the polynomial $X^n - x$ in the ring $R[X]$. The ideal (x) is prime in the coefficient ring R since $R/(x) = \mathbb{Q}[x]/(x)$ is the integral domain $\mathbb{Q}$. Eisenstein's Criterion for the ideal (x) of R applies directly to show that $X^n - x$ is irreducible in $R[X]$. Note that this construction works with $\mathbb{Q}$ replaced by any field or, indeed, by any integral domain.

There are now efficient algorithms for factoring polynomials over certain fields. For polynomials with integer coefficients these algorithms have been implemented in a number of computer packages. An efficient algorithm for factoring polynomials over $\mathbb{F}_p$, called the Berlekamp Algorithm, is described in detail in the exercises at the end of Section 14.3.

EXERCISES

1. Determine whether the following polynomials are irreducible in the rings indicated. For those that are reducible, determine their factorization into irreducibles. The notation $\mathbb{F}_p$ denotes the finite field $\mathbb{Z}/p\mathbb{Z}$, p a prime.
(a) $x^2 + x + 1$ in $\mathbb{F}_2[x]$.
(b) $x^3 + x + 1$ in $\mathbb{F}_3[x]$.
(c) $x^4 + 1$ in $\mathbb{F}_5[x]$.
(d) $x^4 + 10x^2 + 1$ in $\mathbb{Z}[x]$.

2. Prove that the following polynomials are irreducible in $\mathbb{Z}[x]$:
(a) $x^4 - 4x^3 + 6$
(b) $x^6 + 30x^5 - 15x^3 + 6x - 120$
(c) $x^4 + 4x^3 + 6x^2 + 2x + 1$ [Substitute $x - 1$ for x.]
(d) $\dfrac{(x+2)^p - 2^p}{x}$, where p is an odd prime.

3. Show that the polynomial $(x-1)(x-2)\cdots(x-n) - 1$ is irreducible over $\mathbb{Z}$ for all $n \geq 1$. [If the polynomial factors consider the values of the factors at $x = 1, 2, \dots, n$.]

4. Show that the polynomial $(x-1)(x-2)\cdots(x-n) + 1$ is irreducible over $\mathbb{Z}$ for all $n \geq 1$, $n \neq 4$.

5. Find all the monic irreducible polynomials of degree ≤ 3 in $\mathbb{F}_2[x]$, and the same in $\mathbb{F}_3[x]$.

6. Construct fields of each of the following orders: (a) 9, (b) 49, (c) 8, (d) 81 (you may exhibit these as $F[x]/(f(x))$ for some F and f). [Use Exercises 2 and 3 in Section 2.]

7. Prove that $\mathbb{R}[x]/(x^2 + 1)$ is a field which is isomorphic to the complex numbers.

8. Prove that $K_1 = \mathbb{F}_{11}[x]/(x^2 + 1)$ and $K_2 = \mathbb{F}_{11}[y]/(y^2 + 2y + 2)$ are both fields with 121 elements. Prove that the map which sends the element $p(\bar{x})$ of K_1 to the element $p(\bar{y} + 1)$ of K_2 (where p is any polynomial with coefficients in $\mathbb{F}_{11}$) is well defined and gives a ring (hence field) isomorphism from K_1 to K_2.

9. Prove that the polynomial $x^2 - \sqrt{2}$ is irreducible over $\mathbb{Z}[\sqrt{2}]$ (you may use the fact that $\mathbb{Z}[\sqrt{2}]$ is a U.F.D. — cf. Exercise 9 of Section 8.1).

10. Prove that the polynomial $p(x) = x^4 - 4x^2 + 8x + 2$ is irreducible over the quadratic field $F = \mathbb{Q}(\sqrt{-2}) = \{a + b\sqrt{-2} \mid a, b \in \mathbb{Q}\}$. [First use the method of Proposition 11 for the Unique Factorization Domain $\mathbb{Z}[\sqrt{-2}]$ (cf. Exercise 8, Section 8.1) to show that if $\alpha \in \mathbb{Z}[\sqrt{-2}]$ is a root of $p(x)$ then α is a divisor of 2 in $\mathbb{Z}[\sqrt{-2}]$. Conclude that α must be ± 1, $\pm\sqrt{-2}$ or ± 2, and hence show $p(x)$ has no linear factor over F. Show similarly that $p(x)$ is not the product of two quadratics with coefficients in F.]

11. Prove that $x^2 + y^2 - 1$ is irreducible in $\mathbb{Q}[x, y]$.

12. Prove that $x^{n-1} + x^{n-2} + \cdots + x + 1$ is irreducible over $\mathbb{Z}$ if and only if n is a prime.

13. Prove that $x^3 + nx + 2$ is irreducible over $\mathbb{Z}$ for all integers $n \neq 1, -3, -5$.

14. Factor each of the two polynomials: $x^8 - 1$ and $x^6 - 1$ into irreducibles over each of the following rings: **(a)** $\mathbb{Z}$, **(b)** $\mathbb{Z}/2\mathbb{Z}$, **(c)** $\mathbb{Z}/3\mathbb{Z}$.

15. Prove that if F is a field then the polynomial $X^n - x$ which has coefficients in the ring $F[[x]]$ of formal power series (cf. Exercise 3 of Section 7.2) is irreducible over $F[[x]]$. [Recall that $F[[x]]$ is a Euclidean Domain — cf. Exercise 5, Section 7.2 and Example 4, Section 8.1.]

16. Let F be a field and let $f(x)$ be a polynomial of degree n in $F[x]$. The polynomial $g(x) = x^n f(1/x)$ is called the *reverse* of $f(x)$.

(a) Describe the coefficients of g in terms of the coefficients of f.

(b) Prove that f is irreducible if and only if g is irreducible.

17. Prove the following variant of Eisenstein's Criterion: let P be a prime ideal in the Unique Factorization Domain R and let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial in $R[x]$, $n \geq 1$. Suppose $a_n \notin P$, $a_{n-1}, \ldots, a_0 \in P$ and $a_0 \notin P^2$. Prove that $f(x)$ is irreducible in $F[x]$, where F is the quotient field of R.

18. Show that $6x^5 + 14x^3 - 21x + 35$ and $18x^5 - 30x^2 + 120x + 360$ are irreducible in $\mathbb{Q}[x]$.

19. Let F be a field and let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in F[x]$. The *derivative*, $D_x(f(x))$, of $f(x)$ is defined by

$$D_x(f(x)) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1$$

where, as usual, $na = a + a + \cdots + a$ (n times). Note that $D_x(f(x))$ is again a polynomial with coefficients in F.

The polynomial $f(x)$ is said to have a *multiple root* if there is some field E containing F and some $\alpha \in E$ such that $(x - \alpha)^2$ divides $f(x)$ in $E[x]$. For example, the polynomial $f(x) = (x-1)^2(x-2) \in \mathbb{Q}[x]$ has $\alpha = 1$ as a multiple root and the polynomial $f(x) = x^4 + 2x^2 + 1 = (x^2+1)^2 \in \mathbb{R}[x]$ has $\alpha = \pm i \in \mathbb{C}$ as multiple roots. We shall prove in Section 13.5 that a nonconstant polynomial $f(x)$ has a multiple root if and only if $f(x)$ is not relatively prime to its derivative (which can be detected by the Euclidean Algorithm in $F[x]$). Use this criterion to determine whether the following polynomials have multiple roots:

(a) $x^3 - 3x - 2 \in \mathbb{Q}[x]$

(b) $x^3 + 3x + 2 \in \mathbb{Q}[x]$

(c) $x^6 - 4x^4 + 6x^3 + 4x^2 - 12x + 9 \in \mathbb{Q}[x]$

(d) Show for any prime p and any $a \in \mathbb{F}_p$ that the polynomial $x^p - a$ has a multiple root.

20. Show that the polynomial $f(x) = x$ in $\mathbb{Z}/6\mathbb{Z}[x]$ factors as $(3x+4)(4x+3)$, hence is not an irreducible polynomial.

(a) Show that the reduction of $f(x)$ modulo both of the nontrivial ideals (2) and (3) of $\mathbb{Z}/6\mathbb{Z}$ is an irreducible polynomial, showing that the condition that R be an integral domain in Proposition 12 is necessary.

(b) Show that in any factorization $f(x) = g(x)h(x)$ in $\mathbb{Z}/6\mathbb{Z}[x]$ the reduction of $g(x)$ modulo (2) is either 1 or x and the reduction of $h(x)$ modulo (2) is then either x or 1, and similarly for the reductions modulo (3). Determine all the factorizations of $f(x)$ in $\mathbb{Z}/6\mathbb{Z}[x]$. [Use the Chinese Remainder Theorem.]

(c) Show that the ideal $(3, x)$ is a principal ideal in $\mathbb{Z}/6\mathbb{Z}[x]$.

(d) Show that over the ring $\mathbb{Z}/30\mathbb{Z}[x]$ the polynomial $f(x) = x$ has the factorization

$f(x) = (10x+21)(15x+16)(6x+25)$. Prove that the product of any of these factors is again of the same degree. Prove that the reduction of $f(x)$ modulo any prime in $\mathbb{Z}/30\mathbb{Z}$ is an irreducible polynomial. Determine all the factorizations of $f(x)$ in $\mathbb{Z}/30\mathbb{Z}[x]$. [Consider the reductions modulo (2), (3) and (5) and use the Chinese Remainder Theorem.]

(e) Generalize part (d) to $\mathbb{Z}/n\mathbb{Z}[x]$ where n is the product of k distinct primes.

9.5 POLYNOMIAL RINGS OVER FIELDS II

Let F be a field. We prove here some additional results for the one-variable polynomial ring $F[x]$. The first is a restatement of results obtained earlier.

Proposition 15. The maximal ideals in $F[x]$ are the ideals $(f(x))$ generated by irreducible polynomials $f(x)$. In particular, $F[x]/(f(x))$ is a field if and only if $f(x)$ is irreducible.

Proof: This follows from Proposition 7 of Section 8.2 applied to the Principal Ideal Domain $F[x]$.

Proposition 16. Let $g(x)$ be a nonconstant element of $F[x]$ and let

$$g(x) = f_1(x)^{n_1} f_2(x)^{n_2} \cdots f_k(x)^{n_k}$$

be its factorization into irreducibles, where the $f_i(x)$ are distinct. Then we have the following isomorphism of rings:

$$F[x]/(g(x)) \cong F[x]/(f_1(x)^{n_1}) \times F[x]/(f_2(x)^{n_2}) \times \cdots \times F[x]/(f_k(x)^{n_k}).$$

Proof: This follows from the Chinese Remainder Theorem (Theorem 7.17), since the ideals $(f_i(x)^{n_i})$ and $(f_j(x)^{n_j})$ are comaximal if $f_i(x)$ and $f_j(x)$ are distinct (they are relatively prime in the Euclidean Domain $F[x]$, hence the ideal generated by them is $F[x]$).

The next result concerns the number of roots of a polynomial over a field F. By Proposition 9, a root α corresponds to a linear factor $(x-\alpha)$ of $f(x)$. If $f(x)$ is divisible by $(x-\alpha)^m$ but not by $(x-\alpha)^{m+1}$, then α is said to be a root of *multiplicity* m.

Proposition 17. If the polynomial $f(x)$ has roots $\alpha_1, \alpha_2, \ldots, \alpha_k$ in F (not necessarily distinct), then $f(x)$ has $(x-\alpha_1)\cdots(x-\alpha_k)$ as a factor. In particular, a polynomial of degree n in one variable over a field F has at most n roots in F, even counted with multiplicity.

Proof: The first statement follows easily by induction from Proposition 9. Since linear factors are irreducible, the second statement follows since $F[x]$ is a Unique Factorization Domain.

This last result has the following interesting consequence.