

Chapter 12. Polynomial Rings

12.1 Note: Here are a few remarks about polynomials. Recall that $R[x]$ denotes the ring of polynomials with coefficients in the ring R , and R^R denotes the ring of all functions $f : R \rightarrow R$.

(1) A polynomial $f \in R[x]$ determines a function $f \in R^R$. Given $f(x) = \sum_{i=0}^n a_i x^i \in R[x]$ we obtain the function $f : R \rightarrow R$ given by $f(x) = \sum_{i=0}^n a_i x^i$.

(2) Although we do not usually distinguish notationally between the polynomial $f \in R[x]$ and its corresponding function $f \in R^R$, they are not always identical. If the ring R is not commutative then multiplication of polynomials does not agree with multiplication of functions. For $f, g \in R[x]$ given by $f(x) = a + bx$ and $g(x) = c + dx$, in the ring $R[x]$ we have $(fg)(x) = (a + bx)(c + dx) = (ac) + (ad + bc)x + (bd)x^2$, but in the ring R^R we have $(fg)(x) = (a + bx)(c + dx) = ac + adx + bxc + bxdx$.

(3) Equality of polynomials may not agree with equality of functions. For $f, g \in R[x]$ given by $f(x) = \sum_{i=0}^n a_i x^i$ and $g(x) = \sum_{i=0}^m b_i x^i$ we have $f = g \in R[x]$ if and only if $a_i = b_i$ for all i (and if say $n < m$ then $b_i = a_i = 0$ for $i > n$), but $f = g \in R^R$ if and only if $f(x) = g(x)$ for all $x \in R$. These two notions of equality do not always agree. For example if R is finite then the ring $R[x]$ is infinite but the ring R^R is finite. Indeed if $|R| = n$ then $R[x]$ is countably infinite but $|R^R| = n^n$. For a more specific example, if $f(x) = x^p - x$ then we have $f \neq 0 \in \mathbb{Z}_p[x]$ (because its coefficients are not equal to zero) but $f = 0 \in \mathbb{Z}_p^{\mathbb{Z}_p}$ because, by Fermat's Little Theorem, we have $f(x) = 0$ for all $x \in \mathbb{Z}_p$.

(4) Recall that for $f(x) = \sum_{i=0}^n a_i x^i$ with each $a_i \in R$ and $a_n \neq 0$, the element $a_n \in R$ is called the leading coefficient of f , and the non-negative integer n is called the degree of $f(x)$, and we write $\deg(f) = n$. For convenience, we also define $\deg(0) = -1$. When R is an integral domain, it is easy to see that for $0 \neq f, g \in R[x]$ we have $\deg(fg) = \deg(f) + \deg(g)$. When R is not an integral domain, however, we only have $\deg(fg) \leq \deg(f) + \deg(g)$ because the product of the two leading coefficients can be equal to zero.

(5) When R is an integral domain, because we have $\deg(fg) = \deg(f) + \deg(g)$ for all $0 \neq f, g \in R[x]$, it is easy to see that the units in $R[x]$ are the constant polynomials $f(x) = c$ where c is a unit in R . In particular, when F is a field, the units in $F[x]$ are the elements $f \in F[x]$ with $\deg(f) = 0$. In the ring $\mathbb{Z}_4[x]$ (which is not an integral domain) we have $(1 + 2x)^2 = 1 + 4x + 4x^2 = 1$, so $f(x) = (1 + 2x)$ is a unit in $\mathbb{Z}_4[x]$.

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

Proof: First we prove existence. If $\deg(f) < \deg(g)$ then we can take $q = 0$ and $r = f$. Suppose that $\deg(f) \geq \deg(g)$. Say $f(x) = \sum_{i=0}^n a_i x^i$ with $a_i \in R$ and $a_n \neq 0$ and $g(x) = \sum_{i=0}^m b_i x^i$ with $b_i \in R$ and b_m is a unit. Note that the polynomial $a_n b_m^{-1} x^{n-m} g(x)$ has degree n and leading coefficient a_n . It follows that the polynomial $f(x) - a_n b_m^{-1} x^{n-m} g(x)$ has degree smaller than n (because the leading coefficients cancel). We can suppose, inductively, that there exist polynomials $p, r \in R[x]$ such that $f(x) - a_n b_m^{-1} x^{n-m} g(x) = p(x)g(x) + r(x)$ and $\deg(r) < \deg(g)$. Then we have $f = qg + r$ by taking $q(x) = a_n b_m^{-1} x^{n-m} + p(x)$.

Next we prove uniqueness. Suppose that $f = qg + r = pg + s$ where $q, p, r, s \in R[x]$ with $\deg(r) < \deg(g)$ and $\deg(s) < \deg(g)$. Then we have $(q - p)g = s - r$ and so $\deg((q - p)g) = \deg(s - r)$. Since the leading coefficient of g is a unit (hence not a zero divisor), it follows that $\deg((q - p)g) = \deg(q - p) + \deg(g)$. If we had $q - p \neq 0$ then we would have $\deg((q - p)g) \geq \deg(g)$ but $\deg(s - r) < \deg(g)$, giving a contradiction. Thus we must have $q - p = 0$. Since $q - p = 0$ we have $s - r = (q - p)g = 0$. Since $q - p = 0$ and $s - r = 0$ we have $q = p$ and $r = s$, proving uniqueness.

12.3 Corollary: (*The Remainder Theorem*) Let R be a ring, let $f \in R[x]$, and let $a \in R$. When we divide $f(x)$ by $(x - a)$ to obtain the quotient $q(x)$ and remainder $r(x)$, the remainder is the constant polynomial $r(x) = f(a)$.

Proof: Use the division algorithm to obtain $q, r \in R[x]$ such that $f = q(x)(x - a) + r(x)$ and $\deg(r) < \deg(x - a)$. Since $\deg(x - a) = 1$ we have $\deg(r) \in \{-1, 0\}$, and so r is a constant polynomial, say $r(x) = c$ with $c \in R$. Then we have $f(x) = q(x)(x - a) + c$. Put in $x = a$ to get $f(a) = q(a)(a - a) + c = q(a) \cdot 0 + c = c$.

12.4 Corollary: (*The Factor Theorem*) Let R be a commutative ring, let $f \in R[x]$ and let $a \in R$. Then $f(a) = 0$ if and only if $(x - a) \mid f(x)$.

Proof: Suppose that $f(a) = 0$. Choose $q, r \in R[x]$ such that $f(x) = q(x)(x - a) + r(x)$ and $\deg(r) < \deg(x - a)$. Then $r(x)$ is the constant polynomial $r(x) = f(a) = 0$ and so we have $f(x) = q(x)(x - a)$. Since $f(x) = (x - a)q(x)$ we have $(x - a) \mid f(x)$. Conversely, suppose that $(x - a) \mid f(x)$ and choose $p \in R[x]$ so that $f(x) = (x - a)p(x)$. Then $f(a) = (a - a)p(a) = 0 \cdot p(a) = 0$.

12.5 Definition: Let R be a commutative ring, let $f \in R[x]$, and let $a \in R$. We say that a is a **root** of f when $f(a) = 0$. When $f \neq 0$, we define the **multiplicity** of a as a root of f to be the largest $m = m(f, a) \in \mathbb{N}$ such that $(x - a)^m \mid f(x)$ (where we use the convention that $(x - a)^0 = 1$). Note that a is a root of f if and only if $m(f, a) \geq 1$.

12.6 Example: Let $f(x) = x^3 - 3x - 2 \in \mathbb{Q}[x]$. Since $f(x) = (x + 1)^2(x - 2) \in \mathbb{Q}[x]$, we have $m(f, 2) = 1$ and $m(f, -1) = 2$.

12.7 Example: Let p be an odd prime and let $f(x) = x^p - a \in \mathbb{Z}_p[x]$. Find $m(f, a)$.

12.8 Theorem: (*The Roots Theorem*) Let R be an integral domain, let $0 \neq f \in R[x]$ and let $n = \deg(f)$. Then

- (1) f has at most n distinct roots in R , and
(2) if a_1, a_2, \dots, a_ℓ are all of the distinct roots of f in R and $m_i = m(f, a_i)$ for $1 \leq i \leq \ell$, then $(x - a_1)^{m_1}(x - a_2)^{m_2} \cdots (x - a_\ell)^{m_\ell} \mid f(x)$ and so $\sum_{i=1}^{\ell} m(f, a_i) \leq n$.

Proof: We prove Part (1) and leave the proof of Part (2) as an exercise. If $\deg(f) = 0$, then $f(x) = c$ for some $0 \neq c \in R$, and so $f(x)$ has no roots. Let f be a polynomial with $\deg(f) = n \geq 1$ and suppose, inductively, that every polynomial $g \in R[x]$ with $\deg(g) = n - 1$ has at most $n - 1$ distinct roots. Suppose that a is a root of f in R . By the Factor Theorem, $(x - a) \mid f(x)$ so we can choose a polynomial $g \in R[x]$ so that $f(x) = (x - a)g(x)$. Note that $\deg(g) = n - 1$ so, by the induction hypothesis, g has at most $n - 1$ distinct roots. Let $b \in R$ be any root of f with $b \neq a$. Since $f(x) = (x - a)g(x)$ and $f(b) = 0$ we have $0 = f(b) = (b - a)g(b)$. Since $(b - a)g(b) = 0$ and $(b - a) \neq 0$ and R has no zero divisors, it follows that $g(b) = 0$. Thus b must be one of the roots of g . Since every root b of f with $b \neq a$ is equal to one of the roots of g , and since g has at most $n - 1$ distinct roots, it follows that f has at most n distinct roots, as required.

12.9 Example: When R is not an integral domain, a polynomial $f \in R[x]$ of degree n can have more than n roots. For example, in the ring $\mathbb{Z}_6[x]$ the polynomial $f(x) = x^2 + x$ has roots 0, 2, 3 and 5.

12.10 Theorem: (*The Rational Roots Theorem*) Let $f(x) = \sum_{i=0}^n c_i x^i \in \mathbb{Z}[x]$ where $n \in \mathbb{Z}^+$ and $c_n \neq 0$. Let $r, s \in \mathbb{Z}$ with $s \neq 0$ and $\gcd(r, s) = 1$. Then if $f(\frac{r}{s}) = 0$ then $r \mid c_0$ and $s \mid c_n$.

Proof: Suppose that $f(\frac{r}{s}) = 0$, that is $c_0 + c_1 \frac{r}{s} + c_2 \frac{r^2}{s^2} + \cdots + c_n \frac{r^n}{s^n} = 0$. Multiply by s^n to get

$$0 = c_0 s^n + c_1 s^{n-1} r + \cdots + c_{n-1} s^1 r^{n-1} + c_n r^n.$$

Thus we have

$$\begin{aligned} c_0 s^n &= -r(c_1 s^{n-1} + \cdots + c_{n-1} s^1 r^{n-2} + c_n r^{n-1}) \text{ and} \\ c_n r^n &= -s(c_0 s^{n-1} + c_1 s^{n-2} r + \cdots + c_{n-1} r^{n-1}) \end{aligned}$$

and it follows that $r \mid c_0 s^n$ and that $s \mid c_n r^n$. Since $\gcd(r, s) = 1$ we also have $\gcd(r, s^n) = 1$, and since $r \mid c_0 s^n$ it follows that $r \mid c_0$. Since $\gcd(s, r) = 1$ we also have $\gcd(s, r^n) = 1$, and since $s \mid c_n r^n$ it follows that $s \mid c_n$.

12.11 Example: Show that $\sqrt{1 + \sqrt{2}} \notin \mathbb{Q}$.

12.12 Note: Here are a few remarks about irreducible polynomials.

(1) When F is a field, we know that $F[x]$ is a unique factorization domain. For $f \in F[x]$ we know that $f = 0$ if and only if $\deg(f) = -1$, and f is a unit if and only if $\deg(f) = 0$, and for $0 \neq f, g \in F[x]$ we know that $\deg(fg) = \deg(f) + \deg(g)$. It follows that for $f \in F[x]$, if $\deg(f) = 1$ then f is irreducible. It also follows that for $f \in F[x]$, if $\deg(f) = 2$ or 3 then f is reducible in $F[x]$ if and only if f has a root in F .

(2) For $f \in \mathbb{C}[x]$, we know (from the Fundamental Theorem of Algebra) that f is irreducible if and only if $\deg(f) = 1$. For $f \in \mathbb{R}[x]$, we know that f is irreducible polynomial if and only if either $\deg(f) = 1$ or $f(x) = ax^2 + bx + c$ for some $a, b, c \in \mathbb{R}$ with $a \neq 0$ and $b^2 - 4ac < 0$.

(3) When p is a fairly small prime number and n is a fairly small positive integer, it is easy to list all reducible and irreducible polynomials $f \in \mathbb{Z}_p[x]$ with $\deg(f) \leq n$. Note that it suffices to list monic polynomials (since for $f \in \mathbb{Z}_p[x]$ and $0 \neq c \in \mathbb{Z}_p[x]$ we have $f \sim cf$). We start by listing all monic polynomials of degree 1, that is all polynomials of the form $f(x) = x + a$ with $a \in \mathbb{Z}_p$, and noting that they are all irreducible. Having constructed all reducible and irreducible monic polynomials of all degrees less than n , we can construct all of the reducible monic polynomials of degree n by forming products of the reducible monic polynomials of smaller degree in all possible ways, and then all the remaining monic polynomials of degree n must be irreducible.

12.13 Example: Note that $f(x) = x^3 - 3x + 1$ is irreducible in $\mathbb{Q}[x]$ because it is cubic and has no roots in \mathbb{Q} by the Rational Roots Theorem. The same polynomial is reducible in $\mathbb{R}[x]$ and in $\mathbb{C}[x]$ because it is cubic.

12.14 Example: List all monic reducible and irreducible polynomials in $\mathbb{Z}_2[x]$ of degree less than 4, then determine the number of irreducible polynomials in $\mathbb{Z}_2[x]$ of degree 4.

12.15 Definition: Let R be an integral domain. Define a binary relation on the set $R \times (R \setminus \{0\})$ by stipulating that

$$(a, b) \sim (c, d) \iff ad = bc.$$

It is easy to check that this is an equivalence relation. Let

$$F = Q(R) = (R \times (R \setminus \{0\})) / \sim = \left\{ [(a, b)] \mid a, b \in R, b \neq 0 \right\}.$$

Define addition and multiplication operations on F by

$$\begin{aligned} [(a, b)] + [(c, d)] &= [(ad + bc, bd)], \\ [(a, b)] [(c, d)] &= [(ac, bd)]. \end{aligned}$$

It is not hard to verify that these operations are well-defined (noting that when $b \neq 0$ and $d \neq 0$ we also have $bd \neq 0$ because R is an integral domain) and that they make F into a field with zero element $[(0, 1)]$ and identity element $[(1, 1)]$. This field $F = Q(R)$ is called the **quotient field** of the integral domain R . For $a, b \in R$ with $b \neq 0$ we use the following notation:

$$\frac{a}{b} = [(a, b)], \quad a = [(a, 1)], \quad \frac{1}{b} = [(1, b)].$$

The use of the notation $a = [(a, 1)]$, for $a \in R$, allows to consider R as a subring of its quotient field F .

12.16 Example: The quotient field of \mathbb{Z} is equal to \mathbb{Q} , and the quotient field of $\mathbb{Z}[\sqrt{2}]$ is equal to $\mathbb{Q}[\sqrt{2}]$.

12.17 Example: When R is an integral domain, the quotient field of the polynomial ring $R[x]$ is the **field of rational functions** $R(x) = \left\{ \frac{f}{g} \mid f, g \in R[x], g \neq 0 \right\}$. More generally, the quotient field of $R[x_1, \dots, x_n]$ is the field of rational functions $R(x_1, \dots, x_n)$.

12.18 Definition: Let R be a unique factorization domain. For a polynomial $f \in R[x]$, the **content** of f , written as $c(f)$, is a greatest common divisor of the coefficients of f . Note that the greatest common divisor is unique up to association and so $c(f)$ is unique up to association, that is up to multiplication by a unit. We often abuse notation by writing $c(f) = a$ when in fact $c(f) \sim a$. We say that f is **primitive** when $c(f) = 1$ (that is when $c(f)$ is a unit). Note that $f = 0$ if and only if $c(f) = 0$. Note that when $f \in R[x]$ and $a \in R$ we have $c(af) = a c(f)$. In particular, we have $f = c(f)g$ for a primitive polynomial $g \in R[x]$.

12.19 Example: For $f(x) = 6x + 30 \in \mathbb{Z}[x]$ we have $c(f) = 6$. Since $\deg(f) = 1$, it follows that f is irreducible in $\mathbb{Q}[x]$. But since $c(f) = 6$, it follows that f is reducible in $\mathbb{Z}[x]$, indeed in $\mathbb{Z}[x]$ we have $f(x) = 2 \cdot 3 \cdot (x + 5)$.

12.20 Theorem: (Gauss' Lemma) Let R be a UFD with quotient field F .

- (1) For all $f, g \in R[x]$ we have $c(fg) = c(f)c(g)$.
- (2) Let $0 \neq f \in R[x]$ and let $g(x) = \frac{1}{c(f)}f(x) \in R[x]$. Then f is irreducible in $F[x]$ if and only if g is irreducible in $R[x]$.
- (3) Let $0 \neq f \in R[x]$. Then f is reducible in $F[x]$ if and only if f can be factored as a product of two nonconstant polynomials in $R[x]$.

Proof: Let $f, g \in R[x]$. If $f = 0$ or $g = 0$ then we have $c(fg) = 0 = c(f)c(g)$. Suppose that $f \neq 0$ and $g \neq 0$. Let $h(x) = \frac{1}{c(f)}f(x)$ and $k(x) = \frac{1}{c(g)}g(x)$. Then we have $h, k \in R[x]$ with $c(h) = c(k) = 1$ and $fg = c(f)c(g)hk$ so that $c(fg) = c(f)c(g)c(hk)$. Thus to prove Part (1) it suffices to show that $c(hk) = 1$. Let $h(x) = \sum_{i=0}^n a_i x^i$ and $k(x) = \sum_{i=0}^m b_i x^i$ with $a_n \neq 0$ and $b_m \neq 0$. Suppose, for a contradiction, that $c(hk) \neq 1$. Let p be a prime factor of $c(hk)$. Then p divides all of the coefficients of $(hk)(x) = (a_0 b_0) + (a_1 b_0 + a_0 b_1)x + \dots + (a_n b_m)x^{n+m}$. Since $c(h) = 1$, p does not divide all the coefficients of $h(x)$, so we can choose an index $r \geq 0$ so that $p|a_i$ for all $i < r$ and $p \nmid a_r$. Since $c(k) = 1$ we can choose an index $s \geq 0$ so that $p|b_i$ for all $i < s$ and $p \nmid b_s$. Since p divides every coefficient of $(hk)(x)$, it follows that in particular p divides the coefficient

$$c_{r+s} = a_0 b_{r+s} + a_1 b_{r+s-1} + \dots + a_r b_s + \dots + a_{r+s-1} b_1 + a_{r+s}.$$

Since $p|c_{r+s}$ and $p|a_i$ for all $i < r$ and $p|b_i$ for all $i < s$ it follows that $p|a_r b_s$. Since p is prime and $p \nmid a_r$ it follows that $p|b_s$. But r and s were chosen so that $p \nmid a_r$ and $p \nmid b_s$ so we have obtained the desired contradiction. This proves Part (1).

To prove Parts (2) and (3), let $0 \neq f(x) \in R[x]$ and let $g(x) = \frac{1}{c(f)}f(x)$, and note that $g \in R[x]$ with $c(g) = 1$. Suppose that g is reducible in $R[x]$, say $g(x) = h(x)k(x)$ where $h(x)$ and $k(x)$ are non-units in $R[x]$. Since $c(h)c(k) = c(hk) = c(g) = 1$ it follows that $c(h) = c(k) = 1$. Note that $h(x)$ cannot be a constant polynomial since if we had $h(x) = r$ with $r \in R$, then we would have $c(h) = r$ and also $c(h) = 1$ so that r is a unit in R , but then h would be a unit in $R[x]$. Similarly $k(x)$ cannot be a constant polynomial. Since $h(x)$ and

$k(x)$ are nonconstant polynomials in $R[x]$, they are also nonconstant polynomials in $F[x]$. Since $f(x) = c(f)g(x) = c(f)h(x)k(x)$ and since $c(f)h(x)$ and $k(x)$ are both nonconstant polynomials (hence nonunits) in $F[x]$, it follows that $f(x)$ is reducible in $F[x]$.

Conversely, suppose that $f(x)$ is reducible in $F[x]$, say $f(x) = h(x)k(x)$ where h and k are nonzero, nonunits in $F[x]$. Since h and k are nonzero nonunits in $F[x]$, they are nonconstant polynomials. Let a be a least common multiple of the denominators of the coefficients of $h(x)$ and let b be a least common multiple of denominators of the coefficients of $k(x)$, and note that $ah(x) \in R[x]$ and $bk(x) \in R[x]$. Let $p(x) = \frac{1}{c(ah)}ah(x)$ and let $q(x) = \frac{1}{c(bk)}bk(x)$ and note that $p(x), q(x) \in R[x]$ with $c(p) = c(q) = 1$ and that $\deg(p) = \deg(h)$ and $\deg(q) = \deg(k)$. Since $f(x) = ah(x)bk(x) = c(ah)c(bk)p(x)q(x)$ we have $c(f) = c(ah)c(bk)c(pq) = c(ah)c(bk)$ so $g(x) = \frac{1}{c(f)}f(x) = \frac{1}{c(ah)c(bk)}ah(x)bk(x) = p(x)q(x)$. Since $g(x) = p(x)q(x)$ where $p(x)$ and $q(x)$ are nonconstant polynomials in $R[x]$, we see that $g(x)$ is reducible in $R[x]$.

12.21 Theorem: (Modular Reduction) Let $f(x) = \sum_{i=0}^n c_i x^i$ with $n \in \mathbb{Z}^+$, $c_i \in \mathbb{Z}$ and $c_n \neq 0$. Let p be a prime number with $p \nmid c_n$. Let $\bar{f}(x) = \sum_{i=0}^n \bar{c}_i x^i \in \mathbb{Z}_p[x]$ where $\bar{c}_i = [c_i] \in \mathbb{Z}_p$. If \bar{f} is irreducible in $\mathbb{Z}_p[x]$ then f is irreducible in $\mathbb{Q}[x]$.

Proof: Suppose that $f(x)$ is reducible in $\mathbb{Q}[x]$. By Gauss' Lemma, we can choose two nonconstant polynomials $g, h \in \mathbb{Z}[x]$ such that $f = gh \in \mathbb{Z}[x]$. Write $g(x) = \sum_{i=0}^k a_i x^i \in \mathbb{Z}[x]$ and $h(x) = \sum_{i=0}^\ell b_i x^i \in \mathbb{Z}[x]$ with $a_k \neq 0$, $b_\ell \neq 0$ and $k, \ell \geq 1$. Let $\bar{g} = \sum_{i=0}^k \bar{a}_i x^i \in \mathbb{Z}_p[x]$ and $\bar{h}(x) = \sum_{i=0}^\ell \bar{b}_i x^i \in \mathbb{Z}_p[x]$, and note that $\bar{f} = \bar{g}\bar{h} \in \mathbb{Z}_p[x]$. Since $c_n = a_k b_\ell$ and $p \nmid c_n$ it follows that $p \nmid a_k$ and $p \nmid b_\ell$ in \mathbb{Z} so $\bar{a}_k \neq 0$ and $\bar{b}_\ell \neq 0$ in \mathbb{Z}_p . Thus $\deg(\bar{g}) = \deg(g) = k$ and $\deg(\bar{h}) = \deg(h) = \ell$ so that \bar{g} and \bar{h} are nonconstant polynomials in $\mathbb{Z}_p[x]$, and so the polynomial $\bar{f} = \bar{g}\bar{h}$ is reducible in $\mathbb{Z}_p[x]$.

12.22 Example: Prove that $f(x) = x^5 + 2x + 4$ is irreducible in $\mathbb{Q}[x]$ by working in $\mathbb{Z}_3[x]$.

12.23 Theorem: (Eisenstein's Criterion) Let $f(x) = \sum_{i=0}^n c_i x^i$ with $n \in \mathbb{Z}^+$, $c_i \in \mathbb{Z}$ and $c_n \neq 0$. Let p be a prime number such that $p_i | c_i$ for $0 \leq i < n$ and $p \nmid c_n$ and $p^2 \nmid c_0$. Then f is irreducible in $\mathbb{Q}[x]$.

Proof: Suppose, for a contradiction, that $f(x)$ is reducible in $\mathbb{Q}[x]$. By Gauss' Lemma, we can choose two nonconstant polynomials $g, h \in \mathbb{Z}[x]$ such that $f = gh \in \mathbb{Z}[x]$. Write $g(x) = \sum_{i=0}^k a_i x^i \in \mathbb{Z}[x]$ and $h(x) = \sum_{i=0}^\ell b_i x^i \in \mathbb{Z}[x]$ with $k, \ell \geq 1$ and $a_k \neq 0$, $b_\ell \neq 0$. Since $c_0 = a_0 b_0$ and $p | c_0$ but $p^2 \nmid c_0$, it follows that p divides exactly one of the two numbers a_0 and b_0 . Suppose that p divides a_0 but not b_0 (the case that p divides b_0 but not a_0 is similar). Since $p | c_1$, that is $p | (a_0 b_1 + a_1 b_0)$, and $p | a_0$ it follows that $p | a_1 b_0$, and since $p \nmid b_0$ it follows that $p | a_1$. Since $p | c_2$, that is $p | (a_0 b_2 + a_1 b_1 + a_2 b_0)$ and $p | a_0$ and $p | a_1$, it follows that $p | a_2 b_0$, and since $p \nmid b_0$ it then follows that $p | a_2$. Repeating this argument we find, inductively, that $p | a_i$ for all $i \geq 0$, and in particular we have $p | a_k$. Since $c_n = a_k b_\ell$ and $p \nmid c_n$ it follows that $p \nmid b_\ell$, giving the desired contradiction.

12.24 Example: Note that $f(x) = 5x^5 + 3x^4 - 18x^3 + 12x + 6$ is irreducible in $\mathbb{Q}[x]$ by Eisenstein's Criterion using $p = 3$.

12.25 Example: Let p be a prime number. Show that $f(x) = 1 + x + x^2 + \cdots + x^{p-1}$ is irreducible in $\mathbb{Q}[x]$,

12.26 Theorem: If R is a UFD then so is $R[x]$.

Proof: Suppose that R is a UFD and let F be the quotient field of R . Note that the units in $R[x]$ are the constant polynomials which are also units in R . Let $f \in R[x]$ be a non-zero non-unit. If f is a constant polynomial, then the factorization of f in $R[x]$ is the same as the factorization of f in R . Suppose that $\deg(f) \geq 1$. Let $g = \frac{1}{c(f)} f$ so that $g \in R[x]$ with $c(g) = 1$. The factorization of $c(f)$ in $R[x]$ is the same as the factorization in R , so it suffices to show that the polynomial g factors uniquely into irreducibles in $R[x]$. Since $F[x]$ is a ED, hence a UFD, we know that g factors into irreducibles in $F[x]$. By Gauss' Lemma, we can multiply each of the irreducible factors in $F[x]$ by an element of F to write g as a product of irreducible factors in $R[x]$, say $g = f_1 f_2 \cdots f_\ell$ where each f_j is irreducible in $R[x]$. Since $c(g) = 1$ we must have $c(f_j) = 1$ for each index j .

Suppose that $g = f_1 f_2 \cdots f_\ell = g_1 g_2 \cdots g_m$ where f_j and g_k are irreducible in $R[x]$ with $c(f_j) = c(g_k) = 1$ for all j, k . Note that each f_j must be non-constant since if we had $f_j(x) = r \in R$ then we would have $c(f_j) = r$ and $c(f_j) = 1$ so that r is a unit in R , but then f_j would be a unit in $R[x]$. Similarly each g_k is non-constant. It follows that the polynomials f_j and g_k are also irreducible in $F[x]$. By unique factorization in $F[x]$, we must have $m = \ell$ and, after possibly reordering the polynomials g_k , we have $f_j \sim g_j$ in $F[x]$ for all indices j . Since $f_j \sim g_j$ in $F[x]$, we have $g_j = u f_j$ for some $0 \neq u \in F$. Say $u = \frac{a}{b}$ where $a, b \in R$ with $\gcd(a, b) = 1$. Then we have $a f_j = b g_j$ in $R[x]$. Since $c(f_j) = c(g_j) = 1$ we have $c(a f_j) = a$ and $c(b g_j) = b$ and it follows that $a \sim b$ in R , hence $a = bv$ for some unit $v \in R$. Thus we have $g_j = u f_j = \frac{a}{b} f_j = v f_j$ and so $f_j \sim g_j$ in $R[x]$.

12.27 Corollary: If R is a UFD then so is the polynomial ring $R[x_1, x_2, \dots, x_n]$.