7 Divisibility in Integral Domains

Definition 7.1 Let D be an integral domain and let $a, b \in D$. Then a is said to *divide* b in D, in symbols $a \mid b$, if $ac = b$ for some $c \in D$, i.e., $\langle b \rangle \subseteq \langle a \rangle$.

Elements a, $b \in D$ are called *associates* if $a \mid b$ and $b \mid a$, i.e., $\langle a \rangle = \langle b \rangle$ and equivalently there is a unit $u \in D$ such that $b = ua$. In this case, we write $a \sim b$. (Exercises 2 and 5)

A nonzero element a is called *irreducible* if it is not a unit and if $a = bc$ for some b, $c \in D$ then b or c is a unit, i.e., $\langle a \rangle \neq \{0\}, R$ and $\langle a \rangle \subseteq \langle b \rangle \subset R$ implies $\langle a \rangle = \langle b \rangle$.

A nonzero element a is called *prime* if a is not a unit and $a \mid bc$ implies $a \mid b$ or $a \mid c$, equivalently if $\langle a \rangle$ is a prime ideal.

Example 7.1 Let $D = \boldsymbol{Z}[\sqrt{-3}]$. Then $2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$. $1 \pm \sqrt{-3}$ and 2 are irreducible but not prime.

Let $\alpha \in D$. Then $\alpha \in U(D) \Leftrightarrow N(\alpha) = 1 \Leftrightarrow \alpha \in \{1, -1\}$. $N(2) = N(1 \pm \sqrt{-3}) = 4$ and $2 \notin N(D)$.

Lemma 7.1 (Theorem 18.1) *Let D be an integral domain and p a prime. Then p is irreducible.*

Proof. Let $p = ab$. Then $\langle p \rangle \subseteq \langle a \rangle \cap \langle b \rangle$. So $a \in \langle p \rangle$ implies $b \in U(D)$ and $b \in \langle p \rangle$ implies $a \in U(D)$. Thus p is irreducible. ■

Proposition 7.2 (Theorem 18.2) *Let I be a non-zero ideal of a principal ideal domain D and $I = \langle p \rangle$. Then the following statements about I are equivalent:* *(Exercise 10)*

(i) *I is maximal,*

(ii) *I is prime, i.e., p is prime,*

(iii) *p is an irreducible element of D.*

Proof. (i) $\Rightarrow$ (ii) is from Theorem 3.3, and (ii) $\Rightarrow$ (iii) is from Lemma 7.1.

Suppose p is irreducible. Let $\langle p \rangle \subseteq \langle a \rangle$. Then $p = ab$. Hence either p and a are associates, or $a \in U(D)$. Thus $\langle p \rangle = \langle a \rangle$ or $\langle a \rangle = D$, and $I = \langle p \rangle$ is maximal.. ■

Definition 7.2 An integral domain D is a *unique factorization domain* if

1. Every nonzero element of D that is not a unit can be written as a product of irreducibles of D.

2. The factorization into irreducibles is unique up to associates and the order in which the factors appear.

Definition 7.3 Let D be a unique factorization domain. For $a_1, a_2, \ldots, a_m \in D$, a greatest common divisor $d = \gcd\{a_1, a_2, \ldots, a_m\}$ is an element of D satisfying the following.

1. $d \mid a_1$, $d \mid a_2, \ldots, d \mid a_m$.

2. If $c \mid a_1$, $c \mid a_2, \ldots, c \mid a_m$, then $c \mid d$.

If both d and d' are greatest common divisors, we have $d \sim d'$.

Note that in a unique factorization domain, the greatest common divisor always exists. Let

$$a = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r},\ b = p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r},$$

where $p_1, p_2, \ldots, p_r$ are irreducibles that are not mutually associates, and $e_1, e_2, \ldots, e_r$ and $f_1, f_2, \ldots, f_r$ are nonnegative integers. Then the greatest common divisor of a and b is

$$d = p_1^{g_1} p_2^{g_2} \cdots p_r^{g_r},\ \text{where } g_1 = \min\{e_1, f_1\}, g_2 = \min\{e_2, f_2\}, \ldots, g_r = \min\{e_r, f_r\}.$$

We find the greatest common divisor of $a_1, a_2, \ldots, a_m \in D$ similarly.

Lemma 7.3 *Let D be a unique factorization domain. Then every irreducible element is prime.* *(Ex. 43)*

Proof. Suppose p is an irreducible element. Let $p \mid ab$ $(a, b \in D)$. Set $ab = pc$, $a = p_1 \cdots p_r$, $b = p'_1 \cdots p'_s$ and $c = q_1 \cdots q_t$, where p_i, p'_j, q_k are irreducible elements in D. Then

$$p \cdot q_1 \cdots q_t = pc = ab = p_1 \cdots p_r p'_1 \cdots p'_s.$$

Since D is a unique factorization domain, $p \sim p_i$ for some i, or $p \sim p'_j$ for some j. If $p \sim p_i$, then $p \mid a$. If $p \sim p'_j$, then $p \mid b$. Therefore, p is prime. ■

Lemma 7.4 *In a principal ideal domain, any strictly increasing chain of ideals $I_1 \subset I_2 \subset \cdots$ must be finite in length.* (This condition is called the *Ascending Chain Condition* (ACC).) *(See Exercise 3.)*

Proof. Let $I = \bigcup_{i=1}^{\infty} I_i = \langle a \rangle$, Then there is a number n such that $a \in I_n$. ■

Theorem 7.5 (Theorem 18.3, PID ⇒ UFD) *Every principal ideal domain is a unique factorization domain.*

Proof. Let a be neither a zero nor a unit. If a is not irreducible, then there exist non units a_1, $b \in D$ such that $a = a_1 b$ and $\langle a \rangle$ is properly contained in $\langle a_1 \rangle$. If a_1 is not irreducible, we can continue this process. So by the previous lemma, we may assume that $a = p_1 a_1$ and p_1 is irreducible. Similarly we can continue this process to factor a as a product of irreducibles of D.

Suppose $a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$. Then by Proposition 7.2, $p_1 \mid q_i$ for some i. Now we can proceed by induction. ■

Corollary 7.6 *Let F be a field. Then the polynomial ring in x over F, $F[x]$, is a unique factorization domain.*

Definition 7.4 An integral domain is called a *Euclidean Domain* if there is a function (called the measure) from the nonzero element of D to the nonnegative integers such that

1. $d(a) \leq d(ab)$ for all nonzero $a, b \in D$.

2. If $a, b \in D$, $b \neq 0$ then there exist elements q and $r \in D$ such that $a = bq + r$, where $r = 0$ or $d(r) < d(b)$.

Example 7.2 $\boldsymbol{Z}[\sqrt{-1}]$ is a Euclidean domain. (See Exercise 7.)

Define $d(\alpha) = N(\alpha) = \alpha \cdot \overline{\alpha}$. For $\alpha, \beta \in \boldsymbol{Z}[\sqrt{-1}]$, let

$$\alpha/\beta = (a + b\sqrt{-1}) + (a' + b'\sqrt{-1}), \text{ where } a, b \in \boldsymbol{Z},\ |a| \le \frac{1}{2},\ |b| \le \frac{1}{2}.$$

Set $\gamma = a + b\sqrt{-1}$ and $\rho = (a' + b'\sqrt{-1})\beta$. Then $\alpha = \gamma\beta + \rho$ and

$$N(\rho) = N((a' + b'\sqrt{-1})\beta) = N(a' + b'\sqrt{-1})N(\beta) \le \left(\left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2\right) N(\beta) < N(\beta).$$

Theorem 7.7 (Theorem 18.4 ED $\Rightarrow$ PID) *Every Euclidean domain is a principal ideal domain.*

Proof. Let I be a nonzero ideal. Let $d = \min\{d(a) \mid a \in I,\ a \neq 0\}$ and $d = d(a)$. Suppose $b \in I$. Then there exist $q, r \in D$ such that $b = aq + r$ with $r = 0$ or $r \neq 0$ and $d(r) < d(a)$. The latter does not occur as $r \in I$ as well. ■

Theorem 7.8 (Theorem 18.5) *If D is a unique factorization domain, then so is the polynomial ring $D[x_1, x_2, \ldots, x_k]$.*

7.1 Proof of Theorem 7.8

Definition 7.5 Let R be a UFD and let $0 \neq f(x) \in R[x]$. The gcd of the coefficients of $f(x)$ is called the *content* of $f(x)$, and is denoted by $c(f(x))$. If $c(f(x)) \sim 1$, i.e., $c(f(x)) \in U(R)$, then $f(x)$ is said to be *primitive.*

Lemma 7.9 *Let $0 \neq f(x) \in R[x]$ where R is a UFD. Then $f(x) = cf_0(x)$ where $c = c(f(x))$ and $f_0(x)$ is primitive in $R[x]$.*

Proof. Write $f(x) = a_0 + a_1x + \cdots + a_nx^n$; then $c(f(x)) = \gcd\{a_0, \ldots, a_n\} = c$. Write $a_i = cb_i$ with $b_i \in R$, and put $f_0(x) = b_0 + b_1x + \cdots + b_nx^n \in R[x]$. Thus $f(x) = cf_0(x)$. If $d = \gcd\{b_0, b_1, \ldots, b_n\}$, then $d \mid b_i$ and so $cd \mid cb_i = a_i$. Since c is the gcd of the a_i, it follows that cd divides c and hence that d is a unit and $f_0(x)$ is primitive. ■

Proposition 7.10 *Let R be a UFD and let $f(x)$, $g(x)$ be non-zero polynomials over R. Then $c(f(x)g(x)) \sim c(f(x))c(g(x))$. In particular, if $f(x)$ and $g(x)$ are primitive, then so is $f(x)g(x)$.*

Proof. Consider first the special case where $f(x)$ and $g(x)$ are primitive. If $f(x)g(x) = c(f(x)g(x))h(x)$ (with $h(x)$ is primitive) is not primitive, then $c(f(x)g(x))$ is not a unit and it must be divisible by some irreducible element p of R. There are two proofs.
First Proof: Since R is a UFD, p is prime and $P = \langle p \rangle$ is a prime ideal. Consider in $(R/P)[x]$ using bar notation. Then

$$0 = \overline{c(f(x)g(x))h_0(x)} = \overline{f(x)g(x)} = \overline{f(x)} \cdot \overline{g(x)}.$$

Since $(R/P)[x]$ is an integral domain, $\overline{f(x)} = 0$ or $\overline{g(x)} = 0$ contradicting our assumption that $f(x)$ and $g(x)$ are primitive. ■

Second Proof: Write

$$f(x) = \sum_{i=0}^{m} a_i x^i,\ g(x) = \sum_{j=0}^{n} b_j x^j,\ \text{and } f(x)g(x) = \sum_{k=0}^{m+n} c_k x^k.$$

Since $f(x)$ is primitive, p cannot divide all its coefficients, and so there is an integer $r \geq 0$ such that $p \mid a_0, a_1, \ldots, a_{r-1}$ but $p \nmid a_r$. Similarly there is an $s \geq 0$ such that p divides each of $b_0, b_1, \ldots, b_{s-1}$ but p does not divide b_s. Now consider the coefficient c_{r+s} of x^{r+s} in $f(x)g(x)$; this equals

$$(a_0 b_{r+s} + a_1 b_{r+s-1} + \cdots + a_{r-1} b_{s+1}) + a_r b_s + (a_{r+1} b_{s-1} + \cdots + a_{r+s} b_0).$$

We know that $p \mid c_{r+s}$; also both the expressions in parentheses in the expression above. It follows that $p \mid a_r b_s$. By Lemma 7.3, we must have $p \mid a_r$ or $p \mid b_s$, both of which are impossible. By this contradiction $f(x)g(x)$ is primitive.

Now we are ready for the general case. By Lemma 7.9 we wirte $f(x) = cf_0(x)$ and $g(x) = dg_0(x)$ where $c = c(f(x))$ and $d = c(g(x))$, and the polynomials $f_0(x)$, $g_0(x)$ are primitive in $R[x]$. Then $f(x)g(x) = cd(f_0(x)g_0(x))$ and, as has just been shown in Proposition 7.10, $f_0 g_0$ is primitive. In consequence $c(f(x)g(x)) \sim cd = c(f(x))c(g(x))$. ■

The following proposition is called Gauss's Lemma.

Proposition 7.11 *Let R be a unique factorization domain and let F denote the field of fractions of R. Let $f(x)$ be a primitive polynomial in $R[x]$. Then $f(x)$ is irreducible over R if and only if it is irreducible over F.*

Proof. Of course irreducibility over F certainly implies irreducibility over R. It is the converse implication which needs proof. Assume that $f(x)$ is irreducible over R but reducible over F. Here we can assume that $f(x)$ is primitive on the basis of Proposition 7.10. Then $f(x) = g(x)h(x)$ where $g(x), h(x) \in F[x]$ are not constant. Since F is the field of fractions of R, there exist elements $a, b \neq 0$ in R such that $g_1(x) = ag(x) \in R[x]$ and $h_1(x) = bh(x) \in R[x]$. Write $g_1(x) = c(g_1)g_2(x)$ where $g_2(x) \in R[x]$ is primitive. Then $ag(x) = c(g_1(x))g_2(x)$, so we can divide both sides by $\gcd\{a, c(g_1(x))\}$. On these grounds it is possible to assume that $c(g_1(x))$ and a are relatively prime, and that the same holds for $c(h_1(x))$ and b.

Next we have $(ab)f(x) = (ag)(bh(x)) = g_1(x)h_1(x)$. Taking the constant of each side and using Proposition 7.10, we obtain $ab = c(g_1(x))c(h_1(x))$ since $f(x)$ is primitive. But $c(g_1(x))$ and a are relatively prime, so $a \mid c(h_1(x))$, and for a similar reason $b \in c(g_1(x))$. Therefore we have the factorization $f(x) = (b^{-1}g_1(x))(a^{-1}h_1(x))$ and now both factors are polynomials over R. But this contradicts the irreducibility of $f(x)$ over R and so the proof is complete. ■

Theorem 7.12 *If R is a unique factorization domain, then so is the polynomial ring $R[x_1, x_2, \ldots, x_k]$.*

Proof. We need only to prove this when $k = 1$. For if $k > 1$, then

$$R[x_1, x_2, \ldots, x_k] = R[x_1, x_2, \ldots, x_{k-1}][x_k]$$

and induction on k can be used once the case $k = 1$ is settled. From now on we restrict attention to $S = R[x]$.

(a) Any non-constant polynomial $f(x)$ in S is expressible as a product ot irreducible elements of R and primitive irreducible polynomials over R.

Proof. The key idea in the proof is to introduce the field of fractions F of R, and exploit the fact that $F[x]$ is known to be a PID and hence a UFD. First of all write $f(x) = c(f(x))f_0(x)$ where $f_0(x) \in S$ is primitive using Lemma 7.9. Hence $c(f(x))$ is either a unit or a product of irreducibles of R. So we can assume that $f(x)$ is primitive. Regarding $f(x)$ as an element of the UFD $F[t]$, we write $f = p_1p_2 \cdots p_m$ where $p_i \in F[t]$ is irreducible over F. Now find $a_i \neq 0$ in R such that $f_i(x) = a_ip_i(x) \in S$. Wirting $c(f_i(x)) = c_i$, we have $f_i(x) = c_iq_i(x)$ where $q_i(x) \in R[x]$ is primitive. Hence $p_i(x) = a_i^{-1}x_i = a_i^{-1}c_iq_i(x)$, and $q_i(x)$ is F-irreducible since $p_i(x)$ is. Thus $q_i(x)$ is certainly R-irreducible.

Combining these expressions for $p_i(x)$, we find that

$$f(x) = (a_1^{-1} \cdots a_m^{-1}c_1 \cdots c_m)q_1(x) \cdots q_m(x)$$

and hence $(a_1 \cdots a_m)f(x) = (c_m \cdots)q_1(x) \cdots q_m(x)$. Now take the content of both sides of the equations to get $a_1 \cdots a_m = c_1 \cdots c_m$ up to a unit, since $f(x)$ and $q_i(x)$ are primitive. Consequently, $f(x) = uq_1(x) \cdots q_m(x)$ for some unit u of R. This is what we had to prove. ■

(b) Every irreducible element of S is either an irreducible element of R or a primitive irreducible polynomial in S.

Proof. Let C_1 be a complete set of irreducibles for R, and C_2 is a set of non-associate primitive irreducible polynomials. Hence every primitive irreducible polynomial in $R[x]$ is associate to some element of C_2. Now put $C = C_1 \cup C_2$. Then C is a complete set of irreducibles for S. ■

(c) Uniqueness.

Proof. Suppose that

$$f(x) = ua_1 \cdots a_kf_1(x) \cdots f_r(x) = vb_1 \cdots b_\ell g_1(x) \cdots g_s(x),$$

where u, v are units, $a_x, b_y \in C_1$, $f_i(x), f_j(x) \in C_2$. By Gauss's Lemma, the $f_i(x)$ and $g_j(x)$ are F-irreducible. Since $F[x]$ is a UFD and C_2 is a complete set of irreducibles for $F[x]$, we conclude that $r = s$ and $f_i(x) = w_ig_i(x)$, (after possible relabelling), where $w_i \in F$. Write $w_i = c_id_i^{-1}$ where $c_i, d_i \in R$. Then $d_if_i(x) = c_ig_i(x)$, and on taking contents we find that $c_i = d_i$ up to a unit. This implies that w_i is a unit of R and so $f_i(x), g_i(x)$ are associate. Hence $f_i(x) = g_i(x)$.

Cancelling the $f_i(x)$ and $g_i(x)$, we are left with $ua_1 \cdots a_k = vb_1 \cdots b_\ell$. Bur R is a UFD with a complete set of irreducibles C_1, so that $k = \ell$, $u = v$ and $a_i = b_i$ (after further relabelling). This completes the proof. ■

Corollary 7.13 *The following rings are unique factorization domains:*
$\boldsymbol{Z}[x_1, x_2, \ldots, x_k]$ *and* $F[x_1, x_2, \ldots, x_k]$ *where* F *is a field.*

Proposition 7.14 (Eisenstein's Criterion (1850)) *Let* R *be a unique factorization domain and let* $f(x) = a_0 + a_1x + \cdots + a_nx^n$ *be a polynomial over* R. *Suppose that there is an irreducible element* p *of* R *such that* $p \mid a_0$, $p \mid a_1, \ldots, p \mid a_{n-1}$, *but* $p \nmid a_n$ *and* $p^2 \nmid a_0$. *Then* $f(x)$ *is irreducible over* R.

Proof. Suppose that $f(x)$ is reducible and

$$f(x) = (b_0 + b_1 x + \cdots + b_r x^r)(c_0 + c_1 x + \cdots + c_s x^s)$$

where b_i, $c_j \in R$, $r, s < n$, and $r + s = n$. Then

$$a_i = b_0 c_i + b_1 c_{i-1} + \cdots + b_i c_0.$$

Now by hypothesis $p \mid a_0 = b_0 c_0$ but $p^2 \nmid a_0$; thus p must divide exactly one of b_0 and c_0, say $p \mid b_0$ and $p \nmid c_0$. Also p cannot divide every b_i since otherwise it would divide $a_n = b_0 c_n + \cdots b_n c_0$. Therefore, there is a smallest positive integer k such that $p \nmid b_k$. Now p divides each of $b_0, b_1, \ldots, b_{k-1}$ and also $p \mid a_k$ since $k \leq r < n$. Since $a_k = (b_0 c_k + \cdots + b_{k-1} c_1) + b_k c_0$, it follows that $p \mid b_k c_0$. By Euclide's lemma, which is valid in any UFD by (7.3.4), $p \mid b_k$ or $p \mid c_0$, both of which are forbidden. ■