3.59 A student claims that \(x - 1\) is not irreducible because \((\sqrt{2} + 1)(\sqrt{2} - 1) = 1\) is a factorization.

**Answer:** Suppose that \(\sqrt{2} + 1, \sqrt{2} - 1\) are polynomials. Then \(0 < \deg(\sqrt{2} + 1) < \deg(x - 1) = 1, 0 < \deg(\sqrt{2} + 1) < \deg(x - 1) = 1\). As there is no integers exist between 0 and 1 and not in \([0, 1]\), a contradiction obtains.

3.60 Prove that there are domains \(R\) containing a pair of elements having no gcd.

**Proof:** Let \(K\) be a field and

\[
R = \{ f(x) \in K[x] : f(x) = s_0 + s_1x + s_2x^2 + s_3x^3 + \cdots \}.
\]

Then one can directly verify that \(R\) is a subring of \(K[x]\). Since \(K[x]\) is a domain, \(R\) is also a domain.

Let \(f(x) = x^5\) and \(g(x) = x^6\). Suppose that \(d(x)\) is a gcd of \(f(x)\) and \(g(x)\). Then \(x^2\) and \(x^3\) are both common divisors of \(f(x)\) and \(g(x)\) in \(R\). Therefore, \(d(x) = x^2u(x)\) and \(d(x) = x^3v(x)\) for some \(u(x)\), \(v(x) \in R\). Since \(d(x) = x^5v(x), \deg(d(x)) \in \{3, 4\}\). If \(\deg(d(x)) = 4\), then \(\deg(v(x)) = 1\), contrary to the assumption that \(v(x) \in R\). If \(\deg(d(x)) = 3\), then \(\deg(u(x)) = 1\), contrary to the assumption that \(u(x) \in R\). Therefore, \(f(x)\) and \(g(x)\) does not have a gcd.

**Remark:** This problem also tells us that there exists a PID \((K[x] in this example), which may have a domain \(R\) that is **not** a PID. Can you find another example with such a property?

3.61 If \(R\) is a PID and \(a, b \in R\), prove that a gcd of \(a\) and \(b\) exists.

**Proof:** We may assume that at least one of \(a\) and \(b\) is not zero (otherwise, the gcd is 0 and the result is obvious). Consider the set \(I\) of all the linear combinations:

\[
I = \{ \alpha a + \beta b, \alpha, \beta \in R \}.
\]

When \((\alpha, \beta) \in \{(0, 1), (1, 0)\}\), we have \(a, b \in I\). When \(\alpha = \beta = 0\), we have \(0 \in I\). For any \(\alpha_1a + \beta_1b, \alpha_2a + \beta_2b \in I\), and for any \(r \in R\), by the definition of \(I\),

\[
(\alpha_1a + \beta_1b) + (\alpha_2a + \beta_2b) = (\alpha_1 + \alpha_2)a + (\beta_1 + \beta_2)b \in I,\]

\[
r(\alpha a + \beta b) = (ra)a + (r\beta)b \in I.
\]

Therefore, \(I\) is an ideal of \(R\). Since \(R\) is a PID, \(\exists \delta \in I\) with \(I = \langle \delta \rangle\).

We claim \(\delta\) is a gcd of \(a\) and \(b\). Since \(a \in I = \langle \delta \rangle\), we have \(a = p\delta\) for some \(p \in R\); that is, \(\delta\) is a divisor of \(a\). Similarly, \(\delta\) is a divisor of \(b\) and so \(\delta\) is a common divisor of \(a\) and \(b\). Since \(\delta \in I\), it is a linear combination of \(a\) and \(b\). There are \(\alpha, \beta \in R\) with \(\delta = \alpha a + \beta b\). If \(\gamma\) is a common divisor of \(a\) and \(b\), then \(\gamma \mid \delta\). So \(\delta\) is the gcd of \(a\) and \(b\).

3.64 Let \(R\) be a euclidean ring with degree function \(\partial\).

(i) Prove that \(\partial(1) \leq \partial(a)\) for all nonzero \(a \in R\).

(ii) Prove that a nonzero \(u \in R\) is a unit if and only if \(\partial(u) \leq \partial(1)\).

**Proof** By the definition of euclidean ring, \(\partial(1) \leq \partial(1a) = \partial(a)\) for all nonzero \(a \in R\).

(ii) Suppose that \(u \in R\) is a unit. Then there is \(v \in R\) such that \(uv = 1\). Then by the definition of euclidean ring, \(\partial(u) \leq \partial(uv) = \partial(1)\). By (i), \(\partial(u) = \partial(1)\).

Conversely, suppose that \(\partial(u) = \partial(1)\). Let \(1 = qu + r\) and \(\partial(r) < \partial(u)\). By (i), \(r = 0\). Then \(u|1\).
3.83 For every commutative ring $R$, prove that $R[x]/(x) \cong R$.

**Proof** Define $f : R[x] \to R$ by setting $f(a_0 + a_1x + \cdots + a_nx^n) = a_0$. Since $f$ is surjective and for any $\alpha = a_0 + a_1x + \cdots + a_nx^n$, $\beta = b_0 + b_1x + \cdots + b_mx^m$, we have $f(\alpha + \beta) = a_0 + b_0 = f(\alpha) + f(\beta)$, $f(\alpha \beta) = a_0b_0 = f(\alpha)f(\beta)$, then $f$ is a ring homomorphism. By the first isomorphism, we have

$$R[x]/Kerf \cong im f$$

Since $Kerf = \langle x \rangle$, then

$$R[x]/\langle x \rangle \cong im f.$$  

3.84 Prove that $F_3[x]/(x^3 - x^2 - 1) \not\cong F_3[x]/(x^3 - x^2 + x + 1)$.

**Proof:** The conclusion is false. Since $x^3 - x^2 - 1$ has a root $x = 2$ in $\mathbb{Z}_3$, it is not irreducible. Therefore, $F_3[x]/(x^3 - x^2 - 1)$ is not a domain. On the other hand, $x^3 - x^2 + x + 1$ is an irreducible polynomial in $\mathbb{Z}_3[x]$ (checking it out), and so $F_3[x]/(x^3 - x^2 + x + 1)$ is a field. Therefore, they are not isomorphic.

Revised 3.84 Prove that $F_3[x]/(x^3 - x^2 + 1) \cong F_3[x]/(x^3 - x^2 + x + 1)$.

**Proof:** In this case, both $x^3 - x^2 + 1$ and $x^3 - x^2 + x + 1$ are irreducible polynomials in $\mathbb{Z}_3[x]$. (Verify this fact).

Let $(x^3 - x^2 - 1) = I$, $(x^3 - x^2 + x + 1) = I'$. Let $\beta = I + x, \beta' = I' + x$.

Then by Proposition 3.117, $1, \beta, \beta^2$ is a basis of $F_3[x]/I$ and $1, \beta', (\beta')^2$ is a basis of $F_3[x]/I'$.

Define $f : F_3[x]/I \to F_3[x]/I'$ by setting $f(a_0 + a_1\beta + a_2\beta^2) = a_0 + a_1\beta' + a_2(\beta')^2$, where $a_0 + a_1\beta + a_2\beta^2$ is an arbitrary element of $F_3[x]/I$. It is not difficult to verify that $f$ is a bijection and it preserves the addition and multiplication and then $f$ is an isomorphism between $F_3[x]/(x^3 - x^2 - 1)$ and $F_3[x]/(x^3 - x^2 + x + 1)$. So we have $F_3[x]/(x^3 - x^2 + 1) \cong F_3[x]/(x^3 - x^2 + x + 1)$.

3.86 let $h(x), p(x) \in K[x]$ be monic polynomials, where $k$ is a field. If $p(x)$ is irreducible and if every root of $h(x)$ is also a root of $p(x)$, prove that $h(x) = p(x)^m$.

**Proof** By induction on the degree of $h(x)$. Suppose that $\beta$ is a root of $h(x)$. Then $\beta$ is also a root of $p(x)$. Since $p(x)$ is irreducible, then $p(x)|h(x)$. Then $h(x) = p(x)h_1(x)$. Then $\partial(p(x)) \leq \partial(h(x))$. If $\partial(p(x)) = \partial(h(x))$, then $p(x) = h(x)$ since they both are monic. Suppose that $\partial(p(x)) < \partial(h(x))$ and the statement is true for any $\partial(p(x)) \leq \partial(h(x)) = n$. Now let $\partial(h(x)) = n + 1$. Since $p(x)|h(x)$ and $\partial(p(x)) < \partial(h(x))$, then $h(x) = p(x)h_1(x)$ for some $h_1(x)$. Then $0 < \partial(h_1(x)) < h(x)$. Suppose that $\beta_1$ is a root of $h_1(x)$ Then $\beta_1$ is a root of $h(x)$ and so a root of $p(x)$. By the induction hypothesis, we have $h_1(x) = p^{n-1}(x)$ for some $m$. Then $h(x) = p^n(x)$.

3.88 (i) Prove that a field $K$ cannot have subfields $k'$ and $k''$ with $k' \cong Q$ and $k'' \cong F_p$ for some prime $p$.

(ii) Prove that a field $K$ cannot have subfields $k'$ and $k''$ with $k' \cong F_p$ and $k'' \cong F_q$, where $p \neq q$ are primes.

**Proof** (i) Suppose that $K$ have subfields $k'$ and $k''$ with $k' \cong Q$ and $k'' \cong F_p$ for some prime $p$. Then by the fact that $k'' \cong F_p$, we have $p|1 = 0$ and $s|1 \neq 0$ for any $s < p$. But by the fact that $k' \cong Q$, there is no $n$ such that $n1 = 0$, a contradiction.

2
(ii) Suppose that $K$ cannot have subfields $k'$ and $k''$ with $k' \cong F_p$ and $k'' \cong F_q$, where $p \neq q$ are primes. Then there are $p \dagger = 0, s \dagger \neq 0$ for any $s < p$ and $q \dagger = 0, t \dagger \neq 0$ for any $t < q$. Since $p \neq q$, a contradiction.

3.90 Let $f(x) = s_0 + s_1x + \cdots + s_{n-1}x^{n-1} + s_nx_n \in k[x]$, where $k$ is a field, and suppose that $f(x) = (x - a_1)(x - a_2) \cdots (x - a_n)$. Prove that $s_{n-1} = -(a_1 + a_2 + \cdots + a_n)$ and that $s_0 = (-1)^n a_1 a_2 \cdots a_n$. Conclude that the sum and the product of all the roots of $f(x)$ lie in $k$.

**Proof** Since $f(x) = s_0 + s_1x + \cdots + s_{n-1}x^{n-1} + s_nx_n \in k[x]$ and $f(x) = (x - a_1)(x - a_2) \cdots (x - a_n)$. Prove that $s_{n-1} = -(a_1 + a_2 + \cdots + a_n)$, by the multiplication of the polynomials, $s_0 = (-a_1)(-a_2) \cdots (-a_n) = (-1)^n a_1 a_2 \cdots a_n$ and $s_{n-1} = (-a_1 + (-a_2) + \cdots (-a_n) = -(a_1 + a_2 + \cdots + a_n)$. Then the sum of all roots of $f(x) = a_1 + a_2 + \cdots + a_n$ and the product of all roots of $f(x) = a_1 \cdots a_n$ lie in $K$.

3.94 (i) Is $F_4$ a subfield of $F_8$?
(ii) For any prime $p$, prove that if $F_{p^n}$ is a subfield of $F_{p^m}$, then $n|m$.

**Proof** (i) Suppose that $F_4 \leq F_8$. Since both $F_4$ and $F_8$ have characteristic 2, both are having $\mathbb{Z}_2$ as the primary subfield. It follows that

$$[F_8 : \mathbb{Z}_2] = [F_8 : F_4][F_4 : \mathbb{Z}_2].$$

Since $[F_8 : \mathbb{Z}_2]$ and $[F_4 : \mathbb{Z}_2] = 2$, it forces that $[F_8 : F_4] = 3/2$, a contradiction to the fact that $[F_8 : F_4]$ must be an integer.

(ii) Suppose that $F_{p^n}$ is a subfield of $F_{p^m}$. Then since both $F_{p^n}$ and $F_{p^m}$ have characteristic $p$, both are having $\mathbb{Z}_p$ as the primary subfield. It follows that

$$[F_{p^m} : \mathbb{Z}_p] = [F_{p^m} : F_{p^n}][F_{p^n} : \mathbb{Z}_p].$$

Since $[F_{p^m} : \mathbb{Z}_p] = m$, and $[F_{p^n} : \mathbb{Z}_p] = n$, we have $n|m$. 

3