19. Special Domains

Let R be an integral domain. Recall that an element $a \neq 0$, of R is said to be prime, if the corresponding principal ideal $\langle p \rangle$ is prime and a is not a unit.

Definition 19.1. *Let a and b be two elements of an integral domain. We say that a* **divides** *b and write $a|b$ if there is an element q such that $b = qa$. We say that a and b are* **associates** *if a divides b and b divides a.*

Example 19.2. *Let $R = \mathbb{Z}$. Then $2|6$. Indeed $6 = 3 \cdot 2$. Moreover 3 and -3 are associates.*

Let R be an integral domain. Note some obvious facts. Every element a of R divides 0. Indeed $0 = 0 \cdot a$. On the other hand, 0 only divides 0. Indeed if $a = q \cdot 0$, then $a = 0$ (obvious!). Finally every unit u divides any other element a. Indeed if $v \in R$ is the inverse of u, so that $uv = 1$ then $a = a \cdot 1 = (av)u$.

Lemma 19.3. *Let R be an integral domain and let $p \in R$.*

Then p is prime if and only if p is not a unit and whenever p divides ab then either p divides a or p divides b, where a and b are elements of R.

Proof. Suppose that p is prime and p divides ab. Let $I = \langle p \rangle$. Then $ab \in I$. As p is prime, then I is prime by definition. Thus either $a \in I$ or $b \in I$. But then either $p|a$ or $p|b$. Thus if p is prime and $p|ab$ then either $p|a$ or $p|b$. The reverse implication is just as easy. □

Lemma 19.4. *Let R be an integral domain and let a and b be two non-zero elements of R.*

TFAE

(1) a and b are associates.
(2) $a = ub$ for some unit u.
(3) $\langle a \rangle = \langle b \rangle$.

Proof. Suppose that a and b are associates. As a divides b, $b = qa$ and b divides a, $a = rb$ for some q and r in R. Thus

$$\begin{aligned} b &= qa \\ &= (qr)b. \end{aligned}$$

As R is an integral domain, and $b \neq 0$, we can cancel b, to get $qr = 1$. But then $u = q$ is a unit. Thus (1) implies (2).

Suppose that $a = qb$ and that $c \in \langle a \rangle$. Then $c = ra = (rq)b$. Thus $c \in \langle b \rangle$ and $\langle a \rangle \subset \langle b \rangle$. Now suppose that $a = ub$, where u is a unit. Let

v be the inverse of u, so that $b = va$. By what we have already proved, $\langle b\rangle \subset \langle a\rangle$. Thus (2) implies (3).

Finally suppose that $\langle a\rangle = \langle b\rangle$. As $a \in \langle a\rangle$, it follows that $a \in \langle b\rangle$, so that $a = rb$, for some $r \in R$. Thus b divides a. By symmetry a divides b and so a and b are associates. Thus (3) implies (1). □

Definition 19.5. *Let R be an integral domain.*

We say that R is a **unique factorisation domain** *(abbreviated to UFD) if every non-zero element a of R, which is not a unit, has a factorisation into a product of primes,*

$$p_1p_2p_3\cdots p_k,$$

which is unique up to order and associates.

The last statement is equivalent to saying that if we can find two factorisations of a,

$$p_1p_2p_3\cdots p_k = q_1q_2q_3\cdots q_l.$$

where p_i and q_j are prime, then $k = l$, and up to re-ordering of $q_1, q_2, \dots, q_l$, p_i and q_i are associates.

Example 19.6. *Of course, by the Fundamental Theorem of Arithmetic, $\mathbb{Z}$ is a UFD. In this case the prime elements of $\mathbb{Z}$ are the ordinary primes and their inverses. For example, suppose we look at the prime factorisation of* 120*. One possibility, the standard one, is*

$$2^3 \cdot 3 \cdot 5.$$

However another possibility is

$$-5 \cdot 3 \cdot (-2)^3.$$

The point is that in an arbitrary ring there is no standard choice of associate. On the other hand, every non-zero integer has two associates, and it is customary to favour the positive one.

Consider the problem of starting with a ring R and proving that R is a UFD. Obviously this consists of two steps. The first is to start with an element a of R and express it as a product of primes. We call this existence. The next step is to prove that this factorisation is unique. We call this uniqueness.

Let us consider the first step, that is, existence of a factorisation. How do we write any integer as a product of primes? Well there is an obvious way to proceed. Try to factorise the integer. If you can, then work with both factors and if you cannot then you already have a prime.

Unfortunately this approach hides one nasty subtelty.

Definition 19.7. *Let R be a ring and let $a \in R$ be an element of R. We say that a is* **irreducible** *if whenever $a = bc$, then either b or c is a unit.*

Equivalently, a is irreducible if and only if whenever b divides a, then b is either a unit or an associate of a. Clearly every prime element a of an integral domain R is automatically irreducible. The subtelty that arises is that in an arbitrary integral domain there are irreducible elements that are not prime. On the other hand, unless the ring is very pathological indeed, it is quite easy to prove that every non-zero element of a ring is a product of irreducibles, in fact using the method outline above. The only issue is that the natural process outlined above terminates in a finite number of steps.

Before we go into this deeper, we need a basic definition, concerning partially ordered sets.

Definition 19.8. *Let X be a set. A* **partial order** *on X is a reflexive and transitive relation on $X \times X$. It is customary to denote a partial order $\leq$. The fact that $\leq$ is reflexive is equivalent to $x \leq x$ and the fact the $\leq$ is transitive is equivalent to*

$$a \leq b \qquad \textit{and} \qquad b \leq c \qquad \textit{implies} \qquad a \leq c.$$

We also require that if $x \leq y$ and $y \leq x$ then $x = y$.

We say that X satisfies the ascending chain condition (ACC) if every infinite increasing chain

$$x_1 \leq x_2 \leq x_3 \leq \cdots \leq x_n \leq \cdots$$

eventually stabilises, that is, there is an n_0 such that $x_n = x_m$ for every n and m at least n_0.

Note that, in the definition of a partial order, we do not require that every two elements of X are comparable. In fact if every pair of elements are comparable, that is, for every x and $y \in X$, either $x \leq y$ of $y \leq x$, then we say that our partial order is a total order.

There is a similar notion for descending chains, knows as the descending chain condition, or DCC for short.

Example 19.9. *Every finite set with a partial order satisfies the ACC and the DCC for obvious reasons.*

Let X be a subset of the real numbers with the obvious relation. Then X is a partially ordered set. The set

$$X = \{\, \frac{1}{n} \,|\, n \in \mathbb{N} \,\} = \{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots\},$$

satisfies the ACC but it clearly does not satisfy the DCC.

Let Y be a set and let X be a subset of the power set of Y, so that X is a collection of subsets of Y. Define a relation $\leq$ by the rule,

$$A \leq B \qquad \text{if and only if} \qquad A \subset B.$$

In the case that X is the whole power set of Y, note that $\leq$ is not a total order, provided that Y has at least two elements a and b, since in this case $A = \{a\}$ and $B = \{b\}$ are incomparable.

Factorisation Algorithm: Let R be an integral domain and let a be a non-zero element of R that is not a unit. Consider the following algorithm, that produces a, possibly infinite, pair of sequences of elements $a_1, a_2, \dots$ and $b_1, b_2, \dots$ of R, where $a_i = a_{i+1}b_{i+1}$ and neither a_i nor b_i is a unit. Suppose that we have already produced $a_1, a_2, \dots, a_k$ and $b_1, b_2, \dots, b_k$.

(1) If a_k and b_k are both irreducible then **stop**.

(2) Otherwise, possibly switching a_k and b_k we may assume that a_k is not irreducible. Thus we may write $a_k = a_{k+1}b_{k+1}$, where neither a_{k+1} nor b_{k+1} are units.

Proposition 19.10. *Let R be an integral domain.*

TFAE

(1) The factorisation algorithm above terminates, starting with any non-zero element a of the ring R and pursuing all possible ways of factorising a. In particular, every non-zero element a of R is either a unit or a product of irreducibles.

(2) The set of principal ideals satisfies the ACC. That is, every increasing chain

$$\langle a_1 \rangle \subset \langle a_2 \rangle \subset \langle a_3 \rangle \subset \cdots \subset \langle a_n \rangle \subset \cdots$$

eventually stabilises.

Proof. Suppose we have a strictly increasing sequence of principal ideals as in (2). We will find an a such that the factorisation algorithm does not terminate.

Note that a principal ideal $\langle a \rangle = R$ if and only if a is a unit. As the sequence of ideals in (2) is increasing, then no ideal can be the whole of R. Thus none of the a_i are units. As $a_i \in \langle a_{i+1} \rangle$, we may find b_{i+1} such that $a_i = b_{i+1}a_{i+1}$. But b_{i+1} cannot be a unit as $\langle a_i \rangle \neq \langle a_{i+1} \rangle$. Thus the factorisation algorithm, with $a = a_1$ does not terminate. Thus (1) implies (2).

The reverse implication follows similarly. □

Lemma 19.11. *Let R be a ring and let*

$$I_1 \subset I_2 \subset I_3 \subset \cdots \subset I_n \subset \cdots,$$

be an ascending sequence of ideals.

Then the union I of these ideals, is an ideal.

Proof. We have to show that I is non-empty and closed under addition and multiplication by any element of R.

I is clearly non-empty. For example it contains I_1, which is non-empty. Suppose that a and b belong to I. Then there are two natural numbers m and n such that $a \in I_m$ and $b \in I_n$. Let k be the maximum of m and n. Then a and b are elements of I_k, as I_m and I_n are subsets of I_k. It follows that $a + b \in I_k$, as I_k is an ideal and so $a + b \in I$. Similarly $-a \in I$. Finally suppose that $a \in I$ and $r \in R$. Then $a \in I_n$, for some n. In this case $ra \in I_n \subset I$. Thus I is an ideal. □

Definition 19.12. *Let R be a integral domain. We say that R is a* **principal ideal domain***, abbreviated to PID, if every ideal I in R is principal.*

Lemma 19.13. *Let R be a principal ideal domain.*

Then every ascending chain of ideals stabilises. In particular every non-zero element a of R, which is not a unit, has a factorisation

$$p_1 p_2 p_3 \cdots p_k,$$

into irreducible elements of R.

Proof. Suppose we have an ascending chain of ideals as in (2) of (19.10). Let I be the union of these ideals. By (19.11) I is an ideal of R. As R is assumed to be a PID, I is principal, so that $I = \langle b \rangle$, for some $b \in R$. Thus $b \in \langle a_n \rangle$, for some n. In this case $b = qa_n$, for some q. But then $\langle b \rangle \subset \langle a_n \rangle$. As we have an increasing sequence of ideals, it follows that in fact $\langle a_k \rangle = \langle b \rangle$, for all $m \geq n$, that is the sequence of ideals stabilises. Now apply (19.10). □

Thus we have finished the first step of our program. Given an integral domain R, we have found sufficient conditions for the factorisation of any element a, that is neither zero nor a unit, into irreducible elements.

Now we turn to the other problem, the question of uniqueness.

Lemma 19.14. *Let R be an integral domain and suppose that p divides q, where both p and q are primes.*

Then p and q are associates.

Proof. By assumption

$$q = ap,$$

for some $a \in R$. As q is prime, either q divides a or q divides p. If q divides p then p and q are associates.

Otherwise q divides a. In this case $a = qb$, and so

$$q = ap = (pb)q.$$

Cancelling, we have that p is a unit, absurd. □

Lemma 19.15. *Let R be an integral domain and let a and b be two non-zero elements of R, both of which are not units. Suppose that $a = p_1, p_2, \dots, p_k$ and $b = q_1, q_2, \dots, q_l$ is a factorisation of a and b into primes.*

Then a divides b, if and only if $k \leq l$ and after re-ordering the q_j, we have that p_i and q_i are associates, for $i \leq k$.

In particular there is at most one prime factorisation of every non-zero element a of R, up to associates and re-ordering.

Proof. We prove the first statement. One direction is clear. Otherwise suppose a divides b. As p_1 divides a and a divides b, p_1 divides b. As p_1 is prime and it divides a product, it most divide one of the factors q_i. Possibly re-ordering, we may assume that $i = 1$. By (19.14) p_1 and q_1 are associates. Cancelling p_1 from both sides and absorbing the resulting unit into q_2, we are done by induction on k.

Now suppose that a has two different prime factorisations,

$$p_1 p_2 \cdots p_k \qquad \text{and} \qquad q_1 q_2 \cdots q_l.$$

As $a|a$, it follows that $k \leq l$ and that p_i and q_i are associates. Using $a|a$ again, but now the other way around, we get $l \leq k$. Thus we have uniqueness of prime factorisation. □

Putting all this together, we have

Proposition 19.16. *Let R be an integral domain, in which every ascending chain of principal ideals stabilises.*

Then R is a UFD if and only if every irreducible element of R, which is neither zero nor a unit, is prime.

Definition 19.17. *Let R be an integral domain. Let a and b be two elements of R. We say that d is the* **greatest common divisor** *of a and b if*

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

Note that the gcd is not unique. In fact if d is a gcd, then so is d' if and only if d and d' are associates.

Lemma 19.18. *Let R be a UFD.*

Then every pair of elements has a gcd.

Proof. Let a and b be a pair of elements of R. If either a or b is zero, then it is easy to see that the other element is the gcd. If either element is a unit then in fact the gcd is 1 (or in fact any unit).

So we may assume that neither a nor b are zero or units. Let $a = p_1, p_2, \dots, p_k$ and $b = q_1, q_2, \dots, q_l$ be two prime factorisations of a and b. Note that we may put both factorisations into a more standard form,

$$a = up_1^{m_1} p_2^{m_2} p_3^{m_3} \cdots p_k^{m_k} \qquad \text{and} \qquad vp_1^{n_1} p_2^{n_2} p_3^{n_3} \cdots p_k^{n_k},$$

where u and v are units, and p_i and p_j are associates if and only if $i = j$. In this case it is clear, using (19.15), that the gcd is $d = p_1^{l_1} p_2^{l_2} p_3^{l_3} \cdots p_k^{l_k}$, where l_i is the minimum of m_i and n_i. □

Lemma 19.19. *Let R be a ring, let I_i be a collection of ideals in R and let I be their intersection.*

Then I is an ideal.

Proof. Easy exercise left to the reader. □

Definition-Lemma 19.20. *Let R be a ring and let S be a subset of R. The ideal generated by S, denoted $\langle S \rangle$, is the smallest ideal containing S.*

Proof. Let I_i be the collection of all ideals that contain S. Then the intersection I of these ideals, is an ideal by (19.19) and this is clearly the smallest ideal that contains S. □

Lemma 19.21. *Let R be a ring and let S be subset of R.*

Then the ideal generated by S consists of all finite combinations

$$r_1 a_1 + r_2 a_2 + \cdots + r_k a_k,$$

where $r_1, r_2, \dots, r_k \in R$ and $a_1, a_2, \dots, a_k \in S$.

Proof. It is clear that any ideal that contains S must contain all elements of this form, since any ideal is closed under addition and multiplication by elements of R. On the other hand, it is an easy exercise to check that these combinations do form an ideal. □

Lemma 19.22. *Let R be a PID.*

Then every pair of elements a and b has a gcd d, such that

$$d = ra + sb,$$

where r and $s \in R$.

Proof. Consider the ideal I generated by a and b, $\langle a, b \rangle$. As R is a PID, $I = \langle d \rangle$. As $d \in I$, $d = ra + sb$, for some r and s in R. As $a \in I = \langle d \rangle$, d divides a. Similarly d divides b. Suppose that d' divides a and d' divides b. Then $\langle a, b \rangle \subset \langle d' \rangle$. But then $d|d'$. □

Theorem 19.23. *Let R be a PID.*

Then R is a UFD.

Proof. We have already seen that the set of principal ideals satisfies the ACC. It remains to prove that irreducible implies prime.

Let a be an irreducible element of R. Let b and c be any two elements of R and suppose that a divides the product bc. Then $bc \in \langle a \rangle$. Let d be the gcd of a and b. Then d divides a. As a is irreducible, there are only two possibilities; either d is an associate of a or d is a unit.

Suppose that d is an associate of a. As d divides b, then a divides b and we are done. Otherwise d is a unit, which we may take to be 1. In this case, by (19.22), we may find r and s such that $1 = ra + sb$. Multiplying by c, we have

$$c = rac + sbc = (rc + qs)a,$$

so that a divides c. Thus a is prime and R is a UFD. □