

## Chapter 10. Factorization in Rings

**10.1 Definition:** Let  $R$  be a commutative ring. Let  $a, b \in R$ . We say that  $a$  **divides**  $b$  (or  $a$  is a **divisor** or **factor** of  $b$ , or  $b$  is a **multiple** of  $a$ ), and we write  $a|b$ , when  $b = ar$  for some  $r \in R$ . We say that  $a$  and  $b$  are **associates**, and we write  $a \sim b$ , when  $a|b$  and  $b|a$ .

**10.2 Theorem:** Let  $R$  be a commutative ring. Let  $a, b \in R$ . Then

- (1)  $a \sim b$  if and only if  $a$  and  $b$  have the same multiples and divisors,
- (2)  $a \sim 0$  if and only if  $a = 0$ ,
- (3)  $a \sim 1$  if and only if  $a$  is a unit.
- (4) if  $R$  is an integral domain then  $a \sim b$  if and only if  $b = au$  for some unit  $u \in R$ .

Proof: The proof is left as an exercise.

**10.3 Definition:** Let  $R$  be a commutative ring. Let  $a \in R$  be a non-zero non-unit. We say that  $a$  is **reducible** when  $a = bc$  for some non-units  $b, c \in R$ , and otherwise we say that  $a$  is **irreducible**. Note that if  $a$  is irreducible then the divisors of  $a$  are the units and the associates of  $a$ . We say that  $a$  is **prime** when for all  $b, c \in R$ , if  $a|bc$  then either  $a|b$  or  $a|c$ .

**10.4 Theorem:** Let  $R$  be a commutative ring. Let  $a, b \in R$  with  $a \sim b$ . Then

- (1)  $a$  is reducible if and only if  $b$  is reducible,
- (2)  $a$  is irreducible if and only if  $b$  is irreducible,
- (3)  $a$  is prime if and only if  $b$  is prime.

Proof: The proof is left as an exercise.

**10.5 Theorem:** Let  $R$  be an integral domain. Then every prime element in  $R$  is also irreducible.

Proof: The proof is left as an exercise.

**10.6 Exercise:** Find all primes and irreducible elements in  $\mathbf{Z}_{12}$ .

**10.7 Exercise:** Use the method of the Sieve of Eratosthenes to find several irreducible elements in  $\mathbf{Z}[\sqrt{3}i]$  and also some irreducible elements which are not prime.

**10.8 Definition:** A **Euclidean domain** (or ED) is an integral domain  $R$  together with a function  $N : R \rightarrow \mathbf{N}$ , called a **Euclidean norm**, such that

- N1. for all  $a \in R$  we have  $N(a) = 0 \iff a = 0$ ,
- N2. for all  $a \in R$  we have  $N(a) = 1 \iff a$  is a unit,
- N3. for all nonzero nonunits  $a, b, c \in R$ , if  $a = bc$  then  $N(b) < N(a)$  and  $N(c) < N(a)$ , and
- N4. for all  $a, b \in R$  with  $b \neq 0$  there exist  $q, r \in R$  such that  $a = qb + r$  and  $N(r) < N(b)$ .

**10.9 Definition:** A **unique factorization domain** (or UFD) is an integral domain  $R$  with the property that for every nonzero non-unit  $a \in R$  we have

- (1)  $a = p_1 p_2 \cdots p_\ell$  for some  $\ell \in \mathbf{Z}^+$  and some irreducible elements  $p_i \in R$ , and
- (2) if  $a = p_1 p_2 \cdots p_\ell = q_1 q_2 \cdots q_m$  where  $\ell, m \in \mathbf{Z}^+$  and each  $p_i$  and  $q_j$  is irreducible, then  $m = \ell$  and for some bijection  $\sigma : \{1, 2, \dots, \ell\} \rightarrow \{1, 2, \dots, \ell\}$  we have  $a_i \sim b_{\sigma(i)}$  for all  $i$ .

**10.10 Theorem:** Every Euclidean domain is a unique factorization domain

Proof: The proof is almost identical to the proof of unique factorization in  $\mathbf{Z}$ .

**10.11 Example:**  $\mathbf{Z}$  is a Euclidean domain using the Euclidean norm  $N : \mathbf{Z} \rightarrow \mathbf{N}$  given by  $N(a) = |a|$ .

**10.12 Example:** Every field is a Euclidean domain, using the function  $N : R \rightarrow \mathbf{N}$  given by  $N(0) = 0$  and  $N(a) = 1$  for all  $a \neq 0$ .

**10.13 Example:** If  $F$  is a field then  $F[x]$  is a Euclidean domain with Euclidean norm  $N(f) = \deg(f) + 1$  (where we follow the convention that  $\deg(0) = -1$  so that  $N(0) = 0$ ). The fact that  $N$  satisfies Property N4 follows from the Division Algorithm proven below.

**10.14 Exercise:** Show that for each  $d \in \{-2, -1, 2, 3\}$  the ring  $\mathbf{Z}[\sqrt{d}]$  is a Euclidean domain with Euclidean norm given by  $N(a + b\sqrt{d}) = |a^2 - db^2|$ .

**10.15 Exercise:** Show that the rings  $\mathbf{Z}[\sqrt{3}i]$  and  $\mathbf{Z}[\sqrt{5}]$  are not unique factorization domains.

**10.16 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 does 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  $f \neq 0 \in \mathbf{Z}_p[x]$  (because its coefficients are not equal to zero) but  $f = 0 \in \mathbf{Z}_p^{\mathbf{Z}_p}$  because, by Fermat's Little Theorem, we have  $f(x) = 0$  for all  $x \in \mathbf{Z}_p$ .

(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 positive 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  $\deg(f) = 0$ .

**10.17 Example:** In the ring  $\mathbf{Z}_4[x]$  we have  $(1+2x)^2 = 1+4x+4x^2 = 1$ , so  $f(x) = (1+2x)$  is a unit in  $\mathbf{Z}_4[x]$ .

**10.18 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.

**10.19 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  $f(a) = q(a)(a - a) + c = q(a) \cdot 0 + c = c$ .

**10.20 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  $(x - a) | f(x)$ .

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  $(x - a) | f(x)$ . Conversely, suppose that  $(x - a) | f(a)$  and choose  $p \in R[x]$  so that  $f(x) = (x - a)p(x)$ . Then  $f(a) = (a - a)p(a) = 0 \cdot p(a) = 0$ .

**10.21 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  $m = m(f, a) \in \mathbf{N}$  such that  $(x - a)^m | f(x)$  (where we use the convention that  $(x - a)^0 = 1$ ). Note that  $a$  is a root of  $f$  if and only if  $m(f, a) \geq 1$ .

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

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

**10.24 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  $a_1, a_2, \dots, a_\ell$  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  $0 \in c \in R$ , 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.

**10.25 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) 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  $f \in \mathbf{Z}_p[x]$  with  $\deg(f) \leq n$ . Note that it suffices to list monic polynomials (since for  $f \in \mathbf{Z}_p[x]$  and  $0 \neq c \in \mathbf{Z}_p[x]$  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  $a \in \mathbf{Z}_p$ , 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.

(3) For  $f \in \mathbf{C}[x]$ , we know that  $f$  is irreducible if and only if  $\deg(f) = 1$ . For  $f \in \mathbf{R}[x]$ , we know that  $f$  is irreducible polynomial if and only if either  $\deg(f) = 1$  or  $f(x) = ax^2 + bx + c$  for some  $a, b, c \in \mathbf{R}$  with  $a \neq 0$  and  $b^2 - 4ac < 0$ . For  $R = \mathbf{Z}$  or  $\mathbf{Q}$ , it is a more challenging problem to determine which polynomials are irreducible in  $R[x]$ . The next few theorems are related to this problem.

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

**10.27 Definition:** Let  $f \in \mathbf{Z}[x]$ . The **content** of  $f$ , denoted by  $c(f)$ , is the greatest common divisor of the coefficients of  $f$ . We say that  $f$  is **primitive** when  $c(f) = 1$ .

**10.28 Note:** Let  $a_0, a_1, \dots, a_n \in \mathbf{Z}$ , let  $r \in \mathbf{Z}$  and let  $d = \gcd(a_0, a_1, \dots, a_n)$ . Then  $\gcd(ra_0, ra_1, \dots, ra_n) = |r|\gcd(a_0, a_1, \dots, a_n)$  and  $\gcd\left(\frac{a_0}{d}, \frac{a_1}{d}, \dots, \frac{a_n}{d}\right) = 1$ . It follows that for  $f(x) = \sum_{i=0}^n a_i x^i$  we have  $c(rf) = |r|c(f)$  and that if we let  $g(x) = \frac{1}{c(f)}f(x)$  then we have  $g(x) \in \mathbf{Z}[x]$  and  $c(g) = 1$ .

**10.29 Theorem:** (Gauss' Lemma)

- (1) For all  $f, g \in \mathbf{Z}[x]$  we have  $c(fg) = c(f)c(g)$ .
- (2) Let  $0 \neq f \in \mathbf{Z}[x]$  and let  $g(x) = \frac{1}{c(f)}f(x) \in \mathbf{Z}[x]$ . Then  $f$  is irreducible in  $\mathbf{Q}[x]$  if and only if  $g$  is irreducible in  $\mathbf{Z}[x]$ .

Proof: Let  $f, g \in \mathbf{Z}[x]$ . 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  $h, k \in \mathbf{Z}[x]$  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  $p|a_r b_s$  it follows that  $p|a_r$  or  $p|b_s$ . 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 Part (2), let  $0 \neq f(x) \in \mathbf{Z}[x]$  and let  $g(x) = \frac{1}{c(f)}f(x)$ , and note that  $c(g) = 1$ . Suppose that  $g$  is reducible in  $\mathbf{Z}[x]$ , say  $g(x) = h(x)k(x)$  where  $h(x)$  and  $k(x)$  are non-units in  $\mathbf{Z}[x]$ . 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  $r \in \mathbf{Z}$ , then we would have  $|r| = c(h) = 1$  so that  $h(x) = \pm 1$ , but then  $h$  would be a unit. Similarly  $k(x)$  cannot be a constant polynomial. Since  $h(x)$  and  $k(x)$  are nonconstant polynomials in  $\mathbf{Z}[x]$ , they are also nonconstant polynomials in  $\mathbf{Q}[x]$ . 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  $\mathbf{Q}[x]$ , it follows that  $f(x)$  is reducible in  $\mathbf{Q}[x]$ .

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

**10.30 Corollary:** Let  $0 \neq f(x) \in \mathbf{Z}[x]$ . Then  $f(x)$  is reducible in  $\mathbf{Q}[x]$  if and only if  $f(x)$  can be factored as a product of two nonconstant polynomials in  $\mathbf{Z}[x]$ .

Proof: If  $f(x)$  can be factored as  $f(x) = g(x)h(x)$ , where  $g(x)$  and  $h(x)$  are nonconstant polynomials in  $\mathbf{Z}[x]$ , then because  $g(x)$  and  $h(x)$  are also nonconstant polynomials in  $\mathbf{Q}[x]$  (hence nonunits in  $\mathbf{Q}[x]$ ), it follows immediately that  $f$  is reducible in  $\mathbf{Q}[x]$ . Suppose, conversely, that  $f(x)$  is reducible in  $\mathbf{Q}[x]$ . Let  $p(x) = \frac{1}{c(f)}f(x)$  and note that  $p(x) \in \mathbf{Z}[x]$  with  $c(p) = 1$ . By Gauss' Lemma,  $p(x)$  is reducible in  $\mathbf{Z}[x]$ . Choose nonunits  $k, h \in \mathbf{Z}[x]$  such that  $p = kh \in \mathbf{Z}[x]$ . Since  $c(k)c(h) = c(kh) = c(p) = 1$  we have  $c(k) = c(h) = 1$ . Since  $k$  and  $h$  are nonunits with  $c(k) = c(h) = 1$ , it follows that  $k$  and  $h$  are nonconstant polynomials (indeed, if  $k(x)$  was constant with  $k(x) = r$  then we would have  $|r| = c(k) = 1$  so that  $k(x) = r = \pm 1$ , but then  $k(x)$  would be a unit). Let  $g(x) = c(f)k(x)$  and note that since  $k(x)$  is nonconstant, so is  $g(x)$ . Then we have  $f(x) = g(x)h(x)$ , which is a product of two nonconstant polynomials in  $\mathbf{Z}[x]$ .

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

**10.32 Theorem:** (Rational Roots) Let  $f(x) = \sum_{i=0}^n c_i x^i$  where  $n \in \mathbf{Z}^+$ , each  $c_i \in \mathbf{Z}$  and  $c_n \neq 0$ . Let  $r, s \in \mathbf{Z}$  with  $s \neq 0$  and  $\gcd(r, s) = 1$ . Then if  $f\left(\frac{r}{s}\right) = 0$  then  $r|c_0$  and  $s|c_n$ .

Proof: Suppose that  $f\left(\frac{r}{s}\right) = 0$ , 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

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

Thus we have

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

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

**10.33 Exercise:** Show that  $\sqrt{1 + \sqrt{2}} \notin \mathbf{Q}$ .

**10.34 Theorem:** (Modular Reduction) Let  $f(x) = \sum_{i=0}^n c_i x^i$  with  $n \in \mathbf{Z}^+$ ,  $c_i \in \mathbf{Z}$  and  $c_n \neq 0$ .

Let  $p$  be a prime number with  $p \nmid c_n$ . Let  $\bar{f}(x) = \sum_{i=0}^n \bar{c}_i x^i \in \mathbf{Z}_p[x]$  where  $\bar{c}_i = [c_i] \in \mathbf{Z}_p$ .

If  $\bar{f}$  is irreducible in  $\mathbf{Z}_p[x]$  then  $f$  is irreducible in  $\mathbf{Q}[x]$ .

Proof: Suppose that  $f(x)$  is reducible in  $\mathbf{Q}[x]$ . By the corollary to Gauss' Lemma, we can choose two nonconstant polynomials  $g, h \in \mathbf{Z}[x]$  such that  $f = gh \in \mathbf{Z}[x]$ .

Write  $g(x) = \sum_{i=0}^k a_i x^i \in \mathbf{Z}[x]$  and  $h(x) = \sum_{i=0}^{\ell} b_i x^i \in \mathbf{Z}[x]$  with  $a_k \neq 0, b_\ell \neq 0$  and  $k, \ell \geq 1$ .

Let  $\bar{g} = \sum_{i=0}^k \bar{a}_i x^i \in \mathbf{Z}_p[x]$  and  $\bar{h}(x) = \sum_{i=0}^{\ell} \bar{b}_i x^i \in \mathbf{Z}_p[x]$ , and note that  $\bar{f} = \bar{g} \bar{h} \in \mathbf{Z}_p[x]$ .

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  $\mathbf{Z}$  so  $\bar{a}_k \neq 0$  and  $\bar{b}_\ell \neq 0$  in  $\mathbf{Z}_p$ .

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  $\mathbf{Z}_p[x]$ , and so the polynomial  $\bar{f} = \bar{g} \bar{h}$  is reducible in  $\mathbf{Z}_p[x]$ .

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

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

Proof: Suppose, for a contradiction, that  $f(x)$  is reducible in  $\mathbf{Q}[x]$ . By the corollary to Gauss' Lemma, we can choose two nonconstant polynomials  $g, h \in \mathbf{Z}[x]$  such that  $f = gh \in \mathbf{Z}[x]$ . Write  $g(x) = \sum_{i=0}^k a_i x^i \in \mathbf{Z}[x]$  and  $h(x) = \sum_{i=0}^{\ell} b_i x^i \in \mathbf{Z}[x]$  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  $p|a_k$  it follows that  $p|c_n$ , giving the desired contradiction.

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

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