The importance of the existence of a Division Algorithm on an integral domain R is that it allows a *Euclidean Algorithm* for two elements a and b of R: by successive "divisions" (these actually *are* divisions in the field of fractions of R) we can write

$$a = q_0 b + r_0 \tag{0}$$

$$b = q_1 r_0 + r_1 \tag{1}$$

$$r_0 = q_2 r_1 + r_2 \tag{2}$$

$$\vdots$$

$$r_{n-2} = q_n r_{n-1} + r_n \tag{n}$$

$$r_{n-1} = q_{n+1} r_n \tag{$n+1$}$$

where r_n is the last nonzero remainder. Such an r_n exists since $N(b) > N(r_0) > N(r_1) > \cdots > N(r_n)$ is a decreasing sequence of nonnegative integers if the remainders are nonzero, and such a sequence cannot continue indefinitely. Note also that there is no guarantee that these elements are *unique*.

Examples

(0) Fields are trivial examples of Euclidean Domains where any norm will satisfy the defining condition (e.g., $N(a) = 0$ for all a). This is because for every a, b with $b \neq 0$ we have $a = qb + 0$, where $q = ab^{-1}$.

(1) The integers $\mathbb{Z}$ are a Euclidean Domain with norm given by $N(a) = |a|$, the usual absolute value. The existence of a Division Algorithm in $\mathbb{Z}$ (the familiar "long division" of elementary arithmetic) is verified as follows. Let a and b be two nonzero integers and suppose first that $b > 0$. The half open intervals $[nb, (n+1)b)$, $n \in \mathbb{Z}$ partition the real line and so a is in one of them, say $a \in [kb, (k+1)b)$. For $q = k$ we have $a - qb = r \in [0, |b|)$ as needed. If $b < 0$ (so $-b > 0$), by what we have just seen there is an integer q such that $a = q(-b) + r$ with either $r = 0$ or $|r| < |-b|$; then $a = (-q)b + r$ satisfies the requirements of the Division Algorithm for a and b. This argument can be made more formal by using induction on $|a|$.

Note that if a is not a multiple of b there are always two possibilities for the pair q, r: the proof above always produced a positive remainder r. If for example $b > 0$ and q, r are as above with $r > 0$, then $a = q'b + r'$ with $q' = q + 1$ and $r' = r - b$ also satisfy the conditions of the Division Algorithm applied to a, b. Thus $5 = 2 \cdot 2 + 1 = 3 \cdot 2 - 1$ are the two ways of applying the Division Algorithm in $\mathbb{Z}$ to $a = 5$ and $b = 2$. The quotient and remainder are unique if we require the remainder to be nonnegative.

(2) If F is a field, then the polynomial ring $F[x]$ is a Euclidean Domain with norm given by $N(p(x)) =$ the degree of $p(x)$. The Division Algorithm for polynomials is simply "long division" of polynomials which may be familiar for polynomials with real coefficients. The proof is very similar to that for $\mathbb{Z}$ and is given in the next chapter (although for polynomials the quotient and remainder are shown to be unique). In order for a polynomial ring to be a Euclidean Domain the coefficients must come from a field since the division algorithm ultimately rests on being able to divide arbitrary nonzero coefficients. We shall prove in Section 2 that $R[x]$ is not a Euclidean Domain if R is not a field.

(3) The quadratic integer rings $\mathcal{O}$ in Section 7.1 are integral domains with a norm defined by the absolute value of the field norm (to ensure the values taken are nonnegative;

when $D < 0$ the field norm is itself a norm), but in general $\mathcal{O}$ is not Euclidean with respect to this norm (or any other norm). The Gaussian integers $\mathbb{Z}[i]$ (where $D = -1$), however, are a Euclidean Domain with respect to the norm $N(a+bi) = a^2 + b^2$, as we now show (cf. also the end of Section 3).

Let $\alpha = a+bi$, $\beta = c+di$ be two elements of $\mathbb{Z}[i]$ with $\beta \neq 0$. Then in the field $\mathbb{Q}(i)$ we have $\dfrac{\alpha}{\beta} = r+si$ where $r = (ac+bd)/(c^2+d^2)$ and $s = (bc-ad)/(c^2+d^2)$ are rational numbers. Let p be an integer closest to the rational number r and let q be an integer closest to the rational number s, so that both $|r-p|$ and $|s-q|$ are at most $1/2$. The Division Algorithm follows immediately once we show

$$\alpha = (p+qi)\beta + \gamma \qquad \text{for some } \gamma \in \mathbb{Z}[i] \text{ with } \quad N(\gamma) \leq \frac{1}{2}N(\beta)$$

which is even stronger than necessary. Let $\theta = (r-p) + (s-q)i$ and set $\gamma = \beta\theta$. Then $\gamma = \alpha - (p+qi)\beta$, so that $\gamma \in \mathbb{Z}[i]$ is a Gaussian integer and $\alpha = (p+qi)\beta + \gamma$. Since $N(\theta) = (r-p)^2 + (s-q)^2$ is at most $1/4 + 1/4 = 1/2$, the multiplicativity of the norm N implies that $N(\gamma) = N(\theta)N(\beta) \leq \dfrac{1}{2}N(\beta)$ as claimed.

Note that the algorithm is quite explicit since a quotient $p+qi$ is quickly determined from the rational numbers r and s, and then the remainder $\gamma = \alpha - (p+qi)\beta$ is easily computed. Note also that the quotient need not be unique: if r (or s) is half of an odd integer then there are two choices for p (or for q, respectively).

This proof that $\mathbb{Z}[i]$ is a Euclidean Domain can also be used to show that $\mathcal{O}$ is a Euclidean Domain (with respect to the field norm defined in Section 7.1) for $D = -2, -3, -7, -11$ (cf. the exercises). We shall see shortly that $\mathbb{Z}[\sqrt{-5}]$ is not Euclidean with respect to any norm, and a proof that $\mathbb{Z}[(1+\sqrt{-19})/2]$ is not a Euclidean Domain with respect to any norm appears at the end of this section.

(4) Recall (cf. Exercise 26 in Section 7.1) that a *discrete valuation ring* is obtained as follows. Let K be a field. A *discrete valuation* on K is a function $\nu : K^\times \to \mathbb{Z}$ satisfying

(i) $\nu(ab) = \nu(a) + \nu(b)$ (i.e., ν is a homomorphism from the multiplicative group of nonzero elements of K to $\mathbb{Z}$),

(ii) ν is surjective, and

(iii) $\nu(x+y) \geq \min\{\nu(x), \nu(y)\}$ for all $x, y \in K^\times$ with $x + y \neq 0$.

The set $\{x \in K^\times \mid \nu(x) \geq 0\} \cup \{0\}$ is a subring of K called the valuation ring of ν. An integral domain R is called a discrete valuation ring if there is a valuation ν on its field of fractions such that R is the valuation ring of ν.

For example the ring R of all rational numbers whose denominators are relatively prime to the fixed prime $p \in \mathbb{Z}$ is a discrete valuation ring contained in $\mathbb{Q}$.

A discrete valuation ring is easily seen to be a Euclidean Domain with respect to the norm defined by $N(0) = 0$ and $N = \nu$ on the nonzero elements of R. This is because for $a, b \in R$ with $b \neq 0$

(a) if $N(a) < N(b)$ then $a = 0 \cdot b + a$, and

(b) if $N(a) \geq N(b)$ then it follows from property (i) of a discrete valuation that $q = ab^{-1} \in R$, so $a = qb + 0$.

The first implication of a Division Algorithm for the integral domain R is that it forces every ideal of R to be *principal.*

Proposition 1. Every ideal in a Euclidean Domain is principal. More precisely, if I is any nonzero ideal in the Euclidean Domain R then $I = (d)$, where d is any nonzero element of I of minimum norm.

Proof: If I is the zero ideal, there is nothing to prove. Otherwise let d be any nonzero element of I of minimum norm (such a d exists since the set $\{N(a) \mid a \in I\}$ has a minimum element by the Well Ordering of $\mathbb{Z}$). Clearly $(d) \subseteq I$ since d is an element of I. To show the reverse inclusion let a be any element of I and use the Division Algorithm to write $a = qd + r$ with $r = 0$ or $N(r) < N(d)$. Then $r = a - qd$ and both a and qd are in I, so r is also an element of I. By the minimality of the norm of d, we see that r must be 0. Thus $a = qd \in (d)$ showing $I = (d)$.

Proposition 1 shows that every ideal of $\mathbb{Z}$ is principal. This fundamental property of $\mathbb{Z}$ was previously determined (in Section 7.3) from the (additive) group structure of $\mathbb{Z}$, using the classification of the subgroups of cyclic groups in Section 2.3. Note that these are really the same proof, since the results in Section 2.3 ultimately relied on the Euclidean Algorithm in $\mathbb{Z}$.

Proposition 1 can also be used to prove that some integral domains R are *not* Euclidean Domains (with respect to *any* norm) by proving the existence of ideals of R that are not principal.

Examples

(1) Let $R = \mathbb{Z}[x]$. Since the ideal $(2, x)$ is not principal (cf. Example 3 at the beginning of Section 7.4), it follows that the ring $\mathbb{Z}[x]$ of polynomials with *integer* coefficients is *not* a Euclidean Domain (for any choice of norm), even though the ring $\mathbb{Q}[x]$ of polynomials with *rational* coefficients is a Euclidean Domain.

(2) Let R be the quadratic integer ring $\mathbb{Z}[\sqrt{-5}]$, let N be the associated field norm $N(a+b\sqrt{-5}) = a^2+5b^2$ and consider the ideal $I = (3, 2+\sqrt{-5})$ generated by 3 and $2+\sqrt{-5}$. Suppose $I = (a+b\sqrt{-5})$, $a, b \in \mathbb{Z}$, were principal, i.e., $3 = \alpha(a+b\sqrt{-5})$ and $2+\sqrt{-5} = \beta(a+b\sqrt{-5})$ for some $\alpha, \beta \in R$. Taking norms in the first equation gives $9 = N(\alpha)(a^2+5b^2)$ and since a^2+5b^2 is a positive integer it must be 1,3 or 9. If the value is 9 then $N(\alpha) = 1$ and $\alpha = \pm 1$, so $a+b\sqrt{-5} = \pm 3$, which is impossible by the second equation since the coefficients of $2+\sqrt{-5}$ are not divisible by 3. The value cannot be 3 since there are no integer solutions to $a^2+5b^2 = 3$. If the value is 1, then $a+b\sqrt{-5} = \pm 1$ and the ideal I would be the entire ring R. But then 1 would be an element of I, so $3\gamma + (2+\sqrt{-5})\delta = 1$ for some $\gamma, \delta \in R$. Multiplying both sides by $2-\sqrt{-5}$ would then imply that $2-\sqrt{-5}$ is a multiple of 3 in R, a contradiction. It follows that I is not a principal ideal and so R is not a Euclidean Domain (with respect to any norm).

One of the fundamental consequences of the Euclidean Algorithm in $\mathbb{Z}$ is that it produces a greatest common divisor of two nonzero elements. This is true in any Euclidean Domain. The notion of a greatest common divisor of two elements (if it exists) can be made precise in general rings.