17.3. (b) Let $a$ in $R$ be a nilpotent element. An element $a$ in $R$ is nilpotent if $a^n = 0$ for some positive integer $n$. Show that the set of all nilpotent elements forms an ideal in $R$.

**Solution.** Let $N \subseteq R$ be the set of nilpotent elements, and suppose $a^m = 0$ and $b^n = 0$. Then $(-a)^m = 0$, so $N$ is closed under negation. Moreover, $(a + b)^{m+n} = \sum_{i=0}^{m+n} \binom{m+n}{i} a^i b^{m+n-i} = 0$ since either $i \geq m$ and $a^i = 0$ or $m+n-i \geq n$ and $b^m+n-i = 0$. Thus $N$ is closed under addition. Finally, if $x \in R$ then $(ax)^m = a^m x^m = 0$, so $N$ is an ideal.

16.40. Let $R$ be a ring and $I$ and $J$ be ideals in $R$ such that $I + J = R$.

(a) Show that for any $r$ and $s$ in $R$, the system of equations

$$
\begin{aligned}
x &\equiv r \pmod{I} \\
x &\equiv s \pmod{J}
\end{aligned}
$$

has a solution.

**Solution.** Since $I + J = R$, we may find $i \in I$ and $j \in J$ with $i + j = 1$. Setting $x = si + rj$, we have

$$
\begin{aligned}
x &\equiv rj \equiv r \pmod{I} \\
x &\equiv si \equiv s \pmod{J}.
\end{aligned}
$$

(b) In addition, prove that any two solutions of the system are congruent modulo $I \cap J$.

**Solution.** If $x$ and $y$ are solutions, then $x - y \equiv 0 \pmod{I}$ and $x - y \equiv 0 \pmod{J}$, so $x - y \in I \cap J$.

(c) Let $I$ and $J$ be ideals in a ring $R$ such that $I + J = R$. Show that there exists a ring isomorphism

$$
R/(I \cap J) \cong R/I \times R/J.
$$

**Solution.** Let $\phi : R \to R/I \times R/J$ be defined by $\phi(x) = (x + I, x + J)$. By part (a), $\phi$ is surjective, and by part (b) it has kernel $I \cap J$. So by the First Isomorphism Theorem, it induces the desired isomorphism.

17.2. (b) Compute $(5x^2 + 3x - 4)(4x^2 - x + 9)$ in $\mathbb{Z}_{12}[x]$.

**Solution.** $8x^4 + 7x^3 + 2x^2 + 7x$.

17.3. (b) Let $a(x) = 6x^4 - 2x^3 + x^2 - 3x + 1$ and $b(x) = x^2 + x - 2$ in $\mathbb{Z}_2[x]$. Use the division algorithm to find $q(x)$ and $r(x)$ so that $a(x) = q(x)b(x) + r(x)$ with $\deg r(x) < \deg b(x)$.

**Solution.** We find that $q(x) = 6x^2 + 6x$ and $r(x) = 2x + 1$.

17.4. (c) Find the greatest common divisor $d(x)$ of $p(x) = x^3 + x^2 - 4x + 4$ and $q(x) = x^3 + 3x - 2$ in $\mathbb{Z}_5[x]$ and polynomials $a(x)$ and $b(x)$ such that $a(x)p(x) + b(x)q(x) = d(x)$.
Solution.

\[ x^3 + x^2 - 4x + 4 = 1(x^3 + 3x - 2) + (x^2 + 3x + 1) \]
\[ x^3 + 3x - 2 = (x + 2)(x^2 + 3x + 1) + (x + 1) \]
\[ x^2 + 3x + 1 = (x + 2)(x + 1) + 4 \]
\[ 4 = (x^2 + 3x + 1) - (x + 2)(x + 1) \]
\[ = (x^2 + 3x + 1) - (x + 2)((x^2 + 3x - 2) - (x + 2)(x^2 + 3x + 1)) \]
\[ = (x^2 + 4x)(x^2 + 3x + 1) - (x + 2)(x^3 + 3x - 2) \]
\[ = (x^2 + 4x)((x^3 + x^2 - 4x + 4) - (x^3 + 3x - 2)) - (x + 2)(x^3 + 3x - 2) \]
\[ = (x^2 + 4x)(x^3 + x^2 - 4x + 4) - (x^2 + 2)(x^3 + 3x - 2) \]

Negating this last equation, we get

\[ 1 = (4x^2 + x)(x^3 + x^2 - 4x + 4) + (x^2 + 2)(x^3 + 3x - 2). \]

17.7. Find a unit \( p(x) \) in \( \mathbb{Z}_4[x] \) such that \( \deg p(x) > 1 \).

Solution. Since \( (2x^2 + 1)(2x^2 + 1) = 1 \), we may take \( p(x) = 2x^2 + 1 \).

17.9. Find all of the irreducible polynomials of degrees 2 and 3 in \( \mathbb{Z}_2[x] \).

Solution. A polynomial of degree 2 or 3 is irreducible when it has no roots. The only two possible roots in \( \mathbb{Z}_2 \) are 0 and 1, so \( f(x) = x^2 + ax + b \) is irreducible when \( f(0) = b = 1 \) and \( f(1) = 1+a+b = 1 \), so \( a = b = 1 \).

Similarly, \( f(x) = x^3 + ax^2 + bx + c \) is irreducible when \( g(0) = c = 1 \) and \( g(1) = 1 + a + b + c = 1 \), yielding \( a = 1 \) and \( b = 0 \) or \( a = 0 \) and \( b = 1 \). Thus the irreducible polynomials are

\[ x^2 + x + 1, x^3 + x + 1, x^3 + x^2 + 1. \]

17.10. Give two different factorizations of \( x^2 + x + 8 \) in \( \mathbb{Z}_{10}[x] \).

Solution. We first find the roots by trial and error: \( x = 1, -2, 3, -4 \). Pairing these up so that they have product \(-2\) and sum 1, we get the factorizations

\[ x^2 + x + 8 = (x - 1)(x + 2) \]
\[ = (x - 3)(x + 4). \]

17.18. Let \( p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x] \), with \( a_n \neq 0 \). Prove that if \( p(r/s) = 0 \) with \( \gcd(r, s) = 1 \), then \( r \mid a_0 \) and \( s \mid a_n \).

Solution. Substituting \( r/s \) into \( p(x) \) and multiplying by \( s^n \) we get

\[ 0 = a_n r^n + a_{n-1} r^{n-1} s + \cdots + a_1 rs^{n-1} + a_0 s^n \]
\[ a_n r^n = s(-a_{n-1} r^{n-1} - \cdots - a_1 rs^{n-2} - a_0 s^{n-1}) \]
\[ a_0 s^n = r(-a_n r^{n-1} - a_{n-1} r^{n-2} - \cdots - a_1 s^{n-1}). \]

Thus \( s \) divides \( a_n r^n \) and \( r \) divides \( a_0 s^n \). Since \( r \) and \( s \) are relatively prime, \( s \) divides \( a_n \) and \( r \) divides \( a_0 \).

17.20. Let \( \Phi_p(x) = \frac{x^{p-1} - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1 \). Show that \( \Phi_p(x) \) is irreducible over \( \mathbb{Q} \) for any prime \( p \).
Solution. We make the substitution \( t = x - 1 \), yielding
\[
\Phi_p(x) = \frac{(t + 1)^p - 1}{t} = \sum_{i=1}^{p} \binom{p}{i} t^{i-1}.
\]
Since \( \binom{p}{i} \) is divisible by \( p \) for \( 0 < i < p \) and \( \binom{p}{1} = p \) is not divisible by \( p^2 \) and \( \binom{p}{p} = 1 \) is not divisible by \( p \), this polynomial satisfies the Eisenstein criterion and is thus irreducible. Thus \( \Phi_p(x) \) is irreducible as well.

17.21. If \( F \) is a field, show that there are infinitely many irreducible polynomials in \( F[x] \).

Solution. Euclid’s proof for the infinitude of primes in \( \mathbb{Z} \) applies in essentially the same way here. Suppose that there were finitely many irreducible polynomials \( p_1, \ldots, p_k \). Let \( p = 1 + \prod_{i=1}^{k} p_i \). Since \( p \) has remainder 1 when divided by each \( p_i \), it is not a multiple of any of them. But it must be divisible by some irreducible since \( F[x] \) is Noetherian. Thus there are infinitely many irreducible polynomials.

17.24. Show that \( x^p - x \) has \( p \) distinct zeros in \( \mathbb{Z}_p \), for any prime \( p \). Conclude that
\[
x^p - x = x(x-1)(x-2) \cdots (x-(p-1)).
\]

Solution. By Fermat’s little theorem, \( a^p \equiv a \pmod{p} \) for all \( a \in \mathbb{Z}_p \) and thus \( x^p - x \) is divisible by \( (x-a) \) for all \( a \in \mathbb{Z}_p \). By additivity of degree and the equality of leading coefficients, we get the desired equation.