Definition. Let R be a commutative ring and let $a, b \in R$ with $b \neq 0$.

(1) a is said to be a *multiple* of b if there exists an element $x \in R$ with $a = bx$. In this case b is said to *divide* a or be a *divisor* of a, written $b \mid a$.

(2) A *greatest common divisor* of a and b is a nonzero element d such that

(i) $d \mid a$ and $d \mid b$, and

(ii) if $d' \mid a$ and $d' \mid b$ then $d' \mid d$.

A greatest common divisor of a and b will be denoted by g.c.d.(a, b), or (abusing the notation) simply (a, b).

Note that $b \mid a$ in a ring R if and only if $a \in (b)$ if and only if $(a) \subseteq (b)$. In particular, if d is any divisor of both a and b then (d) must contain both a and b and hence must contain the ideal generated by a and b. The defining properties (i) and (ii) of a greatest common divisor of a and b translated into the language of ideals therefore become (respectively):

if I is the ideal of R generated by a and b, then d is a greatest common divisor of a and b if

(i) I is contained in the principal ideal (d), and

(ii) if (d') is any principal ideal containing I then $(d) \subseteq (d')$.

Thus a greatest common divisor of a and b (if such exists) is a generator for the unique smallest principal ideal containing a and b. There are rings in which greatest common divisors do not exist.

This discussion immediately gives the following *sufficient* condition for the existence of a greatest common divisor.

Proposition 2. If a and b are nonzero elements in the commutative ring R such that the ideal generated by a and b is a principal ideal (d), then d is a greatest common divisor of a and b.

This explains why the symbol (a, b) is often used to denote both the ideal generated by a and b and a greatest common divisor of a and b. An integral domain in which every ideal (a, b) generated by two elements is principal is called a *Bezout Domain*. The exercises in this and subsequent sections explore these rings and show that there are Bezout Domains containing nonprincipal (necessarily infinitely generated) ideals.

Note that the condition in Proposition 2 is *not* a *necessary* condition. For example, in the ring $R = \mathbb{Z}[x]$ the elements 2 and x generate a maximal, nonprincipal ideal (cf. the examples in Section 7.4). Thus $R = (1)$ is the unique principal ideal containing both 2 and x, so 1 is a greatest common divisor of 2 and x. We shall see other examples along these lines in Section 3.

Before returning to Euclidean Domains we examine the uniqueness of greatest common divisors.

Proposition 3. Let R be an integral domain. If two elements d and d' of R generate the same principal ideal, i.e., $(d) = (d')$, then $d' = ud$ for some unit u in R. In particular, if d and d' are both greatest common divisors of a and b, then $d' = ud$ for some unit u.

Proof: This is clear if either d or d' is zero so we may assume d and d' are nonzero. Since $d \in (d')$ there is some $x \in R$ such that $d = xd'$. Since $d' \in (d)$ there is some $y \in R$ such that $d' = yd$. Thus $d = xyd$ and so $d(1 - xy) = 0$. Since $d \neq 0$, $xy = 1$, that is, both x and y are units. This proves the first assertion. The second assertion follows from the first since any two greatest common divisors of a and b generate the same principal ideal (they divide each other).

One of the most important properties of Euclidean Domains is that greatest common divisors always exist and *can be computed algorithmically.*

Theorem 4. Let R be a Euclidean Domain and let a and b be nonzero elements of R. Let $d = r_n$ be the last nonzero remainder in the Euclidean Algorithm for a and b described at the beginning of this chapter. Then

(1) d is a greatest common divisor of a and b, and

(2) the principal ideal (d) is the ideal generated by a and b. In particular, d can be written as an *R-linear combination* of a and b, i.e., there are elements x and y in R such that

$$d = ax + by.$$

Proof: By Proposition 1, the ideal generated by a and b is principal so a, b do have a greatest common divisor, namely any element which generates the (principal) ideal (a, b). Both parts of the theorem will follow therefore once we show $d = r_n$ generates this ideal, i.e., once we show that

(i) $d \mid a$ and $d \mid b$ (so $(a, b) \subseteq (d)$)

(ii) d is an R-linear combination of a and b (so $(d) \subseteq (a, b)$).

To prove that d divides both a and b simply keep track of the divisibilities in the Euclidean Algorithm. Starting from the $(n+1)^{\text{st}}$ equation, $r_{n-1} = q_{n+1}r_n$, we see that $r_n \mid r_{n-1}$. Clearly $r_n \mid r_n$. By induction (proceeding from index n downwards to index 0) assume r_n divides r_{k+1} and r_k. By the $(k+1)^{\text{st}}$ equation, $r_{k-1} = q_{k+1}r_k + r_{k+1}$, and since r_n divides both terms on the right hand side we see that r_n also divides r_{k-1}. From the 1^{st} equation in the Euclidean Algorithm we obtain that r_n divides b and then from the 0^{th} equation we get that r_n divides a. Thus (i) holds.

To prove that r_n is in the ideal (a, b) generated by a and b proceed similarly by induction proceeding from equation (0) to equation (n). It follows from equation (0) that $r_0 \in (a, b)$ and by equation (1) that $r_1 = b - q_1r_0 \in (b, r_0) \subseteq (a, b)$. By induction assume $r_{k-1}, r_k \in (a, b)$. Then by the $(k+1)^{\text{st}}$ equation

$$r_{k+1} = r_{k-1} - q_{k+1}r_k \in (r_{k-1}, r_k) \subseteq (a, b).$$

This induction shows $r_n \in (a, b)$, which completes the proof.

Much of the material above may be familiar from elementary arithmetic in the case of the integers $\mathbb{Z}$, except possibly for the translation into the language of ideals. For example, if $a = 2210$ and $b = 1131$ then the smallest ideal of $\mathbb{Z}$ that contains both a and b (the ideal generated by a and b) is $13\mathbb{Z}$, since 13 is the greatest common divisor of 2210 and 1131. This fact follows quickly from the Euclidean Algorithm:

$$2210 = 1 \cdot 1131 + 1079$$

$$1131 = 1 \cdot 1079 + 52$$
$$1079 = 20 \cdot 52 + 39$$
$$52 = 1 \cdot 39 + 13$$
$$39 = 3 \cdot 13$$

so that $13 = (2210, 1131)$ is the last nonzero remainder. Using the procedure of Theorem 4 we can also write 13 as a linear combination of 2210 and 1131 by first solving the next to last equation above for $13 = 52 - 1 \cdot 39$, then using previous equations to solve for 39 and 52, etc., finally writing 13 entirely in terms of 2210 and 1131. The answer in this case is

$$13 = (-22) \cdot 2210 + 43 \cdot 1131.$$

The Euclidean Algorithm in the integers $\mathbb{Z}$ is extremely fast. It is a theorem that the number of steps required to determine the greatest common divisor of two integers a and b is at worst 5 times the number of digits of the smaller of the two numbers. Put another way, this algorithm is *logarithmic* in the size of the integers. To obtain an appreciation of the speed implied here, notice that for the example above we would have expected at worst $5 \cdot 4 = 20$ divisions (the example required far fewer). If we had started with integers on the order of 10^{100} (large numbers by physical standards), we would have expected at worst only 500 divisions.

There is no uniqueness statement for the integers x and y in $(a, b) = ax + by$. Indeed, $x' = x + b$ and $y' = y - a$ satisfy $(a, b) = ax' + by'$. This is essentially the only possibility — one can prove that if x_0 and y_0 are solutions to the equation $ax + by = N$, then any other solutions x and y to this equation are of the form

$$x = x_0 + m\frac{b}{(a, b)}$$
$$y = y_0 - m\frac{a}{(a, b)}$$

for some integer m (positive or negative).

This latter theorem (a proof of which is outlined in the exercises) provides a complete solution of the *First Order Diophantine Equation* $ax + by = N$ provided we know there is *at least one* solution to this equation. But the equation $ax + by = N$ is simply another way of stating that N is an element of the ideal generated by a and b. Since we know this ideal is just (d), the principal ideal generated by the greatest common divisor d of a and b, this is the same as saying $N \in (d)$, i.e., N is divisible by d. Hence, *the equation* $ax + by = N$ *is solvable in integers* x *and* y *if and only if* N *is divisible by the g.c.d. of* a *and* b (and then the result quoted above gives a full set of solutions of this equation).

We end this section with another criterion that can sometimes be used to prove that a given integral domain is not a Euclidean Domain.[1] For any integral domain let

[1]The material here and in some of the following section follows the exposition by J.C. Wilson in *A principal ideal ring that is not a Euclidean ring*, Math. Mag., 46(1973), pp. 34–38, of ideas of Th. Motzkin, and use a simplification by Kenneth S. Williams in *Note on non-Euclidean Principal Ideal Domains*, Math. Mag., 48(1975), pp. 176–177.