Modern Algebra

Chapter III. Rings

III.6. Factorization in Polynomial Rings—Proofs of Theorems

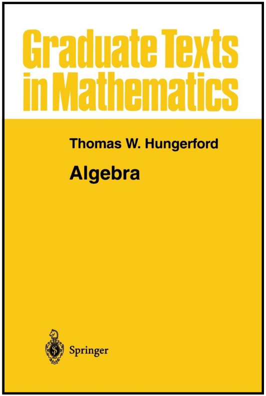

Table of contents

Theorem III.6.2

Theorem III.6.2. The 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 $r = f$.

Theorem III.6.2

Theorem III.6.2. The 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 $\deg(g) \leq \deg(f)$, then $f = \sum_{i=0}^{n} a_i x^i$, $g = \sum_{i=0}^{m} b_i x^i$ with $a_n \neq 0$, $b_m \neq 0$, $m \leq n$, and b_m a unit in R (by hypothesis, the leading coefficient of g is a unit).

Theorem III.6.2

Theorem III.6.2. The 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 $\deg(g) \leq \deg(f)$, then $f = \sum_{i=0}^{n} a_i x^i$, $g = \sum_{i=0}^{m} b_i x^i$ with $a_n \neq 0$, $b_m \neq 0$, $m \leq n$, and b_m a unit in R (by hypothesis, the leading coefficient of g is a unit).
We now apply induction on $n = \deg(f)$. If $n = 0$, then $m = 0$, $f = a_0$, $g = b_0$ and b_0 is a unit (by hypothesis).

Theorem III.6.2

Theorem III.6.2. The 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 $\deg(g) \le \deg(f)$, then $f = \sum_{i=0}^{n} a_i x^i$, $g = \sum_{i=0}^{m} b_i x^i$ with $a_n \neq 0$, $b_m \neq 0$, $m \le n$, and b_m a unit in R (by hypothesis, the leading coefficient of g is a unit).
We now apply induction on $n = \deg(f)$. If $n = 0$, then $m = 0$, $f = a_0$, $g = b_0$ and b_0 is a unit (by hypothesis). Let $q = a_0 b_0^{-1}$ and $r = 0$; then $\deg(r) < \deg(g)$ (from Note III.6.A, $\deg(r) = -\infty$) and $qg + r = (a_0 b_0^{-1}) b_0 = a_0 = f$. So the result holds for $n = 0$.

Theorem III.6.2

Theorem III.6.2. The 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 $\deg(g) \leq \deg(f)$, then $f = \sum_{i=0}^{n} a_i x^i$, $g = \sum_{i=0}^{m} b_i x^i$ with $a_n \neq 0$, $b_m \neq 0$, $m \leq n$, and b_m a unit in R (by hypothesis, the leading coefficient of g is a unit).
We now apply induction on $n = \deg(f)$. If $n = 0$, then $m = 0$, $f = a_0$, $g = b_0$ and b_0 is a unit (by hypothesis). Let $q = a_0 b_0^{-1}$ and $r = 0$; then $\deg(r) < \deg(g)$ (from Note III.6.A, $\deg(r) = -\infty$) and $qg + r = (a_0 b_0^{-1}) b_0 = a_0 = f$. So the result holds for $n = 0$.

Theorem III.6.2 (continued 1)

Proof (continued). Assume that the existence part of the theorem is true for polynomials of degree less than $n = \deg(f)$. Then the polynomial

$$(a_n b_m^{-1} x^{n-m})g = (a_n b_m^{-1} x^{n-m}) \sum_{i=0}^{m} b_i x^i = \sum_{i=0}^{m} a_n b_m^{-1} b_i x^{n-m+i}$$

$$= a_n x^n + \sum_{i=0}^{m-1} a_n b_m^{-1} b_i x^{n-m+i}$$

has degree n and leading coefficient a_n. Hence $f - (a_n b_m^{-1} x^{n-m})g = (a_n x^n + \cdots a_0) - (a_n x^n + \cdots + a_n b_m^{-1} b_0 x^{n-m})$ is a polynomial of degree less than n. By the induction hypothesis there are polynomials q' and r such that $f - (a_n b_m^{-1} x^{n-m})g = q'g + r$ and $\deg(r) < \deg(g)$.

Theorem III.6.2 (continued 1)

Proof (continued). Assume that the existence part of the theorem is true for polynomials of degree less than $n = \deg(f)$. Then the polynomial

$$(a_n b_m^{-1} x^{n-m}) g = (a_n b_m^{-1} x^{n-m}) \sum_{i=0}^{m} b_i x^i = \sum_{i=0}^{m} a_n b_m^{-1} b_i x^{n-m+i}$$

$$= a_n x^n + \sum_{i=0}^{m-1} a_n b_m^{-1} b_i x^{n-m+i}$$

has degree n and leading coefficient a_n. Hence $f - (a_n b_m^{-1} x^{n-m}) g = (a_n x^n + \cdots a_0) - (a_n x^n + \cdots + a_n b_m^{-1} b_0 x^{n-m})$ is a polynomial of degree less than n. By the induction hypothesis there are polynomials q' and r such that $f - (a_n b_m^{-1} x^{n-m}) g = q' g + r$ and $\deg(r) < \deg(g)$. Therefore, if $q = a_n b_m^{-1} x^{n-m} + q'$ then $f = (a_n b_m^{-1} x^{n-m}) g + q' g + r = qg + r$ where $\deg(r) < \deg(g)$. So the existence claim is justified by induction.

Theorem III.6.2 (continued 1)

Proof (continued). Assume that the existence part of the theorem is true for polynomials of degree less than $n = \deg(f)$. Then the polynomial

$$(a_n b_m^{-1} x^{n-m}) g = (a_n b_m^{-1} x^{n-m}) \sum_{i=0}^{m} b_i x^i = \sum_{i=0}^{m} a_n b_m^{-1} b_i x^{n-m+i}$$

$$= a_n x^n + \sum_{i=0}^{m-1} a_n b_m^{-1} b_i x^{n-m+i}$$

has degree n and leading coefficient a_n. Hence $f - (a_n b_m^{-1} x^{n-m}) g = (a_n x^n + \cdots a_0) - (a_n x^n + \cdots + a_n b_m^{-1} b_0 x^{n-m})$ is a polynomial of degree less than n. By the induction hypothesis there are polynomials q' and r such that $f - (a_n b_m^{-1} x^{n-m}) g = q' g + r$ and $\deg(r) < \deg(g)$. Therefore, if $q = a_n b_m^{-1} x^{n-m} + q'$ then $f = (a_n b_m^{-1} x^{n-m}) g + q' g + r = qg + r$ where $\deg(r) < \deg(g)$. So the existence claim is justified by induction.

Theorem III.6.2 (continued 2)

Theorem III.6.2. The 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 (continued). Now for the uniqueness. Suppose $f = q_1 g + r_1 = q_2 g + r_2$ with $\deg(r_1) < \deg(g)$ and $\deg(r_2) < \deg(g)$. Then we have $(q_1 - q_2)g = r_2 - r_1$. Since the leading coefficient of g is a unit (by hypothesis), by Theorem III.6.1(iv) we have
$\deg(q_1 - q_2) + \deg(g) = \deg((q_1 - q_2)g) = \deg(r_2 - r_1)$.

Theorem III.6.2 (continued 2)

Theorem III.6.2. The 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 (continued). Now for the uniqueness. Suppose $f = q_1 g + r_1 = q_2 g + r_2$ with $\deg(r_1) < \deg(g)$ and $\deg(r_2) < \deg(g)$. Then we have $(q_1 - q_2)g = r_2 - r_1$. Since the leading coefficient of g is a unit (by hypothesis), by Theorem III.6.1(iv) we have $\deg(q_1 - q_2) + \deg(g) = \deg((q_1 - q_2)g) = \deg(r_2 - r_1)$. Since $\deg(r_2 - r_1) \leq \max(\deg(r_1), \deg(r_2)) < \deg(g)$, the above equality is true only if $\deg(q_1 - q_2) = -\infty = \deg(r_2 - r_1)$ (that is, the equality does not hold for finite degrees). In other words, $q_1 - q_2 = 0$ and $r_2 - r_1 = 0$. That is, $q_1 = q_2$ and $r_1 = r_2$, so the q and r are unique. □

Theorem III.6.2 (continued 2)

Theorem III.6.2. The 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 (continued). Now for the uniqueness. Suppose $f = q_1 g + r_1 = q_2 g + r_2$ with $\deg(r_1) < \deg(g)$ and $\deg(r_2) < \deg(g)$. Then we have $(q_1 - q_2)g = r_2 - r_1$. Since the leading coefficient of g is a unit (by hypothesis), by Theorem III.6.1(iv) we have $\deg(q_1 - q_2) + \deg(g) = \deg((q_1 - q_2)g) = \deg(r_2 - r_1)$. Since $\deg(r_2 - r_1) \leq \max(\deg(r_1), \deg(r_2)) < \deg(g)$, the above equality is true only if $\deg(q_1 - q_2) = -\infty = \deg(r_2 - r_1)$ (that is, the equality does not hold for finite degrees). In other words, $q_1 - q_2 = 0$ and $r_2 - r_1 = 0$. That is, $q_1 = q_2$ and $r_1 = r_2$, so the q and r are unique. □

Corollary III.6.3

Corollary III.6.3. Remainder Theorem.
Let R be a ring with identity and $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$. For any $c \in R$ there exists a unique $q(x) \in R[x]$ such that $f(x) = q(x)(x - c) + f(c)$.

Proof. The result is trivial if $f \equiv 0$, so WLOG $f \not\equiv 0$.

Corollary III.6.3

Corollary III.6.3. Remainder Theorem.
Let R be a ring with identity and $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$. For any $c \in R$ there exists a unique $q(x) \in R[x]$ such that $f(x) = q(x)(x - c) + f(c)$.

Proof. The result is trivial if $f \equiv 0$, so WLOG $f \not\equiv 0$. With $g(x) = x - c$, Theorem III.6.2 implies that there exist unique polynomials $q(x), r(x) \in R[x]$ such that $f(x) = q(x)(x - c) + r(x)$ and $\deg(r(x)) < \deg(x - c) = 1$. Thus $r(x) = r$ is a constant polynomial (possibly 0).

Corollary III.6.3

Corollary III.6.3. Remainder Theorem.
Let R be a ring with identity and $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$. For any $c \in R$ there exists a unique $q(x) \in R[x]$ such that $f(x) = q(x)(x-c) + f(c)$.

Proof. The result is trivial if $f \equiv 0$, so WLOG $f \not\equiv 0$. With $g(x) = x - c$, Theorem III.6.2 implies that there exist unique polynomials $q(x), r(x) \in R[x]$ such that $f(x) = q(x)(x-c) + r(x)$ and $\deg(r(x)) < \deg(x-c) = 1$. Thus $r(x) = r$ is a constant polynomial (possibly 0). If $q(x) = \sum_{j=0}^{n-1} b_j x^j$ then
$f(x) = q(x)(x-c) + r = -b_0 c + \sum_{k=1}^{n-1}(-b_k c + b_{k-1})x^k + b_{n-1}x^n + r$,
whence $f(c) = -b_0 c + \sum_{k=1}^{n-1}(-b_k c + b_{k-1})c^k + b_{n-1}c^n + r = -\sum_{k=0}^{n-1} b_k c^{k+1} + \sum_{k=1}^{n} b_{k-1} c^k + r = r$. So we have
$f(x) = q(x)(x-c) + r = q(x)(x-c) + f(c)$. □

Corollary III.6.3

Corollary III.6.3. Remainder Theorem.
Let R be a ring with identity and $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$. For any $c \in R$ there exists a unique $q(x) \in R[x]$ such that $f(x) = q(x)(x-c) + f(c)$.

Proof. The result is trivial if $f \equiv 0$, so WLOG $f \not\equiv 0$. With $g(x) = x - c$, Theorem III.6.2 implies that there exist unique polynomials $q(x), r(x) \in R[x]$ such that $f(x) = q(x)(x-c) + r(x)$ and $\deg(r(x)) < \deg(x-c) = 1$. Thus $r(x) = r$ is a constant polynomial (possibly 0). If $q(x) = \sum_{j=0}^{n-1} b_j x^j$ then
$f(x) = q(x)(x-c) + r = -b_0 c + \sum_{k=1}^{n-1}(-b_k c + b_{k-1})x^k + b_{n-1}x^n + r$,
whence $f(c) = -b_0 c + \sum_{k=1}^{n-1}(-b_k c + b_{k-1})c^k + b_{n-1}c^n + r =$
$-\sum_{k=0}^{n-1} b_k c^{k+1} + \sum_{k=1}^{n} b_{k-1} c^k + r = r$. So we have
$f(x) = q(x)(x-c) + r = q(x)(x-c) + f(c)$. □

Corollary III.6.4

Corollary III.6.4. If F is a field, then the polynomial ring $F[x]$ is a Euclidean domain, whence $F[x]$ is a principal ideal domain and a unique factorization domain. The units in $F[x]$ are precisely the nonzero constant polynomials.

Proof. Since F is a field (and hence an integral domain) then by Theorem III.5.1(ii) $F[x]$ is an integral domain. Define $\varphi : F[x] \setminus \{0\} \to \mathbb{N} \cup \{0\}$ by $\varphi(f) = \deg(f)$.

Corollary III.6.4

Corollary III.6.4. If F is a field, then the polynomial ring $F[x]$ is a Euclidean domain, whence $F[x]$ is a principal ideal domain and a unique factorization domain. The units in $F[x]$ are precisely the nonzero constant polynomials.

Proof. Since F is a field (and hence an integral domain) then by Theorem III.5.1(ii) $F[x]$ is an integral domain. Define $\varphi : F[x] \setminus \{0\} \to \mathbb{N} \cup \{0\}$ by $\varphi(f) = \deg(f)$. Every nonzero element of F is a unit since F is a field, so first by Theorem III.6.1(iv), $\varphi(fg) = \varphi(f) + \varphi(g)$, and second by Theorem III.6.2, $f = qg + r$ for some $q, r \in F[x]$ where $\deg(r) < \deg(g)$.

Corollary III.6.4

Corollary III.6.4. If F is a field, then the polynomial ring $F[x]$ is a Euclidean domain, whence $F[x]$ is a principal ideal domain and a unique factorization domain. The units in $F[x]$ are precisely the nonzero constant polynomials.

Proof. Since F is a field (and hence an integral domain) then by Theorem III.5.1(ii) $F[x]$ is an integral domain. Define $\varphi : F[x] \setminus \{0\} \to \mathbb{N} \cup \{0\}$ by $\varphi(f) = \deg(f)$. Every nonzero element of F is a unit since F is a field, so first by Theorem III.6.1(iv), $\varphi(fg) = \varphi(f) + \varphi(g)$, and second by Theorem III.6.2, $f = qg + r$ for some $q, r \in F[x]$ where $\deg(r) < \deg(g)$. So by Definition III.3.8 $F[x]$ is a Euclidean domain. By Theorem III.3.9 $F[x]$ is a principal ideal domain and a unique factorization domain.

Corollary III.6.4

Corollary III.6.4. If F is a field, then the polynomial ring $F[x]$ is a Euclidean domain, whence $F[x]$ is a principal ideal domain and a unique factorization domain. The units in $F[x]$ are precisely the nonzero constant polynomials.

Proof. Since F is a field (and hence an integral domain) then by Theorem III.5.1(ii) $F[x]$ is an integral domain. Define $\varphi : F[x] \setminus \{0\} \to \mathbb{N} \cup \{0\}$ by $\varphi(f) = \deg(f)$. Every nonzero element of F is a unit since F is a field, so first by Theorem III.6.1(iv), $\varphi(fg) = \varphi(f) + \varphi(g)$, and second by Theorem III.6.2, $f = qg + r$ for some $q, r \in F[x]$ where $\deg(r) < \deg(g)$. So by Definition III.3.8 $F[x]$ is a Euclidean domain. By Theorem III.3.9 $F[x]$ is a principal ideal domain and a unique factorization domain.

Corollary III.6.4 (continued)

Corollary III.6.4. If F is a field, then the polynomial ring $F[x]$ is a Euclidean domain, whence $F[x]$ is a principal ideal domain and a unique factorization domain. The units in $F[x]$ are precisely the nonzero constant polynomials.

Proof (continued). If f is a unit in $F[x]$, then there exists $g \in F[x]$ such that $fg = 1$. By Theorem III.6.1(iv), $0 = \deg(1) = \deg(fg) = \deg(f) + \deg(g)$ and so $\deg(f) = 0$. Therefore f is a constant polynomial and it must be nonzero. Conversely, if f is a nonzero constant polynomial in $F[x]$ then there is a multiplicative inverse of f in $F[x]$ since F is a field (so $f \in F$ implies $f^{-1} \in F$, here we draw no distinction between a constant polynomial in $F[x]$ and an element of F). □

Corollary III.6.4 (continued)

Corollary III.6.4. If F is a field, then the polynomial ring $F[x]$ is a Euclidean domain, whence $F[x]$ is a principal ideal domain and a unique factorization domain. The units in $F[x]$ are precisely the nonzero constant polynomials.

Proof (continued). If f is a unit in $F[x]$, then there exists $g \in F[x]$ such that $fg = 1$. By Theorem III.6.1(iv), $0 = \deg(1) = \deg(fg) = \deg(f) + \deg(g)$ and so $\deg(f) = 0$. Therefore f is a constant polynomial and it must be nonzero. Conversely, if f is a nonzero constant polynomial in $F[x]$ then there is a multiplicative inverse of f in $F[x]$ since F is a field (so $f \in F$ implies $f^{-1} \in F$, here we draw no distinction between a constant polynomial in $F[x]$ and an element of F). □

Theorem III.6.6

Theorem III.6.6. Factor Theorem.
Let R be a commutative ring with identity and $f \in R[x]$. Then $c \in R$ is a root of f if and only if $x - c$ divides f.

Proof. (1) By Corollary III.6.3, $f(x) = q(x)(x - c) + f(c)$. If $x - c$ divides $f(x)$ then $h(x)(x - c) = f(x) = q(x)(x - c) + f(c)$ for some $h(x) \in R[x]$. Whence $(h(x) - q(x))(x - c) = f(c)$ (in $R[x]$).

Theorem III.6.6

Theorem III.6.6. Factor Theorem.
Let R be a commutative ring with identity and $f \in R[x]$. Then $c \in R$ is a root of f if and only if $x - c$ divides f.

Proof. (1) By Corollary III.6.3, $f(x) = q(x)(x - c) + f(c)$. If $x - c$ divides $f(x)$ then $h(x)(x - c) = f(x) = q(x)(x - c) + f(c)$ for some $h(x) \in R[x]$. Whence $(h(x) - q(x))(x - c) = f(c)$ (in $R[x]$). By applying the evaluation homomorphism that replaces x with c to give an element of R (see Corollary III.5.6 and the "Remark" after it), we have that $f(c) = (h(c) - q(c))(c - c) = 0$ (in R). So if $x - c$ divides $f(x)$ then $f(c) = 0$.

Theorem III.6.6

Theorem III.6.6. Factor Theorem.
Let R be a commutative ring with identity and $f \in R[x]$. Then $c \in R$ is a root of f if and only if $x - c$ divides f.

Proof. (1) By Corollary III.6.3, $f(x) = q(x)(x - c) + f(c)$. If $x - c$ divides $f(x)$ then $h(x)(x - c) = f(x) = q(x)(x - c) + f(c)$ for some $h(x) \in R[x]$. Whence $(h(x) - q(x))(x - c) = f(c)$ (in $R[x]$). By applying the evaluation homomorphism that replaces x with c to give an element of R (see Corollary III.5.6 and the "Remark" after it), we have that $f(c) = (h(c) - q(c))(c - c) = 0$ (in R). So if $x - c$ divides $f(x)$ then $f(c) = 0$.
(2) Suppose $f(c) = 0$. By the Remainder Theorem (Corollary III.6.3), $f(x) = q(x)(x - c) + f(c) = q(x)(x - c)$ and so $x - c$ divides $f(x)$. (Notice that the Remainder Theorem does not require commutivity and so this result holds even for noncommutative rings with identity.) □

Theorem III.6.6

Theorem III.6.6. Factor Theorem.
Let R be a commutative ring with identity and $f \in R[x]$. Then $c \in R$ is a root of f if and only if $x - c$ divides f.

Proof. (1) By Corollary III.6.3, $f(x) = q(x)(x - c) + f(c)$. If $x - c$ divides $f(x)$ then $h(x)(x - c) = f(x) = q(x)(x - c) + f(c)$ for some $h(x) \in R[x]$. Whence $(h(x) - q(x))(x - c) = f(c)$ (in $R[x]$). By applying the evaluation homomorphism that replaces x with c to give an element of R (see Corollary III.5.6 and the "Remark" after it), we have that $f(c) = (h(c) - q(c))(c - c) = 0$ (in R). So if $x - c$ divides $f(x)$ then $f(c) = 0$.
(2) Suppose $f(c) = 0$. By the Remainder Theorem (Corollary III.6.3), $f(x) = q(x)(x - c) + f(c) = q(x)(x - c)$ and so $x - c$ divides $f(x)$. (Notice that the Remainder Theorem does not require commutivity and so this result holds even for noncommutative rings with identity.) □

Theorem III.6.7

Theorem III.6.7. 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 $c_1, c_2, \ldots$ be the *distinct* roots of f in E.

Theorem III.6.7

Theorem III.6.7. 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 $c_1, c_2, \ldots$ be the *distinct* roots of f in E. By Theorem III.6.6, $f(x) = q_1(x)(x - c_1)$ for some $q_1(x) \in R[x]$. Whence applying an evaluation homomorphism $0 = f(c_2) = q_1(c_2)(c_2 - c_1)$ (Hungerford says "by Corollary III.5.6"). Since we are considering distinct c_i, then $c_1 \neq c_2$.

Theorem III.6.7

Theorem III.6.7. 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 $c_1, c_2, \ldots$ be the *distinct* roots of f in E. By Theorem III.6.6, $f(x) = q_1(x)(x - c_1)$ for some $q_1(x) \in R[x]$. Whence applying an evaluation homomorphism $0 = f(c_2) = q_1(c_2)(c_2 - c_1)$ (Hungerford says "by Corollary III.5.6"). Since we are considering distinct c_i, then $c_1 \neq c_2$. Since E is an integral domain (no divisors of zero) then $q_1(c_2) = 0$. Therefore, $x - c_2$ divides q_2 by Theorem III.6.6 and so $f(x) = q_2(x)(x - c_2)(x - c_1)$. Inductively, for distinct roots $c_1, c_2, \ldots, c_m$ of f in E we have $g_m = (x - c_1)(x - c_2) \cdots (x - c_m)$ divides f.

Theorem III.6.7

Theorem III.6.7. 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 $c_1, c_2, \ldots$ be the *distinct* roots of f in E. By Theorem III.6.6, $f(x) = q_1(x)(x - c_1)$ for some $q_1(x) \in R[x]$. Whence applying an evaluation homomorphism $0 = f(c_2) = q_1(c_2)(c_2 - c_1)$ (Hungerford says "by Corollary III.5.6"). Since we are considering distinct c_i, then $c_1 \neq c_2$. Since E is an integral domain (no divisors of zero) then $q_1(c_2) = 0$. Therefore, $x - c_2$ divides q_2 by Theorem III.6.6 and so $f(x) = q_2(x)(x - c_2)(x - c_1)$. Inductively, for distinct roots $c_1, c_2, \ldots, c_m$ of f in E we have $g_m = (x - c_1)(x - c_2) \cdots (x - c_m)$ divides f. But $\deg(g_m) = m$ by Theorem III.6.1(iv), and by Theorem III.6.1(ii) $m \leq n$. So the total number of distinct roots of f is less than or equal to n. □

Theorem III.6.7

Theorem III.6.7. 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 $c_1, c_2, \ldots$ be the *distinct* roots of f in E. By Theorem III.6.6, $f(x) = q_1(x)(x - c_1)$ for some $q_1(x) \in R[x]$. Whence applying an evaluation homomorphism $0 = f(c_2) = q_1(c_2)(c_2 - c_1)$ (Hungerford says "by Corollary III.5.6"). Since we are considering distinct c_i, then $c_1 \neq c_2$. Since E is an integral domain (no divisors of zero) then $q_1(c_2) = 0$. Therefore, $x - c_2$ divides q_2 by Theorem III.6.6 and so $f(x) = q_2(x)(x - c_2)(x - c_1)$. Inductively, for distinct roots $c_1, c_2, \ldots, c_m$ of f in E we have $g_m = (x - c_1)(x - c_2) \cdots (x - c_m)$ divides f. But $\deg(g_m) = m$ by Theorem III.6.1(iv), and by Theorem III.6.1(ii) $m \leq n$. So the total number of distinct roots of f is less than or equal to n. □

Theorem III.6.8

Proposition III.6.8. Let D be a unique factorization domain with quotient field F (that is, F is the field of quotients produced from D) 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 (so u is in "reduced form"), and u is a root of f, then c divides a_0 and d divides a_n.

Proof. Since we hypothesize that $f(u) = 0$, we have $f(u) = f(c/d) = \sum_{i=0}^{n} a_i (c/d)^i = 0$ or (multiplying both sides by d^n) $\sum_{i=0}^{n} a_i c^i d^{n-i} = 0$ or $a_0 d^n + c \sum_{i=1}^{n} a_i c^{i-1} d^{n-i} = 0$ or $a_0 d^n = c(\sum_{i=1}^{n}(-a_i) c^{i-1} d^{n-i})$. Since c and d are relatively prime then by Exercise III.3.10 we have that c divides a_0.

Theorem III.6.8

Proposition III.6.8. Let D be a unique factorization domain with quotient field F (that is, F is the field of quotients produced from D) 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 (so u is in "reduced form"), and u is a root of f, then c divides a_0 and d divides a_n.

Proof. Since we hypothesize that $f(u) = 0$, we have $f(u) = f(c/d) = \sum_{i=0}^{n} a_i (c/d)^i = 0$ or (multiplying both sides by d^n) $\sum_{i=0}^{n} a_i c^i d^{n-i} = 0$ or $a_0 d^n + c \sum_{i=1}^{n} a_i c^{i-1} d^{n-i} = 0$ or $a_0 d^n = c(\sum_{i=1}^{n} (-a_i) c^{i-1} d^{n-i})$. Since c and d are relatively prime then by Exercise III.3.10 we have that c divides a_0.

Also $\sum_{i=0}^{n} a_i c^i d^{n-i} = 0$ or $\sum_{i=0}^{n-1} a_i c^i d^{n-i} + a_n c^n = 0$ or $-a_n c^n = \left(\sum_{i=0}^{n-1} a_i c^i d^{n-i-1} \right) d$. Since c and d are relatively prime then by Exercise III.3.10 we have that d divides a_n. □

Theorem III.6.8

Proposition III.6.8. Let D be a unique factorization domain with quotient field F (that is, F is the field of quotients produced from D) 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 (so u is in "reduced form"), and u is a root of f, then c divides a_0 and d divides a_n.

Proof. Since we hypothesize that $f(u) = 0$, we have $f(u) = f(c/d) = \sum_{i=0}^{n} a_i (c/d)^i = 0$ or (multiplying both sides by d^n) $\sum_{i=0}^{n} a_i c^i d^{n-i} = 0$ or $a_0 d^n + c \sum_{i=1}^{n} a_i c^{i-1} d^{n-i} = 0$ or $a_0 d^n = c(\sum_{i=1}^{n} (-a_i) c^{i-1} d^{n-i})$. Since c and d are relatively prime then by Exercise III.3.10 we have that c divides a_0.

Also $\sum_{i=0}^{n} a_i c^i d^{n-i} = 0$ or $\sum_{i=0}^{n-1} a_i c^i d^{n-i} + a_n c^n = 0$ or $-a_n c^n = \left(\sum_{i=0}^{n-1} a_i c^i d^{n-i-1} \right) d$. Since c and d are relatively prime then by Exercise III.3.10 we have that d divides a_n. □

Theorem III.6.10

Theorem III.6.10. Let D be an integral domain which is a subring of an integral domain E. Let $f \in D[x]$ and $c \in E$.

(i) c is a multiple root of f if and only if $f(c) = 0$ 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 if and only if $f' \neq 0$ (here, "$f' \neq 0$" means that f' is not the zero polynomial in $D[x]$).

Proof. (i) Let c be a root of f of multiplicity m. Then (by definition) $f(x) = (x - c)^m g(x)$ and $g(c) \neq 0$.

Theorem III.6.10

Theorem III.6.10. Let D be an integral domain which is a subring of an integral domain E. Let $f \in D[x]$ and $c \in E$.

(i) c is a multiple root of f if and only if $f(c) = 0$ 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 if and only if $f' \neq 0$ (here, "$f' \neq 0$" means that f' is not the zero polynomial in $D[x]$).

Proof. (i) Let c be a root of f of multiplicity m. Then (by definition) $f(x) = (x - c)^m g(x)$ and $g(c) \neq 0$. By Lemma III.6.9(iii) $f'(x) = m(x - c)^{m-1} g(x) + (x - c)^m g'(x)$. If c is a multiple root of f (i.e., $m > 1$) then we have that $f'(c) = 0$.

Theorem III.6.10

Theorem III.6.10. Let D be an integral domain which is a subring of an integral domain E. Let $f \in D[x]$ and $c \in E$.

(i) c is a multiple root of f if and only if $f(c) = 0$ 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 if and only if $f' \neq 0$ (here, "$f' \neq 0$" means that f' is not the zero polynomial in $D[x]$).

Proof. (i) Let c be a root of f of multiplicity m. Then (by definition) $f(x) = (x-c)^m g(x)$ and $g(c) \neq 0$. By Lemma III.6.9(iii) $f'(x) = m(x-c)^{m-1}g(x) + (x-c)^m g'(x)$. If c is a multiple root of f (i.e., $m > 1$) then we have that $f'(c) = 0$.

Theorem III.6.10 (continued 1)

Proof (continued). Conversely, let $f(c) = f'(c) = 0$. Since $f(c) = 0$ then $m \geq 1$ by the Factor Theorem (Theorem III.6.6). ASSUME $m = 1$. Then $f'(x) = g(x) + (x - c)g'(x)$. Consequently, since $f'(c) = 0$, we have that $0 = f'(c) = g(c)$ (Hungerford quotes Corollary III.5.6 since we are using the evaluation homomorphism), a CONTRADICTION to the properties of g. So this contradiction implies the assumption that $m = 1$ is incorrect and hence $m > 1$.

Theorem III.6.10 (continued 1)

Proof (continued). Conversely, let $f(c) = f'(c) = 0$. Since $f(c) = 0$ then $m \geq 1$ by the Factor Theorem (Theorem III.6.6). ASSUME $m = 1$. Then $f'(x) = g(x) + (x - c)g'(x)$. Consequently, since $f'(c) = 0$, we have that $0 = f'(c) = g(c)$ (Hungerford quotes Corollary III.5.6 since we are using the evaluation homomorphism), a CONTRADICTION to the properties of g. So this contradiction implies the assumption that $m = 1$ is incorrect and hence $m > 1$.

(ii) Let D be a field and f relatively prime to f'.

Theorem III.6.10 (continued 1)

Proof (continued). Conversely, let $f(c) = f'(c) = 0$. Since $f(c) = 0$ then $m \geq 1$ by the Factor Theorem (Theorem III.6.6). ASSUME $m = 1$. Then $f'(x) = g(x) + (x - c)g'(x)$. Consequently, since $f'(c) = 0$, we have that $0 = f'(c) = g(c)$ (Hungerford quotes Corollary III.5.6 since we are using the evaluation homomorphism), a CONTRADICTION to the properties of g. So this contradiction implies the assumption that $m = 1$ is incorrect and hence $m > 1$.

(ii) Let D be a field and f relatively prime to f'. By Corollary III.6.4, since D is a field then $D[x]$ is a principal ideal domain. Since f and f' are relatively prime, $\gcd(f, f') = 1_D$ and so by Theorem III.3.11(ii) there are $k(x), h(x) \in D[x]$ such that $kf + hf' = 1_D$.

Theorem III.6.10 (continued 1)

Proof (continued). Conversely, let $f(c) = f'(c) = 0$. Since $f(c) = 0$ then $m \geq 1$ by the Factor Theorem (Theorem III.6.6). ASSUME $m = 1$. Then $f'(x) = g(x) + (x - c)g'(x)$. Consequently, since $f'(c) = 0$, we have that $0 = f'(c) = g(c)$ (Hungerford quotes Corollary III.5.6 since we are using the evaluation homomorphism), a CONTRADICTION to the properties of g. So this contradiction implies the assumption that $m = 1$ is incorrect and hence $m > 1$.
(ii) Let D be a field and f relatively prime to f'. By Corollary III.6.4, since D is a field then $D[x]$ is a principal ideal domain. Since f and f' are relatively prime, $\gcd(f, f') = 1_D$ and so by Theorem III.3.11(ii) there are $k(x), h(x) \in D[x]$ such that $kf + hf' = 1_D$. ASSUME c is a multiple root of f. Then by Corollary III.5.6 (the use of the evaluation homomorphism) and part (i), $q_D = k(c)f(c) + h(c)f'(c) = 0$ (part (i) implies $f'(c) = 0$), a CONTRADICTION ($1_D \neq 0$). So the assumption that c is a multiple root of f is false and so c is a simple root of f.

Theorem III.6.10 (continued 1)

Proof (continued). Conversely, let $f(c) = f'(c) = 0$. Since $f(c) = 0$ then $m \geq 1$ by the Factor Theorem (Theorem III.6.6). ASSUME $m = 1$. Then $f'(x) = g(x) + (x - c)g'(x)$. Consequently, since $f'(c) = 0$, we have that $0 = f'(c) = g(c)$ (Hungerford quotes Corollary III.5.6 since we are using the evaluation homomorphism), a CONTRADICTION to the properties of g. So this contradiction implies the assumption that $m = 1$ is incorrect and hence $m > 1$.

(ii) Let D be a field and f relatively prime to f'. By Corollary III.6.4, since D is a field then $D[x]$ is a principal ideal domain. Since f and f' are relatively prime, $\gcd(f, f') = 1_D$ and so by Theorem III.3.11(ii) there are $k(x), h(x) \in D[x]$ such that $kf + hf' = 1_D$. ASSUME c is a multiple root of f. Then by Corollary III.5.6 (the use of the evaluation homomorphism) and part (i), $q_D = k(c)f(c) + h(c)f'(c) = 0$ (part (i) implies $f'(c) = 0$), a CONTRADICTION ($1_D \neq 0$). So the assumption that c is a multiple root of f is false and so c is a simple root of f.

Theorem III.6.10 (continued 2)

Proof (continued). (iii) Let D be a field, f irreducible in $D[x]$, and E contain a root of f. First, let $f' \neq 0$. Since f is irreducible then (by definition) the only divisors of f are unit multiples of f. Since $f' \neq 0$ then $\deg(f) \geq 1$ and so $\deg(f') < \deg(f)$.

Theorem III.6.10 (continued 2)

Proof (continued). (iii) Let D be a field, f irreducible in $D[x]$, and E contain a root of f. First, let $f' \neq 0$. Since f is irreducible then (by definition) the only divisors of f are unit multiples of f. Since $f' \neq 0$ then $\deg(f) \geq 1$ and so $\deg(f') < \deg(f)$. So the only thing that could divide both f' and f is a unit (i.e., a constant polynomial). So f and f' are relatively prime. By part (ii), f has no multiple roots in E.

Theorem III.6.10 (continued 2)

Proof (continued). (iii) Let D be a field, f irreducible in $D[x]$, and E contain a root of f. First, let $f' \neq 0$. Since f is irreducible then (by definition) the only divisors of f are unit multiples of f. Since $f' \neq 0$ then $\deg(f) \geq 1$ and so $\deg(f') < \deg(f)$. So the only thing that could divide both f' and f is a unit (i.e., a constant polynomial). So f and f' are relatively prime. By part (ii), f has no multiple roots in E.

Conversely, suppose f has no multiple roots in E. We have hypothesized that E has a root of f, say b is the root. ASSUME $f' = 0$.

Theorem III.6.10 (continued 2)

Proof (continued). (iii) Let D be a field, f irreducible in $D[x]$, and E contain a root of f. First, let $f' \neq 0$. Since f is irreducible then (by definition) the only divisors of f are unit multiples of f. Since $f' \neq 0$ then $\deg(f) \geq 1$ and so $\deg(f') < \deg(f)$. So the only thing that could divide both f' and f is a unit (i.e., a constant polynomial). So f and f' are relatively prime. By part (ii), f has no multiple roots in E.
Conversely, suppose f has no multiple roots in E. We have hypothesized that E has a root of f, say b is the root. ASSUME $f' = 0$. Then $f'(b) = 0$ and b is a multiple root of f by part (i), a CONTRADICTION. So the assumption is false and $f' \neq 0$. □

Theorem III.6.10 (continued 2)

Proof (continued). (iii) Let D be a field, f irreducible in $D[x]$, and E contain a root of f. First, let $f' \neq 0$. Since f is irreducible then (by definition) the only divisors of f are unit multiples of f. Since $f' \neq 0$ then $\deg(f) \geq 1$ and so $\deg(f') < \deg(f)$. So the only thing that could divide both f' and f is a unit (i.e., a constant polynomial). So f and f' are relatively prime. By part (ii), f has no multiple roots in E.
Conversely, suppose f has no multiple roots in E. We have hypothesized that E has a root of f, say b is the root. ASSUME $f' = 0$. Then $f'(b) = 0$ and b is a multiple root of f by part (i), a CONTRADICTION. So the assumption is false and $f' \neq 0$. □

Lemma III.6.11

Lemma III.6.11. (Gauss) If D is a unique factorization domain and $f, g \in D[x]$, then $C(fg) = C(f)C(g)$. In particular, the product of primitive polynomials is primitive.

Proof. If $a \in D$ and $f \in D[x]$, then $C(af) = aC(f)$ by Exercise II.6.4. Now $f = F(f)f_1$ and $g = C(g)g_1$ where f_1 and g_1 are primitive. Consequently $C(fg) = C(C(f)f_1C(g)g_1) = C(f)C(g)C(f_1g_1)$.

Lemma III.6.11

Lemma III.6.11. (Gauss) If D is a unique factorization domain and $f, g \in D[x]$, then $C(fg) = C(f)C(g)$. In particular, the product of primitive polynomials is primitive.

Proof. If $a \in D$ and $f \in D[x]$, then $C(af) = aC(f)$ by Exercise II.6.4. Now $f = F(f)f_1$ and $g = C(g)g_1$ where f_1 and g_1 are primitive. Consequently $C(fg) = C(C(f)f_1C(g)g_1) = C(f)C(g)C(f_1g_1)$. Hence it suffices to prove that f_1g_1 is primitive (that is, $C(f_1g_1)$ is a unit). If $f_1g_1 = \sum_{i=0}^n a_ix^i$ and $g_1 = \sum_{j=0}^m b_jx^j$, then $f_1g_1 = \sum_{k=0}^{m+n} c_kx^k$ where $c_k = \sum_{i+j=k} a_ib_j$.

Lemma III.6.11

Lemma III.6.11. (Gauss) If D is a unique factorization domain and $f, g \in D[x]$, then $C(fg) = C(f)C(g)$. In particular, the product of primitive polynomials is primitive.

Proof. If $a \in D$ and $f \in D[x]$, then $C(af) = aC(f)$ by Exercise II.6.4. Now $f = F(f)f_1$ and $g = C(g)g_1$ where f_1 and g_1 are primitive. Consequently $C(fg) = C(C(f)f_1C(g)g_1) = C(f)C(g)C(f_1g_1)$. Hence it suffices to prove that f_1g_1 is primitive (that is, $C(f_1g_1)$ is a unit). If $f_1g_1 = \sum_{i=0}^{n} a_i x^i$ and $g_1 = \sum_{j=0}^{m} b_j x^j$, then $f_1g_1 = \sum_{k=0}^{m+n} c_k x^k$ where $c_k = \sum_{i+j=k} a_i b_j$. ASSUME f_1g_1 is not primitive, then $C(f_1g_1)$ is not a unit (by the definition of "primitive") and so by the definition of unique factorization domain (Definition III.3.5(i)) $C(f_1g_1)$ can be written as a product of irreducibles. Since $C(f_1g_1)$ is a greatest common divisor of the c_k, then one of these irreducibles, say p, must be a divisor of each c_k: $p \mid c_k$ for all k.

Lemma III.6.11

Lemma III.6.11. (Gauss) If D is a unique factorization domain and $f, g \in D[x]$, then $C(fg) = C(f)C(g)$. In particular, the product of primitive polynomials is primitive.

Proof. If $a \in D$ and $f \in D[x]$, then $C(af) = aC(f)$ by Exercise II.6.4. Now $f = F(f)f_1$ and $g = C(g)g_1$ where f_1 and g_1 are primitive. Consequently $C(fg) = C(C(f)f_1C(g)g_1) = C(f)C(g)C(f_1g_1)$. Hence it suffices to prove that f_1g_1 is primitive (that is, $C(f_1g_1)$ is a unit). If $f_1g_1 = \sum_{i=0}^n a_ix^i$ and $g_1 = \sum_{j=0}^m b_jx^j$, then $f_1g_1 = \sum_{k=0}^{m+n} c_kx^k$ where $c_k = \sum_{i+j=k} a_ib_j$. ASSUME f_1g_1 is not primitive, then $C(f_1g_1)$ is not a unit (by the definition of "primitive") and so by the definition of unique factorization domain (Definition III.3.5(i)) $C(f_1g_1)$ can be written as a product of irreducibles. Since $C(f_1g_1)$ is a greatest common divisor of the c_k, then one of these irreducibles, say p, must be a divisor of each c_k: $p \mid c_k$ for all k.

Lemma III.6.11 (continued)

Proof (continued). Since $C(f_1)$ is a unit then $p \nmid C(f_1)$ (for if $p \mid C(f_1)$ then we have also that $C(f_1) \mid p$ by Theorem III.3.2(iii) and so, by definition of the fact that p and $C(f_1)$ are associates—but then by Theorem III.3.4(v), $C(f_1)$ is irreducible which contradicts the fact that $C(f_1)$ is a unit and hence, by definition, is irreducible). Whence there is a least nonnegative 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 $c_{s+t} = a_0 b_{s+t} + \cdots + a_{s-1} b_{t+1} + a_s b_t + a_{s+1} b_{t-1} + \cdots a_{s+1} b_0$ then, since p divides $a_0, a_1, \ldots, a_{s-1}$ and $b_0, b_1, \ldots, b_{t-1}$ then p must divide $a_s b_t$.

Lemma III.6.11 (continued)

Proof (continued). Since $C(f_1)$ is a unit then $p \nmid C(f_1)$ (for if $p \mid C(f_1)$ then we have also that $C(f_1) \mid p$ by Theorem III.3.2(iii) and so, by definition of the fact that p and $C(f_1)$ are associates—but then by Theorem III.3.4(v), $C(f_1)$ is irreducible which contradicts the fact that $C(f_1)$ is a unit and hence, by definition, is irreducible). Whence there is a least nonnegative 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 $c_{s+t} = a_0 b_{s+t} + \cdots + a_{s-1} b_{t+1} + a_s b_t + a_{s+1} b_{t-1} + \cdots a_{s+1} b_0$ then, since p divides $a_0, a_1, \ldots, a_{s-1}$ and $b_0, b_1, \ldots, b_{t-1}$ then p must divide $a_s b_t$. Since every irreducible element in D is prime (this follows from Definition III.3.5(ii); see the "Remark" after the definition on page 137), then $p \mid a_s b_t$ implies that either $p \mid a_s$ or $p \mid b_t$. But this CONTRADICTS the choice of s or t. This contradiction shows that the assumption that $f_1 g_1$ is not primitive is false. Therefore $f_1 g_1$ is primitive. So $C(f_1 g_1)$ is a unit and since $C(fg) = C(f)C(g)C(f_1 g_1)$ as shown above, then $C(fg) \approx C(f)C(g)$. □

Lemma III.6.11 (continued)

Proof (continued). Since $C(f_1)$ is a unit then $p \nmid C(f_1)$ (for if $p \mid C(f_1)$ then we have also that $C(f_1) \mid p$ by Theorem III.3.2(iii) and so, by definition of the fact that p and $C(f_1)$ are associates—but then by Theorem III.3.4(v), $C(f_1)$ is irreducible which contradicts the fact that $C(f_1)$ is a unit and hence, by definition, is irreducible). Whence there is a least nonnegative 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 $c_{s+t} = a_0 b_{s+t} + \cdots + a_{s-1} b_{t+1} + a_s b_t + a_{s+1} b_{t-1} + \cdots a_{s+1} b_0$ then, since p divides $a_0, a_1, \ldots, a_{s-1}$ and $b_0, b_1, \ldots, b_{t-1}$ then p must divide $a_s b_t$. Since every irreducible element in D is prime (this follows from Definition III.3.5(ii); see the "Remark" after the definition on page 137), then $p \mid a_s b_t$ implies that either $p \mid a_s$ or $p \mid b_t$. But this CONTRADICTS the choice of s or t. This contradiction shows that the assumption that $f_1 g_1$ is not primitive is false. Therefore $f_1 g_1$ is primitive. So $C(f_1 g_1)$ is a unit and since $C(fg) = C(f)C(g)C(f_1 g_1)$ as shown above, then $C(fg) \approx C(f)C(g)$. □

Lemma III.6.12

Lemma III.6.12. 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 $D[x]$ if and only if they are associates in $F[x]$.

Proof. Let f and g be associates in the integral domain $F[x]$ (since F is a field, $F[x]$ is commutative and has no zero divisors) then $f = gu$ for some unit $u \in F[x]$ by Theorem III.3.2(vi).

Lemma III.6.12

Lemma III.6.12. 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 $D[x]$ if and only if they are associates in $F[x]$.

Proof. Let f and g be associates in the integral domain $F[x]$ (since F is a field, $F[x]$ is commutative and has no zero divisors) then $f = gu$ for some unit $u \in F[x]$ by Theorem III.3.2(vi). By Corollary III.6.4, u is a nonzero constant polynomial and so $u \in F$, whence $u = b/c$ for some $b, c \in D$ and $c \neq 0$. Therefore $f = gb/c$ and $cf = bg$. Since $C(f)$ and $C(g)$ are units in D (because f, g are primitive) then

$$\begin{aligned} c &\approx cC(f) \text{ since } C(f) \text{ is a unit} \\ &\approx C(cf) \text{ by Exercise III.6.4} \\ &= C(bg) \\ &\approx bC(g) \text{ by Exercise II.6.4} \\ &\approx b \text{ since } C(g) \text{ is a unit.} \end{aligned}$$

Lemma III.6.12

Lemma III.6.12. 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 $D[x]$ if and only if they are associates in $F[x]$.

Proof. Let f and g be associates in the integral domain $F[x]$ (since F is a field, $F[x]$ is commutative and has no zero divisors) then $f = gu$ for some unit $u \in F[x]$ by Theorem III.3.2(vi). By Corollary III.6.4, u is a nonzero constant polynomial and so $u \in F$, whence $u = b/c$ for some $b, c \in D$ and $c \neq 0$. Therefore $f = gb/c$ and $cf = bg$. Since $C(f)$ and $C(g)$ are units in D (because f, g are primitive) then

$$\begin{aligned} c &\approx cC(f) \text{ since } C(f) \text{ is a unit} \\ &\approx C(cf) \text{ by Exercise III.6.4} \\ &= C(bg) \\ &\approx bC(g) \text{ by Exercise II.6.4} \\ &\approx b \text{ since } C(g) \text{ is a unit.} \end{aligned}$$

Lemma III.6.12 (continued)

Lemma III.6.12. 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 $D[x]$ if and only if they are associates in $F[x]$.

Proof (continued). Therefore $b = cv$ for some unit $v \in D$ and $cf = bg = cvg$. Consequently $f = vg$ (since $c \neq 0$) whence f and g are associates.

Let f and g be associates in $D[x]$. The by Theorem III.3.2(vi) $f = gu$ for some unit $u \in D[x]$.

Lemma III.6.12 (continued)

Lemma III.6.12. 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 $D[x]$ if and only if they are associates in $F[x]$.

Proof (continued). Therefore $b = cv$ for some unit $v \in D$ and $cf = bg = cvg$. Consequently $f = vg$ (since $c \neq 0$) whence f and g are associates.

Let f and g be associates in $D[x]$. The by Theorem III.3.2(vi) $f = gu$ for some unit $u \in D[x]$. But F is a quotient field of D so $D[x] \subset F[x]$ (as rings, say) so $f = gu$ where u is a unit in $F[x]$ and so f and g are associates in $F[x]$. □

Lemma III.6.12 (continued)

Lemma III.6.12. 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 $D[x]$ if and only if they are associates in $F[x]$.

Proof (continued). Therefore $b = cv$ for some unit $v \in D$ and $cf = bg = cvg$. Consequently $f = vg$ (since $c \neq 0$) whence f and g are associates.

Let f and g be associates in $D[x]$. The by Theorem III.3.2(vi) $f = gu$ for some unit $u \in D[x]$. But F is a quotient field of D so $D[x] \subset F[x]$ (as rings, say) so $f = gu$ where u is a unit in $F[x]$ and so f and g are associates in $F[x]$. □

Lemma III.6.13

Lemma III.6.13. Let D be a unique factorization domain with quotient field F and f a primitive polynomial of positive degree in $D[x]$. Then f is irreducible in $D[x]$ if and only if f is irreducible in $F[x]$.

Proof. Let f be irreducible in $D[x]$ and ASSUME that $f = gh$ with $g, h \in F[x]$ where $\deg(g) \geq 1$, $\deg(h) \geq 1$ (that is, assume f is not irreducible in $F[x]$).

Lemma III.6.13

Lemma III.6.13. Let D be a unique factorization domain with quotient field F and f a primitive polynomial of positive degree in $D[x]$. Then f is irreducible in $D[x]$ if and only if f is irreducible in $F[x]$.

Proof. Let f be irreducible in $D[x]$ and ASSUME that $f = gh$ with $g, h \in F[x]$ where $\deg(g) \geq 1$, $\deg(h) \geq 1$ (that is, assume f is not irreducible in $F[x]$). Then $g = \sum_{i=0}^{n}(a_i/b_i)x^i$ and $h = \sum_{j=0}^{m}(c_j/d_j)x^j$ with $a_i, b_{i,j}, d_j \in D$ and $b_i \neq 0, d_j \neq 0$ for all i and j. Let $b = b_0 b_1 \cdots b_n$ and for each i let $b_i^* = b_0 b_1 \cdots b_{i-1} b_{i+1} \cdots b_n$. If $g_1 = \sum_{i=1}^{n} a_i b_i^* x^i \in D[x]$ then $g_1 = a g_2$ with $a = C(g_1)$ for $g_2 \in D[x]$ and g_2 primitive.

Lemma III.6.13

Lemma III.6.13. Let D be a unique factorization domain with quotient field F and f a primitive polynomial of positive degree in $D[x]$. Then f is irreducible in $D[x]$ if and only if f is irreducible in $F[x]$.

Proof. Let f be irreducible in $D[x]$ and ASSUME that $f = gh$ with $g, h \in F[x]$ where $\deg(g) \geq 1$, $\deg(h) \geq 1$ (that is, assume f is not irreducible in $F[x]$). Then $g = \sum_{i=0}^{n}(a_i/b_i)x^i$ and $h = \sum_{j=0}^{m}(c_j/d_j)x^j$ with $a_i, b_i, _j, d_j \in D$ and $b_i \neq 0, d_j \neq 0$ for all i and j. Let $b = b_0 b_1 \cdots b_n$ and for each i let $b_i^* = b_0 b_1 \cdots b_{i-1} b_{i+1} \cdots b_n$. If $g_1 = \sum_{i=1}^{n} a_i b_i^* x^i \in D[x]$ then $g_1 = a g_2$ with $a = C(g_1)$ for $g_2 \in D[x]$ and g_2 primitive. Now

$$g = \sum_{i=0}^{n}(a_i/b_i)x^i = (b/b)\sum_{i=0}^{n}(a_i/b_i)x^i = (1_D/b)\sum_{i=0}^{n}(a_i b/b_i)x^i$$

$$= (1_D/b)\sum_{i=0}^{n} a_i b_i^* x^i = (a_D/b)g_1 = (a/b)g_2$$

and $\deg(g) = \deg(g_2) = n$.

Lemma III.6.13

Lemma III.6.13. Let D be a unique factorization domain with quotient field F and f a primitive polynomial of positive degree in $D[x]$. Then f is irreducible in $D[x]$ if and only if f is irreducible in $F[x]$.

Proof. Let f be irreducible in $D[x]$ and ASSUME that $f = gh$ with $g, h \in F[x]$ where $\deg(g) \geq 1$, $\deg(h) \geq 1$ (that is, assume f is not irreducible in $F[x]$). Then $g = \sum_{i=0}^{n}(a_i/b_i)x^i$ and $h = \sum_{j=0}^{m}(c_j/d_j)x^j$ with $a_i, b_i,_j, d_j \in D$ and $b_i \neq 0, d_j \neq 0$ for all i and j. Let $b = b_0 b_1 \cdots b_n$ and for each i let $b_i^* = b_0 b_1 \cdots b_{i-1} b_{i+1} \cdots b_n$. If $g_1 = \sum_{i=1}^{n} a_i b_i^* x^i \in D[x]$ then $g_1 = a g_2$ with $a = C(g_1)$ for $g_2 \in D[x]$ and g_2 primitive. Now

$$g = \sum_{i=0}^{n}(a_i/b_i)x^i = (b/b)\sum_{i=0}^{n}(a_i/b_i)x^i = (1_D/b)\sum_{i=0}^{n}(a_i b/b_i)x^i$$

$$= (1_D/b)\sum_{i=0}^{n} a_i b_i^* x^i = (a_D/b)g_1 = (a/b)g_2$$

and $\deg(g) = \deg(g_2) = n$.

Lemma III.6.13 (continued 1)

Proof (continued). Similarly, $h = (c/d)h_2$ with $c, d \in D$, $h_2 \in D[x]$, h_2 primitive, and $\deg(h) = \deg(h_2) = m$. Consequently, $f = gh = (a/b)g_2(c/d)h_2$ whence $bdf = acg_2h_2$. Since f is primitive by hypothesis of the lemma, and g_2h_2 is primitive by Lemma III.6.11, then

$$\begin{aligned} bd &\approx bdC(f) \text{ since } C(f) \text{ is a unit} \\ &\approx C(bdf) \text{ by Exercise III.6.4} \\ &= C(acg_2h_2) \\ &\approx acC(g_2h_2) \text{ by Exercise III.6.4} \\ &\approx ac \text{ since } C(g_2g_2) \text{ is a unit.} \end{aligned}$$

Lemma III.6.13 (continued 1)

Proof (continued). Similarly, $h = (c/d)h_2$ with $c, d \in D$, $h_2 \in D[x]$, h_2 primitive, and $\deg(h) = \deg(h_2) = m$. Consequently, $f = gh = (a/b)g_2(c/d)h_2$ whence $bdf = acg_2h_2$. Since f is primitive by hypothesis of the lemma, and g_2h_2 is primitive by Lemma III.6.11, then

$$\begin{aligned} bd &\approx bdC(f) \text{ since } C(f) \text{ is a unit} \\ &\approx C(bdf) \text{ by Exercise III.6.4} \\ &= C(acg_2h_2) \\ &\approx acC(g_2h_2) \text{ by Exercise III.6.4} \\ &\approx ac \text{ since } C(g_2g_2) \text{ is a unit.} \end{aligned}$$

Therefore $ac = bdv$ for some unit $v \in D$ and so $bdf = acg_2h_2 = bdvg_2h_2$ or $f = vg_2h_2$ where v is a unit in $D[x]$. So f and g_2h_2 are associates in $D[x]$.

Lemma III.6.13 (continued 1)

Proof (continued). Similarly, $h = (c/d)h_2$ with $c, d \in D$, $h_2 \in D[x]$, h_2 primitive, and $\deg(h) = \deg(h_2) = m$. Consequently, $f = gh = (a/b)g_2(c/d)h_2$ whence $bdf = acg_2h_2$. Since f is primitive by hypothesis of the lemma, and g_2h_2 is primitive by Lemma III.6.11, then

$$\begin{aligned} bd &\approx bdC(f) \text{ since } C(f) \text{ is a unit} \\ &\approx C(bdf) \text{ by Exercise III.6.4} \\ &= C(acg_2h_2) \\ &\approx acC(g_2h_2) \text{ by Exercise III.6.4} \\ &\approx ac \text{ since } C(g_2g_2) \text{ is a unit.} \end{aligned}$$

Therefore $ac = bdv$ for some unit $v \in D$ and so $bdf = acg_2h_2 = bdvg_2h_2$ or $f = vg_2h_2$ where v is a unit in $D[x]$. So f and g_2h_2 are associates in $D[x]$. But by Theorem III.3.4(v), every associate of an irreducible is irreducible (here, in integral domain $D[x]$) so vg_2h_2 is irreducible in $D[x]$, a CONTRADICTION (since neither g_2 nor h_2 is a unit in $D \subset F$ since. . .

Lemma III.6.13 (continued 1)

Proof (continued). Similarly, $h = (c/d)h_2$ with $c, d \in D$, $h_2 \in D[x]$, h_2 primitive, and $\deg(h) = \deg(h_2) = m$. Consequently, $f = gh = (a/b)g_2(c/d)h_2$ whence $bdf = acg_2h_2$. Since f is primitive by hypothesis of the lemma, and g_2h_2 is primitive by Lemma III.6.11, then

$$\begin{aligned} bd &\approx bdC(f) \text{ since } C(f) \text{ is a unit} \\ &\approx C(bdf) \text{ by Exercise III.6.4} \\ &= C(acg_2h_2) \\ &\approx acC(g_2h_2) \text{ by Exercise III.6.4} \\ &\approx ac \text{ since } C(g_2g_2) \text{ is a unit.} \end{aligned}$$

Therefore $ac = bdv$ for some unit $v \in D$ and so $bdf = acg_2h_2 = bdvg_2h_2$ or $f = vg_2h_2$ where v is a unit in $D[x]$. So f and g_2h_2 are associates in $D[x]$. But by Theorem III.3.4(v), every associate of an irreducible is irreducible (here, in integral domain $D[x]$) so vg_2h_2 is irreducible in $D[x]$, a CONTRADICTION (since neither g_2 nor h_2 is a unit in $D \subset F$ since...

Lemma III.6.13 (continued 2)

Lemma III.6.13. Let D be a unique factorization domain with quotient field F and f a primitive polynomial of positive degree in $D[x]$. Then f is irreducible in $D[x]$ if and only if f is irreducible in $F[x]$.

Proof (continued). ...the only units in F [and hence in D] are the nonzero constant polynomials by Corollary III.6.4). So the assumption that f is not irreducible in $F[x]$ is false and we have shown that f is irreducible in $D[x]$ implies that f is irreducible in $F[x]$ and $f = gh$ for some $g, h \in D[x]$.

Lemma III.6.13 (continued 2)

Lemma III.6.13. Let D be a unique factorization domain with quotient field F and f a primitive polynomial of positive degree in $D[x]$. Then f is irreducible in $D[x]$ if and only if f is irreducible in $F[x]$.

Proof (continued). ...the only units in F [and hence in D] are the nonzero constant polynomials by Corollary III.6.4). So the assumption that f is not irreducible in $F[x]$ is false and we have shown that f is irreducible in $D[x]$ implies that f is irreducible in $F[x]$ and $f = gh$ for some $g, h \in D[x]$. Then by Corollary III.6.4, one of g, h (say g) is a constant polynomial. Thus $C(f) = C(gh) \approx gC(h)$ by Exercise III.6.4. Since f is hypothesized to be primitive then $C(f)$ is a unit in D and has an inverse $C(f)^{-1}$ in D.

Lemma III.6.13 (continued 2)

Lemma III.6.13. Let D be a unique factorization domain with quotient field F and f a primitive polynomial of positive degree in $D[x]$. Then f is irreducible in $D[x]$ if and only if f is irreducible in $F[x]$.

Proof (continued). . . . the only units in F [and hence in D] are the nonzero constant polynomials by Corollary III.6.4). So the assumption that f is not irreducible in $F[x]$ is false and we have shown that f is irreducible in $D[x]$ implies that f is irreducible in $F[x]$ and $f = gh$ for some $g, h \in D[x]$. Then by Corollary III.6.4, one of g, h (say g) is a constant polynomial. Thus $C(f) = C(gh) \approx gC(h)$ by Exercise III.6.4. Since f is hypothesized to be primitive then $C(f)$ is a unit in D and has an inverse $C(f)^{-1}$ in D. Since $C(f) \approx gC(h)$ then $C(f) = gC(h)u$ for some unit $u \in D$. But then $1_D = gC(h)uC(f)^{-1}$ and so g is a unit in D and hence in $D[x]$. So $f = gh$ in $D[x]$ implies that g (or h) is a unit in $D[x]$ and so f is irreducible in $D[x]$. □

Lemma III.6.13 (continued 2)

Lemma III.6.13. Let D be a unique factorization domain with quotient field F and f a primitive polynomial of positive degree in $D[x]$. Then f is irreducible in $D[x]$ if and only if f is irreducible in $F[x]$.

Proof (continued). . . . the only units in F [and hence in D] are the nonzero constant polynomials by Corollary III.6.4). So the assumption that f is not irreducible in $F[x]$ is false and we have shown that f is irreducible in $D[x]$ implies that f is irreducible in $F[x]$ and $f = gh$ for some $g, h \in D[x]$. Then by Corollary III.6.4, one of g, h (say g) is a constant polynomial. Thus $C(f) = C(gh) \approx gC(h)$ by Exercise III.6.4. Since f is hypothesized to be primitive then $C(f)$ is a unit in D and has an inverse $C(f)^{-1}$ in D. Since $C(f) \approx gC(h)$ then $C(f) = gC(h)u$ for some unit $u \in D$. But then $1_D = gC(h)uC(f)^{-1}$ and so g is a unit in D and hence in $D[x]$. So $f = gh$ in $D[x]$ implies that g (or h) is a unit in $D[x]$ and so f is irreducible in $D[x]$. □

Theorem III.6.14

Theorem III.6.14. If D is a unique factorization domain, then so is the polynomial ring $D[x_1, x_2, \ldots, x_n]$.

Proof. We shall prove that $D[x]$ is a unique factorization domain. Since $D[x_1, x_2, \ldots, x_n] = D[x_1, x_2, \ldots, x_{n-1}][x_n]$ by Corollary III.5.7, a routine inductive argument completes the proof. Now we show that $D[x]$ satisfies both parts of the definition of a unique factorization domain (Definition III.3.5).

Theorem III.6.14

Theorem III.6.14. If D is a unique factorization domain, then so is the polynomial ring $D[x_1, x_2, \ldots, x_n]$.

Proof. We shall prove that $D[x]$ is a unique factorization domain. Since $D[x_1, x_2, \ldots, x_n] = D[x_1, x_2, \ldots, x_{n-1}][x_n]$ by Corollary III.5.7, a routine inductive argument completes the proof. Now we show that $D[x]$ satisfies both parts of the definition of a unique factorization domain (Definition III.3.5).

(i) Factorization. If $f \in D[x]$ has positive degree, then $f = C(f)f_1$ with f_1 a primitive polynomial in $D[x]$ of positive degree. Since D is a unique factorization domain then either $C(f)$ is a unit or $C(f) = c_1c_2 \cdots c_m$ with each c_i irreducible in D and hence in $D[x]$ (by part (i) of the definition of unique factorization domain).

Theorem III.6.14

Theorem III.6.14. If D is a unique factorization domain, then so is the polynomial ring $D[x_1, x_2, \ldots, x_n]$.

Proof. We shall prove that $D[x]$ is a unique factorization domain. Since $D[x_1, x_2, \ldots, x_n] = D[x_1, x_2, \ldots, x_{n-1}][x_n]$ by Corollary III.5.7, a routine inductive argument completes the proof. Now we show that $D[x]$ satisfies both parts of the definition of a unique factorization domain (Definition III.3.5).

(i) Factorization. If $f \in D[x]$ has positive degree, then $f = C(f)f_1$ with f_1 a primitive polynomial in $D[x]$ of positive degree. Since D is a unique factorization domain then either $C(f)$ is a unit or $C(f) = c_1c_2 \cdots c_m$ with each c_i irreducible in D and hence in $D[x]$ (by part (i) of the definition of unique factorization domain). Let F be the field of quotients of D. Since $F[x]$ is a unique factorization domain by Corollary III.6.4 which contains $D[x]$, then $f_1 = p_1^* p_2^* \cdots p_n^*$ with each p_i^* an irreducible polynomial in $F[x]$ (by part (i) of the definition of unique factorization domain).

Theorem III.6.14

Theorem III.6.14. If D is a unique factorization domain, then so is the polynomial ring $D[x_1, x_2, \ldots, x_n]$.

Proof. We shall prove that $D[x]$ is a unique factorization domain. Since $D[x_1, x_2, \ldots, x_n] = D[x_1, x_2, \ldots, x_{n-1}][x_n]$ by Corollary III.5.7, a routine inductive argument completes the proof. Now we show that $D[x]$ satisfies both parts of the definition of a unique factorization domain (Definition III.3.5).

(i) Factorization. If $f \in D[x]$ has positive degree, then $f = C(f)f_1$ with f_1 a primitive polynomial in $D[x]$ of positive degree. Since D is a unique factorization domain then either $C(f)$ is a unit or $C(f) = c_1 c_2 \cdots c_m$ with each c_i irreducible in D and hence in $D[x]$ (by part (i) of the definition of unique factorization domain). Let F be the field of quotients of D. Since $F[x]$ is a unique factorization domain by Corollary III.6.4 which contains $D[x]$, then $f_1 = p_1^* p_2^* \cdots p_n^*$ with each p_i^* an irreducible polynomial in $F[x]$ (by part (i) of the definition of unique factorization domain).

Theorem III.6.14 (continued 1)

Proof (continued). As shown in the proof of Lemma III.6.13 (take it from the "Similarly $h = (c/d)h_2 \ldots$" part), for each i we have $p_i^* = (a_i/b_i)p_i$ with $a_i, b_i \in D$, $b_i \neq 0$, $a_i/b_i \in F$, $p_i \in D[x]$ and p_i primitive. Since each p_i^* is irreducible in $F[x]$ then each $p_i = (b_i/a_i)p_i^*$ is irreducible in $F[x]$ (from the definition of irreducible). Whence by Lemma III.6.13 each p_i is irreducible in $D[x]$. If we define $a = a_1 a_2 \cdots a_n$ and $b = b_1 b_2 \cdots b_n$ then $f_1 = p_1^* p_2^* \cdots p_n^* = (a/b)p_1 p_2 \cdots p_n$. Consequently, $bf_1 = ap_1 p_2 \cdots p_n$.

Theorem III.6.14 (continued 1)

Proof (continued). As shown in the proof of Lemma III.6.13 (take it from the "Similarly $h = (c/d)h_2 \ldots$" part), for each i we have $p_i^* = (a_i/b_i)p_i$ with $a_i, b_i \in D$, $b_i \neq 0$, $a_i/b_i \in F$, $p_i \in D[x]$ and p_i primitive. Since each p_i^* is irreducible in $F[x]$ then each $p_i = (b_i/a_i)p_i^*$ is irreducible in $F[x]$ (from the definition of irreducible). Whence by Lemma III.6.13 each p_i is irreducible in $D[x]$. If we define $a = a_1 a_2 \cdots a_n$ and $b = b_1 b_2 \cdots b_n$ then $f_1 = p_1^* p_2^* \cdots p_n^* = (a/b)p_1 p_2 \cdots p_n$. Consequently, $bf_1 = ap_1 p_2 \cdots p_n$. Since f_1 is primitive by the choice of it above and $p_1 p_2 \cdots p_n$ is primitive by Lemma III.6.11, it follows as in the proof of Lemma III.6.12 that a and b are associates in D $(b \approx bC(f_1) \approx C(bf_1) = C(ap_1 p_2 \cdots p_n) \approx aC(p_1 p_2 \cdots p_n) \approx a)$. Thus $a = bu$ or $a/b = u$ with u a unit in D by Theorem III.3.2(iv).

Theorem III.6.14 (continued 1)

Proof (continued). As shown in the proof of Lemma III.6.13 (take it from the "Similarly $h = (c/d)h_2 \ldots$" part), for each i we have $p_i^* = (a_i/b_i)p_i$ with $a_i, b_i \in D$, $b_i \neq 0$, $a_i/b_i \in F$, $p_i \in D[x]$ and p_i primitive. Since each p_i^* is irreducible in $F[x]$ then each $p_i = (b_i/a_i)p_i^*$ is irreducible in $F[x]$ (from the definition of irreducible). Whence by Lemma III.6.13 each p_i is irreducible in $D[x]$. If we define $a = a_1 a_2 \cdots a_n$ and $b = b_1 b_2 \cdots b_n$ then $f_1 = p_1^* p_2^* \cdots p_n^* = (a/b)p_1 p_2 \cdots p_n$. Consequently, $bf_1 = ap_1 p_2 \cdots p_n$. Since f_1 is primitive by the choice of it above and $p_1 p_2 \cdots p_n$ is primitive by Lemma III.6.11, it follows as in the proof of Lemma III.6.12 that a and b are associates in D $(b \approx bC(f_1) \approx C(bf_1) = C(ap_1 p_2 \cdots p_n) \approx aC(p_1 p_2 \cdots p_n) \approx a)$. Thus $a = bu$ or $a/b = u$ with u a unit in D by Theorem III.3.2(iv). Therefore, if $C(f)$ is a nonunit, say $C(f) = c_1 c_2 \cdots c_m$ where each c_i is irreducible in D (since D is a unique factorization domain).

Theorem III.6.14 (continued 1)

Proof (continued). As shown in the proof of Lemma III.6.13 (take it from the "Similarly $h = (c/d)h_2\ldots$" part), for each i we have $p_i^* = (a_i/b_i)p_i$ with $a_i, b_i \in D$, $b_i \neq 0$, $a_i/b_i \in F$, $p_i \in D[x]$ and p_i primitive. Since each p_i^* is irreducible in $F[x]$ then each $p_i = (b_i/a_i)p_i^*$ is irreducible in $F[x]$ (from the definition of irreducible). Whence by Lemma III.6.13 each p_i is irreducible in $D[x]$. If we define $a = a_1a_2\cdots a_n$ and $b = b_1b_2\cdots b_n$ then $f_1 = p_1^*p_2^*\cdots p_n^* = (a/b)p_1p_2\cdots p_n$. Consequently, $bf_1 = ap_1p_2\cdots p_n$. Since f_1 is primitive by the choice of it above and $p_1p_2\cdots p_n$ is primitive by Lemma III.6.11, it follows as in the proof of Lemma III.6.12 that a and b are associates in D $(b \approx bC(f_1) \approx C(bf_1) = C(ap_1p_2\cdots p_n) \approx aC(p_1p_2\cdots p_n) \approx a)$. Thus $a = bu$ or $a/b = u$ with u a unit in D by Theorem III.3.2(iv). Therefore, if $C(f)$ is a nonunit, say $C(f) = c_1c_2\cdots c_m$ where each c_i is irreducible in D (since D is a unique factorization domain).

Theorem III.6.14 (continued 2)

Proof (continued). Then $f = C(f)f_1 = c_1c_2 \cdots c_m(up_1)p_2 \cdots p_n$ (with $n = a/b$) where each c_i and p_i are irreducible in $D[x]$ as described above (and underlined) and up_1 is irreducible in $D[x]$ since p_1 is irreducible and u is a unit. So f is a product of irreducibles.

Theorem III.6.14 (continued 2)

Proof (continued). Then $f = C(f)f_1 = c_1 c_2 \cdots c_m (up_1) p_2 \cdots p_n$ (with $n = a/b$) where each c_i and p_i are irreducible in $D[x]$ as described above (and underlined) and up_1 is irreducible in $D[x]$ since p_1 is irreducible and u is a unit. So f is a product of irreducibles. Similarly, if $C(f)$ is a unit then $f = C(f)f_1 = C(f)(up_1)p_2 \cdots p_n$ where $p_2, p_3, \ldots, p_n$ are irreducible in $D[x]$ as described above (and underlined) and $C(f)up_1$ is irreducible in $D[x]$ since p_1 is irreducible and $C(f)u$ is a unit. So f is a product of irreducibles.

Theorem III.6.14 (continued 2)

Proof (continued). Then $f = C(f)f_1 = c_1c_2 \cdots c_m(up_1)p_2 \cdots p_n$ (with $n = a/b$) where each c_i and p_i are irreducible in $D[x]$ as described above (and underlined) and up_1 is irreducible in $D[x]$ since p_1 is irreducible and u is a unit. So f is a product of irreducibles. Similarly, if $C(f)$ is a unit then $f = C(f)f_1 = C(f)(up_1)p_2 \cdots p_n$ where $p_2, p_3, \ldots, p_n$ are irreducible in $D[x]$ as described above (and underlined) and $C(f)up_1$ is irreducible in $D[x]$ since p_1 is irreducible and $C(f)u$ is a unit. So f is a product of irreducibles.

(ii) Uniqueness. Let $f \in D[x]$ have positive degree.

Theorem III.6.14 (continued 2)

Proof (continued). Then $f = C(f)f_1 = c_1c_2\cdots c_m(up_1)p_2\cdots p_n$ (with $n = a/b$) where each c_i and p_i are irreducible in $D[x]$ as described above (and underlined) and up_1 is irreducible in $D[x]$ since p_1 is irreducible and u is a unit. So f is a product of irreducibles. Similarly, if $C(f)$ is a unit then $f = C(f)f_1 = C(f)(up_1)p_2\cdots p_n$ where $p_2, p_3, \ldots, p_n$ are irreducible in $D[x]$ as described above (and underlined) and $C(f)up_1$ is irreducible in $D[x]$ since p_1 is irreducible and $C(f)u$ is a unit. So f is a product of irreducibles.

(ii) Uniqueness. Let $f \in D[x]$ have positive degree. Then, as argued in part (i), $f = c_1c_2\cdots c_mp_1p_2\cdots p_n$ with each c_i irreducible in D, $C(f) = c_1c_2\cdots c_m$, and each p_i is irreducible in $D[x]$ (this is established in (i) for both $C(f)$ a nonunit and $C(f)$ a unit [in which case $m = 0$]—when $C(f)$ is a nonunit we replace up_1 of (i) with $p_1 = up_1$ since up_1 is irreducible as well where u is a unit; when $C(f)$ is a unit we replace $C(f)up_1$ with $p_1 = C(f)up_1$ since $C(f)up_1$ is irreducible as well where $C(f)u$ is a unit).

Theorem III.6.14 (continued 2)

Proof (continued). Then $f = C(f)f_1 = c_1c_2\cdots c_m(up_1)p_2\cdots p_n$ (with $n = a/b$) where each c_i and p_i are irreducible in $D[x]$ as described above (and underlined) and up_1 is irreducible in $D[x]$ since p_1 is irreducible and u is a unit. So f is a product of irreducibles. Similarly, if $C(f)$ is a unit then $f = C(f)f_1 = C(f)(up_1)p_2\cdots p_n$ where $p_2, p_3, \ldots, p_n$ are irreducible in $D[x]$ as described above (and underlined) and $C(f)up_1$ is irreducible in $D[x]$ since p_1 is irreducible and $C(f)u$ is a unit. So f is a product of irreducibles.

(ii) Uniqueness. Let $f \in D[x]$ have positive degree. Then, as argued in part (i), $f = c_1c_2\cdots c_mp_1p_2\cdots p_n$ with each c_i irreducible in D, $C(f) = c_1c_2\cdots c_m$, and each p_i is irreducible in $D[x]$ (this is established in (i) for both $C(f)$ a nonunit and $C(f)$ a unit [in which case $m = 0$]—when $C(f)$ is a nonunit we replace up_1 of (i) with $p_1 = up_1$ since up_1 is irreducible as well where u is a unit; when $C(f)$ is a unit we replace $C(f)up_1$ with $p_1 = C(f)up_1$ since $C(f)up_1$ is irreducible as well where $C(f)u$ is a unit).

Theorem III.6.14 (continued 3)

Proof (continued). Suppose $f = c_1 c_2 \cdots c_m p_1 p_2 \cdots p_n$ with each c_i irreducible in D, $C(f) = c_1 c_2 \cdots c_m$, and p_i irreducible in $D[x]$ and $f = d_1 d_2 \cdots d_r q_1 q_2 \cdots q_s$ with each d_i irreducible in D, $C(f) = d_1 d_2 \cdots d_r$ and each q_i is irreducible in $D[x]$. Since each p_i and q_i is irreducible then each p_i and q_i is primitive (or wlse we could factor out nonunit $C(p_i)$ or $C(q_i)$ from p_i or q_i respectively and p_i or q_i would not be irreducible). Since $C(f) = c_1 c_2 \cdots c_m$ and $C(f) = d_1 d_2 \cdots d_r$ then $c_1 c_2 \cdots c_m$ and $d_1 d_2 \cdots d_r$ are associates in $D[x]$ and hence in $F[x]$.

Theorem III.6.14 (continued 3)

Proof (continued). Suppose $f = c_1 c_2 \cdots c_m p_1 p_2 \cdots p_n$ with each c_i irreducible in D, $C(f) = c_1 c_2 \cdots c_m$, and p_i irreducible in $D[x]$ and $f = d_1 d_2 \cdots d_r q_1 q_2 \cdots q_s$ with each d_i irreducible in D, $C(f) = d_1 d_2 \cdots d_r$ and each q_i is irreducible in $D[x]$. Since each p_i and q_i is irreducible then each p_i and q_i is primitive (or wlse we could factor out nonunit $C(p_i)$ or $C(q_i)$ from p_i or q_i respectively and p_i or q_i would not be irreducible). Since $C(f) = c_1 c_2 \cdots c_m$ and $C(f) = d_1 d_2 \cdots d_r$ then $c_1 c_2 \cdots c_m$ and $d_1 d_2 \cdots d_r$ are associates in $D[x]$ and hence in $F[x]$. Since each p_i and q_i is irreducible in $D[x]$, then by Lemma III.6.13, each p_i and q_i is irreducible in $F[x]$. Now by Corollary.6.4, since F is a field (of quotients of D) then $F[x]$ is a unique factorization domain and so $n = s$ and (after reindexing; "permuting" as the definition of unique factorization domain says) each p_i is an associate of q_i in $F[x]$. By Lemma III.6.12 each p_i is an associate of q_i in $D[x]$.

Theorem III.6.14 (continued 3)

Proof (continued). Suppose $f = c_1 c_2 \cdots c_m p_1 p_2 \cdots p_n$ with each c_i irreducible in D, $C(f) = c_1 c_2 \cdots c_m$, and p_i irreducible in $D[x]$ and $f = d_1 d_2 \cdots d_r q_1 q_2 \cdots q_s$ with each d_i irreducible in D, $C(f) = d_1 d_2 \cdots d_r$ and each q_i is irreducible in $D[x]$. Since each p_i and q_i is irreducible then each p_i and q_i is primitive (or wlse we could factor out nonunit $C(p_i)$ or $C(q_i)$ from p_i or q_i respectively and p_i or q_i would not be irreducible). Since $C(f) = c_1 c_2 \cdots c_m$ and $C(f) = d_1 d_2 \cdots d_r$ then $c_1 c_2 \cdots c_m$ and $d_1 d_2 \cdots d_r$ are associates in $D[x]$ and hence in $F[x]$. Since each p_i and q_i is irreducible in $D[x]$, then by Lemma III.6.13, each p_i and q_i is irreducible in $F[x]$. Now by Corollary.6.4, since F is a field (of quotients of D) then $F[x]$ is a unique factorization domain and so $n = s$ and (after reindexing; "permuting" as the definition of unique factorization domain says) each p_i is an associate of q_i in $F[x]$. By Lemma III.6.12 each p_i is an associate of q_i in $D[x]$. Hence, part (ii) of the definition of unique factorization domain is satisfied in $D[x]$ and so $D[x]$ is a unique factorization domain. □

Theorem III.6.14 (continued 3)

Proof (continued). Suppose $f = c_1 c_2 \cdots c_m p_1 p_2 \cdots p_n$ with each c_i irreducible in D, $C(f) = c_1 c_2 \cdots c_m$, and p_i irreducible in $D[x]$ and $f = d_1 d_2 \cdots d_r q_1 q_2 \cdots q_s$ with each d_i irreducible in D, $C(f) = d_1 d_2 \cdots d_r$ and each q_i is irreducible in $D[x]$. Since each p_i and q_i is irreducible then each p_i and q_i is primitive (or wlse we could factor out nonunit $C(p_i)$ or $C(q_i)$ from p_i or q_i respectively and p_i or q_i would not be irreducible). Since $C(f) = c_1 c_2 \cdots c_m$ and $C(f) = d_1 d_2 \cdots d_r$ then $c_1 c_2 \cdots c_m$ and $d_1 d_2 \cdots d_r$ are associates in $D[x]$ and hence in $F[x]$. Since each p_i and q_i is irreducible in $D[x]$, then by Lemma III.6.13, each p_i and q_i is irreducible in $F[x]$. Now by Corollary.6.4, since F is a field (of quotients of D) then $F[x]$ is a unique factorization domain and so $n = s$ and (after reindexing; "permuting" as the definition of unique factorization domain says) each p_i is an associate of q_i in $F[x]$. By Lemma III.6.12 each p_i is an associate of q_i in $D[x]$. Hence, part (ii) of the definition of unique factorization domain is satisfied in $D[x]$ and so $D[x]$ is a unique factorization domain. □

Theorem III.6.15

Theorem III.6.15. (Eisenstein's Criterion) Let D be a unique factorization domain with quotient field F. If $f = \sum_{i=0}^{n} a_i x^i \in D[x]$, $\deg(f) \geq 1$ and p is an irreducible element of D such that

$$p \nmid a_n; \;\; p | a_i \text{ for } i = 0, 1, \ldots, n-1; \;\; p^2 \nmid a_0,$$

then f is irreducible in $F[x]$. If f is primitive, then f is irreducible in $D[x]$.

Proof. Let $f = C(f)f_1$ where f_1 is primitive in $D[x]$ and $C(f) \in D$ (in particular, $f_1 = f$ if f is primitive). Since $C(f)$ is a unit in F (F is a field; Corollary III.6.4 technically), it suffices to show that f_1 is irreducible in $F[x]$.

Theorem III.6.15

Theorem III.6.15. (Eisenstein's Criterion) Let D be a unique factorization domain with quotient field F. If $f = \sum_{i=0}^{n} a_i x^i \in D[x]$, $\deg(f) \geq 1$ and p is an irreducible element of D such that

$$p \nmid a_n; \;\; p|a_i \text{ for } i = 0, 1, \ldots, n-1; \;\; p^2 \nmid a_0,$$

then f is irreducible in $F[x]$. If f is primitive, then f is irreducible in $D[x]$.

Proof. Let $f = C(f)f_1$ where f_1 is primitive in $D[x]$ and $C(f) \in D$ (in particular, $f_1 = f$ if f is primitive). Since $C(f)$ is a unit in F (F is a field; Corollary III.6.4 technically), it suffices to show that f_1 is irreducible in $F[x]$. By Lemma III.6.13, f_1 is irreducible in $F[x]$ if and only if it is irreducible in $D[x]$ so it suffices to prove that F_1 is irreducible in $D[x]$.

Theorem III.6.15

Theorem III.6.15. (Eisenstein's Criterion) Let D be a unique factorization domain with quotient field F. If $f = \sum_{i=0}^{n} a_i x^i \in D[x]$, $\deg(f) \geq 1$ and p is an irreducible element of D such that

$$p \nmid a_n; \;\; p | a_i \text{ for } i = 0, 1, \ldots, n-1; \;\; p^2 \nmid a_0,$$

then f is irreducible in $F[x]$. If f is primitive, then f is irreducible in $D[x]$.

Proof. Let $f = C(f)f_1$ where f_1 is primitive in $D[x]$ and $C(f) \in D$ (in particular, $f_1 = f$ if f is primitive). Since $C(f)$ is a unit in F (F is a field; Corollary III.6.4 technically), it suffices to show that f_1 is irreducible in $F[x]$. By Lemma III.6.13, f_1 is irreducible in $F[x]$ if and only if it is irreducible in $D[x]$ so it suffices to prove that F_1 is irreducible in $D[x]$. ASSUME that f_1 is not irreducible in $D[x]$ and that $f_1 = gh$ with $g = b_r x^r + \cdots + b_1 x + b_0 \in D[x]$, $\deg(g) = r \geq 1$, and $h = c_2 x^2 + \cdots + c_1 c + c_0 \in D[x]$, $\deg(h) = s \geq 1$.

Theorem III.6.15

Theorem III.6.15. (Eisenstein's Criterion) Let D be a unique factorization domain with quotient field F. If $f = \sum_{i=0}^{n} a_i x^i \in D[x]$, $\deg(f) \geq 1$ and p is an irreducible element of D such that

$$p \nmid a_n; \;\; p | a_i \text{ for } i = 0, 1, \ldots, n-1; \;\; p^2 \nmid a_0,$$

then f is irreducible in $F[x]$. If f is primitive, then f is irreducible in $D[x]$.

Proof. Let $f = C(f) f_1$ where f_1 is primitive in $D[x]$ and $C(f) \in D$ (in particular, $f_1 = f$ if f is primitive). Since $C(f)$ is a unit in F (F is a field; Corollary III.6.4 technically), it suffices to show that f_1 is irreducible in $F[x]$. By Lemma III.6.13, f_1 is irreducible in $F[x]$ if and only if it is irreducible in $D[x]$ so it suffices to prove that F_1 is irreducible in $D[x]$. ASSUME that f_1 is not irreducible in $D[x]$ and that $f_1 = gh$ with $g = b_r x^r + \cdots + b_1 x + b_0 \in D[x]$, $\deg(g) = r \geq 1$, and $h = c_2 x^2 + \cdots + c_1 c + c_0 \in D[x]$, $\deg(h) = s \geq 1$.

Theorem III.6.15 (continued 1)

Proof (continued). Now p does not divide $C(f)$ (the greatest common divisor of the coefficients of f) since $p \nmid a_n$ (and p is irreducible), whence the coefficients of $f_1 = \sum_{i=0}^{n} a_i^* x^i$ satisfy the same divisibility conditions with respect to p as do the coefficients of f. Since p divides $a_0^* = b_0 c_0$ and every irreducible in D is prime (by part (ii) of the definition of unique factorization domain, Definition III.3.5; see the "Remark" on page 137) then either $p \mid b_0$ or $p \mid c_0$. Say $p \mid b_0$. Since $p^2 \nmid a_0^*$ then $p \nmid c_0$.

Theorem III.6.15 (continued 1)

Proof (continued). Now p does not divide $C(f)$ (the greatest common divisor of the coefficients of f) since $p \nmid a_n$ (and p is irreducible), whence the coefficients of $f_1 = \sum_{i=0}^{n} a_i^* x^i$ satisfy the same divisibility conditions with respect to p as do the coefficients of f. Since p divides $a_0^* = b_0 c_0$ and every irreducible in D is prime (by part (ii) of the definition of unique factorization domain, Definition III.3.5; see the "Remark" on page 137) then either $p \mid b_0$ or $p \mid c_0$. Say $p \mid b_0$. Since $p^2 \nmid a_0^*$ then $p \nmid c_0$.

Now some coefficient b_k of g is not divisible by p (otherwise p would divide every coefficient of g and hence every coefficient of $f_1 = gh$ which is a contradiction to the fact that f_1 is primitive and so $C(f_1)$ is a unit, not a multiple of an irreducible).

Theorem III.6.15 (continued 1)

Proof (continued). Now p does not divide $C(f)$ (the greatest common divisor of the coefficients of f) since $p \nmid a_n$ (and p is irreducible), whence the coefficients of $f_1 = \sum_{i=0}^{n} a_i^* x^i$ satisfy the same divisibility conditions with respect to p as do the coefficients of f. Since p divides $a_0^* = b_0 c_0$ and every irreducible in D is prime (by part (ii) of the definition of unique factorization domain, Definition III.3.5; see the "Remark" on page 137) then either $p \mid b_0$ or $p \mid c_0$. Say $p \mid b_0$. Since $p^2 \nmid a_0^*$ then $p \nmid c_0$.

Now some coefficient b_k of g is not divisible by p (otherwise p would divide every coefficient of g and hence every coefficient of $f_1 = gh$ which is a contradiction to the fact that f_1 is primitive and so $C(f_1)$ is a unit, not a multiple of an irreducible). Let k be the least positive integer such that $p \mid b_i$ for $i < k$ and $p \nmid b_k$. Then $1 \leq k \leq r < n$ (since $p \mid b_0$ as described above, since $\deg(f_1) = \deg(g) + \deg(h)$, by Theorem III.6.1(iv), and since $\deg(h) \geq 1$ by the choice of h, then $\deg(g) \leq n - 1$ and so $r \leq n - 1$).

Theorem III.6.15 (continued 1)

Proof (continued). Now p does not divide $C(f)$ (the greatest common divisor of the coefficients of f) since $p \nmid a_n$ (and p is irreducible), whence the coefficients of $f_1 = \sum_{i=0}^{n} a_i^* x^i$ satisfy the same divisibility conditions with respect to p as do the coefficients of f. Since p divides $a_0^* = b_0 c_0$ and every irreducible in D is prime (by part (ii) of the definition of unique factorization domain, Definition III.3.5; see the "Remark" on page 137) then either $p \mid b_0$ or $p \mid c_0$. Say $p \mid b_0$. Since $p^2 \nmid a_0^*$ then $p \nmid c_0$.

Now some coefficient b_k of g is not divisible by p (otherwise p would divide every coefficient of g and hence every coefficient of $f_1 = gh$ which is a contradiction to the fact that f_1 is primitive and so $C(f_1)$ is a unit, not a multiple of an irreducible). Let k be the least positive integer such that $p \mid b_i$ for $i < k$ and $p \nmid b_k$. Then $1 \leq k \leq r < n$ (since $p \mid b_0$ as described above, since $\deg(f_1) = \deg(g) + \deg(h)$, by Theorem III.6.1(iv), and since $\deg(h) \geq 1$ by the choice of h, then $\deg(g) \leq n-1$ and so $r \leq n-1$).

Theorem III.6.15 (continued 2)

Theorem III.6.15. (Eisenstein's Criterion) Let D be a unique factorization domain with quotient field F. If $f = \sum_{i=0}^{n} a_i x^i \in D[x]$, $\deg(f) \geq 1$ and p is an irreducible element of D such that

$$p \nmid a_n; \;\; p|a_i \text{ for } i = 0, 1, \ldots, n-1; \;\; p^2 \nmid a_0,$$

then f is irreducible in $F[x]$. If f is primitive, then f is irreducible in $D[x]$.

Proof (continued). Since $a_k^* = b_0 c_k + b_1 c_{k-1} + \cdots + b_{k-1} c_1 + b_k c_0$ and $p \mid a_k^*$ (since $p \mid a_k$ because $k \leq n-1$). Since $p \mid b_i$ for $i < k$ then p must divide $b_k c_0$. As above, p is prime so this implies that $p \mid b_k$ or $p \mid c_0$, both a CONTRADICTION. So the assumption that f_1 is not irreducible is false and hence f_1 is irreducible in $D[x]$. Whence f is irreducible in $D[x]$ and so is irreducible in $F[x]$.

Theorem III.6.15 (continued 2)

Theorem III.6.15. (Eisenstein's Criterion) Let D be a unique factorization domain with quotient field F. If $f = \sum_{i=0}^{n} a_i x^i \in D[x]$, $\deg(f) \geq 1$ and p is an irreducible element of D such that

$$p \nmid a_n; \;\; p | a_i \text{ for } i = 0, 1, \ldots, n-1; \;\; p^2 \nmid a_0,$$

then f is irreducible in $F[x]$. If f is primitive, then f is irreducible in $D[x]$.

Proof (continued). Since $a_k^* = b_0 c_k + b_1 c_{k-1} + \cdots + b_{k-1} c_1 + b_k c_0$ and $p \mid a_k^*$ (since $p \mid a_k$ because $k \leq n-1$). Since $p \mid b_i$ for $i < k$ then p must divide $b_k c_0$. As above, p is prime so this implies that $p \mid b_k$ or $p \mid c_0$, both a CONTRADICTION. So the assumption that f_1 is not irreducible is false and hence f_1 is irreducible in $D[x]$. Whence f is irreducible in $D[x]$ and so is irreducible in $F[x]$. Also, if f is primitive, then say $f = f_1$ and we have seen that f_1 is irreducible in $D[x]$. □

Theorem III.6.15 (continued 2)

Theorem III.6.15. (Eisenstein's Criterion) Let D be a unique factorization domain with quotient field F. If $f = \sum_{i=0}^{n} a_i x^i \in D[x]$, $\deg(f) \geq 1$ and p is an irreducible element of D such that

$$p \nmid a_n; \;\; p | a_i \text{ for } i = 0, 1, \ldots, n-1; \;\; p^2 \nmid a_0,$$

then f is irreducible in $F[x]$. If f is primitive, then f is irreducible in $D[x]$.

Proof (continued). Since $a_k^* = b_0 c_k + b_1 c_{k-1} + \cdots + b_{k-1} c_1 + b_k c_0$ and $p \mid a_k^*$ (since $p \mid a_k$ because $k \leq n-1$). Since $p \mid b_i$ for $i < k$ then p must divide $b_k c_0$. As above, p is prime so this implies that $p \mid b_k$ or $p \mid c_0$, both a CONTRADICTION. So the assumption that f_1 is not irreducible is false and hence f_1 is irreducible in $D[x]$. Whence f is irreducible in $D[x]$ and so is irreducible in $F[x]$. Also, if f is primitive, then say $f = f_1$ and we have seen that f_1 is irreducible in $D[x]$. □