66. For the polynomial $a(x) = 2 + x + 2x^2 + x^3 + 0x^4 + 2x^5$ in $\mathbb{Z}_3[x]$, calculate $a(c)$ for every $c \in \mathbb{Z}_3$. Are there any roots for $a(x)$ in $\mathbb{Z}_3$?

$$a(0) = 2 \quad a(1) = 2 \quad a(2) = 0$$

The only root of $a(x)$ in $\mathbb{Z}_3$ is 2.

67. Suppose A and K are commutative rings with unity and $f : A \to K$ is a nonzero ring homomorphism. Prove: If $c \in A$ is a root for $a(x) \in A[x]$ then $f(c)$ is a root for $\overline{f}(a(x))$ in $K[x]$.

Suppose A and K are commutative rings with unity and $f : A \to K$ is a nonzero ring homomorphism. Let $c \in A$ be a root for $a(x) \in A[x]$. Thus $a(c) = 0_A$.

$$a(x) = \sum_{i=0}^{n} a_i x^i \qquad \overline{f}(a(x)) = \sum_{i=0}^{n} f(a_i) x^i$$

By definition $a(c) = \sum_{i=0}^{n} a_i c^i$ and $\overline{f}(f(c)) = \sum_{i=0}^{n} f(a_i)((f(c))^i$. We see that $\overline{f}(f(c)) = 0_K$ below, so $f(c)$ is a root of $\overline{f}(a(x))$ in $K[x]$

Answers for Chapter 7 Exercises

$$\overline{f}(f(c)) = \sum_{i=0}^{n} f(a_i)((f(c))^i = \sum_{i=0}^{n} f(a_ic^i) = f\left(\sum_{i=0}^{n} a_ic^i\right) = f(a(c)) = f(0_A) = 0_K$$

68. Complete the proof of Theorem 7.35 by showing that $h_c(a(x) + b(x)) = a(c) + b(c) = h_c(a(x)) + h_c(b(x))$ for $a(x), b(x) \in A[x]$.

    Let A be an integral domain and $c \in A$. Recall $h_c : A[x] \to A$ is defined by $h_c(a(x)) = a(c)$. Let $a(x), b(x) \in A[x]$, and denote $d(x) = a(x) + b(x)$. We need to show that $h_c(d(x)) = a(c) + b(c)$.

$$a(x) = \sum_{i=0}^{n} a_ix^i \qquad b(x) = \sum_{i=0}^{n} b_ix^i \qquad d(x) = \sum_{i=0}^{n} d_ix^i$$

    Using the fact that $d_i = a_i + b_i$ for each i we see that :

$$h_c(d(x)) = d(c) = \sum_{i=0}^{n} d_ic^i = \sum_{i=0}^{n}(a_i + b_i)c^i = \sum_{i=0}^{n}(a_ic^i + b_ic^i) = \sum_{i=0}^{n} a_ic^i + \sum_{i=0}^{n} b_ic^i$$

    Thus $h_c(d(x)) = a(c) + b(c) = h_c(a(x)) + h_c(b(x))$ as we needed to show.

69. Suppose A is an integral domain and $a(x) \in A[x]$ with $a(x) \neq 0(x)$. Prove: If $a_0 = 0_A$ then 0_A is a root of $a(x)$.

    Assume A is an integral domain and $a(x) \in A[x]$ with $a(x) \neq 0(x)$. Thus $a(0_A) = \sum_{i=0}^{n} a_i(0_A)^i$. For $i > 0$ we know $(0_A)^i = 0_A$ and $(0_A)^0 = 1_A$, so $a(0_A) = a_0 + 0_A$. Since we assumed that $a_0 = 0_A$ then $a(0_A) = 0_A$ and 0_A is a root of $a(x)$.

70. Define $S = \{a(x) \in \mathbb{Z}[x] : a(0) = 0 \text{ and } a(2) = 0\}$. Prove that S is an ideal of $\mathbb{Z}[x]$.

    Let $S = \{a(x) \in \mathbb{Z}[x] : a(0) = 0 \text{ and } a(2) = 0\}$. Clearly $S \subseteq \mathbb{Z}[x]$. Since the zero polynomial $0(x)$ has $0(0) = 0$ and $0(2) = 0$ then $0(x) \in S$ and $S \neq \emptyset$. Let $a(x), b(x) \in S$. Using the fact that the substitution function is a ring homomorphism we find for $c(x) = a(x) - b(x)$ that $c(0) = a(0) - b(0) = 0 - 0 = 0$ and $c(2) = a(2) - b(2) = 0 - 0 = 0$. Thus we know $c(x) \in S$ and S is closed under subtraction. Now let $a(x) \in S$ and $p(x) \in \mathbb{Z}[x]$. Then for $d(x) = a(x)p(x)$ we find $d(0) = a(0)p(0) = 0 \cdot p(0) = 0$ and $d(2) = a(2)p(2) = 0 \cdot p(2) = 0$. Thus $d(x) \in S$ and S absorbs products from $\mathbb{Z}[x]$. Hence S is an ideal of $\mathbb{Z}[x]$.

1. Prove: If K is a field and $a(x) \in K[x]$ then every nonzero constant polynomial in $K[x]$ is a factor of $a(x)$.

Assume K is a field and $a(x) \in K[x]$. Let $c(x) = c_0$ be a constant polynomial, with $c_0 \neq 0$. Since K is a field then c_0 is a unit, so there is $q \in K$ with $qc_0 = 1_K$. Define $b(x) = qa(x)$. Then $q(x) \in K[x]$ and $c(x)q(x) = c_0qa(x) = a(x)$. Thus $c(x)$ is a factor of $a(x)$.

4. Find nonzero polynomials $a(x), b(x) \in \mathbb{Z}_{10}[x]$ which are associates but $deg(a(x)) \neq deg(b(x))$.

   (Answers will vary.) Let $a(x) = 2 + 5x + 3x^2 + 5x^3$ and $b(x) = 4 + 0x + 6x^2$. Then clearly $deg(a(x)) \neq deg(b(x))$. But for $c = 2$ we have $c \in \mathbb{Z}_{10}$ and $ca(x) = b(x)$.

5. Suppose K is a field and $a(x) \in K[x]$ with $a(x) \neq 0(x)$. Prove: If $b(x), c(x) \in K[x]$ with $a(x) = b(x)c(x)$ and $deg(c(x)) \neq 0$, then $deg(b(x)) < deg(a(x))$.

   Suppose K is a field and $a(x) \in K[x]$ with $a(x) \neq 0(x)$. Assume we have $b(x), c(x) \in K[x]$ with $a(x) = b(x)c(x)$ and $deg(c(x)) \neq 0$. Let $deg(c(x)) = n$ and $deg(a(x)) = m$, so we know $n > 0$ and $m \geq 0$. If $b(x) = 0(x)$ then $a(x) = 0(x)c(x) = 0(x)$ but we assumed $a(x) \neq 0(x)$, so we must have $b(x) \neq 0(x)$ as well. Let $deg(b(x)) = k$. We know $deg(b(x)) \geq 0$.

   We want to show that $k < m$ so assume instead that $k \geq m$. By K a field, Theorem 7.20 tells us that $deg(a(x)) = deg(b(x)) + deg(c(x)$ so $m = k + n$. Since $n, m, k \in \mathbb{Z}$ we know that if $k > m$ then $k + n > m + n$. Thus $m > m + n$ or $0 > n$. However $n > 0$ tells us this is a contradiction. Thus we must have $m = k$ and so $m + n = n + k$ or $m + n = m$. Subtracting we have $n = 0$ which again contradicts $n > 0$. Hence $k \geq m$ is impossible and we must have $k < m$ as needed.

19. Find two nonconstant polynomials $a(x), b(x) \in \mathbb{Z}_5[x]$ which have exactly the same roots in $\mathbb{Z}_5$ but are not associates.

Let $a(x) = 1 + 4x$ and $b(x) = 1 + 3x + x^2$. Since the polynomials have different degrees they are not associates (exercise 3). From the list below we see both have only 1 as a root, thus they have the same roots.

$$\begin{array}{lllll} a(0) = 1 & a(1) = 0 & a(2) = 4 & a(3) = 3 & a(4) = 2 \\ b(0) = 1 & b(1) = 0 & b(2) = 1 & b(3) = 4 & b(4) = 4 \end{array}$$

25. Prove Theorem 8.12.

Let K be a field and assume $p(x) \in K[x]$ is irreducible over K. Suppose we have $a(x), b(x) \in K[x]$ and $p(x)$ is a factor of $a(x)b(x)$. Since $p(x)$ is irreducible over K then by Theorem 8.11 the ideal $S = \langle p(x) \rangle$ is a maximal ideal of $K[x]$. But by Theorem 6.23 we now have S as a prime ideal as well. Since $a(x)b(x) \in S$ and S is prime we know that either $a(x) \in S$ or $b(x) \in S$. If $a(x) \in S$ then $a(x) = p(x)q(x)$ for some $q(x) \in K[x]$ so $p(x)$ is a factor of $a(x)$. Similarly if $b(x) \in S$ then $b(x) = p(x)r(x)$ for some $r(x) \in K[x]$ so $p(x)$ is a factor of $b(x)$. Thus either $p(x)$ is a factor of $a(x)$ or $p(x)$ is a factor of $b(x)$ as needed.

28. Show that the assumption of $p(x)$ irreducible in Theorem 8.12 was needed, by finding non-constant polynomials $a(x), b(x), c(x) \in \mathbb{Z}_5[x]$ so that $b(x)$ is a factor of $a(x)c(x)$ but $b(x)$ is not a factor of either $a(x)$ or $c(x)$.

Let $a(x) = 1+3x+3x^2+x^3$, $b(x) = 3+4x+x^2$, and $c(x) = 2+2x+4x^2+x^3$. Notice that $b(x)$ is reducible by $b(x) = (3+x)(1+x)$ Also $a(x)c(x) = b(x)(4+4x+2x^2+3x^3+x^4)$. But when using the division algorithm $a(x) = b(x)(4+x)+(4+4x)$ and $c(x) = b(x)(0+x)+(2+4x)$ so $b(x)$ is not a factor of either $a(x)$ or $b(x)$.