Polynomial rings

Night Shift in Math • 7 Jun 2024

Theorem 1. *Let R be a ring and let $R[x]$ denote the set of all sequences of elements of R, $(a_0, a_1, \cdots)$, such that $a_i = 0$ for all but finitely many indices.*

(i) $R[x]$ is a ring with addition and multiplication defined by

$$(a_0, a_1, \cdots) + (b_0, b_1, \cdots) = (a_0 + b_0, a_1 + b_1, \cdots)$$

$$(a_0, a_1, \cdots)(b_0, b_1, \cdots) = (c_0, c_1, \cdots)$$

where $c_n = \sum_{i=0}^{n} a_{n-i} b_i$.

(ii) If R is commutative [resp. a ring with identity, ring with no zero divisors, integral domain], so is $R[x]$.

(iii) The map $R \to R[x]$ given by $r \mapsto (r, 0, 0, \cdots)$ is a monomorphism of rings.

The ring $R[x]$ is called the ring of polynomials over R.

Theorem 2. *Let R be a ring with identity and denote by x the element $(0, 1_R, 0, 0, 0, \cdots) \in R[x]$.*

(i) $x^n = (0, 0, \cdots, 0, 1_R, 0, \cdots)$ where 1_R is the $(n+1)th$ coordinate.

(ii) If $r \in R$, $rx^n = x^n r = (0, \cdots, 0, r, 0, \cdots)$ where r is the $(n+1)th$ coordinate.

(iii) For every nonzero polynomial $f \in R[x]$, $\exists n \in \mathbb{N}$, elements $a_0, a_1, \cdots, a_n \in R$ such that $f = a_0 x^0 + a_1 x^1 + \cdots + a_n x^n$. The elements n and a_i are unique in the sense that $f = b_0 x^0 + b_1 x^1 + \cdots + b_m x^m$ implies $m \geq n$, $a_i = b_i$ for $i \in \{0, 1, \cdots, n\}$ and $b_i = 0$ for $n < i \leq m$.

If R has an identity, $x^0 = 1_R$ and we write polynomials as
$f = a_0 + a_1 x + a_2 x^2 + cdots + a_n x^n$. If R is a ring without identity, embed R to a ring S with identity. Identify R with its image under the embedding map so that R is a subring of S. Then $R[x]$ is a subring of $S[x]$. Thus every polynomial $f = (a_0, a_1, \cdots) \in R[x]$ can be written uniquely as
$f = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ where $a_i \in R, a_n \neq 0$,
$x = (0, 1_S, 0, 0, \cdots) \in S[x]$. If $f = \sum_{i=0}^{n} a_i x^i \in R[x]$, the elements $a_i \in R$ are called the coefficients of f. The element a_0 is called the constant term. Elements of R which have the form $r = (r, 0, 0, \cdots)$ are called constant polynomials. If

$f = \sum_{i=0}^{n} a_i x^i$ and $a_n \neq 0$, then a_n is called the leading coefficient of f. If R has an identity and f has leading coefficient 1_R, then f is said to be a monic polynomial.

Let R be a ring with identity. The element $x = (0, 1_R, 0, 0, \cdots)$ of $R[x]$ is called an indeterminate. If S is another ring with identity, the indeterminate $x \in S[x]$ is not the same element as $x \in R[x]$. We can also define polynomials in more than one indeterminate.

Theorem 3. *Let R be a ring and denote by $R[x_1, x_2, \cdots, x_n]$ the set of functions $f : \mathbb{N}^n \to R$ such that $f(u) \neq 0$ for at most a finite number of elements u of $\mathbb{N}^n$.*

(i) *$R[x_1, x_2, \cdots, x_n]$ is a ring with addition and multiplication defined by*

$$(f+g)(u) = f(u) + g(u), \quad (fg)(u) = \sum_{v+w=u} f(v)g(w)$$

where $f, g \in R[x_1, x_2, \cdots, x_n]$ and $u \in \mathbb{N}^n$.

(ii) *If R is commutative [resp. ring with identity, ring without zero divisors, integral domain], so is $R[x_1, x_2, \cdots, x_n]$.*

(iii) *The map $R \to R[x_1, x_2, \cdots, x_n] : r \mapsto f_r$ where $f_r(0, 0, \cdots, 0) = r$ and $f_r(u) = 0$ for all $u \in \mathbb{N}^n \setminus \{(0, 0, \cdots, 0)\}$ is a monomorphism of rings.*

The ring $R[x_1, x_2, \cdots, x_n]$ is called the ring of polynomials in n determinates over R. R is considered a subring of $R[x_1, x_2, \cdots, x_n]$. Let n be a positive integer and for $i \in \{1, 2, \cdots, n\}$, let $\epsilon_i = (0, \cdots, 0, 1, 0, \cdots, 0) \in \mathbb{N}^n$ where 1 is the ith coordinate of ϵ_i. Every element of $\mathbb{N}^n$ may be written as $k_1\epsilon_1 + k_2\epsilon_2 + \cdots + k_n\epsilon_n$.

Theorem 4. *Let R be a ring with identity and n a positive integer. $\forall i \in \{1, 2, \cdots, n\}$, let $x_i \in R[x_1, x_2, \cdots, x_n]$ be defined by $x_i(\epsilon_i) = 1_R$ and $x_i(u) = 0$ for $u \neq \epsilon_i$.*

(i) *$\forall k \in \mathbb{N}, x_i^k(k\epsilon_i) = 1_R$ and $x_i^k(u) = 0$ for $u \neq k\epsilon_i$.*

(ii) *$\forall (k_1, k_2, \cdots, k_n) \in \mathbb{N}^n, (x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n})(k_1\epsilon_1 + k_2\epsilon_2 + \cdots + k_n\epsilon_n) = 1_R$ and $x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}(u) = 0$ for $u \neq k_1\epsilon_1 + k_2\epsilon_2 + \cdots + k_n\epsilon_n$.*

(iii) *$\forall t, s \in \mathbb{N}, \forall i, j \in \{1, 2, \cdots, n\}, x_i^t x_j^s = x_j^s x_i^t$*

(iv) *$\forall r \in R, t \in \mathbb{N}, x_i^t r = r x_i^t$*

(v) *$\forall f \in R[x_1, x_2, \cdots, x_n]$ there exists unique elements $a_{k_1,k_2,\cdots,k_n} \in R$ indexed by all $(k_1, k_2, \cdots, k_n) \in \mathbb{N}^n$ and nonzero for at most a finite number of $(k_1, k_2, \cdots, k_n) \in \mathbb{N}^n$ such that $f = \sum a_{k_1,k_2,\cdots,k_n} x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$.*

If R is a ring with identity, the elements $x_1, x_2, \cdots, x_n$ are called indeterminates. The elements $a_{k_1,k_2,\cdots,k_n}$ are called coefficients of the polynomial f. A polynomial of the form $ax_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$ is called a monomial. The notation and terminology is extended to polynomial rings where R has no identity. Embed the ring R to a ring S with identity and consider $R[x_1, x_2, \cdots, x_n]$ as a subring of $S[x_1, x_2, \cdots, x_n]$. If R is any ring, for any subset $\{i_1, i_2, \cdots, i_k\} \subseteq \{1, 2, \cdots, n\}$, the monomorphism $R[x_{i_1}, x_{i_2}, \cdots, x_{i_k}] \to R[x_1, x_2, \cdots, x_n]$ exists.

Let $\phi : R \to S$ be a homomorphism of rings, $f \in R[x_1, x_2, \cdots, x_n]$, $s_1, s_2, \cdots, s_n \in S$. Let $f = \sum_{i=0}^{m} a_i x_1^{k_{i1}} \cdots x_n^{k_{in}}$. Let

$$\phi f(s_1, s_2, \cdots, s_n) = \sum_{i=0}^{n} \phi(a_i) s_1^{k_{i1}} s_2^{k_{i2}} \cdots s_n^{k_{in}} \in S$$

Theorem 5. *Let R and S be commutative rings with identity and $\phi : R \to S$ a homomorphism of rings such that $\phi(1_R) = 1_S$. If $s_1, s_2, \cdots, s_n \in S$, then there is a unique homomorphism of rings $\bar{\phi} : R[x_1, x_2, \cdots, x_n] \to S$ such that $\bar{\phi} \mid_R = \phi$ and $\bar{\phi}(x_i) = s_i$ for $i \in \{1, 2, \cdots, n\}$. This property determines the polynomial ring $R[x_1, x_2, \cdots, x_n]$ up to isomorphism.*

Proof. If $f \in R[x_1, x_2, \cdots, x_n]$, then $f = \sum_{i=0}^{m} a_i x_1^{k_{i1}} x_2^{k_{i2}} \cdots x_n^{k_{in}}$. The map $\bar{\phi}$ given by $\bar{\phi}(f) = \phi f(s_1, s_2, \cdots, s_n)$ is a well-defined map such that $\bar{\phi} \mid_R = \phi$ and $\bar{\phi}(x_i) = s_i$. It is easy to verify that $\bar{\phi}$ is a homomorphism. Suppose that $\psi : R[x_1, x_2, \cdots, x_n] \to S$ is a homomorphism with $\psi \mid_R = \phi$, $\psi(x_i) = s_i$. Then $\psi(f) = \bar{\phi}(f)$ by direct computation. Define a category $\mathscr{C}$ whose objects are tuples $(\psi, K, s_1, s_2, \cdots, s_n)$ where K is a commutative ring with identity, $s_1, s_2, \cdots, s_n \in K$, $\psi : R \to K$ a homomorphism with $\psi(1_R) = 1_K$. A morphism in $\mathscr{C}$ from $(\psi, K, s_1, \cdots, s_n)$ to $(\theta, T, t_1, t_2, \cdots, t_n)$ is a homomorphism $\zeta : K \to T$ such that $\zeta(1_K) = 1_T$, $\zeta \circ \psi = \theta$ and $\zeta(s_i) = t_i$. Verify that ζ is an equivalence in $\mathscr{C}$ iff ζ is an equivalence of rings. If $\iota : R \to R[x_1, x_2, \cdots, x_n]$ is the inclusion map, $(\iota, R[x_1, x_2, \cdots, x_n], x_1, \cdots, x_n)$ is a universal object in $\mathscr{C}$. Thus $R[x_1, x_2, \cdots, x_n]$ is completely determined up to isomorphism. □

Corollary 1. *If $\phi : R \to S$ is a homomorphism of commutative rings and $s_1, s_2, \cdots s_n \in S$ then the map $R[x_1, x_2, \cdots, x_n] \to S$ given by $f \mapsto \phi f(s_1, \cdots, s_n)$ is a homomorphism of rings.*

Proof. The proof that $f \mapsto \phi f(s_1, s_2, \cdots, s_n)$ is a homomorphism does not rely on R containing an identity. □

The map $R[x_1, x_2, \cdots, x_n] \to S$ is called the evaluation homomorphism. The corollary may be false when R and S are not commutative.

Corollary 2. *Let R be a commutative ring with identity and n a positive integer. $\forall k \in \{1, 2, \cdots, n\}$, there are isomorphisms of rings $R[x_1, x_2, \cdots, x_k][x_{k+1}, \cdots, x_n] \cong R[x_1, x_2, \cdots, x_n] \cong R[x_{k+1}, \cdots, x_n][x_1, x_2, \cdots, x_k]$.*

Proof. Given a homomorphism $\phi : R \to S$ of commutative rings with identity, elements $s_1, s_2, \cdots, s_n \in S$, there exists a homomorphism $\bar{\phi} : R[x_1, x_2, \cdots, x_k] \to S$ such that $\bar{\phi} \mid_R = \phi, \bar{\phi}(x_i) = s_i$. Applying the theorem with $R[x_1, x_2, \cdots, x_k]$ in place of R gives $\bar{\bar{\phi}} : R[x_1, x_2, \cdots, x_k][x_{k+1}, \cdots, x_n] \to S$ such that $\bar{\bar{\phi}} \mid_R = \phi$ and $\bar{\bar{\phi}}(x_i) = s_i$ for all $i \in \{1, 2, \cdots, n\}$. Due to the uniqueness up to isomorphism, $R[x_1, x_2, \cdots, x_k][x_{k+1}, \cdots, x_n] \cong R[x_1, x_2, \cdots, x_n]$. The other isomorphism follows similarly. □

Theorem 6. *Let R be a ring and denote $R[[x]]$ the set of all sequences of elements in R.*

(i) $R[[x]]$ is a ring with addition and multiplication defined in the same way as the operations for $R[x]$.

(ii) $R[x]$ is a subring of $R[[x]]$.

(iii) If R is commutative (resp. ring with identity, no zero divisors, integral domain), then so is $R[[x]]$.

The ring $R[[x]]$ is called the ring of formal power series over the ring R. Its elements are called power series.

Theorem 7. *Let R be a ring with identity and $f = \sum_{i=0}^{\infty} a_i x^i \in R[[x]]$.*

(i) f is a unit in $R[[x]]$ iff its constant term a_0 is a unit in R.

(ii) If a_0 is irreducible in R, then f is irreducible in $R[[x]]$.

Proof. (i). If $\exists g \in R[[x]], g = \sum_i b_i x^i$ such that $fg = gf = 1_R$, it follows immediately that $a_0 b_0 = b_0 a_0 = 1_R$. Whence a_0 is a unit. Suppose a_0 is a unit in R. If $\exists g \in R[[x]], g = \sum_i b_i x^i$ such that $fg = 1_R$, then

$$\begin{aligned} a_0 b_0 &= 1_R \\ a_0 b_1 + a_1 b_0 &= 0 \\ &\vdots \\ a_0 b_n + a_1 b_{n-1} + \cdots + a_n b_0 &= 0 \\ &\vdots \end{aligned}$$

Conversely, if a solution $(b_0, b_1, \cdots)$ exists for this system of equations in R, then $g = \sum_{i=0}^{\infty} b_i x^i \in R[[x]]$ satisfies $fg = 1_R$. Take $b_0 = a_0^{-1}, b_1 = a_0^{-1}(-a_1 b_0)$. Similarly, $b_n = -a_0^{-1}(a_1 b_{n-1} + \cdots + a_n b_0)$. Thus the system of equations is solvable. A similar argument shows the existence of a left inverse for f in $R[[x]]$. (ii) is an immediate consequence of (i). □

Corollary 3. *If R is a division ring, the units in $R[[x]]$ are precisely those power series with nonzero constant terms. The principal ideal (x) consists precisely of the nonunits in $R[[x]]$ and is the unique maximal ideal of $R[[x]]$. Thus if R is a field, $R[[x]]$ is a local ring.*

The degree of a nonzero monomial $ax_1^{k_1} x_2^{k_2} \cdots x_n^{k_n} \in R[x_1, x_2, \cdots, x_n]$ is the nonnegative integer $k_1 + k_2 + \cdots + k_n$. If f is a nonzero polynomial, the degree of f is the maximum of the degrees of the monomials making up f. The degree of f is denoted $\deg f$. A polynomial which is a sum of monomials, each with the same degree k, is said to be homogeneous of degree k. The degree of f in x_k is the degree of f considered as a polynomial in one indeterminate x_k over the ring $R[x_1, x_2, \cdots, x_{k-1}, x_{k+1}, \cdots, x_n]$. We define the degree of the zero polynomial to be $-\infty$.

Theorem 8. *Let R be a ring and $f, g \in R[x_1, x_2, \cdots, x_n]$.*

(i) $\deg(f+g) \le \max\{\deg f, \deg g\}$

(ii) $\deg(fg) \le \deg f + \deg g$

(iii) If R has no zero divisors, $\deg(fg) = \deg f + \deg g$.

(iv) If $n = 1$ and the leading coefficient of f or g is not a zero divisor in R, $\deg(fg) = \deg f + \deg g$.

Theorem 9 (Division Algorithm)**.** *Let R be a ring with identity and $f, g \in R[x]$ nonzero polynomials such that the leading coefficient of g is a unit in R. Then there exist unique polynomials $q, r \in R[x]$ such that $f = qg + r$ and* $\deg r < \deg g$.

Proof. If $\deg g > \deg f$, let $q = 0$ and $r = f$. If $\deg g \le \deg f$, $f = \sum_{i=0}^{n} a_i x^i, g = \sum_{i=0}^{m} b_i x^i$ with $a_n \neq 0, b_m \neq 0, m \le n$, b_m a unit in R. Proceed by induction on n. If $n = 0, m = 0$ and $q_0 = a_0 b_0^{-1}, r = 0$. Assume the existence is true for polynomials with degree less than n. The polynomial $a_n b_m^{-1} x^{n-m} g$ has degree n and leading coefficient a_n. Hence $f - a_n b_m^{-1} x^{n-m} g$ is a polynomial of degree less than n. There exist polynomials q', r such that $f - a_n b_m^{-1} x^{n-m} g = q'g + r$ and $\deg r < \deg g$. Thus if $q = a_n b_m^{-1} x^{n-m} + q', f = qg + r$. For uniqueness, suppose $f = q_1 g + r_1 = q_2 g + r_2$, $\deg r_1 < \deg g$ and $\deg r_2 < \deg g$. $q_1 g + r_1 = q_2 g + r_2$ implies $(q_1 - q_2)g = r_2 - r_1$. Since the leading coefficient of g is a unit,

$$\deg(q_1 - q_2) + \deg g = \deg(r_2 - r_1)$$

Since $\deg(r_2 - r_1) < \deg g$, the above inequality is true only if $q_1 = q_2$ and $r_1 = r_2$. □

Corollary 4 (Remainder Theorem)**.** *Let R be a ring with identity and $f \in R[x]$. $\forall c \in R, \exists! q \in R[x]$ such that $f(x) = q(x)(x - c) + f(c)$*

Corollary 5. *If F is a field, then the polynomial $F[x]$ is a Euclidean domain. The units in $F[x]$ are precisely the nonzero constant polynomials.*

Proof. Since F is an integral domain, $F[x]$ is an integral domain. Define $\phi : F[x] \setminus \{0\} \to \mathbb{N}$ by $\phi(f) = \deg f$. By the division algorithm, $F[x]$ is a Euclidean domain. Since each unit in $F[x]$ must have degree 0, the units of $F[x]$ are precisely the nonzero constant polynomials. □

Definition 1. *Let R be a subring of a commutative ring S, $c_1, c_2, cdots, c_n \in S$ and $f = \sum_{i=0}^{m} a_i x_1^{k_{i1}} x_2^{k_{i2}} \cdots x_n^{k_{in}} \in R[x_1, x_2, \cdots, x_n]$ a polynomial such that $f(c_1, c_2, \cdots, c_n) = 0$. Then $(c_1, c_2, \cdots, c_n)$ is said to be a root or zero of f.*

Theorem 10. *Let R be a commutative ring with identity and $f \in R[x]$. Then $c \in R$ is a root of f iff $x - c \mid f$.*

Proof. $f(x) = q(x)(x - c) + f(c)$. If $x - c \mid f(x)$, then $h(x)(x - c) = q(x)(x - c) + f(c)$ for $h \in R[x]$. Whence $(h(x) - q(x))(x - c) = f(c)$. Thus substituting $x = c$ gives $f(c) = 0$. If $f(c) = 0$, $f(x) = q(x)(x - c)$. □

Theorem 11. *If D is an integral domain contained in an integral domain E and $f \in D[x]$ has degree n, then f has at most n distinct roots in E.*

Proof. Let $c_1, c_2, c_3, \cdots$ be the distinct roots of f in E. $f(x) = q_1(x)(x - c_1)$ whence $0 = f(c_2) = q_1(c_2)(c_2 - c_1)$. Since $c_1 \neq c_2$ and E is an integral domain, $q_1(c_2) = 0$. Thus $f(x) = q_2(x)(x - c_2)(x - c_1)$. An inductive argument shows for distinct roots $c_1, c_2, \cdots, c_m$, $g_m = (x - c_1)(x - c_2) \cdots (x - c_m)$ divides f. But $\deg g_m = m$. Thus $m \leq n$. □

Theorem 12. *Let D be a unique factorization domain with quotient field F and let $f = \sum_{i=0}^{n} a_i x^i \in D[x]$. If $u = c/d \in F$ with c and d relatively prime, u is a root of f, then $c \mid a_0$ and $d \mid a_n$.*

Proof. $f(u) = 0$ implies that $a_0 d^n = c(\sum_{i=1}^{n}(-a_i)c^{i-1}d^{n-i})$, $-a_n c^n = (\sum_{i=0}^{n-1} c^i d^{n-i-1})d$. If $(c, d) = 1_D$, then $c \mid a_0$ and $d \mid a_n$. □

Let D be an integral domain and $f \in D[x]$. If $c \in D$ and c is a root of f, then there is a greatest integer m such that $f(x) = (x - c)^m g(x)$ where $g \in D[x]$ and $x - c \nmid g(x)$. The integer m is called the multiplicity of the root c of f. If c has multiplicity 1, c is said to be a simple root. If c has multiplicity greater than 1, c is called a multiple root.

Lemma 1. *Let D be an integral domain and $f = \sum_{i=0}^{n} a_i x^i \in D[x]$. Let $f' \in D[x]$ be the polynomial $f' = \sum_{k=1}^{n} k a_k x^{k-1}$. Then $\forall f, g \in D[x], c \in D$:*

(i) $(cf)' = cf'$

(ii) $(f+g)' = f' + g'$

(iii) $(fg)' = f'g + f'g$

(iv) $(g^n)' = ng^{n-1}g'$

The polynomial f' is called the formal derivative of f.

Theorem 13. *Let D be an integral domain and a subring of integral domain E. Let $f \in D[x]$ and $c \in E$.*

(i) c is a multiple root of f iff $f(c) = 0$ and $f'(c) = 0$.

(ii) If D is a field and f is relatively prime to f', then f has no multiple roots in E.

(iii) If D is a field, f is irreducible in $D[x]$ and E contains a root of f, then f has no multiple roots in E iff $f' \neq 0$.

Proof. (i). $f(x) = (x-c)^m g(x)$ where $g(c) \neq 0$.

$$f'(x) = m(x-c)^{m-1}g(x) + (x-c)^m g'(x)$$

If $m > 1$, then $f'(c) = 0$. Conversely, if $f(c) = 0$, then $m \geq 1$.If $m = 1$, then $f'(x) = g(x) + (x-c)g'(x)$. Thus $f'(c) = 0$ means $f'(c) = g(c)$ which is a contradiction. Therefore $m > 1$.
(ii). Since $D[x]$ is a Euclidean domain, $\exists k, h \in D[x]$ such that $kf + hf' = 1_D$. If c is a multiple root of f, then $1_D = k(c)f(c) + h(c)f'(c) = 0$, a contradiction. Thus c is a simple root.
(iii). If f is irreducible and $f' \neq 0$, then f and f' are relatively prime since $\deg f' < \deg f$. Therefore, f has no multiple roots in E. Conversely, suppose f has no multiple roots in E and b is a root of f in E. If $f' = 0$, then b is a multiple root of f, a contradiction. Hence $f' \neq 0$. □

Let D be an integral domain, the following facts hold:

1. The units of $D[x]$ are precisely the constant polynomials that are units in D.
2. If $c \in D$ and c is irreducible in D, c is irreducible in $D[x]$.
3. Every first degree polynomial whose leading coefficient is a unit in D is irreducible in $D[x]$. In particular, every first degree polynomial over a field is irreducible.

4. Suppose D is a subring of integral domain E and $f \in D[x]$. Then f may be irreducible in $E[x]$ but not in $D[x]$ and vice versa.

For the last point, note that $2x + 2$ is irreducible in $\mathbb{Q}[x]$ but not in $\mathbb{Z}[x]$. $x^2 + 1$ is irreducible in $\mathbb{R}[x]$ but not in $\mathbb{C}[x]$.

Let D be a unique factorization domain and $f = \sum_{i=0}^{n} a_i x^i$ a nonzero polynomial in $D[x]$. A greatest common divisor of $a_0, a_1, \cdots, a_n$ is called a content of f and is denoted $C(f)$. Write $b \approx c$ whenever b and c are associates in D. Then $\approx$ is an equivalence relation on D. Since D is an integral domain, $b \approx c \iff \exists u \in D, b = cu$ and u is a unit. If $a \in D$ and $f \in D[x]$ then $C(af) \approx aC(f)$. If $f \in D[x]$ and $C(f)$ is a unit in D, then f is said to be primitive. For any polynomial $g \in D[x]$, $g = C(g)g_1$ with g_1 primitive.

Lemma 2. *If D is a unique factorization domain and $f, g \in D[x]$, then $C(fg) \approx C(f)C(g)$. The product of primitive polynomials is primitive.*

Proof. Let $f = C(f)f_1, g = C(g)g_1$, f_1, g_1 primitive. It suffices to prove that $f_1 g_1$ is primitive. Let $f_1 = \sum_{i=0}^{n} a_i x^i$ and $g_1 = \sum_{j=0}^{m} b_j x^j$. $f_1 g_1 = \sum_{k=0}^{m+n} c_k x^k$ with $c_k = \sum_{i+j=k} a_i b_j$. If $f_1 g_1$ is not primitive, there exists an irreducible element $p \in R$ such that $\forall k, p \mid c_k$. Since $C(f_1)$ is a unit, $p \nmid C(f_1)$ whence there is a least integer s such that $p \mid a_i$ for $i < s$ and $p \nmid a_s$. Similarly, there is a least integer t such that $p \mid b_j$ for $j < t$ and $p \nmid b_t$. Since p divides c_{s+t} and

$$c_{s+t} = a_0 b_{s+t} + \cdots + a_{s-1} b_{t+1} + a_s b_t + a_{s+1} b_{t-1} + \cdots + a_{s+t} b_0$$

$p \mid a_s b_t$ implying $p \mid a_s$ or $p \mid b_t$, a contradiction. □

Lemma 3. *Let D be a unique factorization domain with quotient field F and let f and g be primitive polynomials in $D[x]$. Then f and g are associates in $D[x]$ iff they are associates in $F[x]$.*

Proof. If f and g are associates in $F[x]$, $f = gu$ for some $u \in F[x]$ a unit. $u \in F$ so $u = b/c$ where $b, c \in D, c \neq 0$. Thus $cf = bg$. Since $C(f), C(g)$ are units in D, $c \approx C(cf) \approx C(bg) \approx b$. Thus $\exists v \in D$ a unit such that $b = cv$. $cf = bg = cvg$. Thus $f = vg$ whence f and g are associates in $D[x]$. The converse is obvious. □

Lemma 4. *Let D be a UFD with quotient field F and f a primitive polynomial of positive degree in $D[x]$. Then f is irreducible in $D[x]$ iff f is irreducible in $F[x]$.*

Proof. Suppose f is irreducible in $D[x]$ and $f = gh$ with $g, h \in F[x]$, $\deg g \geq 1, \deg h \geq 1$. $g = \sum_{i=0}^{n} (a_i/b_i) x^i$ and $h = \sum_{j=0}^{m} (c_j/d_j) x^j$ with $a_i, b_i, c_j, d_j \in D$ and $b_i \neq 0, d_j \neq 0$. Let $b = b_0 b_1 b_2 \cdots b_n$ and for each i let $b_i^* = b_0 b_1 \cdots b_{i-1} b_{i+1} \cdots b_n$. If $g_1 = \sum_{i=0}^{n} a_i b_i^* x^i \in D[x]$, then $g_1 = a g_2$ with $a = C(g_1), g_2 \in D[x]$ and g_2 primitive. $g = (1_D/b) g_1 = (a/b) g_2$ and $\deg g = \deg g_2$. Similarly, $h = (c/d) h_2$ with $c, d \in D, h_2 \in D[x]$, h_2 primitive

and $\deg h = \deg h_2$. $f = (a/b)(c/d)g_2h_2$ thus $bdf = acg_2h_2$ implying $bd \approx ac$. $\exists v \in D$ a unit such that $bd = acv$. $acg_2h_2 = acvf \implies g_2h_2 = vf$ so $f \approx g_2h_2$. Then f is reducible in $D[x]$, a contradiction. Thus f is irreducible in $F[x]$. Conversely, if f is irreducible in $F[x]$, $f = gh$ with $g, h \in D[x]$, then one of them, say g is a constant. Thus $C(f) \approx gC(h)$. Since f is primitive, g is a unit in D and hence in $D[x]$. Thus f is irreducible in $D[x]$. □

Theorem 14. *If D is a UFD, so is $D[x_1, x_2, \cdots, x_n]$.*

Proof. We only need to prove $D[x]$ is UFD since $D[x_1, x_2, \cdots, x_n] \cong D[x_1, x_2, \cdots, x_{n-1}][x_n]$. If f has positive degree, $f = C(f)f_1$ with f_1 primitive and positive degree. Since D is a UFD, $C(f)$ is a unit or $C(f) = c_1c_2 \cdots c_m$ with each c_i irreducible in D and hence in $D[x]$. Let F be the quotient field of F. Since $F[x]$ is a UFD containing $D[x]$, $f_1 = p_1^*p_2^* \cdots p_n^*$ with each p_i^* an irreducible polynomial in $F[x]$. For each i, $p_i^* = (a_i/b_i)p_i$ with $a_i, b_i \in D$, $b_i \neq 0$, $p_i \in D[x]$, p_i primitive. Each p_i is irreducible in $F[x]$ whence each p_i is irreducible in $D[x]$. If $a = a_1a_2 \cdots a_n$, $b = b_1b_2 \cdots b_n$, $f_1 = (a/b)p_1p_2 \cdots p_n$. Thus $bf_1 = ap_1p_2 \cdots p_n$. Since $f_1, p_1, p_2, \cdots, p_n$ are primitive, a and b are associates in D. Thus $a/b = u$, with u a unit in D. Thus if $C(f)$ is a nonunit, $f = uc_1c_2 \cdots c_np_1p_2 \cdots p_n$. Remove $c_1, c_2, \cdots, c_m$ if $C(f)$ is a unit.

For uniqueness, suppose f is a nonprimitive polynomial in $D[x]$ of positive degree. Any factorization of f as a product of irreducible elements may be written as $f = c_1c_2 \cdots c_mp_1p_2 \cdots p_n$ with each c_i irreducible in D, each p_i irreducible and hence primitive in $D[x]$ of positive degree. Suppose $f = d_1 \cdots d_rq_1 \cdots q_s$ where d_i irreducible in D, q_j irreducible in $D[x]$ of positive degree. Then $c_1c_2 \cdots c_m$ and $d_1 \cdots d_r$ are associates in D. Unique factorization in D implies $m = r$ and after reindexing, c_i is an associate of d_i. $p_1p_2 \cdots p_n$ is associate to $q_1q_2 \cdots q_s$ in $D[x]$. Since $F[x]$ is a UFD, $n = s$ and each p_i is associate of q_i in $F[x]$ after reindexing. They are associates in $D[x]$ by the lemma. □

Theorem 15 (Eisenstein's Criterion)**.** *Let D be a UDF with quotient field F. If $f = \sum_{i=0}^{n} a_ix^i \in D[x]$, $\deg f \geq 1$ and p is an irreducible element of D such that $p \nmid a_n$, $p \mid a_i$ for $i \in \{0, 1, 2, \cdots, n-1\}$, $p^2 \nmid a_0$, then f is irreducible in $F[x]$. If f is primitive, then f is irreducible in $D[x]$.*

Proof. $f = C(f)f_1$, f_1 primitive in $D[x]$, $C(f) \in D$. Since $C(f)$ is a unit in F, it suffices to show f_1 is irreducible in $F[x]$. We only need to prove f_1 is irreducible in $D[x]$. Suppose $f_1 = gh$ with

$$g = b_rx^r + \cdots + b_0 \in D[x], \quad \deg g = r \geq 1$$

$$h = c_sx^s + \cdots + c_0 \in D[x], \quad \deg h = s \geq 1$$

Since $p \nmid C(f)$, p has the same divisibility conditions to a_i^*, the coefficients of f_1, as it does to a_i. Since $p \mid a_0^* = b_0 c_0$, either $p \mid b_0$ or $p \mid c_0$, say $p \mid b_0$. Since $p^2 \nmid a_0$, $p \nmid c_0$. Some coefficient b_k of g is not divisible by p otherwise f_1 would not be primitive. Let k be the least integer such that $p \mid b_i$ for $i < k$ and $p \nmid b_k$. Then $1 \leq k \leq r < n$. Since

$$a_k^* = b_0 c_k + b_1 c_{k-1} + \cdots + b_{k-1} c_1 + b_k c_0$$

and $p \mid a_k^*$, $p \mid b_k c_0$ whence $p \mid b_k$ or $p \mid c_0$, a contradiction. Thus f_1 must be irreducible in $D[x]$. $\square$