Introduction to Modern Algebra

Part IV. Rings and Fields

IV.23. Factorizations of Polynomials over a Field

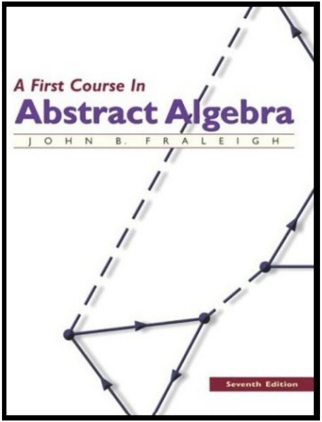

Table of contents

Theorem 23.1

Theorem 23.1. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$ and $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_2 x^2 + b_1 x + b_0$ be in $F[x]$, with a_n and b_n both nonzero and $m > 0$. Then there are unique polynomials $g(x)$ and $r(x)$ in $F[x]$ such that $f(x) = q(x)g(x) + r(x)$, where either $r(x) = 0$ or the degree of $r(x)$ is less than the degree m of $g(x)$.

Proof. Consider the set $S = \{f(x) - g(x)s(x) \mid s(x) \in F[x]\}$. If $0 \in S$ then there exists $s(x)$ such that $f(x) - g(x)s(x) = 0$, so $f(x) = g(x)s(x)$. With $g(x) = s(x)$ and $r(x) = 0$,the result follows. Otherwise, let $r(x)$ be an element of minimal degree in S. Then $f(x) = g(x)g(x) + r(x)$ for some $g(x) \in F[x]$.

Theorem 23.1

Theorem 23.1. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2x^2 + a_1x + a_0$ and $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_2x^2 + b_1x + b_0$ be in $F[x]$, with a_n and b_n both nonzero and $m > 0$. Then there are unique polynomials $g(x)$ and $r(x)$ in $F[x]$ such that $f(x) = q(x)g(x) + r(x)$, where either $r(x) = 0$ or the degree of $r(x)$ is less than the degree m of $g(x)$.

Proof. Consider the set $S = \{f(x) - g(x)s(x) \mid s(x) \in F[x]\}$. If $0 \in S$ then there exists $s(x)$ such that $f(x) - g(x)s(x) = 0$, so $f(x) = g(x)s(x)$. With $g(x) = s(x)$ and $r(x) = 0$,the result follows. Otherwise, let $r(x)$ be an element of minimal degree in S. Then $f(x) = g(x)g(x) + r(x)$ for some $g(x) \in F[x]$. To show that the degree of $r(x)$ is less than m, suppose $r(x) = c_t x^t + c_{t-1} + \cdots + c_2x^2 + c_1x + c_0$, with $c_j \in F$ and $c_t \neq 0$. ASSUME $t \geq m$, then

$$f(x) - q(x)g(x) - \left(\left(\frac{c_t}{b_m}\right)x^{t-m}g(x)\right) = r(x) - \left(\left(\frac{c_t}{b_m}\right)x^{t-m}g(x)\right). \quad (*)$$

Theorem 23.1

Theorem 23.1. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2x^2 + a_1x + a_0$ and $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_2x^2 + b_1x + b_0$ be in $F[x]$, with a_n and b_n both nonzero and $m > 0$. Then there are unique polynomials $g(x)$ and $r(x)$ in $F[x]$ such that $f(x) = q(x)g(x) + r(x)$, where either $r(x) = 0$ or the degree of $r(x)$ is less than the degree m of $g(x)$.

Proof. Consider the set $S = \{f(x) - g(x)s(x) \mid s(x) \in F[x]\}$. If $0 \in S$ then there exists $s(x)$ such that $f(x) - g(x)s(x) = 0$, so $f(x) = g(x)s(x)$. With $g(x) = s(x)$ and $r(x) = 0$,the result follows. Otherwise, let $r(x)$ be an element of minimal degree in S. Then $f(x) = g(x)g(x) + r(x)$ for some $g(x) \in F[x]$. To show that the degree of $r(x)$ is less than m, suppose $r(x) = c_t x^t + c_{t-1} + \cdots + c_2x^2 + c_1x + c_0$, with $c_j \in F$ and $c_t \neq 0$. ASSUME $t \geq m$, then

$$f(x) - q(x)g(x) - \left(\left(\frac{c_t}{b_m}\right)x^{t-m}g(x)\right) = r(x) - \left(\left(\frac{c_t}{b_m}\right)x^{t-m}g(x)\right). \quad (*)$$

Theorem 23.1 (continued 1)

Proof (continued). The right-hand-side of $(*)$ is of the form

$$r(x) - \left(c_t x^t + \frac{c_t b_{m-1}}{b_m} x^{t-2} + \cdots + \frac{c_t b_2}{b_m} x^2 + \frac{c_t b_1}{b_m} x + \frac{c_t b_0}{b_m}\right),$$

which is a polynomial of degree $t-1$ or less. However, the left-hand-side of $(*)$ can be written in the form $f(x) = g(x)\left[g(x) + \frac{c_t}{b_m} x^{t-m}\right]$, and this is in S since $g(x) + \left(\frac{c_t}{b_m}\right) x^{t-m} \in F[x]$ ($c_t/b_m \in F$ since F is a field).
But this, CONTRADICTS the fact that $r(x)$ is of minimal (positive) degree in S and is described above. So the assumption that $t \geq m$ is false, and hence $t < m$. That is, $r(x)$ is of degree less than the degree m of $g(x)$, as claimed.

Theorem 23.1 (continued 1)

Proof (continued). The right-hand-side of $(*)$ is of the form

$$r(x) - \left(c_t x^t + \frac{c_t b_{m-1}}{b_m} x^{t-2} + \cdots + \frac{c_t b_2}{b_m} x^2 + \frac{c_t b_1}{b_m} x + \frac{c_t b_0}{b_m} \right),$$

which is a polynomial of degree $t-1$ or less. However, the left-hand-side of $(*)$ can be written in the form $f(x) = g(x) \left[g(x) + \frac{c_t}{b_m} x^{t-m} \right]$, and this is in S since $g(x) + \left(\frac{c_t}{b_m} \right) x^{t-m} \in F[x]$ ($c_t / b_m \in F$ since F is a field). But this, CONTRADICTS the fact that $r(x)$ is of minimal (positive) degree in S and is described above. So the assumption that $t \geq m$ is false, and hence $t < m$. That is, $r(x)$ is of degree less than the degree m of $g(x)$, as claimed. Now to show the uniqueness of $g(x)$ and $r(x)$. If $f(x) = g(x) g_1(x) + r_1(x)$ and $f(x) = g(x) g_2(x) + r_2(x)$, then subtracting these we

$$g(x)(g_1(x) - g_2(x)) = r_2(x) - r_1(x). \qquad (**)$$

Theorem 23.1 (continued 1)

Proof (continued). The right-hand-side of $(*)$ is of the form

$$r(x) - \left(c_t x^t + \frac{c_t b_{m-1}}{b_m} x^{t-2} + \cdots + \frac{c_t b_2}{b_m} x^2 + \frac{c_t b_1}{b_m} x + \frac{c_t b_0}{b_m} \right),$$

which is a polynomial of degree $t-1$ or less. However, the left-hand-side of $(*)$ can be written in the form $f(x) = g(x)\left[g(x) + \frac{c_t}{b_m} x^{t-m}\right]$, and this is in S since $g(x) + \left(\frac{c_t}{b_m}\right) x^{t-m} \in F[x]$ ($c_t / b_m \in F$ since F is a field). But this, CONTRADICTS the fact that $r(x)$ is of minimal (positive) degree in S and is described above. So the assumption that $t \geq m$ is false, and hence $t < m$. That is, $r(x)$ is of degree less than the degree m of $g(x)$, as claimed. Now to show the uniqueness of $g(x)$ and $r(x)$. If $f(x) = g(x) g_1(x) + r_1(x)$ and $f(x) = g(x) g_2(x) + r_2(x)$, then subtracting these we

$$g(x)(g_1(x) - g_2(x)) = r_2(x) - r_1(x). \qquad (**)$$

Theorem 23.1 (continued 2).

Theorem 23.1. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$ and $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_2 x^2 + b_1 x + b_0$ be in $F[x]$, with a_n and b_n both nonzero and $m > 0$. Then there are unique polynomials $g(x)$ and $r(x)$ in $F[x]$ such that $f(x) = q(x)g(x) + r(x)$, where either $r(x) = 0$ or the degree of $r(x)$ is less than the degree m of $g(x)$.

Proof (continued). As above, the remainders $r_1(x)$ and $r_2(x)$ are either 0 or of degree less than the degree of $g(x)$. So $r_1(x) - r_2(x)$ is either 0 or of degree less than the degree of $g(x)$. These can only hold if $g_1(x) - g_2(x) = 0$; that is, $g_1(x) = g_2(x)$. But then the left-hand-side of $(**)$ is 0 and so $r_1(x) = r_2(x)$. Therefore, $r_1(x) = r_2(x)$ and $g_1(x) = g_2(x)$ and the remainders and quotient functions are unique, as claimed. □

Corollary 23.3. Factor Theorem

Corollary 23.3. Factor Theorem. An element $a \in F$ (for F a field) is a zero of $f(x) \in F[x]$ if and only if $x = a$ is a factor of $f(x)$ in $F[x]$.

Proof. Suppose that for $a \in F$, $f(a) = 0$. By Theorem 23.1, there exists $g(x), r(x) \in F[x]$ such that $f(x) = (x - a)g(x) + r(x)$ where either $r(x) = 0$ or the degree of $r(x)$ is less than the degree of $g(x) = x - a$ (i.e., less than 1). But then $r(x)$ must be a constant function $r(x) = c$ for some $c \in F$. So $f(x) = (x - a)g(x) + c$. Applying the evaluation homomorphism φ_a to $f(x)$ gives $0 = f(a) = 0g(x) + c = c$.

Corollary 23.3. Factor Theorem

Corollary 23.3. Factor Theorem. An element $a \in F$ (for F a field) is a zero of $f(x) \in F[x]$ if and only if $x = a$ is a factor of $f(x)$ in $F[x]$.

Proof. Suppose that for $a \in F$, $f(a) = 0$. By Theorem 23.1, there exists $g(x), r(x) \in F[x]$ such that $f(x) = (x - a)g(x) + r(x)$ where either $r(x) = 0$ or the degree of $r(x)$ is less than the degree of $g(x) = x - a$ (i.e., less than 1). But then $r(x)$ must be a constant function $r(x) = c$ for some $c \in F$. So $f(x) = (x - a)g(x) + c$. Applying the evaluation homomorphism φ_a to $f(x)$ gives $0 = f(a) = 0g(x) + c = c$. So, $c = 0$, and $f(x) = (x - a)g(x)$. That is, $(x - a)$ is a factor of $f(x)$. Now suppose $(x - a)$ is a factor of $f(x)$ in $F[x]$, where $a \in F$. Then applying φ_a to $f(x) = (x - a)g(x)$, we get $f(a) = 0$. □

Corollary 23.3. Factor Theorem

Corollary 23.3. Factor Theorem. An element $a \in F$ (for F a field) is a zero of $f(x) \in F[x]$ if and only if $x = a$ is a factor of $f(x)$ in $F[x]$.

Proof. Suppose that for $a \in F$, $f(a) = 0$. By Theorem 23.1, there exists $g(x), r(x) \in F[x]$ such that $f(x) = (x - a)\,g(x) + r(x)$ where either $r(x) = 0$ or the degree of $r(x)$ is less than the degree of $g(x) = x - a$ (i.e., less than 1). But then $r(x)$ must be a constant function $r(x) = c$ for some $c \in F$. So $f(x) = (x - a)\,g(x) + c$. Applying the evaluation homomorphism φ_a to $f(x)$ gives $0 = f(a) = 0g(x) + c = c$. So, $c = 0$, and $f(x) = (x - a)\,g(x)$. That is, $(x - a)$ is a factor of $f(x)$. Now suppose $(x - a)$ is a factor of $f(x)$ in $F[x]$, where $a \in F$. Then applying φ_a to $f(x) = (x - a)\,g(x)$, we get $f(a) = 0$. □

Corollary 23.5

Corollary 23.5. A nonzero polynomial $f(x) \in F[x]$ of degree n can have at most n zeros in a field F.

Proof. By the Factor Theorem, $a_1 \in F$ is a zero of $f(x)$ implies $f(x) = (x - a_1) g_1(x)$ where $g(x)$ is of degree $n - 1$. A zero $a_2 \in F$ of $g_1(x)$ then yields a factorization $f(x) = (x - a_1)(x - a_2) g_2(x)$.

Corollary 23.5

Corollary 23.5. A nonzero polynomial $f(x) \in F[x]$ of degree n can have at most n zeros in a field F.

Proof. By the Factor Theorem, $a_1 \in F$ is a zero of $f(x)$ implies $f(x) = (x - a_1)\, g_1(x)$ where $g(x)$ is of degree $n - 1$. A zero $a_2 \in F$ of $g_1(x)$ then yields a factorization $f(x) = (x - a_1)(x - a_2)\, g_2(x)$. Similarly, we can further factor as $f(x) = (x - a_1)(x - a_2) \cdots (x - a_r)\, q_r(x)$ where $q_r(x)$ has no zero in F. Since $f(x)$ is of degree n, then $r \leq n$. If $b \in F$ and $b \neq a_i$ for $i = 1, 2, \ldots, r$ then
$f(b) = (b - a_1)(b - a_2) \cdots (b - x_r)\, q_r(b) \neq 0$ since none of $b - a_i$ is zero, $g_r(b) \neq 0$ by construction of q_r, and F has no zero divisors (F is a field). So the a_i for $i = 1, 2, \ldots, r$ are all of the zeros of $f(x)$ and so $f(x)$ has at most n zeros in F (because $r \leq n$), as claimed. □

Corollary 23.5

Corollary 23.5. A nonzero polynomial $f(x) \in F[x]$ of degree n can have at most n zeros in a field F.

Proof. By the Factor Theorem, $a_1 \in F$ is a zero of $f(x)$ implies $f(x) = (x - a_1)\, g_1(x)$ where $g(x)$ is of degree $n - 1$. A zero $a_2 \in F$ of $g_1(x)$ then yields a factorization $f(x) = (x - a_1)(x - a_2)\, g_2(x)$. Similarly, we can further factor as $f(x) = (x - a_1)(x - a_2) \cdots (x - a_r)\, q_r(x)$ where $q_r(x)$ has no zero in F. Since $f(x)$ is of degree n, then $r \leq n$. If $b \in F$ and $b \neq a_i$ for $i = 1, 2, \ldots, r$ then
$f(b) = (b - a_1)(b - a_2) \cdots (b - x_r)\, q_r(b) \neq 0$ since none of $b - a_i$ is zero, $g_r(b) \neq 0$ by construction of q_r, and F has no zero divisors (F is a field). So the a_i for $i = 1, 2, \ldots, r$ are all of the zeros of $f(x)$ and so $f(x)$ has at most n zeros in F (because $r \leq n$), as claimed. $\square$

Corollary 23.6

Corollary 23.6. If G is a finite subgroup of the multiplicative group $\langle F^*, \cdot \rangle$ of a field F, then G is cyclic. In particular, the multiplicative group of all nonzero elements of a finite field is cyclic.

Proof. Since $\langle F^*, \cdot \rangle$ is abelian, then G is a finite abelian group. So by the Fundamental Theorem of Finitely Generated Abelian Groups (Theorem I.11.12) G is isomorphic to a direct product $\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_r}$, $d_i = (p_i)^{n_i}$, where each d_i is a proven of a prime. So each $\mathbb{Z}_{d_i}$ is a cyclic group of order d_i - we use multiplication notation for each since we are dealing with subgroups of the multiplicative group $\langle F^*, \cdot \rangle$.

Corollary 23.6

Corollary 23.6. If G is a finite subgroup of the multiplicative group $\langle F^*, \cdot \rangle$ of a field F, then G is cyclic. In particular, the multiplicative group of all nonzero elements of a finite field is cyclic.

Proof. Since $\langle F^*, \cdot \rangle$ is abelian, then G is a finite abelian group. So by the Fundamental Theorem of Finitely Generated Abelian Groups (Theorem I.11.12) G is isomorphic to a direct product $\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_r}$, $d_i = (p_i)^{n_i}$, where each d_i is a proven of a prime. So each $\mathbb{Z}_{d_i}$ is a cyclic group of order d_i - we use multiplication notation for each since we are dealing with subgroups of the multiplicative group $\langle F^*, \cdot \rangle$. Let $m = \text{lcm}\,(d_1, d_2, \ldots, d_r)$. Then $m \leq d_1 d_2 \cdots d_r$. If $a_i \in \mathbb{Z}_{d_i}$ then $a_i^{d_i} = 1$ (notice $d_i \equiv 0$ in $\mathbb{Z}_{d_i}$) and $a_i^m = 1$ (since $m \equiv 0$ in $\mathbb{Z}_{d_i}$). So for any $a \in G$, we have $a^m = 1$. So every element of G is a zero of $x^m - 1$ in $G[x]$. But G has $d_1 d_2 \cdots d_r$ elements while $x^m - 1$ has at most m zeros in F by Corollary 23.5, so $m \geq d_1 d_2 \ldots d_m$.

Corollary 23.6

Corollary 23.6. If G is a finite subgroup of the multiplicative group $\langle F^*, \cdot \rangle$ of a field F, then G is cyclic. In particular, the multiplicative group of all nonzero elements of a finite field is cyclic.

Proof. Since $\langle F^*, \cdot \rangle$ is abelian, then G is a finite abelian group. So by the Fundamental Theorem of Finitely Generated Abelian Groups (Theorem I.11.12) G is isomorphic to a direct product $\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_r}$, $d_i = (p_i)^{n_i}$, where each d_i is a proven of a prime. So each $\mathbb{Z}_{d_i}$ is a cyclic group of order d_i - we use multiplication notation for each since we are dealing with subgroups of the multiplicative group $\langle F^*, \cdot \rangle$. Let $m = \text{lcm}\,(d_1, d_2, \ldots, d_r)$. Then $m \le d_1 d_2 \cdots d_r$. If $a_i \in \mathbb{Z}_{d_i}$ then $a_i^{d_i} = 1$ (notice $d_i \equiv 0$ in $\mathbb{Z}_{d_i}$) and $a_i^m = 1$ (since $m \equiv 0$ in $\mathbb{Z}_{d_i}$). So for any $a \in G$, we have $a^m = 1$. So every element of G is a zero of $x^m - 1$ in $G\,[x]$. But G has $d_1 d_2 \cdots d_r$ elements while $x^m - 1$ has at most m zeros in F by Corollary 23.5, so $m \ge d_1 d_2 \ldots d_m$. Therefore $m = d_1 d_2 \cdots d_r$ and the primes involved in the prime powers $d_1 d_2 \cdots d_r$ are distinct. By Corollary 11.6, $G \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_r}$ is cyclic and isomorphic to $\mathbb{Z}_m$. □

Corollary 23.6

Corollary 23.6. If G is a finite subgroup of the multiplicative group $\langle F^*, \cdot \rangle$ of a field F, then G is cyclic. In particular, the multiplicative group of all nonzero elements of a finite field is cyclic.

Proof. Since $\langle F^*, \cdot \rangle$ is abelian, then G is a finite abelian group. So by the Fundamental Theorem of Finitely Generated Abelian Groups (Theorem I.11.12) G is isomorphic to a direct product $\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_r}$, $d_i = (p_i)^{n_i}$, where each d_i is a proven of a prime. So each $\mathbb{Z}_{d_i}$ is a cyclic group of order d_i - we use multiplication notation for each since we are dealing with subgroups of the multiplicative group $\langle F^*, \cdot \rangle$. Let $m = \operatorname{lcm}(d_1, d_2, \ldots, d_r)$. Then $m \leq d_1 d_2 \cdots d_r$. If $a_i \in \mathbb{Z}_{d_i}$ then $a_i^{d_i} = 1$ (notice $d_i \equiv 0$ in $\mathbb{Z}_{d_i}$) and $a_i^m = 1$ (since $m \equiv 0$ in $\mathbb{Z}_{d_i}$). So for any $a \in G$, we have $a^m = 1$. So every element of G is a zero of $x^m - 1$ in $G[x]$. But G has $d_1 d_2 \cdots d_r$ elements while $x^m - 1$ has at most m zeros in F by Corollary 23.5, so $m \geq d_1 d_2 \ldots d_m$. Therefore $m = d_1 d_2 \cdots d_r$ and the primes involved in the prime powers $d_1 d_2 \cdots d_r$ are distinct. By Corollary 11.6, $G \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_r}$ is cyclic and isomorphic to $\mathbb{Z}_m$. □

Theorem 23.10

Theorem 23.10. 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 then $f(x) = g(x)h(x)$ where the degrees of $g(x)$ and $h(x)$ are both less than the degree of $f(x)$. Since the degree of $f(x)$ is 2 or 3, then the degree of either $g(x)$ or $h(x)$ must be 1. The factor of degree 1 yields a zero of $f(x)$ in F, as claimed.

If $f(a) = 0$ for $a \in F$, then $x - a$ is a factor of $f(x)$ (by the Factor Theorem), as claimed. $\square$

Theorem 23.10

Theorem 23.10. 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 then $f(x) = g(x)h(x)$ where the degrees of $g(x)$ and $h(x)$ are both less than the degree of $f(x)$. Since the degree of $f(x)$ is 2 or 3, then the degree of either $g(x)$ or $h(x)$ must be 1. The factor of degree 1 yields a zero of $f(x)$ in F, as claimed.

If $f(a) = 0$ for $a \in F$, then $x - a$ is a factor of $f(x)$ (by the Factor Theorem), as claimed. $\square$

Corollary 23.12

Corollary 23.12. If $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ 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 by the Factor Theorem, $x - a$ is a factor of $f(x)$. By Theorem 23.11, $f(x)$ has a factorization in $\mathbb{Z}[x]$ also involving a linear term $(x - m)$ for some $m \in \mathbb{Z}$:
$f(x) = (x - m)\left(x^{n-1} + \cdots - \frac{a_0}{m}\right)$. So $a_0/m \in \mathbb{Z}$ and m divides a_0. □

Corollary 23.12

Corollary 23.12. If $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ 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 by the Factor Theorem, $x - a$ is a factor of $f(x)$. By Theorem 23.11, $f(x)$ has a factorization in $\mathbb{Z}[x]$ also involving a linear term $(x - m)$ for some $m \in \mathbb{Z}$:
$f(x) = (x - m)\left(x^{n-1} + \cdots - \frac{a_0}{m}\right)$. So $a_0/m \in \mathbb{Z}$ and m divides a_0. □

Theorem 23.15. Eisenstein Criterion

Theorem 23.15. Let $p \in \mathbb{Z}$ be a prime. Suppose $f(x) = a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0 \in \mathbb{Z}[x]$, and $a_n \not\equiv 0 \pmod{p}$, but $a_i = 0 \pmod{p}$ and for all $i < n$, with $a_0 \not\equiv 0 \left(\text{mod } p^2\right)$. Then $f(x)$ is irreducible over $\mathbb{Q}$.

Proof. By Theorem 23.11, it is sufficient to show that $f(x)$ is irreducible over $\mathbb{Z}$. Assume

$$f(x) = \left(b_r x^r + \cdots + b_2 x^2 + b_1 x + b_0\right)\left(c_s x^s + \cdots + c_2 x^2 + c_1 x + c_0\right)$$

is a factorization in $\mathbb{Z}[x]$ with $b_r \neq 0$, $c_s \neq 0$, $r, s < n$. Since $a_0 = b_0 c_0 \not\equiv 0 \left(\text{mod } p^2\right)$ then b_0 and c_0 are not both congruent to 0 modulo p. WLOG, suppose $b_0 \not\equiv 0 \pmod{p}$ and $c_0 \not\equiv 0 \pmod{p}$ since $a_0 = b_0 c_0 \equiv 0 \pmod{p}$.

Theorem 23.15. Eisenstein Criterion

Theorem 23.15. Let $p \in \mathbb{Z}$ be a prime. Suppose $f(x) = a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0 \in \mathbb{Z}[x]$, and $a_n \not\equiv 0 \pmod{p}$, but $a_i = 0 \pmod{p}$ and for all $i < n$, with $a_0 \not\equiv 0 \left(\bmod\ p^2\right)$. Then $f(x)$ is irreducible over $\mathbb{Q}$.

Proof. By Theorem 23.11, it is sufficient to show that $f(x)$ is irreducible over $\mathbb{Z}$. Assume

$$f(x) = \left(b_r x^r + \cdots + b_2 x^2 + b_1 x + b_0\right)\left(c_s x^s + \cdots + c_2 x^2 + c_1 x + c_0\right)$$

is a factorization in $\mathbb{Z}[x]$ with $b_r \neq 0$, $c_s \neq 0$, $r, s < n$. Since $a_0 = b_0 c_0 \not\equiv 0 \left(\bmod\ p^2\right)$ then b_0 and c_0 are not both congruent to 0 modulo p. WLOG, suppose $b_0 \not\equiv 0 \pmod{p}$ and $c_0 \not\equiv 0 \pmod{p}$ since $a_0 = b_0 c_0 \equiv 0 \pmod{p}$. 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

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

Theorem 23.15. Eisenstein Criterion

Theorem 23.15. Let $p \in \mathbb{Z}$ be a prime. Suppose $f(x) = a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0 \in \mathbb{Z}[x]$, and $a_n \not\equiv 0 \pmod{p}$, but $a_i = 0 \pmod{p}$ and for all $i < n$, with $a_0 \not\equiv 0 \left(\bmod\ p^2\right)$. Then $f(x)$ is irreducible over $\mathbb{Q}$.

Proof. By Theorem 23.11, it is sufficient to show that $f(x)$ is irreducible over $\mathbb{Z}$. Assume

$$f(x) = \left(b_r x^r + \cdots + b_2 x^2 + b_1 x + b_0\right)\left(c_s x^s + \cdots + c_2 x^2 + c_1 x + c_0\right)$$

is a factorization in $\mathbb{Z}[x]$ with $b_r \neq 0$, $c_s \neq 0$, $r, s < n$. Since $a_0 = b_0 c_0 \not\equiv 0 \left(\bmod\ p^2\right)$ then b_0 and c_0 are not both congruent to 0 modulo p. WLOG, suppose $b_0 \not\equiv 0 \pmod{p}$ and $c_0 \not\equiv 0 \pmod{p}$ since $a_0 = b_0 c_0 \equiv 0 \pmod{p}$. 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

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

Theorem 23.15 (continued)

Theorem 23.15. Let $p \in \mathbb{Z}$ be a prime. Suppose $f(x) = a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0 \in \mathbb{Z}[x]$, and $a_n \not\equiv 0 \pmod{p}$, but $a_i = 0 \pmod{p}$ and for all $i < n$, with $a_0 \not\equiv 0 \left(\bmod\ p^2\right)$. Then $f(x)$ is irreducible over $\mathbb{Q}$.

Proof (continued). Since neither b_0 nor c_m are congruent to 0 modulo p, while $c_{m-1}, c_{m-2}, \ldots, c_0$ are all congruent to 0 modulo p implies that $a_m \not\equiv 0 \left(\bmod\ p^2\right)$, which implies that $c_m \neq 0$ and so $s = n$ and $r = 0$. But this contradicts the property that $s < n$. Therefore $f(x)$ is irreducible over $\mathbb{Z}$ and therefore over $\mathbb{Q}$, as claimed. □

Corollary 23.17

Corollary 23.17. The polynomial

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

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

Proof. By Theorem 23.11, it is sufficient to show that $\Phi_p(x)$ is irreducible over $\mathbb{Z}$. Applying

$$\begin{aligned}\varphi_{x+1}(\Phi_p(x)) &= \Phi_p(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} \\ &= \frac{x^p + \binom{p}{1} + \cdots + \binom{p}{r} x^{p-r} + \cdots + px}{x} \equiv g(x).\end{aligned}$$

The coefficient of x^{p-v} in the numerator $\binom{p}{r} = \frac{p!}{r!(p-r)!}$ and is divisible by p for $0 < r < p$ since p divides neither $r!$ nor $(p-r)!$ for $0 < r < p$.

Corollary 23.17

Corollary 23.17. The polynomial

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

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

Proof. By Theorem 23.11, it is sufficient to show that $\Phi_p(x)$ is irreducible over $\mathbb{Z}$. Applying

$$\begin{aligned} \varphi_{x+1}(\Phi_p(x)) &= \Phi_p(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} \\ &= \frac{x^p + \binom{p}{1} + \cdots + \binom{p}{r} x^{p-r} + \cdots + px}{x} \equiv g(x). \end{aligned}$$

The coefficient of x^{p-v} in the numerator $\binom{p}{r} = \frac{p!}{r!(p-r)!}$ and is divisible by p for $0 < r < p$ since p divides neither $r!$ nor $(p-r)!$ for $0 < r < p$.

Corollary 23.17 (continued)

Corollary 23.17. The polynomial

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

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

Proof (continued). So

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

satisfies the Eisenstein Criterion for prime p. Therefore $g(x)$ is irreducible over $\mathbb{Q}$. ASSUME $\Phi_p(x) = h(x)\, r(x)$ is a nontrivial factorization of $g(x)$ in $\mathbb{Z}[x]$. Then $\Phi_p(x+1) = g(x) = h(x+1)\, r(x+1)$ is a nontrivial factorization of $g(x)$ in $\mathbb{Z}[x]$, a CONTRADICTION. Therefore $\Phi_p(x)$ is irreducible over $\mathbb{Z}$ and also $\mathbb{Q}$. $\square$

Corollary 23.17 (continued)

Corollary 23.17. The polynomial

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

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

Proof (continued). So

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

satisfies the Eisenstein Criterion for prime p. Therefore $g(x)$ is irreducible over $\mathbb{Q}$. ASSUME $\Phi_p(x) = h(x)\, r(x)$ is a nontrivial factorization of $g(x)$ in $\mathbb{Z}[x]$. Then $\Phi_p(x+1) = g(x) = h(x+1)\, r(x+1)$ is a nontrivial factorization of $g(x)$ in $\mathbb{Z}[x]$, a CONTRADICTION. Therefore $\Phi_p(x)$ is irreducible over $\mathbb{Z}$ and also $\mathbb{Q}$. $\square$

Theorem 23.20

Theorem 23.20. 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 reducible then $f(x) = g(x)h(x)$ with the degrees of $g(x)$ and $h(x)$ both less than the degree of $f(x)$ by the definition of irreducible. If $f(x)$ and $g(x)$ are both irreducible, we are done. Otherwise, we can factor them into polynomials of lower degree. Continuing the process, we arrive at factorization $f(x) = p_1(x)p_2(x)\cdots p_r(x)$ where each $p_i(x)$, $i = 1, 2, \ldots, r$, is irreducible, as claimed.

Theorem 23.20

Theorem 23.20. 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 reducible then $f(x) = g(x)h(x)$ with the degrees of $g(x)$ and $h(x)$ both less than the degree of $f(x)$ by the definition of irreducible. If $f(x)$ and $g(x)$ are both irreducible, we are done. Otherwise, we can factor them into polynomials of lower degree. Continuing the process, we arrive at factorization $f(x) = p_1(x)p_2(x)\cdots p_r(x)$ where each $p_i(x)$, $i = 1, 2, \ldots, r$, is irreducible, as claimed.

Now to show uniqueness. Suppose

$$f(x) = p_1(x)p_2(x)\cdots p_r(x) = q_1(x)q_2(x)\cdots q_s(x)$$

are two factorizations of $f(x)$ into irreducible polynomials.

Theorem 23.20

Theorem 23.20. 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 reducible then $f(x) = g(x)h(x)$ with the degrees of $g(x)$ and $h(x)$ both less than the degree of $f(x)$ by the definition of irreducible. If $f(x)$ and $g(x)$ are both irreducible, we are done. Otherwise, we can factor them into polynomials of lower degree. Continuing the process, we arrive at factorization $f(x) = p_1(x)p_2(x)\cdots p_r(x)$ where each $p_i(x)$, $i = 1, 2, \ldots, r$, is irreducible, as claimed.

Now to show uniqueness. Suppose

$$f(x) = p_1(x)p_2(x)\cdots p_r(x) = q_1(x)q_2(x)\cdots q_s(x)$$

are two factorizations of $f(x)$ into irreducible polynomials.

Theorem 23.20 (continued)

Theorem 23.20. 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 (continued). Then by Corollary 23.19, $p_1(x)$ divides some q_j, let us assume $q_1(x)$. Since $q_1(x)$ is irreducible, then $q_1(x) = u_1 p_1(x)$ where $u_1 \neq 0$ and so u_1 is an unit in field F. So $p_1(x) p_2(x) \cdots p_r(x)$ $= u_1 p_1(x) q_2(x) \cdots q_s$. Since F has no zero divisors, then $F[x]$ has no zero divisors by Theorem 22.2, so cancellation holds and we have $p_2(x) \cdots p_r(x) = u_1 q_2(x) \cdots q_s(x)$. Similarly, $p_i(x)$ divides $q_i(x)$ for $i = 1, 2, \ldots, r$ and so $1 = u_1 u_2 \cdots u_r \in F$. So $s = r$ and $1 = u_1, u_2, \ldots, u_r$. So the decompositions $p_1(x) p_2(x) \cdots p_r(x)$ and $q_1(x) q_2(x) \cdots q_s(x)$ are the same, except for the order in which polynomials are written and the possible presence of unit factors, as claimed. □

Theorem 23.20 (continued)

Theorem 23.20. 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 (continued). Then by Corollary 23.19, $p_1(x)$ divides some q_j, let us assume $q_1(x)$. Since $q_1(x)$ is irreducible, then $q_1(x) = u_1 p_1(x)$ where $u_1 \neq 0$ and so u_1 is an unit in field F. So $p_1(x) p_2(x) \cdots p_r(x)$ $= u_1 p_1(x) q_2(x) \cdots q_s$. Since F has no zero divisors, then $F[x]$ has no zero divisors by Theorem 22.2, so cancellation holds and we have $p_2(x) \cdots p_r(x) = u_1 q_2(x) \cdots q_s(x)$. Similarly, $p_i(x)$ divides $q_i(x)$ for $i = 1, 2, \ldots, r$ and so $1 = u_1 u_2 \cdots u_r \in F$. So $s = r$ and $1 = u_1, u_2, \ldots, u_r$. So the decompositions $p_1(x) p_2(x) \cdots p_r(x)$ and $q_1(x) q_2(x) \cdots q_s(x)$ are the same, except for the order in which polynomials are written and the possible presence of unit factors, as claimed. □