3.30 Show that if \( R \) is a nonzero commutative ring, then \( R[x] \) is never a field.

**Solution.** If \( f(x) = x^{-1} \), then \( xf(x) = 1 \). But the degree of the left side is at least 1, while the degree of the right side is 0.

3.33 Show that if \( f(x) = x^p - x \in \mathbb{F}_p[x] \), then its polynomial function \( f^p: \mathbb{F}_p \rightarrow \mathbb{F}_p \) is identically zero.

**Solution.** Let \( f(x) = x^p - x \in \mathbb{F}_p[x] \). If \( a \in \mathbb{F}_p \), Fermat’s theorem gives \( a^p = a \), and so \( f(a) = a^p - a = 0 \).

3.39 If \( R \) is a commutative ring, define \( R[[x]] \) to be the set of all formal power series over \( R \).

(i) Show that the formulas defining addition and multiplication on \( R[x] \) make sense for \( R[[x]] \), and prove that \( R[[x]] \) is a commutative ring under these operations.

**Solution.** Each ring axiom can be verified for formal power series, as in Proposition 3.25 (that a formal power series \((s_0, s_1, \ldots)\) is a polynomial, i.e., that its coordinates are eventually 0, does not enter into the proof).

(ii) Prove that \( R[x] \) is a subring of \( R[[x]] \).

**Solution.** The set \( R[x] \) is a subset of \( R[[x]] \), for every polynomial over \( R \) is a formal power series that is eventually 0. The definitions of addition and multiplication for power series are the same as for polynomials. Since \( 1 \in R[x] \) and \( R[x] \) is closed under the operations, it is a subring.

(iii) Denote a formal power series \( \sigma = (s_0, s_1, s_2, \ldots, s_n, \ldots) \) by

\[
\sigma = s_0 + s_1 x + s_2 x^2 + \cdots.
\]

Prove that if \( \sigma = 1 + x + x^2 + \cdots \), then \( \sigma = 1/(1 - x) \) is in \( R[[x]] \).

**Solution.** We have

\[
1 + x + x^2 + \cdots = 1 + x(1 + x + x^2 + \cdots).
\]

Hence, if \( \sigma = 1 + x + x^2 + \cdots \), then

\[
\sigma = 1 + x \sigma.
\]

Solving for \( \sigma \) gives \( \sigma = 1/(1 - x) \).
3.40 If $\sigma = (s_0, s_1, s_2, \ldots, s_n, \ldots)$ is a nonzero formal power series, define $\text{ord}(\sigma) = m$, where $m$ is the smallest natural number for which $s_m \neq 0$.

(i) Prove that if $R$ is a domain, then $R[[x]]$ is a domain.

Solution. If $\sigma = (s_0, s_1, \ldots)$ and $\tau = (t_0, t_1, \ldots)$ are nonzero power series, then each has an order ($\sigma \neq 0$ if and only if it has an order); let $\text{ord}(\sigma) = p$ and $\text{ord}(\tau) = q$. Write

$$\sigma \tau = (c_0, c_1, \ldots).$$

For any $n \geq 0$, we have $c_n = \sum_{i+j=n} s_it_j$. In particular, if $n < p + q$, then $i < p$ and $s_i = 0$ or $j < q$ and $t_j = 0$; it follows that $c_n = 0$ because each summand $s_it_j = 0$. The same analysis shows that $c_{p+q} = s_pl_q$, for all the other terms are 0. Since $R$ is a domain, $s_p \neq 0$ and $t_q \neq 0$ imply $s_pl_q \neq 0$. Therefore,

$$\text{ord}(\sigma \tau) = \text{ord}(\sigma) + \text{ord}(\tau).$$

(ii) Prove that if $k$ is a field, then a nonzero formal power series $\sigma \in k[[x]]$ is a unit if and only if $\text{ord}(\sigma) = 0$; that is, if its constant term is nonzero.

Solution. Let $u = a_0 + a_1x + a_2x^2 + \cdots$. If $u$ is a unit, then there is $v = b_0 + b_1x + b_2x^2 + \cdots$ with $uv = 1$. By Exercise 3.39(iii),

$$\text{ord}(u) + \text{ord}(v) = \text{ord}(1) = 0.$$

Since $\text{ord}(\sigma) \geq 0$ for all (nonzero) $\sigma \in k[[x]]$, it follows that $\text{ord}(u) = 0 = \text{ord}(v)$. Therefore, $a_0 \neq 0$.

We show that $u = a_0 + a_1x + a_2x^2 + \cdots$ is a unit by constructing the coefficients $b_n$ of its inverse $v = b_0 + b_1x + b_2x^2 + \cdots$ by
induction on $n \geq 0$. Define $b_0 = a_0^{-1}$. If $v$ exists, then the equation $uv = 1$ would imply that $\sum_{i+j=n} a_ib_j = 0$ for all $n > 0$. Assuming that $b_0, \ldots, b_{n-1}$ have been defined, then we have

$$0 = a_0b_n + \sum_{i+j=n} a_ib_j,$$

and this can be solved for $b_n$ because $a_0$ is invertible.

(iii) Prove that if $\sigma \in k[[x]]$ and $\text{ord}(\sigma) = n$, then

$$\sigma = x^n u,$$

where $u$ is a unit in $k[[x]]$.

**Solution.** Since $\text{ord}(\sigma) = n$, we have

$$\sigma = a_nx^n + a_{n+1}x^{n+1} + a_{n+2}x^{n+2} + \cdots = x^n(a_n + a_{n+1}x + a_{n+2}x^2 + \cdots).$$

As $a_n \neq 0$, we have $a_n + a_{n+1}x + a_{n+2}x^2 + \cdots$ a unit, by part (ii).

3.42 Let $A$ be a commutative ring. Prove that a subset $J$ of $A$ is an ideal if and only if $0 \in J$, $u, v \in J$ implies $u - v \in J$, and $u \in J$, $a \in A$ imply $au \in J$.

(In order that $J$ be an ideal, $u, v \in J$ should imply $u + v \in J$ instead of $u - v \in J$.)

**Solution.** The properties of $J$ differ from those in the definition of an ideal in that (ii') $u, v \in I$ implies $u - v \in I$ replaces (ii) $u, v \in I$ implies $u + v \in I$. Now $a = -1$, says $v \in J$ if and only if $-v \in J$. If (ii) holds, then $u - (-v) = u + v \in J$, and so (ii) holds. Conversely, if (ii') holds, then $u + (-v) = u - v \in J$, and so (ii') holds.

3.46 Let $R$ be a commutative ring. Show that the function $\eta: R[x] \to R$, defined by

$$\eta: a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \mapsto a_0,$$

is a homomorphism. Describe $\ker \eta$ in terms of roots of polynomials.

**Solution.** First of all, $\eta(1) = 1$. Next, if $f(x) = \sum a_ix^i$ and $g(x) = \sum b_ix^i$, then $f(x) + g(x) = \sum (a_i + b_i)x^i$, and so

$$\eta(f + g) = a_0 + b_0 = \eta(f) + \eta(g).$$

Finally, since the constant term of $f(x)g(x)$ is $a_0b_0$, we have

$$\eta(fg) = a_0b_0 = \eta(f)\eta(g).$$

Therefore, $\eta$ is a ring homomorphism.

The kernel of $\eta$ consists of all polynomials having constant term 0; these are precisely all the polynomials having 0 as a root.
3.55 (i) Prove that the set $F$ of all $2 \times 2$ real matrices of the form $A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ is a field with operations matrix addition and matrix multiplication.

**Solution.** It is easy to check that $F$ is a commutative subring of the (noncommutative) ring of all $2 \times 2$ real matrices (note that the identity matrix $I \in F$). If $A \neq 0$, then $\det(A) = a^2 + b^2 \neq 0$, and so $A^{-1}$ exists; since $A^{-1}$ has the correct form, it lies in $F$, and so $F$ is a field.

(ii) Prove that $F$ is isomorphic to $\mathbb{C}$.

**Solution.** It is straightforward to check that $\varphi$ is a homomorphism of fields; it is an isomorphism because its inverse is given by $a + ib \mapsto A$. 