5. Types of domains

It turns out that in number theory the fact that certain rings have unique factorisation has very strong arithmetic consequences.

We first write down some definitions.

Definition 5.1. *Let R be an integral domain.*

*If a and b are two elements of R then we say that a **divides** b, denoted $a|b$, if $b = ac$. We say that $u \in R$ is a **unit** if u has a multiplicative inverse, that is, there is an element $v \in R$ such that $uv = 1 = vu$. We say that a and b are **associates** if $a|b$ and $b|a$. We say that p is **prime**, if the only divisors of p are units or associates of p.*

Lemma 5.2. *Let R be an integral domain and let a and b be two non-zero elements of R.*

The following are equivalent:

(1) a and b are associates.
(2) There is a unit u such that $a = ub$.

Proof. Suppose that (1) holds. As $a|b$ we may find $c \in R$ such that $b = ac$. As $b|a$ we may find $d \in R$ such that $a = bd$. In this case

$$\begin{aligned} a &= bd \\ &= (cd)a. \end{aligned}$$

Cancelling, we see that $cd = 1$. Thus d is a unit and so (2) holds.

Now suppose that (2) holds. Then certainly $b|a$. As u is a unit, it follows $uv = 1$ for some $v \in R$. But then

$$\begin{aligned} va &= v(ub) \\ &= (vu)b \\ &= 1 \cdot b \\ &= b. \end{aligned}$$

Thus $a|b$ and so a and b are associates. Thus (2) implies (1). □

In the ring $\mathbb{Z}$, the units are ±1 and so the associates of 2 are ±2, etc.

In general it can be quite hard to decide if a ring is a UFD (unique factorisation domain, that is, unique factorisation holds in R). There is one case it is relatively easy:

Definition 5.3. *An integral domain is called a **Euclidean domain** if there is a function*

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

such that for every pair of non-zero elements a and b of R we have:

(1) $s(ab) \geq s(b)$ with equality if and only if a is a unit.

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

$$a = qb + r$$

where either $r = 0$ or $s(r) < s(b)$.

The integers is a Euclidean domain where $s(a) = |a|$.

Theorem 5.4. *The Gaussian integers*

$$\mathbb{Z}[i] = \{\, a + bi \mid a, b \in \mathbb{Z} \,\},$$

is a Euclidean domain.

Proof. We have already seen that $\mathbb{Z}[i]$ is an integral domain; in fact $\mathbb{C}$ is a field (meaning you can add, subtract, multiply and divide by non-zero elements of $\mathbb{C}$) and any subset of a field which is closed under addition, subtraction, and multiplication is automatically an integral domain.

We define

$$s \colon \mathbb{Z}[i] - \{0\} \longrightarrow \mathbb{N}$$

by sending $\alpha = a + bi$ to $a^2 + b^2$.

To see properties (1) and (2), it helps to think of complex numbers in polar coordinates:

$$\alpha = a + bi = re^{i\theta}.$$

Here r is the distance to the origin and θ is the angle the line connecting $(0, 0)$ to (a, b) makes with the real line. Note that $s(\alpha) = r^2$, by Pythagoras.

Note that $\alpha = a + bi$ is a unit if its multiplicative inverse in $\mathbb{C}$ is a Gaussian integer.

$$\begin{aligned} \frac{1}{\alpha} &= \frac{1}{a + bi} \\ &= \frac{a - bi}{(a + bi)(a - bi)} \\ &= \frac{a - bi}{a^2 + b^2}. \end{aligned}$$

For this to be a Gaussian integer we need,

$$\frac{a}{a^2 + b^2} \qquad \text{and} \qquad \frac{b}{a^2 + b^2}$$

to be integers. It is easy to see this is only possible if $a^2 + b^2 = 1$, that is, $a = \pm 1$ and $b = 0$, or $a = 0$ and $b = \pm 1$. Therefore the units of the Gaussian integers are 1, -1, i and $-i$.

(1) is an exercise for the reader. To see (2) it might help to understand geometrically how complex multiplication works. In polar coordinates we multiply the two distances to the origin and we add the two angles. If we want to divide β into α and get a small remainder, we have to understand all possible multiples of β. The Gaussian integers form a square lattice with integer vertices; after we multiply by β this lattice gets rotated through an angle of θ and it is dilated by the factor r, the distance of β to origin, so that the squares of the lattice are skew and they have sides of length r. So we can always find a point of the new lattice within $r^2/2$, by Pythagoras.

Algebraically we proceed as follows. We can divide β into α to get a complex number γ,

$$\gamma = \frac{\alpha}{\beta} \in \mathbb{C}.$$

The only problem is that γ is not necessarily a Gaussian integer. Pick the closest Gaussian integer q to γ. Note that the square of the distance from γ to q is at most $1/2$ (when γ is at the centre of a unit square with integer coordinates). If we multiply both sides by β distances get rescalled by a factor of r. It follows that the square of the distance between α and $q\beta$ is at most $r^2/2$. Thus

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

where either $\rho = 0$ or

$$s(\rho) \leq \frac{r^2}{2} < r^2 = s(\beta). \qquad \square$$

Definition 5.5. *We say that an integral domain R is a* ***unique factorisation domain*** *(abbreviated to UFD) if every non-zero element a of R is a product of a unit u and primes $p_1, p_2, \dots, p_k$,*

$$a = up_1p_2 \dots p_k,$$

where the factorisation is unique up to re-ordering and associates.

Note that for the integers we might write

$$-6 = 2 \cdot (-3) = 3 \cdot (-2).$$

Theorem 5.6. *Every Euclidean domain R is a UFD.*

The easiest thing to check is that every element of R is either a unit or a product of primes:

Lemma 5.7. *Let R be a Euclidean domain.*

If a is neither zero nor a unit then a is a product of primes.

Proof. We may suppose that $a \neq 0$. We proceed by induction on $s(a) \in \mathbb{N}$. If $s(a) = 1$ then a is a unit and there is nothing to prove. Suppose that we know the result for all natural numbers less than $s(a)$.

There are two cases. If a is prime then we are done. Otherwise, we may write $a = bc$, where b and c are not units. In this case

$$s(b) < s(a) \qquad \text{and} \qquad s(c) < s(a).$$

By induction we may find primes $q_1, q_2, \dots, q_k$ and $r_1, r_2, \dots, r_l$ such that

$$b = q_1 q_2 \dots q_k \qquad \text{and} \qquad c = r_1 r_2 \dots r_l.$$

In this case

$$\begin{aligned} a &= bc \\ &= q_1 q_2 \dots q_k \cdot r_1 r_2 \dots r_l. \end{aligned}$$

Thus a is a product of primes. This completes the induction and the proof. □

Now we turn to uniqueness. Once again the key property is that a Euclidean domain has greatest common divisors and these are linear combinations of the original elements.

Definition 5.8. *Let a and b be two elements of an integral domain R, not both zero. The* ***greatest common divisor*** *of a and b is an element $d \in R$ with the following properties*

(1) $d|a$ and $d|b$.
(2) If $d'|a$ and $d'|b$ then $d'|d$.

Note that not every ring has greatest common divisors.

Theorem 5.9. *If R is a Euclidean domain then every pair of elements a and $b \in R$, not both zero, has a gcd $d \in R$. Moreover there are elements λ and μ of R such that that*

$$d = \lambda a + \mu b.$$

Proof. If $b = 0$ then it is easy to see that $d = a$ is the greatest common divisor. In this case we may take $\lambda = \mu = 1$. Similarly if $a = 0$.

So we may suppose that neither a nor b is zero. We may suppose that $s(a) \leq s(b)$. We proceed by induction on $s(a)$. As R is a Euclidean domain we may write

$$b = qa + r,$$

where either $r = 0$ or $s(r) < s(a)$. If $r = 0$ then a is the greatest common divisor and we may take $\lambda = \mu = 1$. Otherwise $s(r) < s(a)$.

By induction a and r have a greatest common divisor d and we may find λ and μ such that

$$d = \lambda a + \mu r.$$

Note that $\{a, b\}$ and $\{a, r\}$ have the same divisors. So d is also the greatest common divisor of a and b. We have

$$\begin{aligned} d &= \lambda a + \mu r \\ &= \lambda a + \mu(b - qa) \\ &= (\lambda - \mu q)a + \mu b. \end{aligned}$$

□

Corollary 5.10. *Let R be a Euclidean domain.*

If p is a prime and $p|ab$ then either $p|a$ or $p|b$.

Proof. We may suppose that p does not divide a. As the only divisors of p are associates of p and units, and p does not divide a, it follows that the greatest common divisor of p and a is 1.

By (5.9) it follows that we may find λ and $\mu \in R$ such that

$$1 = \lambda p + \mu a.$$

Multiplying both sides by b we get

$$\begin{aligned} b &= b \cdot 1 \\ &= b(\lambda p + \mu a) \\ &= (b\lambda)p + \mu ab. \end{aligned}$$

Now the first term is visibly divisible by p and the second term is divisible by p by assumption. Thus p divides b. □

Lemma 5.11. *Let R be a Euclidean domain.*

If p and q are prime and p divides q then p and q are associates.

Proof. By assumption $q = pa$, for some $a \in R$. As q is prime it follows that either p or a is a unit. p is not a unit as it is a prime. Thus a is a unit and p and q are associates. □

Proof of (5.6). By (5.7) it suffices to prove uniqueness. Suppose that we can factor a into two different products of primes,

$$q_1 \cdot q_2 \cdot \dots \cdot q_m = r_1 \cdot r_2 \cdot \dots \cdot r_n.$$

Consider the prime q_m. It divides the LHS and so it divides the RHS. But we have already shown that if a prime divides a product it must divide one of the factors. Possibly reordering we may assume that q_m divides r_n. As r_n is prime (5.11) implies that q_m and r_n are associates. It follows that $r_n = uq_m$, where u is a unit. But then cancelling, we have

$$q_1 \cdot q_2 \cdot \dots \cdot q_{m-1} = ur_1 \cdot r_2 \cdot \dots \cdot r_{n-1}.$$

Note that ur_1 is prime and an associate of r_1. Thus we are done by induction on the number of prime factors. □

Corollary 5.12. *The Gaussian integers are a UFD.*

Proof. By (5.4) the Gaussian integers are a Euclidean domain. Now apply (5.6). □

There is one other rich source of Euclidean domains. Let R be a ring. Let $R[x]$ be the set of polynomials with coefficients in R,

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n,$$

so that $a_0, a_1, \dots, a_n \in R$. We can add two polynomials $f(x)$ and $g(x)$ with coefficients in R in the obvious way; just add their coefficients. We can multiply two polynomials with coefficients in R; just use the distributive law to multiply. With this rule of addition and multiplication, $R[x]$ becomes a ring.

For number theory, there are two very important examples, $\mathbb{Z}[x]$ polynomials with integer coefficients and $\mathbb{Q}[x]$ polynomials with rational coefficients. It is not hard to check that both rings are integral domains. $\mathbb{Q}[x]$ is a Euclidean domain where the function

$$s\colon \mathbb{Q}[x] - \{0\} \longrightarrow \mathbb{N} \cup \{0\},$$

just sends $f(x)$ to its degree.

It follows, using a Lemma due to Gauss (which we won't prove) that $\mathbb{Z}[x]$ is also a UFD.