3.85 Let $\zeta = e^{2\pi i/n}$.

(i) Prove that

$$x^n - 1 = (x - 1)(x - \zeta)(x - \zeta^2) \cdots (x - \zeta^{n-1})$$

and, if $n$ is odd, that

$$x^n + 1 = (x + 1)(x + \zeta)(x + \zeta^2) \cdots (x + \zeta^{n-1}).$$

**Solution.** The $n$ numbers $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$ are all distinct. But they are all roots of $x^n - 1$, and so Theorem 3.50 gives the first equation:

$$x^n - 1 = (x - 1)(x - \zeta)(x - \zeta^2) \cdots (x - \zeta^{n-1}).$$

If $n$ is odd, then replace $x$ by $-x$ to get

$$(-x)^n - 1 = (-x - 1)(-x - \zeta)(-x - \zeta^2) \cdots (-x - \zeta^{n-1})$$

$$= (-1)^n(x + 1)(x + \zeta)(x + \zeta^2) \cdots (x + \zeta^{n-1}).$$

Since $n$ is odd,

$$(-x)^n - 1 = -x^n - 1 = -(x^n + 1),$$

and one can now cancel the minus sign from each side.

(ii) For numbers $a$ and $b$, prove that

$$a^n - b^n = (a - b)(a - \zeta b)(a - \zeta^2 b) \cdots (a - \zeta^{n-1} b)$$

and, if $n$ is odd, that

$$a^n + b^n = (a + b)(a + \zeta b)(a + \zeta^2 b) \cdots (a + \zeta^{n-1} b).$$

**Solution.** If $b = 0$, then both sides equal $a^n$; if $b \neq 0$, then set $x = a/b$ in part (ii).

(iii) $f(x) = 2x^3 - x - 6$.

**Solution.** There are no rational roots: the candidates are

$$\pm \frac{1}{2}, \pm 1, \pm \frac{3}{2}, \pm 2, \pm 3, \pm 6.$$

Therefore, $f(x)$ is irreducible, by Proposition 3.65.

(vi) $f(x) = x^5 - 4x + 2$.

**Solution.** $f(x)$ is irreducible, by the Eisenstein criterion with $p = 2$.  

(viii) \( f(x) = x^4 - 10x^2 + 1. \)

**Solution.** \( f(x) \) has no rational roots, for the only candidates are \( \pm 1 \). Suppose that
\[
x^4 - 10x^2 + 1 = (x^2 + ax + b)(x^2 - ax + c) \text{ in } \mathbb{Q}[x]
\]
(we may assume the coefficient of \( x \) in the second factor is \(-a\) because \( f(x) \) has no cubic term). Expanding and equating coefficients gives the following equations:
\[
c + b - a^2 = 10
\]
\[
a(c - b) = 0
\]
\[
bc = 1.
\]
The middle equation gives \( a(c - b) = 0 \), so that either \( a = 0 \) or \( b = c \). In the first case, we obtain
\[
c + b = 10
\]
\[
bc = 1.
\]
Substituting \( c = b^{-1} \), the first equation gives \( b^2 - 10b + 1 = 0 \).
But the quadratic formula gives \( b = 5 \pm 2\sqrt{6} \), which is irrational.
On the other hand, if \( b = c \), then \( bc = 1 \) implies \( b = \pm 1 = c \). The first equation gives \( a^2 = -10 \pm 2 < 0 \), and this is also impossible.
We conclude that there is no factorization of \( f(x) \) in \( \mathbb{Q}[x] \).

(ix) \( f(x) = x^6 - 210x - 616. \)

**Solution.** Eisenstein’s criterion applies, for \( 7 \mid 210 \) and \( 7 \mid 616 \), but \( 7^2 \nmid 616 \).

(x) \( f(x) = 350x^3 + x^2 + 4x + 1. \)

**Solution.** Reducing mod 3 to gives an irreducible cubic in \( \mathbb{F}_3[x] \).
3.89 Prove that there are exactly 6 irreducible quintics in $\mathbb{F}_2[x]$.

**Solution.** There are 32 quintics in $\mathbb{F}_2[x]$, 16 of which have constant term 0; that is, have 0 as a root. Of the 16 remaining polynomials, we may discard those having an even number of nonzero terms, for 1 is a root of these; and now there are 8. If a quintic $f(x)$ with no roots is not irreducible, then its factors are irreducible polynomials of degrees 2 and 3; that is,

$$f(x) = (x^2 + x + 1)(x^3 + x + 1) = x^5 + x^4 + 1,$$

or

$$f(x) = (x^2 + x + 1)(x^3 + x^2 + 1) = x^5 + x + 1.$$

Thus, the irreducible polynomials are:

$$x^5 + x^3 + x^2 + x + 1 \quad x^5 + x^4 + x^2 + x + 1$$
$$x^5 + x^4 + x^3 + x + 1 \quad x^5 + x^4 + x^3 + x^2 + 1$$
$$x^5 + x^3 + 1 \quad x^5 + x^2 + 1.$$
3.91 Let $k$ be a field, and let $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in k[x]$ have degree $n$. If $f(x)$ is irreducible, then so is $a_n + a_{n-1} x + \cdots + a_0 x^n$.

**Solution.** If $f^*(x)$ denotes the polynomial $f(x)$ with coefficients reversed, then a factorization $f^*(x) = g(x)h(x)$ gives a factorization $f(x)$. One sees this just by using the definition of multiplication of polynomials. Let $g(x) = \sum_{i=0}^{p} b_i x^i$ and $h(x) = \sum_{j=0}^{q} c_j x^j$, where $p + q = n$. Thus,

$$a_{n-m} = \sum_{i+j = m} b_i c_j.$$

It follows that

$$\sum_{i+j = n-m} b_{p-i} c_{q-j} = a_{n-(n-m)} = a_k.$$

Therefore, if we define $g^*(x) = \sum_{i=0}^{p} b_{p-i} x^i$ and $h^*(x) = \sum_{j=0}^{q} c_{q-j} x^j$, then $f(x) = g^*(x)h^*(x)$, contradicting the irreducibility of $f(x)$.

Note that $f(x) \mapsto f^*(x)$, which reverses coefficients, is not a well-defined function $k[x] \to k[x]$, because it is not clear how to define $f^*(x)$ if the constant term of $f(x)$ is zero. And even if one makes a bona fide definition, the function is not a homomorphism. For example, let $f(x) = x^5 + 3x^4$; that is, in sequence notation,

$$f(x) = (0, 0, 0, 0, 3, 1, 0, \ldots).$$

Let $g(x) = x^3 + x$; in sequence notation,

$$g(x) = (0, 1, 0, 1, 0, \ldots).$$

Now $f(x)g(x) = [x^8 + 3x^7 + x^6 + 4x^5 + 3x^4]$; in sequence notation,

$$f(x)g(x) = (0, 0, 0, 0, 3, 4, 1, 3, 1, 0, \ldots).$$

Therefore,

$$[f(x)g(x)]^* = 3x^4 + 4x^3 + 3x^2 + 3x + 1,$$

which is a quartic. But $f^*(x) = 3x + 1$ and $g^*(x) = x^2 + 1$, so that $f^*(x)g^*(x)$ is a cubic. Therefore, $[fg]^* \neq f^*g^*$.

3.103 If $E = \mathbb{F}_2[x]/(p(x))$, where $p(x) = x^3 + x + 1$, then $E$ is a field with 8 elements. Show that a root $\pi$ of $p(x)$ is a primitive element of $E$ by writing every nonzero element of $E$ as a power of $\pi$.

**Solution.** See Example 4.127.
3.105 If $E$ is a finite field, use Cauchy’s theorem to prove that $|E| = p^n$ for some prime $p$ and some $n \geq 1$.

Solution. If $k$ is the prime field of $E$, then Proposition 3.110 says that $k \cong \mathbb{Q}$ or $k \cong \mathbb{F}_p$ for some prime $p$; since $\mathbb{Q}$ is infinite, we have $k$ of characteristic $p$. Therefore, $pa = 0$ for all $a \in E$; that is, as an additive abelian group, every nonzero element in $E$ has order $p$. If there is a prime divisor $q$ of $|E|$ with $q \neq p$, then Cauchy’s theorem gives a nonzero element $b \in E$ with $qb = 0$, contradicting every nonzero element having order $p$. We conclude that $|E| = p^n$ for some $n \geq 1$. 