

H/wk 13, Solutions to selected problems

Ch. 4.1, Problem 5

(a) Find the number of roots of $x^2 - x$ in \mathbb{Z}_4 , $\mathbb{Z}_2 \times \mathbb{Z}_2$, any integral domain, \mathbb{Z}_6 .

(b) Find a commutative ring in which $x^2 - x$ has infinitely many roots.

Solution.

(a) By a direct check we verify that the only roots of $x^2 - x = 0$ in \mathbb{Z}_4 are $\bar{0}$ and $\bar{1}$. Thus $x^2 - x = 0$ has 2 roots in \mathbb{Z}_4 .

For every element a of \mathbb{Z}_2 we have $a^2 = a$ and hence for every $(a, b) \in \mathbb{Z}_2 \times \mathbb{Z}_2$ we have $(a, b)^2 = (a^2, b^2) = (a, b)$, so that (a, b) is a root of $x^2 - x = 0$. Thus $x^2 - x = 0$ has $|\mathbb{Z}_2 \times \mathbb{Z}_2| = 4$ roots in $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Suppose now that R is an integral domain. It is easy to see that $x = 0$ and $x = 1$ are roots of $x^2 - x = 0$ in R . We claim that there are no other roots. Indeed, suppose $a \in R$ is a root, so that $a^2 - a = 0$ in R . Then $0 = a^2 - a = a(a - 1)$. Since R is an integral domain, it follows that either $a = 0$ or $a - 1 = 0$, that is, either $a = 0$ or $a = 1$. Thus $x^2 - x = 0$ has exactly 2 roots in R .

By a direct check we verify that $x^2 - x = 0$ has exactly 4 roots in \mathbb{Z}_6 , namely $\bar{0}$, $\bar{1}$, $\bar{3}$ and $\bar{4}$.

(b) Consider the ring $R = \mathbb{Z}_2^\infty$ where $R = \{(a_1, a_2, a_3, \dots) | a_i \in \mathbb{Z}_2\}$ and where

$$\begin{aligned} (a_1, a_2, a_3, \dots) + (b_1, b_2, b_3, \dots) &= (a_1 + b_1, a_2 + b_2, a_3 + b_3, \dots) \\ (a_1, a_2, a_3, \dots) \cdot (b_1, b_2, b_3, \dots) &= (a_1 b_1, a_2 b_2, a_3 b_3, \dots) \end{aligned}$$

for $a_i, b_i \in \mathbb{Z}_2$.

It is easy to see that R is a commutative ring. Moreover, since for every $a \in \mathbb{Z}_2$ we have $a^2 = a$, it follows that for every $x = (a_1, a_2, a_3, \dots) \in R$ we have

$$x^2 = (a_1^2, a_2^2, a_3^2, \dots) = (a_1, a_2, a_3, \dots) = x \text{ and hence } x^2 - x = 0.$$

Since $R = \mathbb{Z}_2^\infty$ is also infinite and commutative, it satisfies all the required properties.

Ch. 4.1, Problem 17

In each case factor $f(x)$ into linear factors in $F[x]$.

(a) $f(x) = x^4 + 12$, $F = \mathbb{Z}_{13}$.

Solution.

We have $\bar{12} = \overline{-1}$ in \mathbb{Z}_{13} . Hence in $\mathbb{Z}_{13}[x]$ we have $x^4 + 12 = x^4 - 1 = x^4 - 1^2 = (x^2 - 1)(x^2 + 1)$.

Moreover, in \mathbb{Z}_{13} we have $\bar{1} = \overline{-25} = \overline{-5^2}$. Hence in $\mathbb{Z}_{13}[x]$ we have

$$x^4 + 12 = (x^2 - 1)(x^2 + 1) = (x^2 - 1^2)(x^2 - 5^2) = (x - 1)(x + 1)(x - 5)(x + 5).$$

(b) $f(x) = x^3 + 1$, $F = \mathbb{Z}_7$.

Solution.

In \mathbb{Z}_7 we have $-1^3 + 1 = 0$, so that -1 is a root of $f(x) = x^3 + 1$ in \mathbb{Z}_7 . Hence $(x + 1) | f(x)$ in $\mathbb{Z}_7[x]$. By performing division with the remainder, we get $x^3 + 1 = (x + 1)(x^2 - x + 1)$ in $\mathbb{Z}_7[x]$. We then look for roots of $x^2 - x + 1$ in \mathbb{Z}_7 . It is easy to see that 3 is such a root since $3^2 - 3 + 1 = 7 \equiv 0 \pmod{7}$. Dividing

$x^2 - x + 1$ with the remainder by $x - 3$ in $\mathbb{Z}_7[x]$ we get $x^2 - x + 1 = (x - 3)(x + 2)$ in $\mathbb{Z}_7[x]$. Hence

$$x^3 + 1 = (x + 1)(x - 3)(x + 2)$$

in $\mathbb{Z}_7[x]$.

Ch. 4.1, Problem 23

In each case determine the multiplicity of a as a root of $f(x)$.

(b) $f(x) = x^4 + 2x^2 + 2x + 2$, $a = -1$, $R = \mathbb{Z}_3$.

Solution.

Dividing $f(x)$ by $x + 1$ with the remainder in $\mathbb{Z}_3[x]$, we get:

$$f(x) = x^4 + 2x^2 + 2x + 2 = (x + 1)(x^3 - x^2 + 2) \text{ in } \mathbb{Z}_3[x].$$

Observe that $a = -1$ is a root of $x^3 - x^2 + 2$ in $\mathbb{Z}_3[x]$. Dividing $x^3 - x^2 + 2$ by $x + 1$ in $\mathbb{Z}_3[x]$, we get:

$$x^3 - x^2 + 2 = (x + 1)(x^2 - 2x + 2)$$

We see that $1^2 - 2 \cdot 1 + 2 = 1 \neq 0$ in \mathbb{Z}_3 , so that $a = -1$ is not a root of $x^2 - 2x + 2$ in $\mathbb{Z}_3[x]$. Hence the multiplicity of $a = -1$ as a root of $f(x)$ in $\mathbb{Z}_3[x]$ is equal to 2.

Ch. 4.1, Problem 24

If R is a commutative ring, a polynomial $f(x)$ in $R[x]$ is said to **annihilate** R if $f(a) = 0$ for every $a \in R$.

(a) Show that $x^p - x$ annihilates \mathbb{Z}_p for a prime $p \geq 2$.

Solution.

By Fermat's theorem, for every $a \in \mathbb{Z}$ we have $a^p \equiv a \pmod{p}$, that is $\bar{a}^p = \bar{a}$, $\bar{a}^p - \bar{a} = \bar{0}$ in \mathbb{Z}_p .

Thus indeed $x^p - x$ annihilates \mathbb{Z}_p .

(b) Show that $x^5 - x$ annihilates \mathbb{Z}_{10} .

Solution.

Can be verified via a direct check and also follows from (c).

(c) Show that if $p \neq 2$ is a prime then $x^p - x$ annihilates \mathbb{Z}_{2p} .

Solution.

Since p is an odd prime, we have $\gcd(2, p) = 1$. Hence by Corollary 1 to Theorem 8 in Ch 3.4 we have that $\mathbb{Z}_{2p} \cong \mathbb{Z}_2 \times \mathbb{Z}_p$ as rings.

Thus it suffices to show that $x^p - x$ annihilates $\mathbb{Z}_2 \times \mathbb{Z}_p$. By part (a) we already know that for every $b \in \mathbb{Z}_p$ we have $b^p = b$. A direct check shows that for every $a \in \mathbb{Z}_2$ we have $a^2 = a$.

Therefore for every $a \in \mathbb{Z}_2$, $b \in \mathbb{Z}_p$ we have

$$(a, b)^p = (a^p, b^p) = (a, b) \text{ and hence } (a, b)^p - (a, b) = (0, 0)$$

so that $x^p - x$ annihilates $\mathbb{Z}_2 \times \mathbb{Z}_p$ as required.

If $p > 3$ is a prime, show that $x^p - x$ annihilates \mathbb{Z}_{3p} .

Solution.

Since $p > 3$ is a prime, we have $\gcd(3, p) = 1$. Hence by Corollary 1 to Theorem 8 in Ch 3.4 we have that $\mathbb{Z}_{3p} \cong \mathbb{Z}_3 \times \mathbb{Z}_p$ as rings. Thus it suffices to show that $x^p - x$ annihilates $\mathbb{Z}_3 \times \mathbb{Z}_p$.

By part (a) we know that $x^p - x$ annihilates \mathbb{Z}_p . It is easy to see by a direct check that $x^p - x$ annihilates \mathbb{Z}_3 . Indeed, in \mathbb{Z}_3 we have $\bar{0}^p = \bar{0}$, $\bar{1}^p = \bar{1}$ and $\overline{-1}^p = \overline{-1}$, where the last equality holds since $p > 3$ is a prime and hence p is odd. Therefore for every $a \in \mathbb{Z}_3$, $b \in \mathbb{Z}_p$ we have

$$(a, b)^p = (a^p, b^p) = (a, b) \text{ and hence } (a, b)^p - (a, b) = (0, 0)$$

so that $x^p - x$ annihilates $\mathbb{Z}_3 \times \mathbb{Z}_p$ as required.

(e) Does $x^5 - x$ or $x^7 - x$ annihilate \mathbb{Z}_{35} ?

Solution.

Since $\gcd(5, 7) = 1$, it follows that $\mathbb{Z}_{35} \cong \mathbb{Z}_5 \times \mathbb{Z}_7$ as rings. Thus $x^p - x$ annihilates \mathbb{Z}_{35} if and only if it annihilates each of \mathbb{Z}_5 , \mathbb{Z}_7 .

For $\bar{2} \in \mathbb{Z}_7$ we have $\bar{2}^5 = \bar{32} = \bar{4} \neq \bar{2}$ in \mathbb{Z}_7 . Thus $x^5 - x$ does not annihilate \mathbb{Z}_7 and hence it does not annihilate \mathbb{Z}_{35} .

Also, for $\bar{2} \in \mathbb{Z}_5$ we have $\bar{2}^7 = \bar{128} = \bar{3} \neq \bar{2}$ in \mathbb{Z}_5 . Thus $x^7 - x$ does not annihilate \mathbb{Z}_5 and hence it does not annihilate \mathbb{Z}_{35} .

(f) Show that there exists a polynomial of degree n in $\mathbb{Z}_n[x]$ that annihilates \mathbb{Z}_n .

Solution.

Take

$$f(x) = x(x - \bar{1})(x - \bar{2}) \dots (x - \overline{n-1}) \in \mathbb{Z}_n[x].$$

Ch. 4.2, Problem 5

In each case determine whether the polynomial is irreducible over each of the fields \mathbb{Q} , \mathbb{R} , \mathbb{C} , \mathbb{Z}_2 , \mathbb{Z}_3 , \mathbb{Z}_5 and \mathbb{Z}_7 .

(a) $x^2 - 3$.

Solution.

We claim that $x^2 - 3$ is irreducible over \mathbb{Q} . Since $\deg(x^2 - 3) = 2$, to show that $x^2 - 3$ is irreducible over \mathbb{Q} it suffices to prove that $x^2 - 3$ has no rational roots. We have $x^2 - 3 = (x - \sqrt{3})(x + \sqrt{3})$ in $\mathbb{R}[x]$. Since \mathbb{R} is an integral domain, it follows that $x^2 - 3$ has exactly two roots in \mathbb{R} , namely $\pm\sqrt{3}$. Since both of these roots are irrational, it follows that $x^2 - 3$ has no rational roots and hence it is irreducible over \mathbb{Q} .

We have $x^2 - 3 = (x - \sqrt{3})(x + \sqrt{3})$ in $\mathbb{R}[x]$ and in $\mathbb{C}[x]$. Hence $x^2 - 3$ is reducible over \mathbb{R} and over \mathbb{C} .

Also, the following holds in $\mathbb{Z}_2[x]$:

$$x^2 - \bar{3} = x^2 - \bar{1} = (x - \bar{1})(x + \bar{1})$$

and hence $x^2 - \bar{3}$ is reducible over \mathbb{Z}_2 .

Similar, in $\mathbb{Z}_2[x]$ we have:

$$x^2 - \bar{3} = x^2 - \bar{0} = x^2 = x \cdot x$$

and hence $x^2 - \bar{3}$ is reducible over \mathbb{Z}_3 .

A direct check shows that $x^2 - \bar{3}$ has no roots in \mathbb{Z}_5 . Indeed, in \mathbb{Z}_5 we have $\bar{0}^2 - \bar{3} = -\bar{3} \neq \bar{0}$, $\bar{1}^2 - \bar{3} = -\bar{2} \neq \bar{0}$, $\bar{2}^2 - \bar{3} = \bar{1} \neq \bar{0}$, $\bar{3}^2 - \bar{3} = \bar{1} \neq \bar{0}$ and $\bar{4}^2 - \bar{3} = \bar{3} \neq \bar{0}$. Hence $x^2 - \bar{3}$ is irreducible over \mathbb{Z}_5 .

Similarly, a direct check shows that $x^2 - \bar{3}$ has no roots in \mathbb{Z}_7 and hence it is irreducible over \mathbb{Z}_7 .

(b) $x^2 + x + 1$

Via applying the quadratic formula we find the complex roots of x^2+x+1 : $x_{1,2} = \frac{-1 \pm \sqrt{-3}}{2} = \frac{-1 \pm \sqrt{3}i}{2}$, so that in $\mathbb{C}[x]$ we have $x^2+x+1 = (x - \frac{-1 \pm \sqrt{-3}}{2})(x + \frac{-1 \pm \sqrt{-3}}{2})$. Since \mathbb{C} is an integral domain, it follows that $x_{1,2} = \frac{-1 \pm \sqrt{-3}}{2} = \frac{-1 \pm \sqrt{3}i}{2}$ are the only roots of x^2+x+1 in \mathbb{C} . Since none of these roots belong to \mathbb{Q} and none of them belong to \mathbb{R} , it follows that x^2+x+1 has no roots in \mathbb{Q} and no roots in \mathbb{R} . Since $\deg(x^2+x+1) = 2$, this implies that x^2+x+1 is irreducible over \mathbb{Q} and it is also irreducible over \mathbb{R} .

Since $x^2+x+1 = (x - \frac{-1 \pm \sqrt{-3}}{2})(x + \frac{-1 \pm \sqrt{-3}}{2})$ in $\mathbb{C}[x]$, it follows that x^2+x+1 is reducible over \mathbb{C} .

A direct check shows that x^2+x+1 has no roots in \mathbb{Z}_2 . Indeed, $\bar{0}^2 + \bar{0} + \bar{1} = \bar{1} \neq \bar{0}$ and $\bar{1}^2 + \bar{1} + \bar{1} = \bar{1} \neq \bar{0}$ in \mathbb{Z}_2 . Hence x^2+x+1 is irreducible over \mathbb{Z}_2 .

On the other hand, x^2+x+1 has a root in \mathbb{Z}_3 , namely $\bar{1}$. Hence x^2+x+1 is reducible over \mathbb{Z}_3 . One can also see this directly by checking that in $\mathbb{Z}_3[x]$ we have $x^2+x+\bar{1} = x^2 - \bar{2}x + \bar{1} = (x - \bar{1})^2$.

A direct check shows that x^2+x+1 has no roots in \mathbb{Z}_5 . Indeed, in \mathbb{Z}_5 we have $\bar{0}^2 + \bar{0} + \bar{1} = \bar{1} \neq \bar{0}$, $\bar{1}^2 + \bar{1} + \bar{1} = \bar{3} \neq \bar{0}$, $\bar{2}^2 + \bar{2} + \bar{1} = \bar{2} \neq \bar{0}$, $\bar{3}^2 + \bar{3} + \bar{1} = \bar{3} \neq \bar{0}$, $\bar{4}^2 + \bar{4} + \bar{1} = \bar{1} \neq \bar{0}$. Hence x^2+x+1 is irreducible over \mathbb{Z}_5 .

On the other hand, x^2+x+1 has a root in \mathbb{Z}_7 , namely $\bar{2}$. Hence x^2+x+1 is reducible over \mathbb{Z}_7 .

(c) x^3+x+1 .

Solution.

Note that $\lim_{x \rightarrow -\infty} x^3+x+1 = -\infty$ and $\lim_{x \rightarrow \infty} x^3+x+1 = \infty$. Hence by the Intermediate Value Theorem from calculus there exists $x_0 \in \mathbb{R}$ such that $x_0^3+x_0+1=0$. Thus x^3+x+1 has a root in \mathbb{R} and hence it is reducible over \mathbb{R} . Since this real root x_0 also belongs to \mathbb{C} , it follows that x^3+x+1 is reducible over \mathbb{C} .

We claim that x^3+x+1 is irreducible over \mathbb{Q} . Indeed, suppose, on the contrary, that x^3+x+1 is reducible over \mathbb{Q} . Since $\deg(x^3+x+1) = 3$, it follows that x^3+x+1 has a root $r \in \mathbb{Q}$. Then Theorem 9 in Ch 9.1 implies that $r = \frac{c}{d}$ where $c, d \in \mathbb{Z}$ and $c|1, d|1$. Hence $c \in \{1, -1\}$ and $d \in \{1, -1\}$. Therefore $r = \frac{c}{d} \in \{1, -1\}$. However $1^3+1+1=3 \neq 0$ and $(-1)^3+(-1)+1=-1 \neq 0$ in \mathbb{Q} , yielding a contradiction. Thus indeed x^3+x+1 is irreducible over \mathbb{Q} .

Ch. 4.2, Problem 6

Let R be an integral domain and let $f(x) \in R[x]$ be monic. If $f(x)$ factors properly in $R[x]$, show that it has a proper factorization $f(x) = g(x)h(x)$ where $g(x)$ and $h(x)$ are both monic.

Solution.

Let $n = \deg(f)$. Let $f(x) = g_1(x)h_1(x)$ be a proper factorization of $f(x)$ in $R[x]$. Thus $\deg g_1 = m, \deg h_1 = k$ where $m+k=n$ and $0 < m, k < n$.

We have $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$ (since f is monic), $g_1(x) = b_mx^m + \dots + b_0, h_1 = c_kx^k + \dots + c_0$ where $b_m, c_k \in R, b_m \neq 0, c_k \neq 0$.

Then the leading coefficient of g_1h_1 is equal to b_mc_k . Since f is monic, it follows that $b_mc_k = 1$ in R . Since R is an integral domain (and thus is commutative) this means that b_m and c_k are units in R and $b_m = c_k^{-1}$.

Put $g(x) = c_k g_1(x) = c_k(b_m x^m + \cdots + b_0) = c_k b_m x^m + \cdots + c_k b_0 = x^m + \cdots + c_k b_0$, so that $g(x)$ is monic. Also put $h(x) = b_m h_1(x) = b_m(c_k x^k + \cdots + c_0) = b_m c_k x^k + \cdots + b_m c_0 = x^k + \cdots + b_m c_0$, so that $h(x)$ is monic.

We also have

$$f(x) = g_1(x)h_1(x) = c_k b_m g_1(x)h_1(x) = c_k g_1(x)b_m h_1(x) = g(x)h(x).$$

Thus we have found a proper factorization of $f(x)$ as a product of two monic polynomials in $R[x]$.