2.8 Greatest Common Divisors

2.8.1 Definition. Let R be a commutative ring and let $a, b \in R$ be nonzero ring elements. A ring element $d \in R$ is a ***greatest common divisor*** of a and b, denoted by $\gcd(a, b)$, if

- the element d divides both a and b, and
- any element $c \in R$, that divides both a and b, also divides d.

Two ring elements are ***coprime*** if 1 is a greatest common divisor.

2.8.2 Example. In a field, every nonzero element is a greatest common divisor for any pair of nonzero elements. ◇

2.8.3 Example. A greatest common divisor may not exist. In the domain $R = \mathbb{Z}[\sqrt{-5}]$, we have $9 = (3)(3) = (2 + \sqrt{-5})(2 - \sqrt{-5})$. Both 3 and $2 + \sqrt{-5}$ divide 9, but neither divides the other. Hence, 9 and $6 + 3\sqrt{-5}$ do not have a greatest common divisor. ◇

When $R = \mathbb{Z}$, we typically impose uniqueness by requiring the greatest common divisor to be positive. When K is field and $R = K[x]$, we force uniqueness by requiring the greatest common divisor to be monic.

2.8.4 Lemma. *Let R be a domain and let a, b be nonzero ring elements in R. Assume that $d \in R$ is a greatest common divisor for a and b. A ring element $e \in R$ is also a greatest common divisor for a and b if and only if there exists a unit $u \in R$ such that $e = ud$.*

Proof.

($\Rightarrow$) Suppose that $e = \gcd(a, b)$. Since e divides a and b, it follows that e divides d. Similarly, d divides a and b, so d divides e. Hence, there exists elements u and v in R such that $d = ue$ and $e = vd$. It follows that $d = ue = uvd$. Because R is a domain, we deduce that $1 = uv$.

($\Leftarrow$) Suppose there exists a unit $u \in R$ such that $e = ud$. Since d divides a, there exists $x \in R$ such that $a = xd = xue$, so e divides a. By symmetry, we see that e divides b. Assume that c divides a and b. Since d is a greatest common divisor for a and b, there exists $w \in R$ such that $d = wc$, so $e = uwc$. Thus, y is also a greatest common divisor for a and b. □

2.8.5 Theorem. *Let R be a principal ideal domain. For any nonzero ring elements $a, b \in R$, there exists ring elements $x, y \in R$ such that $\gcd(a, b) = ax + by$. In particular, we have $\langle \gcd(a, b) \rangle = \langle a, b \rangle$.*

A domain in which a greatest common divisor of every pair of nonzero elements is a linear combination of the two elements is a ***Bézout domain***.

Proof. Set $I := \langle a, b \rangle$. Since R is a principal ideal domain, there is a ring element $d \in R$ such that $I = \langle d \rangle$. It follows that $d = ax + by$ for some $x, y \in R$. Both a and b are in I and I is generated by d, so d divides a and b. On the other hand, if a ring element c divides a and b, then c divides $ax + by = d$. Hence, we see that $d = \gcd(a, b)$.

Any generator for the ideal $\langle a, b \rangle$ is a greatest common divisor of a and b. Lemma 2.8.4 shows that, for any two greatest common divisors d and e, there exists a unit $u \in R$ such that $e = ud$ and $d = u^{-1}e$. Thus, we have $\langle e \rangle \subseteq \langle d \rangle$ and $\langle d \rangle \subseteq \langle e \rangle$, so $\langle d \rangle = \langle e \rangle$. □

Greatest common divisors are computable in Euclidean domains.

2.8.6 Lemma. *Let R be a Euclidean domain and let a, b be nonzero ring elements in R. For any ring elements $a, r \in R$ such that $a = qb + r$ with $r \neq 0$, we have* $\gcd(a, b) = \gcd(b, r)$.

Proof. Let $d := \gcd(a, b)$. Since d divides a and b, this ring element divides $a - qb = r$. Moreover, any ring element c, dividing b and r, also divides $a = bq + r$. It follows that c divides d. We deduce that d is a greatest common divisor of b and r. □

2.8.7 Algorithm (Extended Euclidean Algorithm).
Input: Let a and b be elements in a Euclidean domain R.
Output: Ring elements $x, y \in R$ such that $ax + by = \gcd(a, b)$.

$(r', r, s', s, t', t) := (a, b, 1, 0, 0, 1)$;
While $r \neq 0$ do
  Find $q, r'' \in R$ such that $r' = q\,r + r''$ and $\partial(r'') < \partial(r)$;
  $(r', r, s', s, t', t) := (r, r' - q\,r, s, s' - q\,s, t, t' - q\,t)$;
Return (s', t').

Outline of Proof. From the remainders r'' , we obtain a decreasing sequence of nonnegative integer $\partial(r'')$, so eventually one of the remainders will be zero. Thus, the while loop must terminate.

Lemma 2.8.6 proves that $\gcd(a, b) = \gcd(r', r)$, and one shows that the equations $r = s\,a + t\,b$ and $r' = s'\,a + t'\,b$ hold throughout the calculation. □

2.8.8 Example. When $a = 1254$, and $b = 1110$, Algorithm 2.8.7 gives

Table 2.1: Values of the local variables when using Algorihm 2.8.7 to compute $\gcd(1254, 1110)$

r'	r	s'	s	t'	t	q
1254	1110	1	0	0	1	1
1110	144	0	1	1	−1	7
144	102	1	−7	−1	8	1
102	42	−7	8	8	−9	2
42	18	8	−23	−9	26	2
18	6	−23	54	26	−61	3
6	0	54	−185	−61	209	

We deduce that $(54)(1254)+(-61)(1110) = 6 = \gcd(1254, 1110)$. ◇

2.8.9 Example. When $R = \mathbb{F}_3[x]$, $f = x^3+2x^2+2$, and $g = x^2+2x+1$, Algorithm 2.8.7 gives

Table 2.2: Values of the local variables when using Algorihm 2.8.7 to compute $\gcd(x^3 + 2x^2 + 2, x^2 + 2x + 1)$

r'	r	s'	s	t'	t	q
$x^3 + 2x^2 + 2$	$x^2 + 2x + 1$	1	0	0	1	x
$x^2 + 2x + 1$	$2x + 2$	0	1	1	$2x$	$2x + 2$
$2x + 2$	0	1	$x + 1$	$2x$	$2x^2 + 2x + 1$	

We have $(1)(x^3+2x^2+2)+(2x)(x^2+2x+1) = 2x+2 = \gcd(f, g)$. ◇

2.9 Factorization

2.9.1 Definition. A ring element a is ***irreducible*** if a is nonzero, a is not a unit, and the relation $a = bc$ implies that either b or c is a unit.

2.9.2 Example. The quotient ring $\mathbb{Z}/\langle 6\rangle$ has no irreducible elements because $2 = (2)(4)$, $3 = (3)(3)$, $4 = (2)(2)$, and $(\mathbb{Z}/\langle 6\rangle)^{\times} = \{1, 5\}$. Without irreducibles, an element may have many distinct factorizations: $4 = (2)(2) = (2)(2)(2)(2) = (2)(2)(2)(2)(2)(2) = \cdots$. ◇

2.9.3 Lemma. *Let R be a domain. If the ideal $\langle f\rangle$ is prime, then the ring element is irreducible.*

Proof. Suppose that $f = gh$. Since the principal ideal $\langle f\rangle$ is prime, Proposition 2.3.8 shows that the ring element f divides either g or h. Without loss of generality, assume that f divides g, so there exists $q \in R$ such that $g = qf$. It follows that $f = gh = qfh$. Since R is a domain, we deduce that $1 = qh$ so h is a unit and f is irreducible. □

2.9.4 Example. Consider the subring $\mathbb{C}[x^2, x^3] \subset \mathbb{C}[x]$. Comparing degrees, we see that the elements x^2 and x^3 are irreducible. They are not prime because x^2 divides $(x^3)^2 = x^6$ but x^2 does not divide x^3 and x^3 divides $x^4\,x^2 = x^6$ but x^3 does not divide either x^4 or x^2. ◇

2.9.5 Problem. Show that $2 \in \mathbb{Z}[\sqrt{-3}]$ is irreducible but not prime.

Solution. Suppose $2 = (a + b\sqrt{-3})(c + d\sqrt{-3})$ with $a, b, c, d \in \mathbb{Z}$. Taking conjugates gives $2 = (a - b\sqrt{-3})(c - d\sqrt{-3})$. Multiplying these equations gives $4 = (a^2 + 3b^2)(c^2 + 3d^2)$. Since the equation $x^2 + 3y^2 = 2$ has no integral solutions, it follows that $a^2 + 3b^2 = 1$ and $a = \pm 1$, $b = 0$. Since $2(p + q\sqrt{-3}) = 1$ has no integral solutions, the ring element 2 is not a unit. We see that 2 is irreducible. To see that 2 is not prime, observe that 2 divides $4 = (1 + \sqrt{-3})(1 - \sqrt{-3})$, but 2 does not divide either factor. □

2.9.6 Proposition. *Let R be a principal ideal domain. For any element $f \in R$, the following are equivalent:*
(a) *the ring element f is irreducible;*
(b) *$\langle f\rangle$ is a nonzero maximal ideal;*
(c) *$\langle f\rangle$ is a nonzero prime ideal.*

Proof.
(a) ⇒ (b): Suppose $\langle f\rangle \subseteq \langle g\rangle$ for some $g \in R$. Equivalently, there exists $h \in R$ such that $f = gh$. Since f is irreducible, either g or h is a unit, so $\langle f\rangle = \langle g\rangle$ or $\langle g\rangle = R$. Because every ideal is prinicipal, we see that $\langle f\rangle$ is maximal.
(b) ⇒ (c): Every nonzero maximal ideal is a nonzero prime ideal.
(c) ⇒ (a): Follows from Lemma 2.9.3. □

2.9.7 Definition. A domain R is a ***unique factorization domain*** if

- every nonzero $f \in R$ can be written in the form $f = u \prod_{j=1}^{m} g_j^{e_j}$ where u is a unit, each g_j is irreducible, and $e_j \in \mathbb{N}$;
- if $f = u \prod_{j=1}^{m} g_j^{e_j} = v \prod_{j=1}^{n} h_j^{\ell_j}$ are two such factorizations then we have $m = n$ and $g_j = c_j h_{\sigma(j)}$ for some units c_j and $\sigma \in \mathfrak{S}_m$.

2.9.8 Proposition. *Let R be a domain in which every nonzero nonunit is a product of irreducibles. The ring R to be a unique factorization domain if and only if, for any irreducible element $f \in R$, the ideal $\langle f \rangle$ is prime.*

Proof.

(⇒) Suppose that R is a unique factorization domain. If $g, h \in R$, and $gh \in \langle f \rangle$, then there exists a ring element $q \in R$ such that $gh = qf$. Factor g, h, and q into irreducibles. Uniqueness of factorization implies that the irreducible uf, for some unit $u \in R$ appears on the left side. This element arose as a factor of either g or h, so we see that $g \in \langle f \rangle$ or $h \in \langle f \rangle$. Proposition 2.3.8 shows the principal ideal $\langle f \rangle$ is prime.

(⇐) Suppose that any principal ideal generated by an irreducible element is prime. Consider two factorizations

$$g_1 \, g_2 \, \cdots \, g_m = h_1 \, h_2 \, \cdots \, h_n$$

where $g_j \in R$ and $h_k \in R$ are irreducible for all $1 \leqslant j \leqslant m$ and $1 \leqslant k \leqslant n$. We proceed, by induction on $\max\{m, n\} \geqslant 1$, to show that $m = n$ and $g_j = c_j \, h_{\sigma(j)}$ for some units c_j and $\sigma \in \mathfrak{S}_m$. The base step $\max\{m, n\} = 1$ has $g_1 = h_1$ and the claim is trivial. For the inductive step, the given equation shows that g_m divides $h_1 \, h_2 \, \cdots \, h_n$. By hypothesis, the ideal $\langle g_m \rangle$ is prime, so there exists $1 \leqslant k \leqslant n$ such that g_m divides h_k. Since h_k is irreducible, there exists a unit c_k such that $g_m = c_k h_k$. Canceling g_1 from both sides yields $g_1 \, g_2 \cdots g_{m-1} = c_k \, h_1 \, h_2 \, \cdots \, h_{k-1} \, h_{k+1} \cdots \, h_n$. The induction hypothesis establishes that $m - 1 = n - 1$ and $g_j = c_j \, h_{\sigma(j)}$ for some units $c_j \in R$, for all $2 \leqslant j \leqslant m - 1$, and $\sigma \in \mathfrak{S}_{m-1}$. □