UNIT 14 SPECIAL INTEGRAL DOMAINS

Structure

14.1 INTRODUCTION

In this unit we shall look at three special kinds of integral domains. These domains were mainly studied with a view to develop number theory. Let us say a few introductory sentences about them.

In Unit 13 you saw that the division algorithm holds for $F[x]$, where F is a field. In Unit 1 you saw that it holds for $\mathbb{Z}$. Actually, there are lots of other domains for which this algorithm is true. Such integral domains are called Euclidean domains. We sliall discuss their properties in Sec. 14.2.

In the next section we shall look at some domains which are algebraically very similar to $\mathbb{Z}$. These are the principal ideal domains, so called because every ideal in them is principal.

Finally, we shall discuss domains in which every non-zero non-invertible element can be uniquely factorised in a particular way. Such domains are very appropriately called unique factorisation domains. While discussing them we shall introduce you to irreducible elements of a domain. .

While going through the unit you will also see the relationship between Euclidean domains, principal ideal domains and unique factorisation domains.

Objectives

After studying this unit, you should be able to

- check whether a function is a Euclidean valuation or not;
- identify principal ideal domains;
- identify unique factorisation domains;
- obtain the g.c.d of any pair of elements in a unique factorisation domain;
- prove and use the relationship between Euclidean domains, principal ideal domains and unique factorisation domains.

14.2 EUCLIDEAN DOMAIN

In this course you have seen that $\mathbb{Z}$ and $F[x]$ satisfy a division algorithm. There are many other domains that have this property. In this section we will introduce you to them and discuss some of their properties. Let us start with a definition.

Definition : Let **R** be an integral domain. We say that a function $d : R \setminus \{0\} \to N \cup \{0\}$ is a **Euclidean valuation** on **R** if the following conditions are satisfied:

i) $d(a) \leq d(ab)$ $\forall$ $a, b \in R \setminus \{0\}$, and

ii) for any $a, b \in R$, $b \neq 0$ $\exists$ $q, r \in R$ such that

$a = bq + r$, where $r = 0$ or $d(r) < d(b)$.

And then R is called a **Euclidean domain.**

Thus, a domain on which we can define a Euclidean valuation is a Euclidean domain.

Let us consider an example.

Example 1 : Show that Z is a Euclidean domain.

Solution : Define, $d : \mathbf{Z} \to \mathbf{N} \cup \{0\} : d(n) = |n|$.

Then, for any $a,b \in Z \setminus \{0\}$,

$$d(ab) = |ab| = |a|\,|b| \geq |a| \text{ (since } |b| \geq 1 \text{ for } b \neq 0)$$

$$= d(a),$$

i.e., $d(a) \leq d(ab)$.

Further, the division algorithm in Z (see Sec.1. 6.2) says that if a, $b \in Z$, $b \neq 0$, then $\exists\, q, r \in Z$ such that

$$a = bq+r, \text{ where } r = 0 \text{ or } 0 < |r| < |b|,$$

i.e., $a = bq+r$, where $r = 0$ or $d(r) < d(b)$.

Hence, d is a Euclidean valuation and Z is a Euclidean domain.

For other examples, try the following exercises.

E 1) Let F be a field. Show that F, with the Euclidean valuation d defined by $d(a) = 1\ \forall\ a \in F\setminus\{0\}$, is a Euclidean domain.

E 2) Let F be a field. Define the function

$d : F[x] \setminus \{0\} \to \mathbf{N} \cup \{0\} : d(f(x)) = \deg f(x)$.

Show that d is a Euclidean valuation on F[x], and hence, F[x] is a Euclidean domain.

Let us now discuss some properties of Euclidean domains. The first property involves the concept of units. SO let us define this concept. Note that this definition is valid for any integral domain.

Definition: Let R be an integral domain. An element $a \in R$ is called a unit (or an invertible element) in R, if we can find an element $b \in R$, such that $ab = 1$, i.e., if a has a multiplicative inverse.

For example, both 1 and –1 are units in Z since $1.1 = 1$ and $(-1).(-1) = 1$.

Caution : Note. the difference between a unit .in R and the unity in R. The unity is the identity with respect to multiplication, and is certainly a unit. But a ring can have other units ton, as you have just seen in the case of Z.

Now, can we obtain all the units in a domain? You know that every non-zero element in a field F is invertible. Thus, the set of units of F is $F \setminus \{0\}$. Let us look at some other cases also.

Example 2 :.Obtain all the units in F[x], where F is a field.

Solution : Let $f(x) \in F[x]$ be a unit, Then $\exists\ g(x) \in F[x]$ such that $f(x)\,g(x) = 1$. Therefore,

$\deg (f(x)\,g(x)) = \deg (1) = 0$, i.e.,

$\deg f(x) + \deg g(x) = 0$.

Since deg f(x) and deg g(x) are non-negative integers, this equation can hold only if deg f(x) = 0 = deg g(x). Thus, f(x) must be a non-zero constant, i.e., an element of $F \setminus \{0\}$. Thus, the units of F[x] are the non-zero elements of F. That is, the units of F and F[x] coincide.

Example 3 : Find all the units in $R = \{a + b\sqrt{-5} \mid a,b \in Z\}$.

Solution : Let $a+b\sqrt{-5}$ be a unit in R. Then there exists

$c+d\sqrt{-5} \in R$ such that

$$(a+b\sqrt{-5})\ (c+d\sqrt{-5})= 1$$

$\Rightarrow$ $(ac-5bd)+(bc+ad)\sqrt{-5} = 1$

$\Rightarrow$ $ac-5bd = 1$ and $bc+ad = 0$

$\Rightarrow$ $abc-5b^2d = b$ and $bc+ad = 0$

$\Rightarrow$ $a(-ad)-5b^2d = b$, substituting $bc=-ad$.

$\Rightarrow$ $(a^2+5b^2)d = -b$.

So, if $b \neq 0$, then $(a^2+5b^2) \mid b$, which is not possible.

$\therefore$ $b=0$.

Thus, the only units of R are the invertible elements of Z.

We have asked you to find these elements and other units in E 3 below.

E 3) Find all the units in

a) $\mathbb{Z}$, b) $\mathbb{Z}_6$, c) $\mathbb{Z}/5\mathbb{Z}$, d) $\mathbb{Z}+i\mathbb{Z}$.

E 4) Let R be an integral domain. Prove that $u \in R$ is a unit iff

$Ru = R$.

Now we are in a position to discuss some very simple properties of a Euclidean domain.

Theorem 1 : Let R be a Euclidean domain with Euclidean valuation d. Then, for any $a \in R \setminus \{0\}$, $d(a) = d(1)$ iff a is a unit in R.

Proof : Let us first assume that $a \in R \setminus \{0\}$ with $d(a) = d(1)$.

By the division algorithm in R, $\exists$ q, $r \in R$ such that $1 = aq+r$,

where $r = 0$ or $d(r) < d(a) = d(1)$.

Now, if $r \neq 0$, $d(r) = d(r.1) \geq d(1)$. Thus, $d(r) < d(1)$ can't happen.

Thus, the only possibility for r is $r = 0$.

Therefore, $1 = aq$, so that a is a unit.

Conversely, assume that a is a unit in R. Let $b \in R$ such that $ab = 1$. Then $d(a) \leq d(ab) = d(1)$. But we know that $d(a) = d(a.1) \geq d(1)$. So, we must have $d(a) = d(1)$.

Using this theorem, we can immediately solve Example 2, since $f(x)$ is a unit in $F[x]$ iff $\deg f(x) = \deg (1) = 0$.

Similarly, Theorem 1 tells us that $n \in Z$ is a unit in Z iff $|n| = |1| = 1$. Thus, the only units in Z are 1 and (-1).

Now let us look at the ideals of a Euclidean domain.

Theorem 2 : Let R be a Euclidean domain with Euclideae valuation d. Then every ideal I of R is of the form $I = Ra$ for some $a \in R$.

Proof: If $I = \{0\}$, then $I = Ka$, where $a = 0$. So let us assume that $I \neq \{0\}$. Then $I \setminus \{0\}$ is non-empty. Consider the set $\{ d(a) \mid a \in I \setminus \{0\}\}$. By the well ordering principle (see Sec. 1.6.1) this set has a minimal element. Let this be $d(b)$, where $b \in I \setminus \{0\}$. We will show that $I = Rb$.

Since $b \in I$ and I is an ideal of R,

$Rb \subseteq I$. ..... (1)

Now take any $a \in I$. Since $I \subseteq R$ and R is a Euclidean domain, we can find $q, r \in R$ such that

$a = bq + r$, where $r = 0$ or $d(r) < d(b)$.

Now, $b \in I \Rightarrow bq \in I$. Also, $a \in I$. Therefore, $r = a - bq \in I$.

But $r = 0$ or $d(r) < d(b)$. The way we have chosen $d(b)$, $d(r) < d(b)$ is not possible.

Therefore, $r = 0$, and hence, $a = bq \in Rb$.

Thus, $I \subseteq Rb$. ...(2)

From (1) and (2) we get

$I = Rb$.

Thus, every ideal I of a Euclidean domain R with Euclidean valuation d is principal, and is genetated by $a \in I$, where $d(a)$ is a minimal element of the set $\{d(x) \mid x \in I \setminus \{0\}\}$.

We also denote the principal ideal Ra by $< a >$.

So, for example, every ideal of $\mathbf{Z}$ is principal, a fact that you have already proved in Unit 10.

Now try the following exercises involving the ideals of a Euclidean domain.

E 5) Show that every ideal of $F[x]$ is principal, where F is a field.

E 6) Using Z as an example, show that the set

$S = (a \in R \setminus \{0\} \mid d(a) > d(1)\} \cup \{0\}$ is not an ideal of the Euclidean domain R with Euclidean valuation d.

Theorem 2 leads us to a concept that we shall discuss now.

14.3 PRINCIPAL IDEAL DOMAIN (PID)

In the previous section you have ptoved that every ideal of $F[x]$ is principal, where F is a field. There are several other integral domains, apart from Euclidean domains, which have this property. We give such rings a very appropriate name.

Definition : We call an integral domain R a **principal ideal domain** (PID, in short) if every ideal in R is a principal ideal.

Every Euclidean domain is a PID.

Thus, $\mathbf{Z}$ is a PID. Can you think of another example of a PID? What about Q and $\mathbf{Q}[x]$? In fact, by Theorem 2 all Euclidean domains are PIDs. But, the converse is not true. That is, every principal ideal domain is not a Euclidean domain.

For example, the ring of all complex numbers of the form $a+\frac{b}{2}(1+i\sqrt{19})$, where $a, b \in \mathbf{Z}$, is a principal ideal domain, but not a Euclidean domain. The proof of this is too technical for this course, so you can take our word for it for the present!

Now let us look at an example of an integral domain that is not a PID.

Example 4 : Show that $\mathbf{Z}[x]$ is not a PID,

Solution : You know that $\mathbf{Z}[x]$ is a domain, since Z is one. We will show that all its ideals are not principal. Consider the ideal of $\mathbf{Z}[x]$ generated by 2 and x, i.e., $< 2,x >$. We want to show that $< 2, x > \neq <f(x)>$ for any $f(x) \in \mathbf{Z}[x]$.

On the contrary, suppose that $\exists f(x) \in \mathbf{Z}[x]$ such that $<2,x> = <f(x)>$. Clearly, $f(x) \neq 0$. Also, $\exists g(x), h(x) \in \mathbf{Z}[x]$ such that

$2 = f(x)\,g(x)$ and $x = f(x)\,h(x)$.

Thus, deg $f(x)$ + deg $g(x)$ = deg 2 = 0 .....(1)

and deg $f(x)$+deg $h(x)$ = deg x = 1 .....(2)

(1) shows that deg $f(x) = 0$, i.e., $f(x) \in Z$, say $f(x) = n$.

Then (2) shows that deg $h(x) = 1$. Let $h(x) = ax+b$ with $a,b \in Z$.

Then $x = f(x)\, h(x) = n(ax+b)$.

Comparing the coefficients on either side of this equation, we see that $na = 1$ and $nb = 0$. Thus, n is a unit in Z, that is, $n = \pm 1$.

Therefore, $1 \in \langle f(x) \rangle = \langle x,2 \rangle$. Thus, we can write

$1 = x(a_0+a_1x+\ldots+a_rx^r) + 2(b_0+b_1x+\ldots.+b_sx^s)$, where $a_i, b_j \in Z\ \forall\ i = 0, 1,\ldots\ldots,r$ and $j = 0,1,\ldots.,s$.

Now, on comparing the constant term on either side we see that $1 = 2b_0$. This can't be true, since 2 is not invertible in Z. So we reach a contradiction.

Thus, $\langle x,2 \rangle$ is not a principal ideal.

Thus, $Z[x]$ is not a P.I.D.

Now, try the following exercises.

E 7) Show that a subring of a PID need not be a PID.

E 8) Will any quotient ring of a PID be a PID? Why?
Remember that a PID must be an integral domain.

We will now discuss some properties of divisibility in PIDs. You may recall from Unit 12 that if R is a ring and $a,b \in R$, with $a \neq 0$, then a **divides** b if there exists $c \in R$ such that $b = ac$.

Now we would like to generalise the definition of some terms that you came across in Unit 1 in the context of Z.

Definition : Given two elements a and b in a ring R, we say that $c \in R$ is a **common divisor** of a and b if $c \mid a$ and $c \mid b$.

An element $d \in R$ is a **greatest common divisor** (g.c.d. in short) of $a, b \in R$ if

i) $d \mid a$ and $d \mid b$, and

ii) for any common divisor c of a and b, $c \mid d$.

For example, in Z a g.c.d of 5 and 15 is 5, and a g.c.d of 5 and 7 is 1.

We will show you that if the g.c.d of two elements exists, it is unique up to units, i.e., if d and d' are two g.c.ds of a and b, then $d = ud'$, for some unit u. For this we need a result that you can prove in the following exercise.

Two elements a and b in a domain R are called associates if $a = bu$ for some unit u in R.

E 9) Let R be an integral domain. Show that

a) u is a unit in R iff $u \mid 1$.

b) for $a, b \in R$, $a \mid b$ and $b \mid a$ iff a and b are associates in R.

So now let us prove the following result,

Theorem 3 : Let R be an integral domain and $a, b \in R$. If a g.c.d of a and b exists, then it is unique up to units.

Proof : So, let d and d' be two g.c.ds of a and b. Since d is a common divisor and d' is a

g.c.d, we get $d \mid d'$. Similarly, we get $d' \mid d$. Thus, by E 9 we see that d and d' are associates in R. Thus, the g.c.d of a and b is unique up to units.

Theorem 3 allows us to say **the** g.c.d instead of a g.c.d. We denote the g.c.d of a and b by (a,b). (This notation is also used for elements of R x R. But there should be no cause for confusion. The context will clarify what we are using the notation for.)

How do we obtain the g.c.d of two elements in practice? How did we do it in Z? We looked at the common factors of the two elements and their product turned out to be the required g.c.d. We will use the same method in the following example.

Example 5 :.In $\mathbf{Q}[x]$ find the g.c.d of

$p(x) = x^2+3x-10$ and

$q(x) = 6x^2-10x-4$.

Solution: By the quadratic formula, we know that the roots of $p(x)$ are 2 and –5, and fhe roots of $q(x)$ are 2 and $-1/3$.

Therefore, $p(x) = (x-2)(x+5)$ and $q(x) = 2(x-2)(3x+1)$.

The g.c.d of $p(x)$ and $q(x)$ is the product of the common factors of $p(x)$ and $q(x)$, which is $(x-2)$.

Try this exercise now.

E 10) Find the g.c.d of

a) $\bar{2}$ and $\bar{6}$ in $\mathbf{Z} / \langle 8 \rangle$,

b) $x^2+8x+15$ and $x^2+12x+35$ in $\mathbf{Z}[x]$,

c) x^3-2x^2+6x-5 and x^2-2x+1 in $\mathbf{Q}[x]$.

Let us consider the g.c.d of elements in a PID.

Theorem 4 : Let R be a PID and $a, b \in R$. Then (a,b) exists and is of the form $ax+by$ for some $x,y \in R$.

Proof : Consider the ideal $\langle a,b \rangle$. Since R is a PID, this ideal must be principal also. Let $d \in R$ such that $\langle a,b \rangle = \langle d \rangle$. We will show that the g.c.d of a and b is d.

Since $a \in \langle d \rangle$, $d \mid a$, Similarly, $d \mid b$.

Now suppose $c \in R$ such that $c \mid a$ and $c \mid b$.

Since $d \in \langle a,b \rangle$, $\exists\, x, y \in R$ such that $d = ax+by$.

Since $c \mid a$ and $c \mid b$, $c \mid (ax+by)$, i.e., $c \mid d$.

Thus, we have shown that $d = (a,b)$, and $d = ax+by$ for some $x,y \in R$.

The fact that F[x] is a PID gives us the following corollary to Theorem 4.

Corollary : Let F be a field. Then any two polynomials $f(x)$ and $g(x)$ in F[x] have a g.c.d which is of the form $a(x)f(x)+b(x)g(x)$ for some $a(x), b(x) \in F[x]$.

For example, in E 10 (c), $(x-1) = \frac{1}{5}(x^3-2x^2+6x-5)+\frac{(-x)}{5}(x^2-2x+1)$.

Now you can use Theorem 4 to prove the following exercise about relatively prime elements in a PID, i.e., pairs of elements whose g.c.d is 1.

E 11) Let R be a PID and $a,b,c \in R$ such that $a \mid bc$. Show that if $(a,b) = 1$, then $a \mid c$.

(Hint : By Theorem 4, $\exists\, x,y \in R$ such that $ax+by = 1$.)

Let us now discuss a concept related to that of a prime element of a domain (see Sec. 12.4).

Definition : Let R be an integral domain. We say that an element $x \in R$ is irreducible if

i) x is not a unit, and

ii) if $x = ab$ with $a,b \in R$, then a is a unit or b is a unit.

Thus, an element is irreducible if it cannot be factored in a non-trivial way, i.e., its only factors are its associates and the units in the ring.

So, for example, the irreducible elements of Z are the prime numbers and their associates. This means that an element in Z is prime iff it is irreducible.

Another domain in which we can find several examples is F[x], where F is a field. Let us look at the irreducible elements in $\mathbf{R}[x]$ and $\mathbf{C}[x]$, i.e., the irreducible polynomials over R and C. Consider the following important theorem about polynomials in $\mathbf{C}[x]$. You have already come across this in the Linear Algebra course.

Theorem 5 (Fundamental Theorem of Algebra) : Any non-constant polynomial in $\mathbf{C}[x]$ has a root in C. (In fact, it has all its roots in C.)

Does this tell us anything about the irreducible polynomials over C? Yes. In fact, we can also write it as

Theorem 5' : A polynomial is irreducible in $\mathbf{C}[x]$ iff it is linear.

A corollary to this result is

Theorem 6 : Any irreducible polynomial in $\mathbf{R}[x]$ has degree 1 or degree 2.

We will not prove these results here but we will use them often when discussing polynomials over R or C. You can use them to solve the following exercise.

E 12) Which of the following polynomials is irreducible? Give reasons for your choice,

a) $x^2-2x+1 \in \mathbf{R}[x]$

b) $x^2+x+1 \in \mathbf{C}[x]$,

c) $x-i \in \mathbf{C}[x]$

d) $x^3-3x^2+2x+5 \in \mathbf{R}[x]$.

Let us now discuss the relationship between prime and irreducible elements in a PID.

Theorem 7 : In a PID an element is prime iff it is irreducible.

Proof : Let R be a PID and $x \in R$ be irreducible. Let $x \mid ab$, where $a,b \in R$. Suppose $x \nmid a$. Then $(x,a) = 1$, since the only factor of x is itself, up to units. Thus, by E 11, $x \mid b$. Thus, x is prime.

To prove the converse, you must solve the following exercise.

E 13) Let R be a domain and $p \in R$ be a prime element. Show that p is irreducible.

(Hint : Suppose $p = ab$. Then $p \mid ab$. If $p \mid a$, then show that b must be a unit.)

Now, why do you think we have said that Theorem 7 is true for a PID only? From E 13 you can see that one way is true for any domain. Is the other way true for any domain? That is, is every irreducible element of a domain prime? You will get an answer to this question in Example 6. Just now we will look at some uses of Theorem 7.

Theorem 7 allows us to give a lot of examples of prime elements of F[x]. For example, any linear polynomial over F is irreducible, and hence prime. In the next unit we will particularly consider irreducibility (and hence primeness) over $\mathbf{Q}[x]$.

Now we would like to prove a further analogy between prime elements in a PID and prime numbers, namely, a result analogous to Theorem 10 of Unit 1. For this we will first show a very interesting property of the ideals of a PID. This property. called the **ascending chain condition,** says that any increasing chain of ideals in a PID must stop after a finite number of steps.

Theorem 8: Let R be a PID and $I_1, I_2, \ldots\ldots$ be an infinite sequence of ideals of R satisfying .

$I_1 \subseteq I_2 \subseteq \ldots$

Then $\exists\, m \in N$ such that $I_m = I_{m+1} = I_{m+2} = \ldots\ldots$

Proof : Consider the set $I = I_1 \cup I_2 \cup \ldots = \bigcup_{n=1}^{\infty} I_n$. We will prove that I is an ideal of R.

Firstly, $I \neq \phi$, since $I_1 \neq \phi$ and $I_1 \subseteq I$.

Secondly, if $a,b \in I$, then $a \in I$, and $b \in I_s$ for some $r,s \in N$.

Assume $r \geq s$. Then $I_s \subseteq I_r$. Therefore, $a,b \in I_r$. Since I_r is an ideal of R, $a-b \in I_r \subseteq I$. Thus, $a-b \in I\ \forall\ a, b \in I$.

Finally, let $x \in R$ and $a \in I$. Then $a \in I_r$ for some $r \in N$.

$\therefore xa \in I_r \subseteq I$. Thus, whenever $x \in R$ and $a \in I$, $xa \in I$.

Thus, I is an ideal of R. Since R is a PID, $I = \langle a \rangle$ for some $a \in R$. Since $a \in I$, $a \in I_m$ for some $m \in N$.

Then $I \subseteq I_m$. But $I_m \subseteq I$. So we see that $I = I_m$.

Now, $I_m \subseteq I_{m+1} \subseteq I = I_m$. Therefore, $I_m = I_{m+1}$.

Similarly, $I_m = I_{m+2}$, and so on. Thus, $I_m = I_{m+1} = I_{m+2} = \ldots$

Now, for a moment let us go back to Sec. 12.4, where we discussed prime ideals. Over there we said that an element $p \in R$ is prime iff $\langle p \rangle$ is a prime ideal of R. If R is a **PID,** we shall use Theorem 7 to make a stronger statement.

Theorem 9 : Let R be a PID. An ideal $\langle a \rangle$ is a maximal ideal of R iff a is a prime element of R.

Proof : If $\langle a \rangle$ is a maximal ideal of R, then it is a prime ideal of R. Therefore, a is a prime element of R.

Conversely, let a be prime and let I be an ideal of R such that $\langle a \rangle \subsetneq I$. Since R is a **PID,** $I = \langle b \rangle$ for some $b \in R$. We will show that b is a unit in R; and hence. by E 4 , $\langle b \rangle = R$, i.e., $I = R$.

Now, $\langle a \rangle \subseteq \langle b \rangle \Rightarrow a = bc$ for some $c \in R$. Since a is irreducible, either b is an associate of a or b is a unit in R. But if b is an associate of a, then $\langle b \rangle = \langle a \rangle$, a contradiction. Therefore, b is a unit in R. Therefore, $I = R$.

Thus, $\langle a \rangle$ is a maximal ideal of R.

What Theorem 9 says is that **the prime ideals and maximal Ideals coincide in a PID.**

Try the following exercise now.

E 14) Which of the following ideals are maximal? Give reasons for your choice.

a) $\langle 5 \rangle$ in $\mathbf{Z}$,

b) $\langle x^2-1 \rangle$ in $\mathbf{Q}[x]$,

c) $\langle x^2+x+1 \rangle$ in $\mathbf{R}[x]$,

d) $\langle x \rangle$ in $\mathbf{Z}[x]$.

Now, take any integer n. Then we can have $n = 0$, or $n = \pm 1$, or n has a prime factor. This property of integers is true for the elements of any PID, as you will see now.

Theorem 10 : Let R be a PID and a be a non-zero non-invertible element of R. Then there is some prime element p in R such that $p \mid a$.

Proof : If a is prime, take p = a. Otherwise, we can write $a = a_1 b_1$, where neither a, nor b_1 is an associate of a. Then $< a > \subsetneq < a_1 >$. If a_1 is prime, take $p = a_1$. Otherwise, we can write $a_1 = a_2 b_2$, where neither a_2 nor b_2 is an associate of a_1. Then $< a_1 > \subsetneq < a_2 >$. Continuing in this way we get an increasing chain

$$< a > \subsetneq < a_1 > \subsetneq < a_2 > \subsetneq \ldots\ldots$$

By Theorem 8, this chain stops with some $< a, >$. Then a, will be prime, since it doesn't have any non-trivial factors. Take $p = a_{,}$ and the theorem is proved.

And now we are in a position to prove that any non-zero non-invertible element of a PID can be uniquely written as a finite product of prime elements (i.e., irreducible elements).

Theorem 11 : Let R be a PID. Let $a \in R$ such that $a \neq 0$ and a is not a unit. Then $a = p_1 p_2 \ldots p_r$, where $p_1, p_2, \ldots p_r$, are prime elements of R.

Proof : If a is a prime element, there is nothing lo prove. If not, then $p_1 \mid a$ for some prime p_1 in R, by Theorem 10. Let $a = p_1 a_1$. If a_1 is a prime, we are through. Otherwise $p_2 \mid a$, for some prime p_2 in R. Let $a_1 = p_2 a_2$. Then $a = p_1 p_2 a_2$. If a_2 is a prime, we are through. Otherwise we continue the process. Note that since a_1 is a non-trivial factor of a, $< a > \subsetneq < a_1 >$. Similarly, $< a_1 > \subsetneq < a_2 >$. So, as the process continues we get an increasing chain of ideals,

$$< a > \subsetneq < a_1 > \subsetneq < a_2 > \subsetneq \ldots\ldots$$

in the PID R. Just as in the proof of Theorem 10, this chain ends at $< a, >$ for some $m \in N$, and a, is irreducible.

Hence, the process stops after m steps, i.e., we can write $a = p_1 p_2 \ldots p_m$, where p_i is a prime element of $R \forall i = 1, \ldots, m$.

Thus, any non-zero non-invertible element in a PID can be factorised into a product of primes. What is interesting about this factorisation is the following result that you have already proved for Z in Unit 1.

Theorem 12 : Let R be a PID and $a \neq 0$ be non-invertible in R. Let $a = p_1 p_2 \ldots p_n = q_1 q_2 \ldots q_m$, where p_i and q_j are prime elements of R. Then $n = m$ and each p_i is an associate of some q_j for $1 \leq i \leq n$, $1 \leq j \leq m$.

Before going into the proof of this result, we ask you to prove a property of prime elements that you will need in the proof.

E 15) Use induction on n to prove that if p is a prime element in an integral domain R and if $p \mid a_1 a_2 \ldots a_n$ (where $a_1, a_2, \ldots, a_n \in R$), then $p \mid a_i$ for some $i = 1, 2, \ldots, n$.

Now let us start the proof of Theorem 12.

Proof : Since $p_1 p_2 \ldots p_n = q_1 q_2 \ldots q_m$, $p_1 \mid q_1 q_2 \ldots q_m$.

Thus, by E 15, $p_1 \mid q_j$ for some $j = 1, \ldots, m$. By changing the order of the q_i, if necessary, we can assume that $j = 1$, i.e., $p_1 \mid q_1$. Let $q_1 = p_1 u_1$. Since q_1 is irreducible, u_1 must be a unit in R. So p_1 and q_1 are associates. Now we have

$$p_1 p_2 \ldots p_n = (p_1 u_1) q_2 \ldots q_m.$$

Cancelling p_1 from both sides, we get

$$p_2 p_3 \ldots p_n = u_1 q_2 \ldots q_m.$$

Now, if $m > n$, we can apply the same process to p_2, p_3, and so on.

Then we will get

$1 = u_1 u_2 \ldots u_n q_{n+1} \ldots q_m$.

This shows that q_{n+1} is a unit. But this contradicts the fact that q_{n+1} is irreducible.

Thus, $m \leq n$.

Interchanging the roles of the ps and qs and by using a similar argument, we get $n \leq m$.

Thus, $n = m$.

During the proof we have also shown that each p_i is an associate of some q_j, and vice versa.

What Theorem 12 says is that **any two prime factorisations of an element in a PID are identical, apart from the order in which the factors appear and apart from replacement of the factors by their associates.**

Thus,.Theorems 11 and 12 say that every non-zero element in a PID R, which is not a unit, can be expressed uniquely (upto associates) as a product of a finite number of prime elements.

For example, $x^2-1 \in \mathbf{R}[x]$ can be written as $(x-1)(x+1)$ or $(x+1)(x-1)$ or $[\frac{1}{2}(x-tl)][2(x-1)]$ in $\mathbf{R}[x]$.

Now you can try the following exercise.

E 16) Give the prime factorisation of $2x^2-3x+1$ in $\mathbf{Q}[x]$ and $\mathbf{Z}_2[x]$.

The property that we have shown for a PID in Theorems 11 and 12 is true for several other domains also. Let us discuss such rings now.

14.4 UNIQUE FACTORISATION DOMAIN (UFD)

In this section we shall look at some details of a class of domains that includes PIDs.

Definition : We call an integral domain R a **unique factorisation domain** (UFD, in short) if every non-zero element of R which is not a unit in R can be uniquely expressed as a product of a finite number of irreducible elements of R.

Thus, if R is a UFD and $a \in R$, with $a \neq 0$ and a being non-invertible, then

i) a can be written as a product of a finite number of irreducible elements, and

ii) if $a = p_1 p_2 \ldots p_n = q_1 q_2 \ldots q_m$ be two factorisations into irreducibles, then $n = m$ and each p_i is an associate of some q_j, where $1 \leq i \leq n$, $1 \leq j \leq m$.

Can you think of an example of a UFD? Do Theorems 11 and 12 help? Of course! In them we have proved that **every** PID is **a UFD.**

Every Euclidean domain is a UFD.

Thus, $F[x]$ is a UFD for any field F.

Also, since any Euclidean domain is a PID, it is also a UFD. OF course, in Unit 1 you directly proved that Z is a UFD. Why don't you go through that proof and then try and solve the following exercises.

E 17) Directly prove that $F[x]$ is a UFD, for any field F.

(Hint : Suppose you want to factorise f(x). Then use induction on deg **f(x).)**

E 18) Give two different prime factorisations of 10 in Z.

So you have seen several examples of UFDs. Now we give you an example of a domain which is not a UFD (and hence, neither a PID nor a Euclidean domain).

Example 6 : Show that $Z[\sqrt{-5}] = \{a+b\sqrt{-5} \mid a,b \in Z\}$ is not a UFD.

Solution : Let us define a function

$f : Z[\sqrt{-5}] \to N \cup \{0\}$ by $f(a+b\sqrt{-5}) = a^2+5b^2$.

This function is the norm function, and is usually denoted by N.

You can check that this function has the property that

$f(\alpha\beta) = f(\alpha)\, f(\beta)\ \forall\ \alpha,\beta \in Z[\sqrt{-5}]$.

Now, 9 has two factorisations in $Z[\sqrt{-5}]$, namely,

$9 = 3.3 = (2+\sqrt{-5})(2-\sqrt{-5})$.

In Example 3, you have already shown that the only units of $Z[\sqrt{-5}]$ are 1 and –1. Thus, no two of 3, $2+\sqrt{-5}$ and $2-\sqrt{-5}$ are associates of each other.

Also, each of them is irreducible. For suppose any one of them,

say $2+\sqrt{-5}$, is reducible. Then

$2+\sqrt{-5} = \alpha\beta$ for some non-invertible $\alpha,\beta \in Z[\sqrt{-5}]$.

Applying the function f we see that

$f(2+\sqrt{-5}) = f(\alpha)\, f(\beta)$,

i.e., $9 = f(\alpha)\, f(\beta)$.

Since $f(\alpha),\ f(\beta) \in N$ and α, β are not units, the only possibilities are $f(\alpha) = 3 = f(\beta)$.

So, if $a = a+b\sqrt{-5}$, then $a^2+5b^2 = 3$.

But, if $b \neq 0$, then $a^2 + 5b^2 \geq 5$; and if $b = 0$, then $a^2 = 3$ is not possible in Z. So we reach a contradiction. Therefore, our assumption that $2+\sqrt{-5}$ is reducible is wrong. That is, $2+\sqrt{-5}$ is irreducible.

Similarly, we can show that 3 and $2-\sqrt{-5}$ are irreducible. Thus, the factorisation of 9 as a product of irreducible elements is not unique. Therefore, $Z[\sqrt{-5}]$ is not a UFD.

From this example you can also see that an irreducible element need not be a prime element. For example, $2+\sqrt{-5}$ is irreducible and $2+\sqrt{-5} \mid 3.3$, but $2+\sqrt{-5} \nmid 3$. Thus, $2+\sqrt{-5}$ is not a prime element.

Now for an exercise,,

E 19) Give two different factorisations of 6 as a product of irreducible elements in $Z[\sqrt{-5}]$.

Now let us discuss some properties of a UFD. The first property says that any two elements of a UFD have a g.c.d; and their g.c.d is the product of all their common factors. Here we will use the fact that any element a in a UFD R can be written as

$$a = p_1^{r_1} p_2^{r_2} \ldots p_n^{r_n}$$

where the p_is are distinct irreducible elements of R. For example, in $Z[x]$ we have $x^3-x^2-x+1 = (x-1)(x+1)(x-1) = (x-1)^2(x+1)$.

So, let us prove the following result.

Theorem 13 : Any **two** elements of a UFD have a g.c.d.

Proof : Let R be **a** UFD and a,b ∈ R.

Let $a = p_1^{r_1} p_2^{r_2} \ldots p_n^{r_n}$ and $b = p_1^{s_1} p_2^{s_2} \ldots p_n^{s_n}$

where $p_1, p_2, \ldots, p_n$ are distinct irreducible elements of R and r_i and s_i are non-negative integers $\forall\ i = 1,2,\ldots,n$.

(If some p_i does not occur in the factorisation of a, then the corresponding $r_i = 0$. Similarly, if some p_i is not a factor of b, then the corresponding $s_i = 0$. For example, take 20 and 15 in Z. Then $20 = 2^2 \times 3^0 \times 5^1$ and $15 = 2^0 \times 3^1 \times 5^1$.)

Now, let $t_i = \min(r_i, s_i)\ \forall\ i = 1, 2, \ldots, n$.

Then $d = p_1^{t_1} p_2^{t_2} \ldots p_n^{t_n}$ divides a as well as b, since $t_i \le r_i$ and $t_i \le s_i\ \forall\ i = 1,2,\ldots,n$.

Now, let $c \mid a$ and $c \mid b$. Then every irreducible factor of c must be an irreducible factor of a and of b, because of the unique factorisation property.

Thus, $c = p_1^{m_1} p_2^{m_2} \ldots p_n^{m_n}$, where $m_i \le r_i$ and $m_i \le s_i\ \forall\ i = 1,2,\ldots,n$. Thus, $m_i \le t_i\ \forall\ i = 1,2,\ldots,n$.

Therefore, $c \mid d$.

Hence, $d = (a,b)$.

This theorem tells us that the method we used for obtaining the g.c.d in Example 5 and E 10 is correct.

Now, let us go back to Example *6* for a moment. Over there we found a non-UFD in which an irreducible element need not be a prime element. The following result says that this distinction between irreducible and prime elements can only occur in a domain that is not a UFD.

Theorem 14 : Let R be a **UFD.** An element of R is prime iff it is irreducible.

Proof': By E13 we know that every prime in R is irreducible. So let us prove the converse.

Let a ∈ R be irreducible and let $a \mid bc$, where b,c ∈ R.

Consider (a,b). Since a is irreducible, (a,b) ='1 or (a,b) = a.

If (a,b) = a, $a \mid b$.

If (a,b) = I, then $a \nmid b$. Let bc = ad, where d ∈ R.

Let $b = p_1^{r_1} p_2^{r_2} \ldots p_m^{r_m}$ and $c = q_1^{s_1} q_2^{s_2} \ldots q_n^{s_n}$, be irreducible factorisations of b and c. Since bc = ad and a is irreducible, a must be one of the pis or one of the q_js. Since $a \nmid b$, $a \neq p_i$ for any i. Therefore, $a = q_j$ for some j. That is, $a \mid c$.

Thus, if (a,b) = 1 . then $a \mid c$.

So, we have shown that $a \mid bc \Rightarrow a \mid b$ or $a \mid c$.

Hence, a is prime.

For the final property of UFDs that we are going to state, let us go back to. Example 4 for a moment. Over there we gave you an example of a PID R, for which R [x] is not a PID. You may ask what happens to R[x] if R is a UFD. We state the following result.

Theorem 15 : Let R be a UFD. Then R[x] is a UFD.

We will not prove this result here, even though it is very useful to mathematicians. But let us apply it. You can use it to solve the following exercises.

E 20) Give an example of a UFD which is not a PID.

E 21) If p is an irreducible element of a UFD R, then is it irreducible in every quotient ring of R?

E 22) Is the quotient ring of a UFD a UFD? Why?

E 23) Is a subring of a UFD a UFD? Why?

Let us wind up this unit now, with a brief description of what we have covered in it.

14.5 SUMMARY

In this unit we have discussed the following points.

1) The definition and examples of a Euclidean domain.
2) Z, any field and any polynomial ring over a field are Euclidean domains.
3) Units, associates, factors, the g.c.d of two elements, prime elements and irreducible elements in an integral domain.
4) The definition and examples of a principal ideal domain (PID).
5) Every Euclidean domain is a PID, but the converse is not true.

   Thus, Z, F and F[x] are PIDs, for any field F.
6) The g.c.d of any two elements a and b in a PID R exists and is of the form ax+by for some $x,y \in R$.
7) The Fundamental Theorem of Algebra: Any non-constant polynomial over C has all its roots in C.
8) In a PID every prime ideal is a maximal ideal.
9) The definition and examples of a unique factorisation domain (UFD).
10) Every PID is a UFD, but the converse is not true. Thus Z, F and F[x] are UFDs, for any field F.
11) In a UFD (and hence, in a PID) an element is prime iff it is irreducible.
12) Any two elements in a UFD have a g.c.d.
13) If R is a UFD. then so is R[x].

14.6 SOLUTIONS/ANSWERS

E 1) $d : F \setminus \{0\} \to N \cup \{0\} : d(x) = 1$

For any $a, b \in F \setminus (0)$,

$d(ab) = 1 = d(a)$.

$\therefore d(a) = d(ab)\ \forall\ a,b \in F \setminus \{0\}$,

Also, for any $a,b \in F$, $b \neq 0$,

$a = (ab^{-1})b + 0$.

So, F trivially satisfies the second condition for a domain to be Euclidean.

Thus. F is a Euclidean domain,

E 2) In Unit 13, you have seen that

deg (f(x) g(x)) = deg f(x)+deg g(x) $\forall$ f(x), g(x) $\in$ F [x] \ {0}.

Now, use Theorem 5 of Unit 13, and you will have proved the result.

E 3) a) $m \in \mathbf{Z}$ is a unit iff $\exists\ n \in \mathbf{Z}$ such that mn = 1, i.e., iff $m = \pm 1$.

b) Let $\bar{m} \in \mathbf{Z}_6$ be a unit. Then $\exists\ \bar{n} \in \mathbf{Z}_6$ such that $\bar{m}\,\bar{n} = \bar{1}$.

Thus, from Sec. 1.6.2 we see that m is a unit if the g.c.d of m and 6 is 1.

$\therefore$ $\bar{m} = \bar{1}$ or $\bar{5}$.

c) $\mathbf{Z}/5\mathbf{Z}$ is a field. Thus, the units are all its non-zero elements.'

d) Let a+ib be a unit. Then $\exists$ c+id $\in$ $\mathbf{Z}+i\mathbf{Z}$ such that.

(a+ib) (c+id) = 1.

$\Rightarrow$ (ac–bd)+(ad+bc)i = 1

$\Rightarrow$ ac–bd = 1 and ad+bc = 0.

$\Rightarrow$ b = 0, as in Example 3.

Thus, a+ib = 1 or –1, using (a) above.

E 4) Let $u \in R$ be a unit. Then $\exists\ v \in R$ such that vu = 1. Thus, for any $r \in R$, r = r. 1 = r(vu) = (rv)u $\in$ Ru.

Thus. R $\subseteq$ Ru. $\therefore$ R = Ru.

Conversely, let Ru = R. Since $1 \in R = Ru$, $\exists\ v \in R$ such that

1 = vu. Thus, u is a unit in R.

E 5) Apply Theorem 2 to the Euclidean domain F[x].

E 6) Let R = Z. Then $S = \{n \in Z^* \mid |n| > 1\} \cup \{0\}$.

Then $2 \in S$, $3 \in S$ but $2-3 \notin S$ since 12–31 = 1.

Thus, S is not even a subring of R.

E 7) For example, Z[x] is a subring of Q[x], which is a PID. But Z[x] is not a PID.

E 8) Z is a PID. But 2/62 is not even a domain. Thus, it is not a PID.

E 9) a) u is a unit iff uv = 1 for some $v \in R$ iff u | 1.

b) a | b and b | a

$\Rightarrow$ b = ac and a = bd for some b,d $\in$ R.

$\Rightarrow$ b = bdc

$\Rightarrow$ b = 0 or dc = 1

If b = 0, then a = 0, and then a and b are associates.

If $b \neq 0$, then dc = 1. Thus, c is a unit and b = ac.

Therefore, a and bare associates.

Conversely, let a and b be associates in R, say a = bu, where u is a unit in R. Then b | a. Also, let $v \in R$ such that uv = 1. Then av = buv = b.

Thus, a | b.

E 10) a) $\bar{2}$.

b) $x^2+8x+15 = (x+3)(x+5)$, $x^2+12x+35 = (x+5)(x+7)$

Thus, their g.c.d is x+5

c) $x^3-2x^2+6x-5 = (x-1)(x^2-x+5)$, $x^2-2x+1 = (x-1)^2$.

Thus, their g.c.d is x–1.

E 11) $\exists\ x,y \in R$ such that $ax+by = 1$.

Then $c = 1.c = (ax+by)c = acx+bcy$

Since $a \mid ac$ and $a \mid bc$, $a \mid (acx+bcy) = c$.

E 12) (c) is, because of Theorem 5'.

(a) is not, since it is $(x-1)^2$.

(b) is not, because of Theorem 5'.

(d) is not, because of Theorem 6.

E 13) Let $p = ab$. Then $p \mid ab \Rightarrow p \mid a$ or $p \mid b$. Suppose $p \mid a$. Let $a = pc$. Then $p = ab = pcb$ $\Rightarrow p(1-cb) = 0 \Rightarrow 1-cb = 0$, since R is a domain and $p \neq 0$. Thus, $bc = 1$, i.e., b is a unit. Similarly, you can show that if $p \mid b$, then a is a unit.

So, $p = ab \Rightarrow$ a is a unit or b is a unit, i.e., p is irreducible.

E 14) (a), (c), since 5 and x^2+x+1 are irreducible in Z and $\mathbf{R}[x]$, respectively.

(b) is not, using Theorem 9.

(d) is not, since $\mathbf{Z}[x]/\langle x \rangle \simeq Z$, which is not a field.

E 15) The result is clearly true for $n = 1$. Assume that it holds for all $m < n$, i.e., whenever $m < n$ and $p \mid a_1 a_2 \ldots a_m$, then $p \mid a_i$ for some $i = 1,2,\ldots,m$.

Now let $p \mid a_1 a_2 \ldots a_n$. Then $p \mid (a_1 a_2 \ldots a_{n-1})a_n$.

Since p is a prime element, we find that $p \mid a_1 a_2 \ldots a_n$ or $p \mid a_n$.

If $p \mid a_1 a_2 \ldots a_{n-1}$, then $p \mid a_i$ for some $i = 1,\ldots,n-1$ by our assumption.

If $p \nmid a_1 \ldots a_{n-1}$, $p \mid a_n$.

Thus, in either case, $p \mid a_i$ for some $i = 1,\ldots, n$.

So, our result is true for n.

Hence, it is true $\forall\ n \in N$.

E 16) $2x^2-3x+1 = (2x-1)(x-1)$ in $\mathbf{Q}[x]$.

In $\mathbf{Z}_2[x]$ the given polynomial is $x+\bar{1}$, since $\bar{2} = \bar{0}$ and $-\bar{3} = \bar{1}$.

This polynomial is linear, and hence, irreducible over $\mathbf{Z}_2$.

Thus, its prime factorisation is just $x+\bar{1}$.

E 17) Let $f(x)$ be a non-zero non-unit in $F[x]$ and let deg $f(x) = n$.

Then $n > 0$. We will prove that $f(x)$ can be written as a product of irreducible elements, by induction on n. If $n = 1$, then $f(x)$ is linear, and hence irreducible.

Now suppose that the result is true for polynomials of degree $< n$. Now take $f(x)$. If $f(x)$ is irreducible, there is nothing to prove. Otherwise, there is a prime $f_1(x)$ such that $f_1(x) \mid f(x)$. Let $f(x) = f_1(x)g_1(x)$. Note that deg $f_1(x) > 0$.

Hence, deg $g_1(x) <$ deg $f(x)$. If $g_1(x)$ is prime, we are through. Otherwise we can find a prime element $f_2(x)$ such that $g_1(x) = f_2(x)g_2(x)$. Then deg $g_2(x) <$ deg $g_1(x)$. This process must stop after a finite number of steps, since, each time we get polynomials of lower degree. Thus, we Shall finally get

$f(x) = f_1(x) f_2(x) \ldots f_m(x)$,

where each $f_i(x)$ is prime in $F[x]$.

Now, to show that the factorisation is unique you go along the lines of the proof of Theorem 12.

E 18) $10 = 2 \times 5 = 5 \times 2$.

E 19) $6 = 2.3 = (1+\sqrt{-5})(1-\sqrt{-5})$.

Using the norm function you should check that each of $2, 3, 1+\sqrt{-5}$ and $1-\sqrt{-5}$ are irreducible in $\mathbf{Z}[\sqrt{-5}]$.

E 20) $\mathbf{Z}[x]$.

E 21) No. For example, x is irreducible in $\mathbf{Z}[x]$; but $\bar{x}$ is zero in $\mathbf{Z}[x]/< x >\simeq \mathbf{Z}$.

E 22) The quotient ring of a domain need not be a domain. For example, $\mathbf{Z}$ is a UFD, but $\mathbf{Z}/<4>$ is not.

Also, even if the quotient ring is a domain, it may not be a UFD. For example, $\mathbf{Z}[\sqrt{-5}] \simeq \mathbf{Z}[x]/< x^2+5 >$ is not a UFD, while $\mathbf{Z}[x]$ is.

E 23) No. For example, $\mathbf{Z}[\sqrt{-5}]$ is a subring of $\mathbf{C}$, a UFD. But $\mathbf{Z}[\sqrt{-5}]$ is not a UFD.