Note that the preceding definition concerns the concept *irreducible over F* and not just the concept *irreducible*. A polynomial $f(x)$ may be irreducible over F, but may not be irreducible if viewed over a larger field E containing F. We illustrate this.

28.9 Example Theorem 27.11 shows that $x^2 - 2$ viewed in $\mathbb{Q}[x]$ has no zeros in $\mathbb{Q}$. This shows that $x^2 - 2$ is irreducible over $\mathbb{Q}$, for a factorization $x^2 - 2 = (ax + b)(cx + d)$ for $a, b, c, d \in \mathbb{Q}$ would give rise to zeros of $x^2 - 2$ in $\mathbb{Q}$. However, $x^2 - 2$ viewed in $\mathbb{R}[x]$ is not irreducible over $\mathbb{R}$, because $x^2 - 2$ factors in $\mathbb{R}[x]$ into $(x - \sqrt{2})(x + \sqrt{2})$. ▲

It is worthwhile to remember that *the units in F[x] are precisely the nonzero elements of F*. Thus we could have defined an irreducible polynomial $f(x)$ as a nonconstant polynomial such that in any factorization $f(x) = g(x)h(x)$ in $F[x]$, either $g(x)$ or $h(x)$ is a unit.

28.10 Example Let us show that $f(x) = x^3 + 3x + 2$ viewed in $\mathbb{Z}_5[x]$ is irreducible over $\mathbb{Z}_5$. If $x^3 + 3x + 2$ factored in $\mathbb{Z}_5[x]$ into polynomials of lower degree then there would exist at least one linear factor of $f(x)$ of the form $x - a$ for some $a \in \mathbb{Z}_5$. But then $f(a)$ would be 0, by Corollary 28.4. However, $f(0) = 2$, $f(1) = 1$, $f(-1) = -2$, $f(2) = 1$, and $f(-2) = -2$, showing that $f(x)$ has no zeros in $\mathbb{Z}_5$. Thus $f(x)$ is irreducible over $\mathbb{Z}_5$. This test for irreducibility by finding zeros works nicely for quadratic and cubic polynomials over a finite field with a small number of elements. ▲

Irreducible polynomials will play a very important role in our work from now on. The problem of determining whether a given $f(x) \in F[x]$ is irreducible over F may be difficult. We now give some criteria for irreducibility that are useful in certain cases. One technique for determining irreducibility of quadratic and cubic polynomials was illustrated in Examples 28.9 and 28.10. We formalize it in a theorem.

28.11 Theorem Let $f(x) \in F[x]$, and let $f(x)$ be of degree 2 or 3. Then $f(x)$ is reducible over F if and only if it has a zero in F.

Proof If $f(x)$ is reducible so that $f(x) = g(x)h(x)$, where the degree of $g(x)$ and the degree of $h(x)$ are both less than the degree of $f(x)$, then since $f(x)$ is either quadratic or cubic, either $g(x)$ or $h(x)$ is of degree 1. If, say, $g(x)$ is of degree 1, then except for a possible factor in F, $g(x)$ is of the form $x - a$. Then $g(a) = 0$, which implies that $f(a) = 0$, so $f(x)$ has a zero in F.

Conversely, Corollary 28.4 shows that if $f(a) = 0$ for $a \in F$, then $x - a$ is a factor of $f(x)$, so $f(x)$ is reducible. ◆

We turn to some conditions for irreducibility over $\mathbb{Q}$ of polynomials in $\mathbb{Q}[x]$. The most important condition that we shall give is contained in the next theorem. The proof is to be worked out in Exercises 38–40.

28.12 Theorem If $f(x) \in \mathbb{Z}[x]$, then $f(x)$ factors into a product of two polynomials of lower degrees r and s in $\mathbb{Q}[x]$ if and only if it has such a factorization with polynomials of the same degrees r and s in $\mathbb{Z}[x]$. ⧫

28.13 Corollary If $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ is in $\mathbb{Z}[x]$ with $a_0 \neq 0$, and if $f(x)$ has a zero in $\mathbb{Q}$, then it has a zero m in $\mathbb{Z}$, and m must divide a_0.

Proof If $f(x)$ has a zero a in $\mathbb{Q}$, then $f(x)$ has a linear factor $x - a$ in $\mathbb{Q}[x]$ by Corollary 28.4. But then by Theorem 28.12, $f(x)$ has a factorization with a linear factor in $\mathbb{Z}[x]$, so for some $m \in \mathbb{Z}$ we must have

$$f(x) = (x - m)\big(x^{n-1} + \cdots - a_0/m\big).$$

Thus a_0/m is in $\mathbb{Z}$, so m divides a_0. ◆

28.14 Example Corollary 28.13 gives us another proof of the irreducibility of $x^2 - 2$ over $\mathbb{Q}$, for $x^2 - 2$ factors nontrivially in $\mathbb{Q}[x]$ if and only if it has a zero in $\mathbb{Q}$ by Theorem 28.11. By Corollary 28.13, it has a zero in $\mathbb{Q}$ if and only if it has a zero in $\mathbb{Z}$, and moreover the only possibilities are the divisors ± 1 and ± 2 of 2. A quick check shows that none of these numbers is a zero of $x^2 - 2$. ▲

28.15 Example Let us use Theorem 28.12 to show that

$$f(x) = x^4 - 2x^2 + 8x + 1$$

viewed in $\mathbb{Q}[x]$ is irreducible over $\mathbb{Q}$. If $f(x)$ has a linear factor in $\mathbb{Q}[x]$, then it has a zero in $\mathbb{Z}$, and by Corollary 28.13, this zero would have to be a divisor in $\mathbb{Z}$ of 1, that is, either ± 1. But $f(1) = 8$, and $f(-1) = -8$, so such a factorization is impossible.

If $f(x)$ factors into two quadratic factors in $\mathbb{Q}[x]$, then by Theorem 28.12, it has a factorization.

$$(x^2 + ax + b)(x^2 + cx + d)$$

in $\mathbb{Z}[x]$. Equating coefficients of powers of x, we find that we must have

$$bd = 1, \quad ad + bc = 8, \quad ac + b + d = -2, \quad \text{and} \quad a + c = 0$$

for integers $a, b, c, d \in \mathbb{Z}$. From $bd = 1$, we see that either $b = d = 1$ or $b = d = -1$. In any case, $b = d$ and from $ad + bc = 8$, we deduce that $d(a + c) = 8$. But this is impossible since $a + c = 0$. Thus a factorization into two quadratic polynomials is also impossible and $f(x)$ is irreducible over $\mathbb{Q}$. ▲

We conclude our irreducibility criteria with the famous Eisenstein criterion for irreducibility. An additional very useful criterion is given in Exercise 37.

28.16 Theorem **(Eisenstein Criterion)** Let $p \in \mathbb{Z}$ be a prime. Suppose that $f(x) = a_n x^n + \cdots + a_0$ is in $\mathbb{Z}[x]$, and $a_n \not\equiv 0 \pmod{p}$, but $a_i \equiv 0 \pmod{p}$ for all $i < n$, with $a_0 \not\equiv 0 \pmod{p^2}$. Then $f(x)$ is irreducible over $\mathbb{Q}$.

Proof By Theorem 28.12 we need only show that $f(x)$ does not factor into polynomials of lower degree in $\mathbb{Z}[x]$. If

$$f(x) = \left(b_r x^r + \cdots + b_0\right)\left(c_s x^s + \cdots + c_0\right)$$

is a factorization in $\mathbb{Z}[x]$, with $b_r \not\equiv 0, c_s \not\equiv 0$ and $r, s < n$, then $a_0 \not\equiv 0 \pmod{p^2}$ implies that b_0 and c_0 are not both congruent to 0 modulo p. Suppose that $b_0 \not\equiv 0 \pmod{p}$ and $c_0 \equiv 0 \pmod{p}$. Now $a_n \not\equiv 0 \pmod{p}$ implies that $b_r, c_s \not\equiv 0 \pmod{p}$, since $a_n = b_r c_s$. Let m be the smallest value of k such that $c_k \not\equiv 0 \pmod{p}$. Then

$$a_m = b_0 c_m + b_1 c_{m-1} + \cdots + \begin{cases} b_m c_0 \text{ if } r \geq m, \\ b_r c_{m-r} \text{ if } r < m. \end{cases}$$

The fact that neither b_0 nor c_m are congruent to 0 modulo p while $c_{m-1}, \cdots, c_0$ are all congruent to 0 modulo p implies that $a_m \not\equiv 0$ modulo p, so $m = n$. Consequently, $s = n$, contradicting our assumption that $s < n$; that is, that our factorization was nontrivial. ◆

Note that if we take $p = 2$, the Eisenstein criterion gives us still another proof of the irreducibility of $x^2 - 2$ over $\mathbb{Q}$.

28.17 Example Taking $p = 3$, we see by Theorem 28.16 that

$$25x^5 - 9x^4 - 3x^2 - 12$$

is irreducible over $\mathbb{Q}$. ▲

28.18 Corollary The polynomial

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

is irreducible over $\mathbb{Q}$ for any prime p.

Proof Again by Theorem 28.12, we need only consider factorizations in $\mathbb{Z}[x]$. We remarked following Theorem 27.4 that its proof actually shows that evaluation homomorphisms can be used for commutative rings. Here we want to use the evaluation homomorphism $\phi_{x+1} : \mathbb{Q}[x] \to \mathbb{Q}[x]$. It is natural for us to denote $\phi_{x+1}(f(x))$ by $f(x+1)$ for $f(x) \in \mathbb{Q}[x]$. Let

$$g(x) = \Phi_p(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = \frac{x^p + \binom{p}{1} x^{p-1} + \cdots + px}{x}.$$

The coefficient of x^{p-r} for $0 < r < p$ is the binomial coefficient $p!/[r!(p-r)!]$, which is divisible by p because p divides $p!$ but does not divide either $r!$ or $(p-r)!$ when $0 < r < p$. Thus

$$g(x) = x^{p-1} + \binom{p}{1} x^{p-2} + \cdots + p$$

satisfies the Eisenstein criterion for the prime p and is thus irreducible over $\mathbb{Q}$. But if $\Phi_p(x) = h(x)r(x)$ were a nontrivial factorization of $\Phi_p(x)$ in $\mathbb{Z}[x]$, then

$$\Phi_p(x+1) = g(x) = h(x+1)r(x+1)$$

would give a nontrivial factorization of $g(x)$ in $\mathbb{Z}[x]$. Thus $\Phi_p(x)$ must also be irreducible over $\mathbb{Q}$. ◆

The polynomial $\Phi_p(x)$ in Corollary 28.18 is the **p^{th} cyclotomic polynomial.**

Uniqueness of Factorization in $F[x]$

Polynomials in $F[x]$ can be factored into a product of irreducible polynomials in $F[x]$ in an essentially unique way. For $f(x), g(x) \in F[x]$ we say that $g(x)$ **divides** $f(x)$ **in** $F[x]$ if there exists $q(x) \in F[x]$ such that $f(x) = g(x)q(x)$. Note the similarity of the theorem that follows with Property (1) for $\mathbb{Z}$ following Example 6.9.

28.19 Theorem Let $p(x)$ be an irreducible polynomial in $F[x]$. If $p(x)$ divides $r(x)s(x)$ for $r(x), s(x) \in F[x]$, then either $p(x)$ divides $r(x)$ or $p(x)$ divides $s(x)$.

Proof We delay the proof of this theorem to Section 31. (See Theorem 31.27.) ◆

28.20 Corollary If $p(x)$ is irreducible in $F[x]$ and $p(x)$ divides the product $r_1(x) \cdots r_n(x)$ for $r_i(x) \in F[x]$, then $p(x)$ divides $r_i(x)$ for at least one i.

Proof Using mathematical induction, we find that this is immediate from Theorem 28.19. ◆

28.21 Theorem If F is a field, then every nonconstant polynomial $f(x) \in F[x]$ can be factored in $F[x]$ into a product of irreducible polynomials, the irreducible polynomials being unique except for order and for unit (that is, nonzero constant) factors in F.

Proof Let $f(x) \in F[x]$ be a nonconstant polynomial. If $f(x)$ is not irreducible, then $f(x) = g(x)h(x)$, with the degree of $g(x)$ and the degree of $h(x)$ both less than the degree of $f(x)$.