7. Euclidean Domains

Let R be an integral domain. We want to find natural conditions on R such that R is a PID. Looking at the case of the integers, it is clear that the key property is the division algorithm.

Definition 7.1. *Let R be an integral domain. We say that R is **Euclidean**, if there is a function*

$$d\colon R - \{0\} \longrightarrow \mathbb{N} \cup \{0\},$$

which satisfies, for every pair of non-zero elements a and b of R,

(1)

$$d(a) \leq d(ab).$$

(2) There are elements q and r of R such that

$$b = aq + r,$$

where either $r = 0$ or $d(r) < d(a)$.

Example 7.2. *The ring $\mathbb{Z}$ is a Euclidean domain. The function d is the absolute value.*

Definition 7.3. *Let R be a ring and let $f \in R[x]$ be a non-zero polynomial with coefficients in R. The **degree** of f is the largest n such that the coefficient of x^n is non-zero.*

Lemma 7.4. *Let R be an integral domain and let f and g be two non-zero elements of $R[x]$.*

Then fg is non-zero and its degree is the sum of the degrees of f and g. In particular $R[x]$ is an integral domain.

Proof. Suppose that f has degree m and g has degree n. If a is the leading coefficient of f and b is the leading coefficient of g then

$$f = ax^m + \dots \qquad \text{and} \qquad f = bx^n + \dots,$$

where $\dots$ indicate lower degree terms and

$$fg = (ab)x^{m+n} + \dots.$$

As R is an integral domain, $ab \neq 0$, so that fg is non-zero and the degree of fg is $m + n$. □

Definition-Lemma 7.5. *Let k be a field and let $R = k[x]$ be the polynomial ring. Define a function*

$$d\colon R - \{0\} \longrightarrow \mathbb{N} \cup \{0\}$$

by sending f to its degree.

Then R is a Euclidean domain.

Proof. The first property of d follows from (7.4).

We prove the second property. Suppose that we are given two polynomials f and g. We want to divide f into g. We proceed by induction on the degree of g. If the degree of g is less than the degree of f, there is nothing to prove, take $q = 0$ and $r = g$. Suppose the result holds for all degrees less than the degree of g. We may suppose that

$$g = bx^n + g_1 \qquad \text{and} \qquad f = ax^m + f_1,$$

where f_1 and g_1 are of degree less than m and n. Put $q_0 = cx^{n-m}$, where $c = b/a$. Let $h = g - q_0 f$. Then h has degree less than g. By induction then,

$$h = q_1 f + r,$$

where r has degree less than f. It follows that

$$\begin{aligned} g &= h + q_0 f \\ &= (q_0 + q_1) f + r \\ &= qf + r, \end{aligned}$$

where $q = q_0 + q_1$. □

Definition-Lemma 7.6. *Let $R = \mathbb{Z}[i]$ be the ring of Gaussian integers. Define a function*

$$d\colon R - \{0\} \longrightarrow \mathbb{N} \cup \{0\},$$

by sending $a + bi$ to its norm, which is by definition $a^2 + b^2$.

Then the ring of Gaussian integers is a Euclidean domain.

Proof. Note first that if z is a complex number, then the absolute value of z, defined as the square root of the product of z with its complex conjugate $\bar{z}$, is closely related to the norm of z.

In fact if z is a Gaussian integer $x + iy$, then

$$|z|^2 = z\bar{z} = x^2 + y^2 = d(z).$$

On the other hand, suppose we use polar coordinates, rather than Cartesian coordinates, to represent a complex number,

$$z = re^{i\theta}.$$

Then $r = |z|$.

For any pair z_1 and z_2 of complex numbers, we have

$$|z_1 z_2| = |z_1||z_2|.$$

Indeed this is clear if we use polar coordinates. Now suppose that both z_1 and z_2 are Gaussian integers. If we square both sides of the equation above, we get

$$d(z_1 z_2) = d(z_1) d(z_2).$$

As the absolute value of a Gaussian integer is always at least one, (1) follows easily.

To prove (2), it helps to think about this problem geometrically. First note that one may think of the Gaussian integers as being all points in the plane with integer coordinates. Fix a Gaussian integer α. To obtain all multiples of $\alpha = re^{i\theta}$, that is, the principal ideal $\langle\alpha\rangle$, it suffices to take this lattice, rotate it through an angle of θ and stretch it by an amount r. With this picture, it is clear that given any other Gaussian integer β, there is a multiple of α, call it $q\alpha$, such that the square of the distance between β and $q\alpha$ is at most $r^2/2$. Indeed let $\gamma = \beta/\alpha$. Pick a Gaussian integer q such that the square of the distance between γ and q is at most $1/2$. Then the distance between $\beta = \gamma\alpha$ and $q\alpha$ is at most $r^2/2$. Thus we may write

$$\beta = q\alpha + r,$$

(different r of course) such that $d(r) < d(\alpha)$. □

It might help to see a simple example of how this works in practice. Suppose that we take $a = 1 + i$ and $b = 4 - 5i$. The first step is to construct

$$c = \frac{b}{a}.$$

Now $a\bar{a} = 1^2 + 1^2 = 2$, so that the inverse of a is

$$\frac{\bar{a}}{2} = \frac{1-i}{2}.$$

Multiplying by b we get

$$\begin{aligned} c &= \frac{\bar{a}b}{2} \\ &= \frac{1}{2}(1-i)(4-5i) \\ &= -\frac{1}{2}(1+9i) \\ &= -\frac{1}{2} - \frac{9}{2}i. \end{aligned}$$

Now we pick a Gaussian integer that is no more than a distance of 1 from c. For example $-4i$ will do (indeed any one of $-1-5i$, $-5i$, $-4i$ and $-1-4i$ will work). This is our quotient q. The error at this point is

$$s = c - q = -(\frac{1}{2} + \frac{i}{2}).$$

Now multiplying both sides by a, we get

$$r = sa = b - qa,$$

so that

$$b = qa + r.$$

Thus

$$r = -\frac{1}{2}(1+i)^2 = -i.$$

Clearly

$$d(r) = 1 = 2d(s) < d(a) = 2,$$

as required.

Lemma 7.7. *Every Euclidean domain is a PID.*

In particular every Euclidean domain is a UFD.

Proof. Let I be an ideal in a Euclidean domain. We want to show that I is a principal ideal. If I is the zero ideal then $I = \langle 0 \rangle$. Otherwise, pick $a \neq 0$ an element of I, such that $d(a)$ is minimal. I claim that $I = \langle a \rangle$. Suppose not. Clearly $\langle a \rangle \subset I$, so that there must be an element $b \in I$ such that $b \notin \langle a \rangle$.

We may write

$$b = qa + r,$$

where $d(r) < d(a)$ and by assumption $r \neq 0$. But $r = b - qa \in I$, and $d(r) < d(a)$, which contradicts our choice of a. □

Corollary 7.8. *The Gaussian integers and the polynomials over any field are a UFD.*

Of course, one reason why the division algorithm is so interesting, is that it furnishes a method to construct the gcd of two natural numbers a and b, using Euclid's algorithm. Clearly the same method works in an arbitrary Euclidean domain.