a_0 b_k = \sum_{i=0}^k a_{k-i} b_i$ for each $k = 1, \dots, m+n$. Then since ϕ is a ring homomorphism, we obtain

$$\phi(c_k) = \phi\left(\sum_{i=0}^k a_{k-i} b_i\right) = \sum_{i=0}^k \phi(a_{k-i} b_i) = \sum_{i=0}^k \phi(a_{k-i}) \phi(b_i).$$

Hence

$$\zeta_\alpha(f(x)g(x)) = \sum_{k=0}^{m+n} \phi(c_k) \alpha^k = \sum_{k=0}^{m+n} \left(\sum_{i=0}^k \phi(a_{k-i}) \phi(b_i)\right) \alpha^k = \zeta_\alpha(f(x)) \zeta_\alpha(g(x)).$$

□

3. Let $R = M_2(\mathbb{Z})$ be the ring of 2×2 matrices with integral entries. Let $C = \begin{bmatrix} 1 & 2 \\ 2 & 3 \end{bmatrix}$.

Define $\sigma : R[x] \rightarrow R$ by

$$A_n x^n + A_{n-1} x^{n-1} + \dots + A_1 x + A_0 \mapsto A_n C^n + A_{n-1} C^{n-1} + \dots + A_1 C + A_0.$$

Prove or disprove that σ is a ring homomorphism.

(This problem will show whether it is necessary to assume that the rings R and S in Problem 2 are commutative rings. Notice that with the notation in Problem 2, this map σ is ζ_C .)

Proof. Let $f(x) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} x + \begin{bmatrix} -1 & 1 \\ 2 & -1 \end{bmatrix}$ and $g(x) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} x - \begin{bmatrix} -1 & 1 \\ 2 & -1 \end{bmatrix}$ be the elements of $R[x]$. Let $A = \begin{bmatrix} -1 & 1 \\ 2 & -1 \end{bmatrix}$. Then

$$\sigma(f(x)g(x)) = \sigma\left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} x^2 - A^2\right) = C^2 - A^2 \neq (C + A)(C - A) = \sigma(f(x))\sigma(g(x)),$$

which shows that σ is not a ring homomorphism. □