32. Let R be any ring. The **ascending chain condition** (ACC) **for ideals** holds in R if every strictly increasing sequence $N_1 \subset N_2 \subset N_3 \subset \cdots$ of ideals in R is of finite length. The **maximum condition** (MC) **for ideals** holds in R if every nonempty set S of ideals in R contains an ideal not properly contained in any other ideal of the set S. The **finite basis condition** (FBC) **for ideals** holds in R if for each ideal N in R, there is a finite set $B_N = \{b_1, \cdots, b_n\} \subseteq N$ such that N is the intersection of all ideals of R containing B_N. The set B_N is a **finite generating set for** N.

Show that for every ring R, the conditions ACC, MC, and FBC are equivalent.

33. Let R be any ring. The **descending chain condition** (DCC) **for ideals** holds in R if every strictly decreasing sequence $N_1 \supset N_2 \supset N_3 \supset \cdots$ of ideals in R is of finite length. The **minimum condition** (mC) **for ideals** holds in R if given any set S of ideals of R, there is an ideal of S that does not properly contain any other ideal in the set S.

Show that for every ring, the conditions DCC and mC are equivalent.

34. Give an example of a ring in which ACC holds but DCC does not hold. (See Exercises 32 and 33.)

SECTION 35 EUCLIDEAN DOMAINS

We have remarked several times on the importance of division algorithms. Our first contact with them was the *division algorithm for* $\mathbb{Z}$ in Section 6. This algorithm was used to prove the important theorem that a subgroup of a cyclic group is cyclic, that is, has a single generator. Of course, this shows at once that $\mathbb{Z}$ is a PID. The *division algorithm for* $F[x]$ appeared in Theorem 28.2 and was used in a completely analogous way to show that $F[x]$ is a PID. A technique of mathematics is to take some clearly related situations and to try to bring them under one roof by abstracting the important ideas common to them. The following definition is an illustration of this technique, as is this whole text! Let us see what we can develop by starting with the existence of a fairly general division algorithm in an integral domain.

35.1 Definition A **Euclidean norm** on an integral domain D is a function ν mapping the nonzero elements of D into the nonnegative integers such that the following conditions are satisfied:

1. For all $a, b \in D$ with $b \neq 0$, there exist q and r in D such that $a = bq + r$, where either $r = 0$ or $\nu(r) < \nu(b)$.
2. For all $a, b \in D$, where neither a nor b is 0, $\nu(a) \leq \nu(ab)$.

An integral domain D is a **Euclidean domain** if there exists a Euclidean norm on D. ■

The importance of Condition 1 is clear from our discussion. The importance of Condition 2 is that it will enable us to characterize the units of a Euclidean domain D.

35.2 Example The integral domain $\mathbb{Z}$ is a Euclidean domain, for the function ν defined by $\nu(n) = |n|$ for $n \neq 0$ in $\mathbb{Z}$ is a Euclidean norm on $\mathbb{Z}$. Condition 1 holds by the division algorithm for $\mathbb{Z}$. Condition 2 follows from $|ab| = |a||b|$ and $|a| \geq 1$ for $a \neq 0$ in $\mathbb{Z}$. ▲

35.3 Example If F is a field, then $F[x]$ is a Euclidean domain, for the function ν defined by $\nu(f(x)) =$ (degree $f(x)$) for $f(x) \in F[x]$, and $f(x) \neq 0$ is a Euclidean norm. Condition 1 holds by Theorem 28.2, and Condition 2 holds since the degree of the product of two polynomials is the sum of their degrees. ▲

Of course, we should give some examples of Euclidean domains other than these familiar ones that motivated the definition. We shall do this in Section 36. In view of the opening remarks, we anticipate the following theorem.

35.4 Theorem Every Euclidean domain is a PID.

Proof Let D be a Euclidean domain with a Euclidean norm ν, and let N be an ideal in D. If $N = \{0\}$, then $N = \langle 0 \rangle$ and N is principal. Suppose that $N \neq \{0\}$. Then there exists $b \neq 0$ in N. Let us choose b such that $\nu(b)$ is minimal among all $\nu(n)$ for $n \in N$. We claim that $N = \langle b \rangle$. Let $a \in N$. Then by Condition 1 for a Euclidean domain, there exist q and r in D such that

$$a = bq + r,$$

where either $r = 0$ or $\nu(r) < \nu(b)$. Now $r = a - bq$ and $a, b \in N$, so that $r \in N$ since N is an ideal. Thus $\nu(r) < \nu(b)$ is impossible by our choice of b. Hence $r = 0$, so $a = bq$. Since a was any element of N, we see that $N = \langle b \rangle$. ◆

35.5 Corollary A Euclidean domain is a UFD.

Proof By Theorem 35.4, a Euclidean domain is a PID and by Theorem 34.18, a PID is a UFD. ◆

Finally, we should mention that while a Euclidean domain is a PID by Theorem 35.4, not every PID is a Euclidean domain. Examples of PIDs that are not Euclidean are not easily found, however.

Arithmetic in Euclidean Domains

We shall now investigate some properties of Euclidean domains related to their multiplicative structure. We emphasize that the arithmetic structure of a Euclidean domain is not affected in any way by a Euclidean norm ν on the domain. A Euclidean norm is merely a useful tool for possibly throwing some light on this arithmetic structure of the domain. The arithmetic structure of a domain D is completely determined by the set D and the two binary operations $+$ and $\cdot$ on D.

Let D be a Euclidean domain with a Euclidean norm ν. We can use Condition 2 of a Euclidean norm to characterize the units of D.

35.6 Theorem For a Euclidean domain with a Euclidean norm ν, $\nu(1)$ is minimal among all $\nu(a)$ for nonzero $a \in D$, and $u \in D$ is a unit if and only if $\nu(u) = \nu(1)$.

Proof Condition 2 for ν tells us at once that for $a \neq 0$,

$$\nu(1) \leq \nu(1a) = \nu(a).$$

On the other hand, if u is a unit in D, then

$$\nu(u) \leq \nu(uu^{-1}) = \nu(1).$$

Thus

$$\nu(u) = \nu(1)$$

for a unit u in D.

Conversely, suppose that a nonzero $u \in D$ is such that $\nu(u) = \nu(1)$. Then by the division algorithm, there exist q and r in D such that

$$1 = uq + r,$$

where either $r = 0$ or $\nu(r) < \nu(u)$. But since $\nu(u) = \nu(1)$ is minimal over all $\nu(d)$ for nonzero $d \in D$, $\nu(r) < \nu(u)$ is impossible. Hence $r = 0$ and $1 = uq$, so u is a unit. ◆

HISTORICAL NOTE

The Euclidean algorithm appears in Euclid's *Elements* as propositions 1 and 2 of Book VII, where it is used as here to find the greatest common divisor of two integers. Euclid uses it again in Book X (propositions 2 and 3) to find the greatest common measure of two magnitudes (if it exists) and to determine whether two magnitudes are incommensurable.

The algorithm appears again in the *Brahmesphutasiddhanta* (Correct Astronomical System of Brahma) (628) of the seventh-century Indian mathematician and astronomer Brahmagupta. To solve the indeterminate equation $rx + c = sy$ in integers, Brahmagupta uses Euclid's procedure to "reciprocally divide" r by s until he reaches the final nonzero remainder. By then using, in effect, a substitution procedure based on the various quotients and remainders, he produces a straightforward algorithm for finding the smallest positive solution to his equation.

The thirteenth-century Chinese algebraist Qin Jiushao also used the Euclidean algorithm in his solution of the so-called Chinese Remainder problem published in the *Shushu jiuzhang* (Mathematical Treatise in Nine Sections) (1247). Qin's goal was to display a method for solving the system of congruences $N \equiv r_i \pmod{m_i}$. As part of that method he needed to solve congruences of the form $Nx \equiv 1 \pmod{m}$, where N and m are relatively prime. The solution to a congruence of this form is again found by a substitution procedure, different from the Indian one, using the quotients and remainders from the Euclidean algorithm applied to N and m. It is not known whether the common element in the Indian and Chinese algorithms, the Euclidean algorithm itself, was discovered independently in these cultures or was learned from Greek sources.

35.7 Example For $\mathbb{Z}$ with $\nu(n) = |n|$, the minimum of $\nu(n)$ for nonzero $n \in \mathbb{Z}$ is 1, and 1 and -1 are the only elements of $\mathbb{Z}$ with $\nu(n) = 1$. Of course, 1 and -1 are exactly the units of $\mathbb{Z}$. ▲

35.8 Example For $F[x]$ with $\nu(f(x)) = (\text{degree}\, f(x))$ for $f(x) \neq 0$, the minimum value of $\nu(f(x))$ for all nonzero $f(x) \in F[x]$ is 0. The nonzero polynomials of degree 0 are exactly the nonzero elements of F, and these are precisely the units of $F[x]$. ▲

We emphasize that everything we prove here holds in *every* Euclidean domain, in particular in $\mathbb{Z}$ and $F[x]$. As indicated in Example 34.21, we can show that any a and b in a UFD have a gcd and actually compute one by factoring a and b into irreducibles, but such factorizations can be very tough to find. However, if a UFD is actually Euclidean, and we know an easily computed Euclidean norm, there is an easy constructive way to find gcd's, as the next theorem shows.

35.9 Theorem **(Euclidean Algorithm)** Let D be a Euclidean domain with a Euclidean norm ν, and let a and b be nonzero elements of D. Let r_1 be as in Condition 1 for a Euclidean norm, that is,

$$a = bq_1 + r_1,$$

where either $r_1 = 0$ or $\nu(r_1) < \nu(b)$. If $r_1 \neq 0$, let r_2 be such that

$$b = r_1 q_2 + r_2,$$

where either $r_2 = 0$ or $\nu(r_2) < \nu(r_1)$. In general, let r_{i+1} be such that

$$r_{i-1} = r_i q_{i+1} + r_{i+1},$$

where either $r_{i+1} = 0$ or $\nu(r_{i+1}) < \nu(r_i)$. Then the sequence $r_i, r_2, \cdots$ must terminate with some $r_s = 0$. If $r_1 = 0$, then b is a gcd of a and b. If $r_1 \neq 0$ and r_s is the first $r_i = 0$, then a gcd of a and b is r_{s-1}.