MODULE 2

UNIT 1 THE BASICS

CONTENT

1.0 INTRODUCTION

We are considering in this unit a special ring, whose specialties lay in the property of their multiplication. We shall examine a type of ring called Integral Domain. In MTH 312 we shall examine Rings into details and also examine their mathematical structures.

Next, we will look at rings like Q, R, C, and Z_p (where p is a prime number). In these rings the non-zero elements form an abelian group under multiplication. Such rings are called fields. These structures are very useful, one reason being that we can "divide" in them.

Related to integral domains and fields are certain special ideals called prime ideals and maximal ideals. In this unit we will also discuss them and their corresponding quotient rings.

Finally, we shall see how to construct the smallest field that contains a given integral domain. This is essentially the way that Q is constructed from Z. we call such a field the field of quotients of the corresponding integral domain.

In this unit, we have tried to introduce you to a lot of new concepts. You may need some time to grasp them. Don't worry; take as much time as you need. But by the time you finish it, make sure that you have attained the following objectives. Only then will you be comfortable in the remaining units of this course.

2.0 OBJECTIVES

At the end of this unit, you should be able to:

- check whether an algebraic system is an integral domain or not
- obtain the characteristic of any ring
- check whether an algebraic system is a field or not
- define and identify prime ideals and maximal ideals
- prove and use simple properties of integral domains and fields
- construct or identify the field of quotients of an integral domain.

3.0 MAIN CONTENT

3.1 Integral Domains

You know that the product of two non-zero integers is a non-zero integer, i.e., if m, n $\in$ Z such that m = 0, n $\neq$ 0, then mn $\neq$ 0. Now consider the ring Z_6. We find that $\bar{2} \neq \bar{0}$ and $\bar{3} \neq \bar{0}$, yet $\bar{2}.\bar{0} = \bar{0}$. So, we find that the product of the non-zero elements $\bar{2}$ and $\bar{3}$ in Z_6 is zero. As you will soon realize, this shows that $\bar{2}$ (and $\bar{3}$) is a zero divisor, i.e., $\bar{0}$ is divisible by $\bar{2}$ (and $\bar{3}$).

So, let us see what a zero divisor s.

Definition

A non-zero element in a ring R is called a zero divisor in R if there exists a non-zero element b in R such that ab = 0

(Note that b will be a zero divisor~ too!)

Now do you agree that $\bar{2}$ is a zero divisor in Z_6? What about $\bar{3}$ in Z_4? Since $\bar{3}$ x $\neq \bar{0}$ for every non-zero x in Z_4, $\bar{3}$ is not a zero divisor in Z_4.

Our short discussion may help you to do the following exercise.

E 1) Let n E N and m | n, 1 < m < n. Then show that $\bar{m}$ is a zero divisor in Z_n.

Now let us look at an example of a zero divisor m C[0,1]. Consider the function f $\in$ C[0,1] given by f(x) =

$$f(x)=\begin{cases} x-\frac{1}{2}, 0\le x\le 1/2 \\ 0, 1/2\le x\le 1 \end{cases}$$

Let us define g: [0,1] $\rightarrow$ R by

$$g(x)=\begin{cases} 0, 0\le x\le 1/2 \\ x-1/2, 1/2\le x\le 1 \end{cases}$$

Then g$\in$ C[0.l], g $\neq$ 0 and (fg) (x) = 0 $\forall x \in$ [0,l], Thus, fg is the zero function. Hence, f is a zero divisor in C[0,1].

For another example, consider the Cartesian product of two non-trivial rings A and B. For every a $\neq$ 0 in A. (a.0) is a zero divisor in A x B, This is because, for any b $\neq$ 0 in B, (a.0) (0.b) = (0.0)

Now let us look al the ring $\wp$(X), where X is a set with at least two elements. Each non empty proper subset A of X is a zero divisor because A.A^c = A$\cap A^c = \phi$, the zero element of $\wp$(X).

Try these exercises now.

E 2) List all the zero divisors m Z.

E 3) For Which rings with unity will I be a zero divisor?

E 4) Let R be a ring and a $\in$R be a zero divisor. Then show that every element of the principal deal Ra is a zero divisor.

Let us now talk of a type of ring that is without zero divisors.

Definition

We call a non-zero ring R an **integral domain** if

i) R is with identity and
ii) R has no Zero divisors.

Thus, an integral domain is a non-zero ring with identity in which the product of two non-zero elements.

This kind of ring gets its name from the set of integer, one of its best known examples. Other examples of domains that immediately come to mind are **Q.R** and **C**. What about $\subset$ [01,]? You have already seen that it has zero divisors. Thus C[0.1] is not a domain

The next result gives us an important class of examples of integral domains

Theorem 1

Zp is an integral domain iff p is a prime number,

Proof

Firstly, let us assume that p is a prime number. Then you know that Z_p is a non-zero ring with identity. Let us see if it has zero divisors/ for this, suppose $\bar{a},\bar{b}\in Z_p$ satisfy $\bar{a},\bar{b}=\bar{0}$ then $a\bar{b}=\bar{0}$, i.e., p | ab. Since p is a prime number, using E 25 of Unit 1 we see that p | a or p | b. Thus, a = $\bar{a}=\bar{0}\ or \bar{b}=\bar{0}$. What we have shown is that if $\bar{a}\neq\bar{0}$ and $\bar{b}\neq\bar{0}$, then $\bar{a}\bar{b}\neq\bar{0}$. Thus, Z_p is the trivial ring, which is not a domain.

Conversely, we will show that if p is not a prime, then Z_p is not a domain. So, suppose p is not a prime. If p = 1, then Z_p is the trivial ring, which is not a domain.

If p is a composite number and m | p, then by E 1 you know that $\bar{m}\in Z_p$ is a zero divisor. Thus, Zp has zero divisors. Hence, it is not a domain.

Try this exercise now

E 5) Which of the following rings are not domains? Why?
Z_4, Z_5, 2Z, Z + iZ, R x R, {0}

Now consider a ring R. we know that the cancellation law for addition holds in R, i.e whether a+b = a+c in R, then b = c. But, does ab = ac imply b = c? it need not. For example, o.1 = 0.2 in Z but $1\neq 2$. So, if a = 0, ab = ac need not imply b = c. But, if $a\neq 0$ and ab = ac, is it true that b = c? We will prove that this is true for integral domains.

Theorem 2

A ring R has no zero divisors if and only if the cancellation law for multiplication holds in R (i.e., if a,b,c$\in$ R such that a $\neq 0$, and ab = ac, then b = c)

Proof

Let us first assume that R contains no zero divisors. Assume that a,b,c$\in$R such that a$\neq 0$. Suppose ab = 0 for some b$\in$R. Then ab = 0 = a0. Using the cancellation law for multiplication, we get b = 0. So, a is not a zero divisor, i.e., R has no zero divisors.

Using this theorem we can immediately say that the cancellation aw holds for multiplication in an integral domain.

Now, you can use this property of domains to solve the following exercises.

E 6) In a domain, show that the only solutions of the equation $x^2 = x$ are x = 0 and x = 1.

E 7) Prove that 0 is the only nilpotent element (see Example 9 of Unit 10) in a domain.

Now let us introduce a number associated with an integral domain, in fact, with any ring. For this let us look at Z_4 first. We known that 4x = $\bar{0} \forall x \in Z_4$. In fact, 8x = $\bar{0}$ and 12 x = $\bar{0}$ also for any x $\in Z_4$.

But 4 is the least element of the set $\{n \in N \mid nx = \bar{0} \forall x \in Z_4\}$. This shows that 4 is the characteristics pf Z_4 as you will see now.

Definition

Let R be a ring. The least positive integer n such that nx = $0 \forall x \in$ R is called the characteristic of R. If there is no positive integer n such that nx= $0 \forall x \in$ R, then we say that the characteristic of R is zero.

We denote the characteristic of the ring R by char R.

You can see that char Z_n = n and char Z = 0.

The following exercises will give you some practice in obtaining the characteristic of a ring.

E 8) Show that char $\wp(X) = 2$, where X is a non empty set.

E 9) Let R be a ring and char R = m. What is char (R x R)

Now let us look at a nice result for integral domains. It helps in considerably reducing our labour when we want to obtain the characteristic of a domain.

Theorem 3

Let m be a positive integer and R be an integral domain. Then the following conditions are equivalent.

a) m 1 = 0.
b) ma = 0 for all a $\in$ R.
c) ma = 0 for some a $\neq$ in R.

Proof

We will prove (a) $\Rightarrow$ (b) $\Rightarrow$ (c) $\Rightarrow$ (a).
(a) $\Rightarrow$ (b): We know that m l = 0.

Thus, for any a $\in$ R, ma = (la) = (ml) (a) = 0a = 0, i.e., (b) holds.

(b) $\Rightarrow$ (c): If ma = 0 a $0 \forall\ a \in$ R, then it is certainly true for some a $\neq$ 0 in R.

(c) $\Rightarrow$ (a) : Let mil = 0 for some a $\neq$ 0 in R. Then 0 = ma = m (1a) = (m.) a. As a $\neq$ 0 and R is without zero divisors, we get m1 = 0.

What Theorem 3'tells us is that **to find** the **characteristic of a domain we on1y need to look at the set {n,1 | n $\in$ N}.**

Let us look at some examples.

i) char Q=0, since n.1 $\neq$ 0 for any n $\in$ N.
ii) Similarly, char R = 0 and char C = 0.
iii) You have already seen that char Z_n = n. Thus, for any positive integer n, there exists a ring with characteristic n.

Now let us look at a peculiarly of the characteristic of a domain.

Theorem 4

The characteristic of an integral domain is either zero or a prime number.

Proof

Let R be a domain. We will prove that if the characteristic of R is not zero, then it is a prime number. So suppose char R = m, where $m \neq 0$. So m Iii the least positive integer such that m.1 = 0. We will show that m is a prime number by supposing that it is not, and then proving that our supposition is wrong.

So suppose m = st, where s,t $\in$ N, 1 < s < m and 1 < t < m. Then m.1 = 0 $\Rightarrow$ (st). l = 0 $\Rightarrow$ (s.l) (t.1) = 0. As R is without zero divisors, we get s.l = 0 or t.1 = 0. But, s and t are less than m. So, we reach a contradiction to the fact that m = char R. Therefore, our assumption that m = st, where 1 < s < m, 1 < t < m is wrong. Thus, the only factors of m are 1 and itself. That is, m is a prime number.

You can now use your knowledge of characteristics to solve the following exercise

E 10) Let R be an integral domain of characteristic p. Pr0ve that

a) $(a+b)^p = a^p + b^p$ and
$(a-b)^p = a^p - b^p$ for all a, b $\in$ R."

b) the subset $\{ a^p \mid a \in R\}$ is it subring of R.

c) the map $\Phi : R \rightarrow R : \Phi(a) = a^p$ is a ring homomorphism.

d) if R is a finite integral domain, then Φ is an isomorphism.

E 11) Let R be a ring with unity 1 and char R = m. Define f: Z $\rightarrow$ R: f (n) = n.1. Show that f is a homomorphism. What is Kerf?

E 12) Find the characteristic of Z_3 x Z_4. Use this ring as an example to show why Theorems 3 and 4 are only true for integral domains.

We will now see what algebraic structure we get after we impose certain restrictions on the multiplication of a domain. If you have gone through our course Linear Algebra, you will already be familiar with the algebraic system that we are going to discuss, namely, a field.

3.2 Field

Let (R, +,.) be a ring. We know that (R, +) is an abelian group. We also know that the operation is commutative and associative. But (R,.) is not an abelian group. Actually, even if R has identity, (R.,) will never be a group since there is no element $a \in R$ such that a.0 = 1. But can (R\{0}.,) be a group? It can, in some cases. For example, from Unit 2 you know that **Q*** and **R*** are groups with respect to multiplication. This allows us to say that **Q** and **R** are fields a term we will now define.

Definition

A ring (r, +.,) is called a **field** if (R\{0}.,) is an abelian group.

Thus, for a system (R, +.,) to be a field it must satisfy the ring axioms R1 to R6 as well as the following axioms.

i) is commutative,
ii) R has identity (which we denote by 1) and $1 \neq 0$, and
iii) every non-zero element x in R has a multiplicative inverse, which we denote by x^{-1}.

Just as a matter of information we would like to tell you that a ring that satisfies only (ii) and (iii) above, is called a **division ring** or a **shew field** or a **non-commutative field**. Such rings are very important in the study of algebra, but we will not be discussing them in this course.

Let us go back to fields now. The notion of a field evolved during the 19^{th} century through the research of the German mathematicians Richard Dedekind and Leopold Kronecker in algebraic number theory. Dedekind used the German word Korper, which assdfsdf field, for this concept. This is why you will often find that a field is denoted by K.

As you may have realized, two of the best known examples of fields are **R** and **C**. These were the fields that Dedekind considered. Yet another example of a field is the following ring.

Example 1

Show that **Q** + $\sqrt{2Q} = \{a + \sqrt{2}b \mid a, b \in Q\}$ is a field.

Solution

From Unit 9 you know that F = Q + $\sqrt{2Q}$ is a commutative ring with identity 1 + $\sqrt{2.0}$.

$$(a+\sqrt{2b}) = \frac{1}{a+\sqrt{2b}} = \frac{2-\sqrt{2b}}{(a+\sqrt{2b})\,(a-\sqrt{2b})} = \frac{a-\sqrt{2b}}{a^2-4b^2}$$

$$= \frac{a}{2^2-2b^2} + \sqrt{2}\ \frac{(-b)}{2^2-2b^2} \in F$$

(Note that a^2-$2b^2 \neq 0$, since $\sqrt{2}$ is not rational and either $a \neq 0$ or $b \neq 0$.)

Thus, every non-zero element has a multiplicative inverse. Therefore, Q+ $\sqrt{2}Q$ is a field.

Can you think of an example of a ring that is not a field? Does every non-zero integer have a multiplicative inverse in Z? No. Thus, Z is not a field.

By now you have seen several examples of fields. Have you observed that all of them happen to be integral domains also? This is not a coincidence. In fact, we have the following result.

Theorem 5

Every field is an integral domain.

Proof

Let F be a field. Then $F \neq \{0\}$ and $1 \in F$. we need to see if F has zero divisors. So let a and b be elements of F such that ab = 0 and $a \neq 0$ and F is a field, a^{-1} exists. Hence, b =1.b = $(a^{-1}a)$ b = a^{-1} (ab) = a^{-1} 0 = 0. Hence, if $a \neq 0$ and ab = 0, we get b = 0. i.e., F has no zero divisors. Thus, F is a domain.

Now you try these exercises!

E 13) Which of the following rings are not fields?
2Z, Z_5, Z_6, Q x Q

E 14) Will a subring of a field be a field? Why?

Theorem 5 may immediately prompt you to ask if every domain is a field. You have already seen that Z is a domain but not a field. But if we restrict ourselves to finite domains, we find that they are fields.

Theorem 6

Every finite integral domain is a field.

Proof

Let R = $\{a_0 = 0, a_1 = 1, a_2\ldots\ldots,2_n\}$ be a finite domain. Then R is commutative also. To show that R is a field we must show that every non-zero element of R has a multiplicative inverse.

So, let $a = a_i$ be a non-zero element of R (i.e., $i \neq 0$). Consider the elements $aa_1,\ldots, aa_n$. For every $j \neq 0$, $aj \neq 0$; and since $a \neq 0$, we get $aaj \neq 0$.

Hence, the set $\{aa_1, aa_2\ldots..,aa_n\} \subseteq \{a_1,\ldots..,a_n\}$.

Also, aa1, aa2,…, aa_n are all distinct elements of the set $\{a_1,\ldots..,a_n\}$, since $aaj = aa_k \Rightarrow aj = ak$, using the cancellation law for multiplication.

Thus, $\{aa_1,\ldots.,aa_n\} = \{a_1,\ldots.,a_n\}$.

In particular, $a_1 = aaj$, i.e., $1 = aaj$ for some j. thus, a is invertible in R. hence every non-zero element of R has a multiplicative inverse. Thus, R is a field.

Using this result we can now prove a theorem which generates several examples of finite fields.

Theorem 7

Z_n is a field if and only if n is a prime number.

Proof

From Theorem 1 you know that Z_n is a domain if and only if n us a prime number. You also know that Z_n has only n elements. Now we can apply Theorem 6 to obtain the result.

Theorem 7 unleashes a load of examples of fields: Z_2, Z_3, Z_5, Z_7, and so on. Looking at these examples, and other examples of fields, can you say anything about the characteristic of a field? In fact. Using Theorems 4 and 5 we can say that.

Theorem 8

The characteristic of a field is either zero or a prime number.

So far the examples of finite fields that you have seen have consisted of p elements, for some prime p. In the following exercise we give you an example of a finite field for which this is not so.

E 15) Let R = {0,1,a,1+a}. Define + and in R as given in the following Cayley tables

+	0	1	a	1+a		.	0	1	a	1+a
0	0	1	a	1+a		0	0	0	0	0
1	1	0	1+a	a	and	1	0	1	a	1+a
a	a	1+a	0	1		a	0	a	1+a	1
1+a	1+a	a	1	0		1+a	0	1+a	1	a

Show that R is a field. Find the characteristic of this field.

Let us now look at an interesting condition for a ring to be a field

Theorem 9

Let R be a ring with identity. Then R is a field if and only if Rand {0} are the only ideals of R.

Proof

Let us first assume that R is a field. Let I be an ideal of R. If $I \neq \{0\}$, there exists a non-zero element $x \in I$. As $x \neq 0$ and R is a field, xy = 1 for some $y \in R$. Since $x \in I$ and I is an ideal, $xy \in I$. i.e., $1 \in I$.

Thus, by Theorem 4 of Unit 10, I = R. So, the only ideals of R are {0} and R.

Conversely, assume that Rand {0} are the only ideals of R. Now, let $a \neq 0$ be an element of R. Then you know that the set $Ra = \{ra \mid r \in R\}$ is a non-zero ideal of R. Therefore, Ra = R. Now, $1 \in R = Ra$. Therefore, 1 = ba for some $b \in R$, i.e., a^{-1} exists. Thus, every non-zero element of R has a multiplicative inverse. Therefore, R is a field.

This result is very useful. You will be applying it again and again in the rest of the units of this block.

Using Theorem 9, we can obtain some interesting facts about **field homeomorphisms** (i.e., ring homeomorphisms from one field to another). We give them to you in the form of an exercise.

E16) Letf: F $\rightarrow$ K be a field homomorphism. Show that either f is the zero map or f is 1-1.

E 17) Let R be a ring isomorphic to a field F. Show that R must be a field.

E 17 again goes to show that isomorphic algebraic structures must be algebraically identical.

Now that we have discussed domains and fields, let us look at certain ideals of a ring, with respect to which the. quotient rings are domains or fields.

3.3 Prime and Maximal Ideals

In Z we know that if P is a prime number and p divides the product of the integers a and b, then either p divides a or p divides b. In other words, if ab $\in$ pZ, then either a $\in$ pZ or b $\in$ pZ. Because of this property we say that pZ is a prime ideal, a term we will define now.

Definition

A proper ideal P of a ring R is called a **prime ideal** of R if whenever ab $\in$ P for a, b$\in$ R, then either a $\in$ P or b $\in$ P.

You can see that {0} is a prime ideal of Z because ab$\in$ {0}$\Rightarrow$ a $\in$ {0} or b$\in$ {0}, where a,b $\in$ Z.

Another example of a prime ideal is

Examp1e 2

Let R be an integral domain. Show that I = {(0,x) | x $\in$ R) is a prime ideal of R x R.

Solution

Firstly, you know that I is an ideal of R x R. Next, it is a proper ideal since I $\neq$R x R. Now, let us check if I is a prime ideal or not. For this let (a_1,b_2), $(a_2,b_2) \in$ R x R such that (a_1,b_2), $(a_2,b_2) \in$ I Then $(a_1a_2b_1,b_2)$ = (0,x) for some x (a_1,b_2), $(a_2,b_2) \in$ R $\therefore$ $a_1a_2 = 0$, i.e., at = 0 or $a_2 = 0$, since R is a domain. Therefore $(a_1,b_1) \in$ I or $(a_1,b_2) \in$ I. Thus, I is a prime ideal.

Try the following exercises now. They will help you get used to prime ideals.

E 18) Show that the set I= {f $\in$ C[0,l] | f(0) = 0} is a prime ideal of C[0,l].
E 19) Show that a ring R with identity is an integral domain if and only if the zero ideal {0} is a prime Ideal of R.

Now we will prove the relationship between integral domains and prime ideals.

Theorem 10

An ideal P of a ring R with identity is a prime ideal of R if and only if the quotient ring R/P is an integral domain.

Proof

Let us first assume that P is a prime ideal of R. Since R has identity, so has R/P. Now, let a+P and b+P be in R/P such that (a+P) (b+P) = P, the zero element of R/P. Then ab+P = P, i.e., ab$\in$P. As P is a prime ideal of R either a$\in$P or b$\in$P. So either a+P = P or b+P = P.

Thus, R/P has no zero divisors.

Hence, R/P is an integral domain.

Conversely, assume that R/P is an integral domain. Let a,b$\in$ R such that ab$\in$P. Then ab + P = P in R/P, i.e., (a+P) (b+P) = P in R/P. As R/P is an integral domain, either a+P = P or b+P = P, i.e., either a$\in$P or b$\in$P. This shows that P is a prime ideal of R.

Using Theorem 10 and Theorem 1 we can say that an ideal mZ of Z is prime in m is a prime number. Can we generalize this relationship between prime numbers and prime ideals in Z to any integral domain? To answer this let us first try and suitably generalize the concepts of divisibility and prime elements.

Definition

In a ring R, we say that an element a **divides** an element b (and denote it by a | b) if b = ra for some r $\in$ R. In this case we also say that a is a factor of b, of a is a **divisor** of b.
Thus, $\bar{3}$ divides $\bar{6}$ in Z_7, since $\bar{3}.\bar{2} = \bar{6}$.

Now let us see what a prime element is.

Definition

A non-zero element p of an integral domain R is called a prime element if

i) p does not have a multiplicative inverse, and

ii) whenever a, b $\in$ R and p | ab, then p | a or p | b.

Can you say what the prime elements of Z are? They are precisely the prime numbers and their negatives.

Now that we know what a prime element is, let us see if we can relate prime ideals and prime elements in an integral domain.

Theorem 11

Let R be an integral domain. A non-zero element p $\in$ R is a prime element if and only if Rp is a prime ideal of R.

Proof

Let us first assume that p is a prime element in R. Since p does not have a multiplicative inverse, 1 $\notin$ Rp. Thus, Rp is a proper ideal of R. Now let a, b $\in$ R such that ab $\in$ Rp. Then ab = rp for some r $\in$ R.

$\Rightarrow$ p | ab
$\Rightarrow$ p | a or p | b, since p is a prime element
$\Rightarrow$ a = xp or b = xp for some x $\in$ R
$\Rightarrow$ a $\in$ Rp or b $\in$ Rp

Thus ab $\in$ Rp $\Rightarrow$ either a $\in$ Rp or b $\in$ Rp, i.e., Rp is a prime ideal of R.

Conversely, assume that Rp is a prime ideal. Then Rp $\neq$ R. Thus, 1 $\notin$ Rp, and hence, p does not have a multiplicative inverse. Now suppose p divides ab, where a, b $\in$ R. Then ab = rp for some r $\in$ R, i.e., ab $\in$ Rp.

As Rp is a prime ideal, either a $\in$ Rp or b $\in$ Rp. Hence, either p | a or p | b. Thys, p is a prime element in R.

Theorem 11 is very useful for checking whether an element is a prime element or not, or for findings out when a principal ideal is a prime ideal. For example, now we can use E 19 to say that 0 is a prime element of R iff R is a domain.

Prime ideals have several useful properties. In the following exercises we ask you to prove some of them

E 20) Let f: R ~ S be a ring epimorphism with kernel N. Show that

a) if J is a prime ideal in S, then f (J) is a prime ideal in R.
b) if 1 is a prime ideal in R containing N, then f(l) is a prime ideal in S.
c) the map 0 between the set of prime ideals of R that contain N and the set of all prime ideals of S given by ϕ (I) = f(I) is a bijection.

E 21) If II and 12 are ideals of a ring such that neither II ,nor 12 contains the other, then show that the ideal $\cap I_1 I_2$ is, not prime.

Now consider the ideal 2Z in Z. Suppose the ideal nZ in Z is such that $2Z \subset nZ \subset Z$. Then $n \mid 2 \therefore n = \pm 1$ or $n = \pm 2$. $\therefore nZ = Z$ or $nZ = 2Z$.

This shows that no ideal can lie between 2Z and Z. That is, 2Z is maximal among the proper ideals of Z that contain it. So we say that it is a "maximal ideal", Let us define this expression.

Definition

A proper ideal M of a ring R is called a maximal ideal if whenever I is an ideal of R such that $M \subseteq I \subseteq R$, then either I = M or 1 = R.

Thus, a proper ideal M is a maximal ideal if there is no proper ideal of R which contains it. An example that comes to mind immediately is the zero ideal in any field F. This is maximal because you know that the only other ideal of F is F. itself.

To generate more examples of maximal ideals, we can use the following characterization of such ideal.

Theorem 12

Let R be a ring with identity. An ideal M in R is maximal if and only if R/M is a field

Proof

Let us first assume that M is a maximal ideal of R. We want to prove that R/M is a field. For this it is e'1ough to prove that R/M has no non-zero proper ideals (see theorem 9). So, let 1 be an ideal of R/M. Consider the canonical homomorphism η: R $\rightarrow$ R/M: η (r) = r + M. Then, from Theorem 3 of Unit 11, you know that η^{-1} (I) is an ideal of R containing

M, the kernel of η. Since M is a maximal ideal of R, η^{-1} (I) = M or η^{-1} (I) = R. Therefore, I = $\eta(\eta^{-1}$ (I)) is either η(M) or η(R), That is, I = $\{\bar{0}\}$ or I = R/M, where 0 = 0+M = M. Thus, RIM is a field.

Conversely, let M be an ideal of R such that R/M is a field. Then the only ideals of R/M are $\{\bar{0}\}$ and R/M. Let I be an ideal of R containing M. Then, as above, η (I) = $\{\bar{0}\}$ or, η (I) = R/M.

$\therefore$ I = η^{-1} (η(I)) is M or R. Therefore, M is a maximal ideal of R.

Now look at the following consequence of Theorem 12 (and a few other theorems too).

Corollary

Every, maximal ideal of a ring with identity is a prime ideal.

We ask you to prove it in the following exercise.

E72) Prove the corollary given above.

Now, the corollary is a one-way statement. What about the converse? That is, is every prime ideal maximal? What about the zero ideal in Z? Since Z is a domain but not a field and Z = Z/{0}, Z/{0} is a domain but not a field. Thus, {0} is a prime ideal but not a maximal ideal of Z.

Now let us use Theorem 12 to get some examples of maximal ideals.

Example 3

Show that an Idea mZ of Z is maximal iff m is a prime number.

Solution

From Theorem 7 you know that Z_m is a field iff m is a prime number. You
Also know that Z/mZ $\tilde{}$ Zm. Thus, by E 17,Z/mZ is a field iff m is prime. Hence, by Theorem 12,mZ is maximal in Z iff m is a prime number.

Example 4

Show that $\bar{2}Z_{12}$is a maximal ideal of Z_{12} $\tilde{}$ Z/27. Thus by E 23 of Unit 11, we see that Z_{12}/ $\bar{2}Z_{12}$ $\tilde{}$ (Z/12Z)/(2Z/12Z) $\tilde{}$ Z/2Z $\tilde{}$ Z_2, which is a field. Therefore, $\bar{2}Z_{12}$= $(\bar{0},\bar{2},\bar{4},\bar{6},\bar{8},\overline{10})$ is maximal in Z_{12}

Now, $\{\bar{0},\bar{4},\bar{8}\} = \bar{4}Z_{12} \subsetneq \bar{2}Z_{12} \subsetneq Z_{12}$.

Try the following exercises now

E 23) Show that $\{\bar{0},\bar{2},\bar{4},\bar{6},\bar{8}\}$ is maximal in Z_{10}.

E 24) Use Example 4 of Unit 11 to prove that the ideal $\{f \in C[0,1] \mid f(\frac{1}{2}) = 0\}$ is maximal in C[0,1].

So, let us see what we have done in this section. We first introduced you to a special ideal of a ring, called a prime ideal. Its speciality lies in the fact that the quotient ring corresponding to it is an integral domain.

Then we discussed a special kind of prime ideal, i.e., a maximal ideal. Why do we consider such an ideal doubly special? Because, the quotient ring corresponding to it is a field, and a field is a very handy algebraic structure to deal with.

Now, if we restrict our attention to domains, can you think of any other method of obtaining a field from a domain? In the next section we look at such a method.

3.4 Field of Quotients

Consider **Z** and **Q**. You know that every element of **Q** is of the form $\frac{a}{b}$, where a $\in$ **Z** and b $\in$ **Z*.** Actually, we can also denote $\frac{a}{b}$ by the ordered pair (a,b) $\in$ **Z** x **Z***. Now, in **Q** we know that $\frac{a}{b} = \frac{c}{d}$ iff ad = bc. Let use put a similar relation on the elements of **Z** x **Z***.

Now, we also know that the operations on **Q** are given by $\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{b\,d}$ *and* $\frac{a}{b}\,\frac{c}{d} = \frac{a\,c}{b\,d}$ $\forall$ $\frac{a}{b}\,\frac{c}{d} \in$ **Q**.

Keeping these in mind we can define operations on **Z** x **Z***. Then we can suitably define an equivalence relation on **Z** x **Z*** to get a field isomorphic to **Q**.

We can generalise this procedure to obtain a field from any integral domain. So, take an integral domain R. Let K be the following set of ordered pairs:

K = {(a,b) | a,b $\in$ R and b $\neq$ 0}

We define a relation ~ in K by

(a,b) ~ (c.d) if ad = bc.

We claim that ~ is an equivalence relation. Let us see if this is so.

i) (a,b) ~ (a,b) $\forall$ (a,b) $\in$ K, since R is commutative. Thus, ~ is reflexive.

ii) Let (a,b), (c.d) $\in$ K such that (a,b) ~ (c.d). Then ad = bc, i.e., cb = da. Therefore, (c,d) ~ (a,b). Thus, ~ is symmetric.

iii) Finally, let (a,b), (c,d), (u,v) $\in$ K such that (a.b) ~ (c,d) and (c,d) ~ (u,v). Then ad = bc and cv = du. Therefore, (ad) v = (bc)v = bdu, i.e., avd = bud. Thus, by the cancellation law for multiplication (which is valid for a domain), we get av = bu, i.e., (a,b) ~ (u,v). Thus, ~ is transitive.

Hence, ~ is an equivalence relation.

Let us denote eequivalence class that contains (a,b) by [a,b]. Thus, [a,b] = {(c,d) | c,d $\in$ R,d $\neq$ 0 and ad = bc}

Let F be the set of all equivalence classes of K with respect to

Let us define + and in F as follows. (Itri1ighthelpyou to keep in mind the rules for adding and multiplying rational numbers.)

[a,b] + [c,d] = [ad+bc,bd] and

[a,b] [c,d] = [ac,bd].

Do you think + and are binary operations on F?

Note that b $\neq$ 0 and d $\neq$ 0 in the integral domain R imply bd $\neq$ 0. So, the right-hand sides of the equations given above are well defined equivalence classes. Thus, the sum and product of two elements in F is again an element in F.

We must make sure that these operations are well defined.

So, let [a,b] = [a´,b´] and [c´,d´] = [c´,d´]. We have to show that [a,b] + [c,d] = [a´,b´] + [c´,d´], i.e:, [ad+bc,bd] = [a´d´+b´c´,b´d´].

Now, (ad+bc)b'd' -(a´d´ + b´c´) bd

= ab´dd´ + cd´bb´- a´bdd´- c´dbb´

= (ab´-a´b)dd´ + (cd´-c´d) bb'

= (0)dd´ + (0)bb´ since (a,b) ~ (a´,b´) and (c,d) ~ (c´,d´).

= 0.

Hence, [ad + bc,bd] = [a´ d´ + b´c´,b´d´], i.e., + is well defined.

Now, let, us show that (a,b] .[c,d] = [a´,b´] . [c´,d´],

i.e., [ac,bd] = [a´c´,b´d´].

Consider (ac) (a´c´,b´d´)

= ab´cd´ - ba´dc´ = ba´cd´ - ba´cd´, since ab´ = ba´ and cd´ = dc´

= 0

Therefore, [ac,bd} = [a´c´,b´d´]. Hence, .is well defined.

We will now prove that F is a field.

i) + is associative : For [a,b], [c,d], [u,v] $\in$ F,
([a,b] + [c,d]) + [u,v] = [ad+bc,bd] + [u,v]
= [(ad+bc)v + ubd, bdv]
= [adv + b(cv+ud), bdv]
= [a,b] + [cv+ud,dv]
= [a,b] + ([c,d] + [u,v])'

ii) +is commulative: For [a,b], [c,d] $\in$ F,
[a,b] + [c,d] = [ad + bc,bd] = [cd + da,db] = [c,d] + [a,b]

iii) [0,1] is the additive identity for F: For [a,b] $\in$ F,
[0,1] + [a.b] = [0.b+l.a, l.b] = [a,b]

iv) The additive inverse of [a,b] $\in$ F is [-a,b]:
[a,b] + [-a,b] = [ab-ab,b^2] = [0,b^2] = [0,1], since 0.1 = 0.b^2,

We would like you to prove the rest of the requirements for F to be a field (see the following exercise).

E 25) Show that, in F is associative, commutative, distributive over +, and [1, 1] is the multiplicative identity for F.

So we have put our heads together and proved that F is a field.
Now, let us define $f : R \to F : f(a) = [a. I]$. We want to show that f is a homomorphism.

Firstly, for $a, b \in R$,

f(a+b) = [a+b,l] = [a,1] + [b,1]. , ..

= f(a) + f(b), and

f(ab) = [ab,l] = [a,1]. [b,1] = f(a) .f(b).

Thus, f is a ring homomorphism.

Next, let $a,b \in R$ such that f(a) = f(b). Then [a, 1] = [b,I], i.e., a = b. Therefore, f is 1 – 1.

Thus, f is a homomorphism.

So, 1m f = f(R) is a subring of F which is isomorphic to R.

As you know, isomorphic structures are algebraically identical.

So, we can identify R with f(R), and think of R as a subring of F. Now, any element of F is of the form

$[a,b] = [a, 1] [1,b] = [a,1] [b,1]^{-1} = f(a) f(b)^{-1}$, where $b \neq 0$. Thus, identifying $x \in R$ with $f(x) \in f(R)$, we can say that any element of. F is of the form ab^{-1}, where $a,b \in R. b \neq 0$.

All that we have discussed in this section adds up to the proof of the following theorem.

Theorem 13

Let R be an integral domain. Then R can be embedded in a field F such that every element of F has the form ab^{-1} for $a, b \in R, b \neq 0$.

The field F whose existence we have just proved is called the **field of quotients** (or the **field of fractions**) of R.

Thus, **Q** is the field of quotients of **Z**. What is the field of quotients of **R**? The following theorem answers this question.

Theorem 14

If f : **R** $\rightarrow$ **K** is a homomorphism of an integral domain R into a field K, then there exists a homomorphism

g : F $\rightarrow$ K : g([a,1]) = f(a), where F is the field of quotients of R.

We will not prove this result here, since it is a little technical. But let u~ look at this theorem closely. It says that **the field of quotients of an integral domain** is the **smallest field containing it**. Thus, the field of quotients of any field is the field itself. So, the field of quotients of **R** is **R** and of $\mathbf{Z}_p$ is $\mathbf{Z}_p$, where p is a prime number.

Try these exercises now.

E 26) Is **R** the field of quotients of **Z** + $\sqrt{2}$ **Z**? Or, is it **C**? Or, is it **Q**+ $\sqrt{2}$ **Q**? Why'?

E 27) At what stage of the construction of the field F in Theorem 13 was it crucial to assume that R is a domain?

Let us now wind up this unit with a summary of what we have done in it.

5.0 SUMMARY

In this unit we have covered the following points.

1. The definition and examples of an integral domain.
2. The definition and examples of a field.
3. Every field is a domain.
4. A finite domain is a field.
5. The characteristic of any domain or field is either zero or a prime number.
6. The definition and examples of prime and maximal ideals.
7. The proof and use of the fact that a proper ideal I of a ring R with identity is prime (or maximal) iff R/I is an integral domain (or a field),
8. Every maximal ideal is a prime ideal.
9. All element p. of an integral domain R is prime iff the principal ideal pR is a prime ideal or R.
10. Z_n is a field iff n is a prime number.
11. The construction of the field of quotients of an Integral domain.

ANSWER TO SELFASSESSMENT EXERCISE

E1) Let n = mr, where r $\in$ N.

Then $\overline{m}\,\overline{r} = \overline{n} = \overline{0}$ *in* Z_n

Since 1 < m < n, $\overline{m} \neq \overline{0}$. Similarly, $\overline{r} \neq \overline{0}$

Thus $\overline{m} \in Z_n$ IS a zero divisor.

E 2) Z has no zero divisors.

E 3) For none since 1 x = x $\neq 0 \; \forall x \neq 0$ in the ring.

E 4) Let b $\neq$ 0 be in R such ab = 0. Then, for any r $\in$ R, (ra)b = 0 Thus, every element of Ra is a zero divisor

E 5) Z_4, since 2 is a zero divisor.

2Z, since 1 $\notin$ 2Z.
R x R, since (1,0) is a zero divisor.

{0}, since a domain must be non-zero.

E 6) $x^2 = x \Rightarrow x(x\text{-}l) = 0 \Rightarrow x = 0$ or x-l = 0

$\Rightarrow$ x = 0 or x = 1.

E 7) Let R be a domain and x $\in$ R be nilpotent. ,
then x^n =.0 .for some n $\in$ N. Since R has no zero divisors, this implies that x = 0.

E 8) We want to show that 2A = $\phi \forall A \subseteq$ X, and that 2 is the least such natural number.
Firstly, for any A $\subseteq$ X,
2A = A Δ A = (A \ A) $\cup$ (A \ A) = ϕ

Also, since X $\neq \phi$, 1.X $\neq \phi$. Thus, char $\wp$ (X) $\neq$ 1.

$\therefore char\, \wp$ (X) = 2

E9) Let char (R x R) = n. We know that mr =0 $\forall$ r $\in$ R.

Now, let (r,s) be any element of R x R.

Then m(r,s) = (mr,ms) = (0,0), since r,s $\in$ R.

Thus, n $\leq$ m

On the other hand, if r $\in$ R, then (r,0) $\in$ R x R
$\therefore$ n(r,0) = (0,0).

i.e., (nr,0) = (0,0)

i.e., nr = 0

This is true for any r $\in$ R.

$\therefore$ m $\leq$ n.

Thus, (1) and (2) show that m = n, i.e., char R = char (R X R)

E 10a) By the binomial expansion (E II of Unit 9),

$$(a+b)^p = a^p + {}^pC_1\, a^{p-1} b + \ldots\ldots + {}^pC_{p-1}\, ab^{p-1} + b^p$$

Since $p \mid {}^pC_n \ \forall\ n = 1,\ldots..,\ p^{-1}$, ${}^pC_n x = 0\ \forall\, x \in R$ and $\forall\, n = 1,\ldots.,P^{-l}$.

Thus, ${}^pC_1\, a^{p-1} b = 0 = .. = {}^pC_1\, ab^{p-1}$

$\therefore (a+b)^p = a^p + b^p$.

You can similarly show that $(a-b)^p = a^p - b^p$,

b) Let $S = \{a^p \mid a \in R\}$

Firstly, $S \neq \phi$.

Secondly, let $\alpha - \beta$ $(a-b)^p \in S$. Then $\alpha = a^p$, $\beta = b^p$ for some a,b $\in$ R.

Then $\alpha - \beta = (a-b)^p \in S$ and $\alpha\beta = (ab)^p \in S$.

Thus, S is, a subring of R

c) $\phi(a+b) = (a+b)^p = a^p + b^p = \phi(a) + \phi(b)$,
$\phi(ab) = (ab)P = aPbP = \phi(a)\,\phi(b)$.
Thus, ϕ is a ring homomorphism.
ϕ is 1-1 because .
$\phi(a) = \phi(b). \Rightarrow a^p = b^p \Rightarrow (a-b)^p = 0$, from (a).
$\Rightarrow$ a-b = 0, since R is without zero divisors.
$\Rightarrow$ a = b.

d) We have to show that if R is finite then 0 is surjective,
Let R have n elements. Since ϕ is 1-1, 1m ϕ also has n elements.
Also 1m $\phi \subseteq$ R. Thus, Im ϕ = R.
Hence, ϕ is surjective.

E 11) You Can easily show that f is a ring homomorphism.

Ker f = $\{n \in Z \mid n.1 = 0\}$
= mZ_4, since char R = m.

E 1 2) char (Z_3 x Z_4) = 1.c.m. of char Z_3 and char Z_4 = 12.

Thus, the characteristic of Z_3 x Z_4 is neither 0 nor a prime.

Note that Z_3 x Z_4 is not a domain, since it has several zero divisors.

Now let us see why Theorem 3 is not valid for Z_3 x Z_4.

Take $(\bar{1},\bar{0}) \in Z_3$ x Z_4. Then $3(\bar{1},\bar{0}) = (\bar{0},\bar{0}) \in Z_3$ x Z_4

But $3(\bar{1},\bar{0}) \neq (\bar{0},\bar{0})$. Thus, Theorem 3(a) and Theorem 3(c) arc not equivalent in this case

E 13) 2Z since $2 \in 2Z$ is not invertible in 2Z.

Z_n since it is not a domain

Q x Q, since it is not a domain.

E 14) No. For example, Z is a subring of **Q**,**Q** is a field, but **Z** is not.

E 15) From the tables you can see that R is commutative with identity and every non-zero element has an inverse: Thus, R is a field.

Also $2x = 0 \ \forall \ x \in R$ and $1.x \neq 0$ for some x E R.

Thus, char R = 2.

E 16) Ker I is an ideal of F. Thus, by Theorem 9.

Ker f = {0} or Ker f = F.

If Ker f = {0}, then f is 1-1.
If Ker f = F, then f = 0.

E 17) Let $\phi\ F \rightarrow R$ be an isomorphism. Then $\phi(1)$ is the identity of $\text{Im}\phi$ = R, Also, since F is commutative, so is R. Now, let $\in$ R. r $\neq$ O. Since ϕ is onto, $\exists$ a $\in$ F such that ϕ (a) = r. Since r $\neq$ 0, 2 $\neq$0. Since F is a field, $\exists$ b $\in$ F such that lib = 1.

Thus, $\phi(ab) = \phi(1)$, i.e., $r\phi(b) = \phi(1)$i.e., r has a multiplicative inverse.

Thus, R is a field

18) Firstly, 1 is an ideal of C[0,1]

(because $f.g. \in I \Rightarrow$ f-g, $\in$ I, and

$T \in$ C[0.I], $f \in I \Rightarrow Tf \in I$.)

Secondly, since any non-zero constant function is in

C[0,1] \I. I is a proper ideal.

Finally, let fg $\in$ J. Then f(0) g(0) = 0 in R. Since R is a domain, we must have f(0) = 0 or g(0) = 0, i.e., f $\in$ I or g $\in$ I

Thus, I is a prime ideal of C[0,1].

E 19) R is a ring with identity. Thus, we need to show that R is without zero divisor iff {0} is a prime ideal in R.

Now, {0} is a prime ideal in R

iff $ab \in \{0\} \Rightarrow a \in \{0\}$ or $b \in \{0\}$ for a, b $\in$ R

iff $ab = 0 \Rightarrow a = 0$ or $b = 0$

iff R is without zero divisors.

So, we have shown what we wanted to show

E 20) a) From Theorem 3 of Unit 11, you know that $f^{-1}(J)$ is an ideal of R. Since f is surjective and $J \neq S$, $f^{-1}(J) \in R$

Now, let $a,b \in R$ such that $ab \in f^{-1}(J)$

$\Rightarrow f(ab) \in J$.

$\Rightarrow f(a)\, f(b) \in J$.

$\Rightarrow f(a) \in J$ or $f(b) \in J$, since J is a prime ideal.

$\Rightarrow a \in f^{-1}(J)$ or $b \in f^{-1}(J)$.

Thus, $f^{-1}(J)$ is a prime ideal in R

b) Firstly, since f is onto, you know that f(I) is an ideal of S. Also, since $1 \notin 1$ and $f^{-1}(f(I)) = I$ (from Theorem 4 of Unit 11). $F(1) \notin f(I)$. Thus, $f(I) \neq S$.

Finally, let $x,y \in S$ such that $xy \in f(I)$

Since $S = \text{Im } f$, $\exists\ a,b \in R$ such that $x = f(a)$ and $y = f(b)$

Then $f(ab) = xy \in f(I)$, i.e., $ab \in f^{-1}(f(I)) = I$

$\therefore a \in I$ or $b \in I$, i.e., $x \in f(I)$ or $y \in f(I)$

Thus, f(I) is a prime ideal of S.

c) ϕ is $1 - 1$: $\phi(I) = \phi(J) \Rightarrow f(I) = f(J)$

$\Rightarrow f^{-1}(f(I)) = f^{-1}(f(I))\ I = J$.

ϕ is onto: Let J be a prime ideal of S. Then $f^{-1}(J)$ is a prime ideal of R and $\phi(f^{-1}(J)) = f(f^{-1}(J)) = J$ (from Unit 11). Thus, $J \in \text{Im } \phi$.

E 21) Let $x \in I_1 \setminus I_2$ and $y \in I_2 \setminus I_1$. Then $xy \in I_1$ and $xy \in I_2$, since I_1 and I_2 are ideals.

$\therefore xy \in I_1 \cap I_2$. But $x \notin I_1 \cap I_2$ and $y \notin I_1 \cap I_2$

Thus, $I_1 \cap I_2$ is not prime.

E 22) M is maximal in R
$\Rightarrow$ R/M is a field, by Theorem 12

$\Rightarrow$ R/M is a domain, by Theorem 5

$\Rightarrow$ M is prime in R, by Theorem 10

E 23) $\{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\} = \bar{2}\, Z_{10}$ and $Z_{10}/\bar{2}\, Z_{10} \simeq Z_2$, a field.

Thus, as in Example 4, $\{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\}$ is maximal in Z_{10}.

E 24) In Unit 11 we have shown that this ideal in the kernel of the onto homomorphism
$\phi : C[0,1] \to \mathbf{R}$: $\phi(f) = f(\frac{1}{2})$.

$\therefore C[0,l]/\text{Ker}\ \phi \simeq \mathbf{R}$, a field.

Thus, Ker ϕ is maximal in C[0,1].

E 25) You can prove all these properties by using the corresponding properties of R.

E 26) Any element of the field of quotients F is of the form $\frac{a+b\sqrt{2}}{c+d\sqrt{2}}$, *where* $c + d\sqrt{2} \neq 0$, a,b,c,d $\in \mathbf{Z}$.

Now, $\frac{a+b\sqrt{2}}{c+d\sqrt{2}}, = \frac{a+b\sqrt{2}\ c+d\sqrt{2}}{c^2-2d^2} = \left(\frac{ac-2bd}{c^2-2d^2}\right) + \sqrt{2}\left(\frac{bc-ad}{c^2-2d^2}\right) \in \mathbf{Q} + \sqrt{2}\mathbf{Q}$

Thus, $F \subseteq \mathbf{Q} + \sqrt{2}\mathbf{Q}$.

Also, any element of $\mathbf{Q} + \sqrt{2}\mathbf{Q}$ *is* $\frac{a}{b} + \sqrt{2}\frac{c}{d}$, a,b,c,d $\in \mathbf{Z}$, b $\neq 0$, d $\neq 0$

Now $\frac{1}{2}+\sqrt{2}\frac{c}{d}=\frac{ad+bc\sqrt{2}}{bd}=\frac{ad+bc\sqrt{2}}{bd+0\sqrt{2}}$ with ad, bc, bd $\in$ **Z**

Thus, $\frac{a}{b}+\sqrt{2}\frac{c}{d}\in F$.

Hence, **Q** + $\sqrt{2}$**Q** $\subseteq F$

Thus, F = **Q** + $\sqrt{2}$**Q**

E 27) If R is 'hot a domain, the relation -need not be transitive, and hence, F is not defined.

6.0 TUTOR-MARKED ASSIGNMENT

7.0 REFERENCES/FURTHER READING

Ansa B. E. (2010). Modern Algebra Ethereal Bliss Publisher. Calabar.

Kiku, A. O. (1992). Abtract Algebra Ibadan. Ibadan University, Press

Ilori, S. A. & Akinyele, O. (1986). Elementary Abstract and Linear Algebra. Ibadan University, Press.

Ilori, S. A. & Ajayi D. O. (2000). University Mathematics Series 2. Algebra Books (A Division of Ass Book Markers Nig. Ltd Ibadan).

Lipschuty, S. (2004). Schaum's Outlines Series on Set Theory and Related Topics. MAcGraw – Hill, NY.

Osisiogu, U. A. (1998). An Introduction to Real Analysis with Special Topic on Functions of Several Variables and Method of Languages Multipliers, Bestsoft Educational Books Nigeria.

UNIT 2 POLYNOMIAL RINGS

CONTENTS

1.0 INTRODUCTION

In the past you must have come across expressions of the form $x+1$, x^2+2x+1, and so on. These are examples of polynomials. You have also dealt with polynomials in the course Linear Algebra. In this unit we will discuss sets whose elements are polynomials of the type $a_0 + a_1 x + \ldots + a_n x^n$, where $a_0, a_1 \ldots\ldots, a_n$ are elements of a ring R. You will see that this set, denoted by R [x], is a ring also.

You may wonder why we are talking of polynomial rings in a block on, domains and fields. The reason for this is that we want to focus on a particular case, namely, R [x], where R is a domain. This will turnout to be a domain also, with 'a lot of useful properties. In particlI1ar, the ring of polynomials over a field satisfies a division algorithm, which is similar to the one satisfied by Z (see Sec. 1.6.2). We will prove this property and use it to show how many roots any polynomial over a field can have.

In the next two units we will continue to work with polynomials and polynomial rings. So read this unit carefully and make sure that you have achieved the following objectives.

2.0 OBJECTIVES

At the end of this unit, you should be able to:

- identify polynomials over a given ring
- prove and use the fact that R [x], the set of polynomials over a ring R, is a ring
- relate certain properties of R[x] to those of R
- prove and use the division algorithm for F[x], where F is a field.

3.0 MAIN CONTENT

3.1 Ring of Polynomials

As we have said above, you may already be familiar with expressions of the type $1 + x$, $2 + 3x^2 + 4x$ or $2 + 3x + 4x^2$, x^5 - l, and so on. These are examples of polynomials over the ring **Z**. Do these examples suggest to you what a polynomial over any ring R is? Let's hope that your definition agrees with the following one.

Definition

A **polynomial** over a ring R in the indeterminate x is an expression of the form

$a_0x^0 + a_lx^l + a_2x^2 + ... + a_nx^n$,

Where n is a non-negative integer and $a_0, a_1, ..., a_n \in R$.

While discussing polynomials we will observe the following conventions. We will

i) write x^0 as1, so that we will write a_0 for a_ox^o!lox\),

ii) write x^1 as x.

iii) write x^m instead of $l.x^m$ (i.e., when $a_m = 1$).

iv) omit terms of the type $0.x^m$.

Thus, the polynomial $2 + 3x^2 - l.x^3$ is $2x^0 + 0.x^1 + 3x^2 + (-1)x^3$

Henceforth, whenever we use the word polynomial, we will mean a polynomial in the indeterminate x. we will also be using the shorter notation $\sum_{i=0}^{n} a_i x^i$ for the polynomial $a_0 + a_1 x + \ldots + a_n x^n$.

Let us consider a few more basic definitions related to a polynomial.

Definition

Let $a_0 + a_1 x + \ldots + a_n x^n$ be a polynomial over a ring R. Each of $a_0\ a_1, \ldots, a_n$ is a coefficient of this polynomial. If $a_n \neq 0$, we call a_n the leading coefficient of this polynomial.

If $a_1 = 0 = a_2 = \ldots = a_n$, we get the constant polynomial, a_0. Thus, every element of R is a constant polynomial.

In particular, the constant polynomial 0 is the **zero polynomial**.

It has no leading coefficient.

Now, there is a natural way of associating a non-negative integer with any non-zero polynomial.

Definition

Let $a_0 + a_1 x + \ldots + a_n x^n$ be a polynomial over a ring R, where $a_n \neq 0$. Then we call the integer n the **degree** of this polynomial, and we write.

$$\deg\left(\sum_{i=0}^{n} a_i x^i\right) = n, \text{ if } a_n \neq 0$$

We define the degree of the zero polynomial to be $-\infty$. Thus, **deg 0** = $-\infty$.

Let us consider some examples.

i) $3x^2 + 4x + 5$ is a polynomial of degree 2, whose coefficients belong to the ring of integers **Z**. Its leading coefficient is 3.

ii) $x^2 + 2x^4 + 6x + 8$ is a polynomial of degree 4, with coefficients in **Z** and leading coefficient 2. (Note that this polynomial can be rewritten as $8 + 6x + x^2 + 2x^4$).

iii) Let R be a ring and $r \in R$, $r \neq 0$. Then r is a polynomial of degree 0, with leading coefficient r.

Before giving more examples we would like to set up some notation

Notation

We will denote the set of all polynomials over a ring R by R[x]. (Please note the use of the square brackets [ ]. Do not use any other kind of brackets because R [x] and R (x) denote different sets).

$$Thus, R[x] = \left\{ \sum_{i=0}^{n} a_i x^i \right) \;\middle|\; a_i \in R \,\forall\, i = 0,1,\ldots\ldots,.. \; n, \; where n \geq 0, n \in Z \right\}$$

We will also often denote a polynomial $a_0 + a_1 x + \ldots + a_n +^n$ by f(x), p (x), q(x), etc.

Thus, an example of an element from Z_4 [x] is f(x) = $\bar{2}\, x^2 + \bar{3}\, x + \bar{1}$

Here deg f(x) = 2, and the leading coefficient of f(x) is $\bar{2}$.

To check your understanding of what we have said so far, you can try these exercises now.

E 1) Identify the polynomials from the following expressions. Which of these are elements of Z[x]?

a) $x^6 + x^5 + x^4 + x^2 + x + 1$

b) $\frac{2}{x^2} + \frac{1}{x} + x + x^2$

c) $\sqrt{3}\, x^2 + \sqrt{2}\, x + \sqrt{5}$

d) $1 + \frac{1}{2} x + \frac{1}{3} x^2 + \frac{1}{4} x^3$

e) $x^{1/2} + 2x^{3/2} + 3 x^{5/2}$

f) -5.

It E 2 Determine the degree and the leading coefficient of the following polynomials in **R**[x].

a) $\sqrt{2}\,x+7$

b) $1- 7x^3 + 3x$

c) $1 + x^3 + x^4 + 0.x^5$

d) $\frac{1}{3}\,x + \frac{1}{5}\,x^2 + \frac{1}{7}\,x^3$

e) 0.

Now, for any ring R, we would like to see if we can define operations on the set R [x] so that it becomes a ring. For this purpose we define the operations of addition and multiplication of polynomials.

Definition

Let $f(x) = 2_0 + a_1x + .. + a_n\, x^n$ and $g(x) = b_0 + b_1\, x + .. + b_m\, x^m$ be two polynomials in R[x]. let us assume that $m \geq n$. Then their **sum** $f(x) + g(x)$ is given by $f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)\, x + .. + (a_n + b_n)\, x^n + b_{n+1}x^{n+1} + .. + b_mx^m$.

$$= \sum_{i=0}^{m} (a_1 + b_i)\, x^i, \text{where } a_i = 0 \text{ for } i > n.$$

For example, consider the two polynomials p(x),q(x) in Z[x] given by
$p(x) =1+2x + 3x^2$, $q(x) = 4 + 5x + 7x^3$

Then

$p(x) + q(x) = (1+4) + (2+5)x + (3+0)\, x^2 + 7x^3 = 5 + 7x + 3X^2 + 7X^3$.

Note that $p(x) + q(x) \in Z[x]$ and that

deg (p(x)+q(x)) = 3 = max(deg p(x), deg q(x)).

From the definition given above, it seems that deg (f(x)+g(x)) = max (deg f (x), deg g (x)). But this is not always the case. For example, consider $p(x) = 1 + x^2$ and $q(x) = 2 + 3x -x^2$ in **Z** [x].

Then $p(x) + q(x) = (1+2) + (0+3)x + (1-1)x^2 = 3 + 3x$.

Here deg $(p(x) + q(x)) = 1 <$ max (deg $p(x)$, deg $q(x)$).

So, what we can say is that

deg (f(x) + g(x) ::; Max (deg f(x), deg g(x)

$\forall$ f(x), g(x) $\in$ R [x].

Now let us define the product of polynomials.

Definition

If $f(x) = a_0 + a_i x + ..+ a_n x^n$ and $g(x) = b_0 + b_i x + ..+ b_m x^m$ are two polynomials in R [x], we define their **product** f(x). g(x) by

$f(x) .g(x) = c_0 + c_1 x +.. + c_{m+n} x^{m+n}$,
where $c_i = a_i b_0 + a_{i-1} b_1 + ...+ a_0 b_i \ \forall$ i=0,1,...,m + n.

Note that $a_i = 0$ for $i > n$ and $b_i = 0$ for $i > m$.

As an illustration, let us multiply the following polynomials in **Z**[x] :

$p(x) = 1 -x + 2x^3$, $q(x) = 2 + 5x + 7x^2$.

Here $a_0 = 1$, $a_i = -1$, $a_2 = 0$, $a_3 = 2$, $b_0 = 2$, $b_1 = 5$, $b_2 = 7$.

Thus, $p(x)\, q(x) = \sum_{i=0}^{5} c_i\, x^i$, where

$c_0 = a_0 b_0 = 2$,

$c_1 = a_1 b_0 + a_0 b_1 = 3$,

$c_2 = a_2 b_0 + a_1 b_1 + a_0 b_2 = 2$,

$c_3 = a_3 b_0 + a_2 b_1 + a_1 b_2 + a_0 b_3 = -3$ (since $b_3 = 0$),

$c_4 = a_4 b_0 + a_3 b_1 + a_2 b_2 + a_1 b_3 + a_0 b_4 = 10$ (since $a_4 = 0 = b_4$),

$c_5 = a_5b_0 + a_4b_1 + a_3b_2 + a_2b_3 + a_1b_4 + a_0b_5 = 14$ (since $a_5 = 0 = b_5$),
So p(x), q(x) $= 2 + 3x + 2x^2 - 3x^3 + 10x^4 + 14x^5$

Note that p(x), q(x) $\in$ **Z**[x], and deg (p(x) q(x)) = 5 = deg p(x) + deg q(x)

As another example, consider

$p(x) = \bar{1} + \bar{2}x$, $q(x) = 2 + 3x^2 \in Z_6[x]$

Then, p(x). q(x) = $\bar{2} + \bar{4}x + \bar{3}x^2 + \bar{6}x^3 = \bar{2} + \bar{4}x + \bar{3}x^2$.

Here, deg (p(x).q(x) = 2 < deg p (x) + deg q (x) (since deg p (x) = 1, deg q(x) = 2).

In the next section we will show you that

deg (f(x) g(x) $\leq$ deg f(x) + deg g(x)

Now try the following exercise. It will give you some practice in adding and multiplying polynomials.

E3) Calculate

a) $(2 + 3x^2 + 4x^3) + (5x + x^3)$ in **Z** [x].
b) $(\bar{6} + \bar{2}x^2) + (\bar{1} - \bar{2}x + \bar{5}x^3)$ in $\mathbf{Z}_7$ [x].
c) $(\bar{1} + x)(\bar{1} + \bar{2}x + x^2)$ in Z[x].
d) $(\bar{1} + x)(\bar{1} + \bar{2}x + x^2)$ in $\mathbf{Z}_3$ [x]
e) $(2 + x + x^2)(5x + x^3)$ in **Z**[x]

By now you must have got used to addition and multiplication of polynomials. We would like to prove that fur any ring R, R [x] is a ring with respect to these operations. For this we must note that by definition, + and. are binary operations over R[x].

Now let us prove the following theorem. It is true for any ring, commutative or not.

Theorem 1

If R is a ring, then so is R [x], where x is an indeterminate.

Proof

We need to establish the axioms RI -R6 of Unit 9 for (R[x], + ,.).

i) Addition is commutative: We need to show that

$p(x) + q(x) = q(x) + p(x)$ for any $p(x), q(x) \in R[x]$.

Let $p(x) = a_0 + a_1x + ... + a_nx^n$, and

$q(x) = b_0 + b_1x + ... + b_mx^m$ be in R[x].

Then, $p(x) + q(x) = c_0 + c_1x + ... + c_tx^t$,

where $c_i = a_i + b_i$ and $t = \max(m,n)$.

Similarly,

$q(x) + p(x) = d_0 + d_1x + ... + d_sx^s$,

Since addition is commutative in R, $c_1 = d_1 \ \forall \ i \geq 0$

So we have

$p(x) + q(x) = q(x) + p(x)$.

ii) Addition is associative: Again, by using the associatively of addition in R, we can show that if $p(x), q(x), s(x) \in R[x]$, then

$\{p(x)+q(x)\} + s(x) = p(x) + (q(x)+ s(x)\}$,

iii) Additive identity : The zero polynomial is the additive identity in R [x]. This is because, for any $p(x) = a_0 + a_1x + ... + a_nx^n \in R[x]$,

$0+p(x) = (0 + a_0) + (0 + a_l)x + ... + (0 + a_n)x^n$

$= a_o + a_1x_1 + ... + a_nx^n.$

$= p(x)$

iv) Additive invers: For $p(x) = a_0 + a_1x + ... + a_nx^n \in R[x]$, consider the polynomial

$-p(x) = -a_0 - a_1x - \ldots - a_nx^n$, $-a_i$ being the additive inverse of at in R. Then

$-p(x) + (-p(x)) = (a_0 - a_0) + (a_1 - a_1)x + ... + (a_n - a_n)x^n$

$= 0 + 0x + 0.x^2 + .., + 0.x^n$
$= 0.$

Therefore, $-p(x)$ is the additive inverse of $p(x)$.

v) Multiplication is associative:

Let $p(x) = a_0 + a_1 x + ... + a_n x^n$,

$q(x) = b_0 + b_1 x + ... + b_m x^m$,

and $t(x) = d_0 + d_1 x + ... + d_r x^r$, be in $R[x]$

Then

$p(x), q(x) = c_0 + c_l x + \ldots + c_s x^s$, where $s = m+n$ and

Therefore,

$\{p(x), q(x)\}\ t(x) = e_0 + e_1 x + \ldots + e_t x^t$,

where $t = s + r = m+n+r$ and

$e_k = c_k d_0 + c_{k-1} d_1 + ... + c_0 d_k$

$= (a_k b_0 + ... + a_0 b_k) d_0 + (a_{k-1} b_0 + ... + a_0 b_{k-1}) d_1 + ... + a_0 b_0 d_k$,

Similarly, we can show that the coefficient of x^k (for any $k \geq 0$).in $p(x)\ \{q(x)\ t(x)1\}$

is $a_k b_0 d_0 + a_{k-1}(b_1 d_0 + b_0 d_l) + ... + a_0, (b_k d_0 + b_{k-1} d_1 + \ldots + b_0 d_k)$

$= e\ k$, by using the properties of + and in R.

Hence, $\{p(x), q(x)\}, t(x) = p(x), \{q(x), t(x)\}$

vi) Multiplication distributes over addition:

Let $p(x) = a_0 + a_l x + ... + a_n x^n$.

$q(x) = b_0 + b_1 x + ... + b_m x^m$

and $t(x) = d_0 + d_1 x + \ldots + d, x^r$ be in R[x].

The coefficient of x^k in p (x). (q(x) +t (x)) is

$$c_k = a_k (b_0+d_0) + a_{k-1} (b_1 +d_1) +... + a_0 (b_k + d_k).$$

And the coefficient of x^k in p (x) q (x) + p (x) t(x) is

$(a_k b_0+a_{k-1}b_1+\ldots+a_0 b_k)+(a_k d_0+a_{k-1}d_1 +\ldots+a_0 d_k)$,

$= a_k(b_0+d_0) + a_{k-l} (b_1+d_1)+\ldots+a_0 (b_k+d_k) = c_k$

This is true $\forall\ k \geq 0$.

Hence, p (x). {q (x) + t (x)} = p (x): q(x) + p (x) t (x).

Similarly, we can prove that

{q(x) + t(x)}. p(x) = q(x) .p(x) + t(x) p(x)

Thus, R [x] is a ring.

Note that the definitions and theorem in this section are true for any ring. We have not restricted ourselves to commutative rings. But, the case that we are really interested in is when R is a domain. In the next section we will progress, towards this case.

3.2 Some Properties of R[x]

In the previous section you must have realised the intimate relationship between the operations on a ring R and the operations on R [x]. The next theorem reinforces this fact.

Theorem 2

Let R be a ring.

a) If R is commutative, ~o is R [x].
b) If R has identity, so does R [x].

Proof

a) Let $p (x) = a_0 + a_t x +... + a_n x^n$ and

$q (x) = b_0 + b_1 x + ...+ b_m x^m$ be in R [x].

Then p (x) q (x) = $c_0 + c_1 x + ...+ c_s x^s$, where s = m + n and

$c_k = a_k b_0 + a_{k-1} b_1 +...+ a_0 b_k$

$= b_k a_0 + b_{k-1} a_l + ...+ b_1 a_{k-1} + b_0 a_k$, since both addition and multiplication are commutative in R.

= coefficient of x^k in q (x) p(x).

Thus, for every ≥ 0 the coefficients of xi in p(x) q(x) and q(x) p(x) are equal

Hence, p (x) q(x) = q(x) p(x).

b) We know that R has identity I. We will prove that the constant polynomial 1 is the identity of R [x]. Take any

p (x) = $a_0 + a_1 x + ...+ a_n x^n \in$ R [x].

Then I. p (x) = $c_0 + c_1 x + ... + c_n x^n$ (since deg 1 = 0),

where $c_k = a_k 1 + a_{k-1} 0 + a_{k-2} 0 + ...+ a_0 0 = a_k$

Thus 1 P (x) = p (x)

Similarly, p (x) l = p(x)
This shows that 1 is the identity of R [xl.
In the following exercise we ask you to check if the converse of Theorem 2 is true.

E 4) If R is a ring such that R [x] is commutative and has identity, then

a) is R commutative?

b) does R have identity

Now let us explicitly state a result which will help in showing us that R is a domain iff R [x] is a domain. This result follows just from the definition of multiplication of polynomial

Theorem 3

Let R be a ring and f(x) and g (x) be two non-zero elements of R [x). Then deg (f (x) g (x) $\leq$ deg f(x) + deg g (x),

with equality if R is an integral domain.

Proof: Let $f(x) = a_0 + a_l x + ... + a_n x^n$, $a_n \neq 0$,

and $g(x) = b_0 + b_1 x + ... + b_m x^m$, $b_m \neq 0$.

Then deg f(x) = n, deg g (x) = m. We know that

$f(x)\, g(x) = c_0 + c_1 x + ... + c_{m+n} x^{m+n}$,

where $C_k = a_k b_0 + a_{k-1} b_1 + ... + a_0 b_k$.

Since a_{n+1}, $a_{n+2}, \ldots$ and b_{m+1} $b_{m+2}, \ldots$ are all zero,

$c_{m+n} = a_n b_m$.

Now, if R is without zero divisors, then $a_n b_m \neq 0$, since $a_n \neq 0$

and $b_m \neq 0$. Thus, in this case,

deg (f(x) g (x) = deg f(x) + deg g (x).

On the other hand, if R has zero divisors, it can happen that $a_n b_m = O$. In this case,

deg (f (x) g (x) < m+n = deg f(x) + deg g(x).

Thus, our theorem is proved.
The following result follows immediately from Theorem 3.

Theorem 4

R [x] is an integral domain <=> R is an integral domain.

Proof

From Theorem 2 and E 4 we know that R is a commutative ring with identity iff R [x] is a commutative ring with identity. Thus, to prove this theorem we need to prove that R is without zero divisors iff R [x] is without zero divisors.

So let us first assume that R is without zero divisors.

Let $p(x) = a_0 + a_1 x + \ldots + a_n x^n$, and $q(x) = b_0 + b_l x + ... + b_m x^m$

be in R [x], where $a_n \neq 0$ and $b_m \neq 0$.

Then, in Theorem 3 we ha'/e seen that deg (p (x) q (x) = m + n $\geq$ 0.

Thus, P (x) q (x) $\neq 0$

Thus, R [x] is without zero divisors.

Conversely, let us assume that R [x] is without zero divisors. Let a and be non-zero elements of R: Then they are non-zero elements of R [x] also. Therefore, ab $\neq$ 0. Thus, R is without zero divisors. So, we have proved the theorem.

See if you can solve the following exercises now.

E 5) Which of the following polynomial rings are free from zero divisors?

a) R[x], where R = {a+ b $\sqrt{-5}$ | a,b $\in$ Z}
b) Z_7 [x]
c) Z_6 [x]
d) R[x], where R = C [0,1]

E 6) Let R be a domain. Show that char R = char R [x].

E 7) Let, R and S be commutative rings and f: R $\rightarrow$+ S be a ring homomorphism. Show that the map

ϕ: R [x] $\rightarrow$S [x] : ϕ (a_0+a_1x + ...+ a_n x^n) = f (a_0) + f (a_l) x + … +, f(a_n) x^n is a homomorphism:

Now, you have seen that many properties of the ring R carry over to R [x1. Thus, if F is a field, we 'should expect F[x] to be a field also. But this is not so. F [x] can never be a field

This is because any polynomial of positive degree in F [x] does not have a multiplicative inverse. Let us see why.

Let f (x) $\in$ F [x] and deg f (x) = n > 0. Suppose g (x) $\in$ F [x] such that

f(x) g (x) = 1. Then

0 = deg 1 = deg (f(x) g (x) = deg f(x) + deg g (x), since F [x] is a domain.

= n +deg g (x) $\geq$ n > 0.

We reach a contradiction.

Thus, F [x] cannot be a field.

But there are several very interesting properties of F [x], which are similar to those of Z, the set of integers. In the next section we shall discuss the properties of division in F [x]. You will see how similar they are to the properties of Z that we have discussed in Sec. 1.6,2.

3.3 The Division Algorithm

In Sec. l.6.2 we discussed various properties of divisibility in Z. In particular, we proved the division algorithm for integers. We will now do the same for polynomials over a field F.

Theorem 5 (Division Algorithm)

Let F be a field. Let f(x) and g(x) be two polynomials in F [x], with $g(x) \neq 0$. Then

a) there exist two polynomials q(x) and r (x) in F [x] such that

f (x) = q (x) g (x) + r (x), where deg r(x) < deg g (x).

b) the polynomials q (x) and r (x) are unique.

Proof

a) If, deg f (x) < deg g (x), we can choose q (x) = 0.

Then f, (x) = 0. g(x) + f (x), where deg f(x) < deg g (x).

Now, let us assume that deg f(x) $\geq$ deg g (x).

Let $f(x) = a_0 + a_1x + \ldots + a_nx^n$, $a_n \neq 0$, and
$g(x) = b_0 + b_1 x + \ldots + b_mx^m$, $b_m \neq 0$, with $n \geq m$.

We shall apply the principle of induction (see Sec. 1.6.1) on deg f(x), i.e., n.

If n = 0, then m = 0, since $g(x) \neq 0$. Now

$f(x) = a_0$, $g(x) = b_0$, and hence

$f(x) = (a_0\, b_0 + 0 = q(x)\, g\,(x) + r\,(x)$, where $q(x) = a_0 b_0^{-1}$ and $r(x) = 0$.

Thus,

$f(x) = q(x)\, g(x) + r(x)$, where deg $r(x) <$ deg $g(x)$.

So the algorithm is true when $n = 0$. Let us assume that the algorithm is valid for all polynomials of degree $\leq n - 1$ and try to establish that it is true for $f(x)$. Consider the polynomial

$f_1\,(x) = f(x)\, a_n b_m^{-1}\, x^{n-m}\, g(x)$

$= (a_0 + a_1\, x + \ldots + a_n x^n) - (a_n b_m^{-1} b_0 x^{n-m} + a_n b_m^{-1} b_1 x^{n-m+1} + \ldots + a_n b_m x^n)$

Thus, the coefficient of x^n in $f_l\,(x)$ is zero; and hence,

deg $f_l(x) \leq n - l$.

By the induction hypothesis, there exist $q_l\,(x)$ and $r\,(x)$ in

$F[x]$ such that $f_l\,(x) = q_l\,(x)\, g(x) + r(x)$, where deg $r(x) <$ deg $g(x)$.

Substituting the value of $f_1(x)$, we get

$f(x) - a_n b_m^{-l}\, x^{n-m}\, g(x) = q_1(x)\, g(x) + r(x)$,

i.e., $f(x) = \{a_n b_m^{-l}\, x^{n-m} + q_1(x)\}\, g(x) + r(x)$

$1 = q(x)\, g(x) + r(x)$, where $q(x) = a_n b_m^{-1}\, x^{n-m} + q_l(x)$
and deg $r(x) <$ deg $g(x)$.

Therefore, the algorithm is true for $f(x)$. and hence, for all polynomials in $F[x]$.

b) Now let us show that $q(x)$ and $r(x)$ are uniquely determined.

If possible, let

$f(x) = q_1(x)\, g(x) + r_1(x)$ where deg $r_l(x) <$deg $g(x)$. and
$f(x) = q_2(x)\, g(x) + r_2(x)$ where deg $r_2(x) <$deg $g(x)$.

Then

$q_1(x)\, g(x)+r_l(x) = q_2(x)\, g(x)+r_2(x)$, so that
$\{q_1(x)-q_2(X)\}\, g(x) = r_2(x)-r_l(x)$ ……(1)

Now if $q_1(x) \neq q_2(x)$ then deg $\{q_1(x) -q_2(x)\} \geq 0$, so that
deg $[\{q_l(x) – q_2(x)\}\, g(x)] \geq$ deg g(x).

On the other hand, deg $\{r_2(x)-r_1(x)\} <$ deg g(x), since
deg $r_2(x) <$deg g(x) and deg $r_1(x) <$ deg g(x).

But this contradicts Equation (1). Hence, Equation (l) will remain valid only if $q_1(x) – q_2(x) = 0$. And then $r_2(x) –r_1(x) = 0$,

i,e., $q_1(x) = q_2(x)$ and $r_l(x) = r_2(x)$.

Thus we have proved the uniqueness of q(x) and r(x) in the expression f(x) = q(x) g(x)+r(x).

Here q(x) is called the quotient and r(x) is called the remainder obtained on dividing f(x) by g(x).

Now, what happens if we take g(x) of Theorem 5 to be a linear polynomial? We get the remainder theorem. Before proving it let us set up some notation.

Notation

Let R be a ring and $f(x) \in R[x]$.Let
$f(x) = a_0 + a_lx +…...+a_n x^n \in R$
Then, for all $r \in R$, we define
$f(r) = a_0+a_1r+...+a_nr^n \in R$.

That is, f(r) is the value of f(x) obtained by substituting r for x.

Thus, if $f(x) = 1+x+x^2 \in Z[x]$, then

f(2) = 1+2+4 = 7 and f(0) = 1+0+0 = 1.

Let us now prove the remainder theorem. which is a corollary to the division algorithm.

Theorem 6 (Remainder Theorem)

Let F be a field. If $f(x) \in F[x]$ and $b \in F$, then here exists unique polynomial $q(x) \in F[x]$ such that $f(x) = (x-b)\, q(x)+f(b,)$.

Proof

Let $g(x) = x-b$. Then, applying the division algorithm to f(x) and g(x), we can find unique q(x) and r(x) in F[x], such that
$f(x) = q(x)\, g(x)+r(x)$

$= q(x)\, (x-b)+r(x)$, where deg r(x) < deg g(x) = 1.

Deg r (x) < 1, r (x) is an element of F, say a.

So, $f(x) = (x-b)\, q(x)+a$.

Substituting b for x, we get

$f(l) = (b-b)\, q(b) + a$

$= 0.q(b)+a = a$

Thus, a = f(b).

Therefore, $f(x) = (x-b)\, q(x)+f(b)$.

Note that deg f(x) = deg(x-b)+deg q(x) = 1 +deg q(x).

Therefore, deg q(x) = deg f(x)–l.

Let us apply the division algorithm in a few situations now.

Example 1

Express $x^4+x^3+5x^2$ -x as

$(x^2+x+l)\, q(x)+r(x)$ in Q[x].

Solution

We will apply long division of polynomials to solve this problem.

$$
\begin{array}{r}
x^2 + 4 \\
x^2+x+1\overline{)\,x^4+x^3+5x^2-x} \\
\underline{x^4+x^3+x^2} \\
4x^2-x \\
\underline{4x^2+4x+4} \\
-5x-4
\end{array}
$$

Now, since the degree of the remainder -5x- 4 is less than deg (x^2+x+ I), we stop the process, We get

$x^4+x^3+5x^2$ -x = (x^2+x+l) (x^2+4) -(5x+4).

Here the quotient is x^2+4 and the remainder is -(5x+4).

Now you can try some exercises.

E 8) Express f as gp+r, where deg r < deg g, in each of the following cases.

a) f = x_4+1, g = x_3 in **Q**[x]
b) f = $x^3 + \bar{2}x^2 - x + \bar{1}$ in $\mathbf{Z}_3$[x]
c) f = $x^3 - 1$, g = x – 1 in **R**[x]

E 9) You know that if p,q $\in$ Z, q $\neq$ 0, then $\frac{p}{q}$ can be written as the sum of an integer and a fraction $\frac{m}{q}$ with | m | < | q |. What is the analogous property, fur elements of F[x]?

Now, let us see what happens when the remainder in the expression f = pg+r is zero

3.4 Roots of Polynomials

In Sec. 12.4 you have seen when we can say that an element in a ring divides another element. Let us recall the definition in the context of F[x], where F is a field.

Definition

Let f(x) and g(x) be in F[x], where F is a field and g (x) $\neq$ 0. We say that g(x) **divides** f(x)(or g(x) is a **factor** of f(x), or f(x) is **divisible** by g(x) if there-exists q(x) $\in$ F[xl such that

$$f(x) = q(x)\, g(x).$$

We write g(x) j f(x) for 'g(x) divides f(x), and g(x) ~ f(x) for 'g(x) does not divide f(x).

Now, if f(x) $\in$ F[x] and g(x) $\in$ F[x], where g(x) $\neq$ 0, then does Theorem say when g(x) | f(x)? It does, We find that g(x) | f(x) if r(x) = 0 in Theorem 5.

In the fol1owing exercise we make an important, similar statement. You can prove it by applying Theorem 6.

E 10) Let F be a field and f(x) $\in$ F[x] with deg f(x) $\geq$ 1. Let a $\in$ F.

show that f(x) is divisible by x-a iff f(a) = 0.

This exercise leads us to the following definition.

Definition

Let F be a field and f(x) $\in$ F[x]. We say that an element a $\in$ F is a root (or zero) of f(x) if f(a) = 0.

For example, 1 is a root of x^2-1 $\in$ **R**[x], since 1^2-1 = 0.

Similarly, - 1 is a root of f(x) = $x^3+x^2+\frac{1}{2}\ x+\frac{1}{2} \in$ **Q** [x], since- .

$$f(-1) = 1+1 - \frac{1}{2} + \frac{1}{2} = 0.$$

Not that, in E 10 you have proved the following criterion for an element to be a root of a polynomial:

Let f be a field and f (x) $\in$ F[x]. Then a $\in$ F is a root of f(x) if and only if (x-a)|f(x).

We can generalize this criterion to define a root of multiplicity m of a polynomial in F[x].

Definition

Let F be a field and f(x) $\in$ F[x] We say that **a $\in$ F is a root of multiplicity m** (where) m is a positive integer of

f(x) it $(x-a)^m$ | f(x) but $(x-a)^{m+l}$ x f(1).
For example, 3 is a root of multiplicity 2 of the polynomial $(x-3)^2$ (x+2) **Q**[x]; and (-2) is a root of multiplicity 1 of this polynomial.

Now is it easy to obtain all the roots of a given polynomial? Any linear polynomial ax+b $\in$ F[x] will have only one root namely, $-a^{-l}b$. This is because ax+b = 0 iff $x = -a^{-l}b$.

In the case of a quadratic polynomial $ax^2+bx+c \in F[x]$, you know that its two roots are obtained by applying the quadratic formula.

$$x=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$$

For polynomials of higher degree we may be able to obtain some roots by trial and error. For example, consider $f(X) = x^5-2x+1 \in \mathbf{R}[x]$, Then, we try out x = 1 and find f(1) = 0. So, we find that l is a zero of f(x). But this method doesn't give us all the roots of f(x),.

Now you can try these exercises.

E 11) Find the roots of the following polynomials, along with their multiplicity.

a) $f(x) = \frac{1}{2}x^2 - \frac{1}{2}x + 3 \in \mathbf{Q}[x]$

b) $f(x) = x^2 + x + \bar{1} \in \mathbf{Z}_3[x]$

c) $f(x) = x^4 + \bar{2}x^3 - \bar{2}x - \bar{1} \in \mathbf{Z}_5[x]$

E 12) Let F be a field and a $\in$ F Define a function

$\phi : F[x] \to F: \phi(f(x)) = f(a)$.

This function is the evaluation at a.

Show that

a) ϕ is an onto ring homomorphism.

b) ϕ (b) = b $\forall$ b $\in$ F.

c) Ker ϕ = < x - a>

So, what does the Fundamental Theorem of Homomorphism say in this case?

As we have just seen; it is not easy to find all the roots of a given polynomial. But we can give a definite result about the number of roots of a polynomial.

Theorem 7

Let f(x) be a non-zero polynomial of degree n over a field F. Then f(x) ha: at most n roots in F.

Proof

If n = 0, then f(x) is anon-zero constant polynomial.

Thus, it has no roots, and hence, it has at most 0 (= n) roots in F.

So, let us assume that n $\geq$ 1. We will use the principle of induction on n. If deg t(x) = 1, then

$f(x) = a_0 + a_1 x$, where $a_0\ a_l \in F$ and $a_l \neq 0$.

So f(x) has only one root, namely, $(-a_1^{-1}\ a_0)$

Now assume that the theorem is true for all polynomials in F[x] of degree < n. We will show that the number of roots of f(x), $\leq$ n.

If f(x) has no root in F, then the number of root of f(x) in F is 0 $\leq$ n. So, suppose f(x) has a root a $\in$ F.

Then f(x) = (x-a) g(x), where deg g(x) = n-l.

Hence, by the induction hypothesis g(x) has at most n-1 roots in F, say a^l,...,a_{n-1} Now,

a_1 is a root of g(x) $\Rightarrow$ g(a_i) = 0 $\Rightarrow$ f(a_i) = (a_i-a) g(a) = 0

$\Rightarrow$ a_i is it root of(x) $\forall$ i = 1,..., n-l.

Thus, each root of g(x) is It root of f(x).

Now, $b \in F$ is a root of f(x) iff f(b) = 0, i.e., iff (b-a) g(b) = 0, i.e., iff b-a = 0 or g(b) = 0, since F is an integral domain. Thus, b is a root of f(x) iff b = a or b is a root of g(x). So, the only roots of f(x) are a and $a_1 \ldots, a_{n-1}$.

Thus, f(x) has at the most n roots, and so, the theorem is true for n.
Hence, the theorem is true for all $n \geq 1$.

Using this result we know that, for example, $x^3-1 \in \mathbf{Q}[x]$ can't have more than 3 roots in **Q**.

In Theorem 7 we have not spoken about the roots being distinct. But an obvious corollary of Theorem 7 is that

if $f(x) \in F[x]$ is of degree n, then f(x) has at most n distinct roots in F.

We will use this result to prove the following useful theorem.

Theorem 8

Let f(x) and g(x) be two non-zero polynomials of degree, n over the field F if there exist n+1 distinct elements $a_l,\ldots,a_{n+1}$ in F such that $f(a_i) = g(a) \ \forall \ i = 1, \ldots, n+1$, then f(x) = g(x).

Proof

Consider the polynomial h(x) = f(x) -g(x)

Then deg $h(x) \leq n$, but it has n+1 distinct roots $a_1, \ldots, a_{n+1}$.

This is impossible, unless h(x) = 0, i.e., f(x) = g(x).

We will now give you an example to show you that Theorem 7 (and hence Theorem 8) need not be true for polynomials over a general ring.

Example 2

Prove that $x^3 + \bar{5}\, x \in Z_6[x]$ has more roots than its degree. (Note that Z_6 is not a field.)

Solution

Since the ring is finite, it is easy for us to run through all its elements and check which of them, are roots of

$f(x) = x^3 + \bar{5}\, x.$

So, by substitution we find that

$f(0) = 0 = f(\bar{1}) = f(\bar{2}) = f(\bar{3}) = f(\bar{4}) = f(\bar{4})$.

In fact, every element of Z_6 is a zero of f(x). Thus, f(x) has 6 zeros, while deg f(x) =3.

Try these exercises now.

E 13) Let p be a prime number. Consider $x^{p-1} - \bar{1} \in Z_p[x]$. Use the fact that Z_p is a group of order p to show that every non-zero element of Z_p is a root of $x^{p-1} - \bar{1}$.

Thus, show that $x^{p-1} - \bar{1} = (x - \bar{1})(x - \bar{2}) ...(x - \overline{p-1})$.

E 14) The polynomial $x^4 + \bar{4}$ can he factored into, linear factors in Z_5 [x]:

Find this factorization.

So far, we have been saying that a polynomial of degree n over F has at most n roots in F. If can happen that the polynomial has no root in F. for example, consider the polynomial $x^2+1 \in R[x]$. From Theorem 7 you know that it can have 2 roots in **R**, at the most. But as you know, this has no roots in **R** (it has two roots, i and – i, in **C**).

We can find many other examples of such polynomials in **R**[x]. We call such polynomials irreducible over **R.** We shall discuss them in detail in the next two units.

4.0 CONCLUSION

Polynomial rings are very important class of rings in mathematics. Hardily can we not come across polynomial expressions in our daily mathematical endeavours, since we need to add or subtract two mathematical algebraic expressions from each other. It is required of you to read this unit carefully before you proceed to the next unit.

5.0 SUMMARY

In this unit we have covered the following points.

1) The definition and examples of polynomials over a ring.
2) The ring structure of R[x], where R is a ring.
3) R is a commutative ring with identity iff R[x] is a commutative ring with identity.
4) R is an integral domain iff R[x] is an integral domain.

5) The division algorithm in F[x], where F is a field, which states that if f(x), g(x) $\in$ F[x], g(x) $\neq$ 0, then there exist unique q(x), r(x) $\in$ F[x] with f(x) = q(x) g(x)+r(x) and deg r(x) < deg g(x).
6) a $\in$ F is a root of f(x) $\in$ F[x] iff (x-a) | f(x).
7) A non-zero polynomial of degree n over a field F can have at the most n roots.

6.0 TUTOR-MARKED ASSIGNMENT

1. The polynomials are (a), (c), (d), (f).

   (b) and (e) are not polynomials since they involve negative and fractional powers of x.

   (a) and (t) are in **Z**[x].

2. The degrees are 1, 3, 4.3, - ∞, respectively. The leading coefficients of the first four are $\sqrt{2}$, 7, 1, $\frac{1}{7}$, respectively, o has no leading coefficient.

3a. $2+5x+3x^2+(4+1)x^3 = 2+5x+3x^2+5x^3$
b. $(\bar{6}+\bar{1})-\bar{2}x+\bar{2}x^2+\bar{5}x^3=-\bar{2}x+\bar{2}x^2+\bar{5}x^3$, $\sin ce\ \bar{7}=\bar{0}$
c. $1+3x+3x^2+x^3$
d. $\bar{1}+x^3, \sin ce\ \bar{3}=\bar{0}$
e. $10x+5x^2+7x^3+x^4+x^5$

4. Every element of R is an element of R[x]. Therefore multiplication in R is also commutative.
   Also, the identity of R[x] is an element of R, and hence is the identity of R.

5. (a) and (b)

6. We know that R[x] is a domain. Let char R = n. By Theorem 3 of Unit 12 we know, that n is the least positive integer sucl1that n.l = 0. Since 1 is also the identity of R[x], the same theorem of Unit 12 tells us that char R.

7. Let $p(x) = a_0+a_1x+...+a_nx^n$, $q(x) = b_0+b_1x+...+b_mx^m \in R[x]$.

Then $\phi(p(x)+q(x)) = \phi\left(\sum_{i=0}^{t}(a_i+b_i)x^i\right)$, where t = max (m,n)

$$= \sum_{i=0}^{t} f(a_i+b_i)x^i$$

$$= \sum_{i=0}^{t} [f(a_i)+f(b_i)]x^i$$

$$= \sum_{i=0}^{t} f(a_i)x^i + \sum_{i=0}^{t} f(b_i)x^i$$

$= \phi\ (p(x))+\phi\ (q(x))$, since $f(a_i) = 0 = f(b_j)$

Whenever $a_i = 0$, $b_j = 0$.

Also, $\phi\ (p(x)q(x)) = \phi\ (\sum_{i=0}^{m+n} c_i x_i)$, where $c_i = a_ib_0+a_{i-1}b_1+\ldots+a_0b_i$

$$= \sum_{i=0}^{m+n} f(c_i)x^i$$

$$= \sum_{i=0}^{m+n} [f(a_i)f(b_0) + f(a_{i-1})\ f(b_1) +\ldots+(a_0)\ f(b_i)]x^i$$

since f is a ring homomorphism;

$= \phi\ (p(x))\ \phi\ (q(x))$.

Thus, ϕ is a ring homomorphism.

8a. $f = x.g+l$, $q = x$, $r = l$

b) $x+\bar{1}\overline{)x^3+\bar{2}x^2-x+\bar{1}}\;\;x^2+x-\bar{2}$

$x^3=x^2$

$x^2-x+\bar{1}$

x^2+x

$-\bar{2}x+\bar{1}$

$-\bar{2}x+\bar{1}$

$\bar{3}$

Thus, f = (x^2 + x - $\bar{2}$) g + $\bar{0}$, since $\bar{3}=\bar{0}$.

c) f = (x^{2+x+1})g + 0

9. Let f(x), g(x) $\in$ F[x], with g(x) $\neq$ 0. By Theorem 5, f(x) = g(x) q(x)+r(x) with deg r(x) < deg g(x). Now, this equality is still true if we consider it over the field of fractions of F[x]. Then, we can divide throughout by g(x), and get

$\frac{f(x)}{g(x)} = q(x)+\frac{r(x)}{g(x)}$, where deg r(x) < deg g(x).

10. By Theorem 6,

f(x) = (x-a) q (x)+f(a)
Thus, f(x) = (x-a) q(x) iff f(a) = 0, i.e.,
(x-a) | f(x) iff f(a) = 0.

11a. By the quadratic formula, the roots are 3 and 2, each with multiplicity 1.
b. $x^2+x+\bar{1}=(x-\bar{1})^2$, since $-\bar{2}=\bar{1}$ in $\mathbf{Z}_3$

Thus, $\bar{1}$ is the only zero, and its multiplicity is 2.

c. By trial, one zero is 1. Now, applying long division, we get
$x^4+\bar{2}\,x^3-\bar{2}\,x-\bar{1}=(x-\bar{1})(x^3+\bar{3}\,x^2+\bar{3}\,x+\bar{1})$ again, by trial and error we find that $x+\bar{1}$ is a factor of thus, $x^4+\bar{2}\,x^3-\bar{2}\,x-\bar{1}=(x+\bar{1})^3$

This shows that $\bar{1}$ is a root of multiplicity 1. and $-\bar{1}$ ($=\bar{4}$) is a root of multiplicity 3.

12a. Let $f(x)=\sum_{i=0}^{n} a_i x^i$, $g(x)=\sum_{i=0}^{m} b_i x^i$.

Then ϕ (f(x)+g(x)) = ϕ ($\sum_{i=0}^{t}$ $(a_i+b_i)\,x^i$), where t = max(m,n).

$$= \sum_{i=0}^{t} (a_i + b_i)a^i$$

$$= \sum_{i=0}^{t} a_i a^i + \sum_{i=0}^{t} b_i a^i$$

= f(a)+g(a)

= ϕ (f(x))+ ϕ (g(x)), and

$$\phi\ (f(x)\ g(x)) = \phi\left(\sum_{i=0}^{m+n} (a_i b_0 + a_{i-1}b_1 + \ldots + a_0 b_i)x^i\right)$$

$$= \sum_{i=0}^{m+n} (a_i b_0 + a_{i-1}b_1 + \ldots + a_0 b_i)a^i$$

= f(a) g(a)

= ϕ (f(x)) ϕ (g(x)).

Thus, ϕ is a homomorphism.

Now, given any element b $\in$ F, $\exists$ the constant polynomial

f(x) $\in$F[x] such that f(a) = b, i.e., (f(x)) = b.

Thus, ϕ is surjective.

b) This is what we have shown in the previous two lines.

c) f(x) $\in$ Ker ϕ iff ϕ (f(x)) = 0 iff f(a) = 0

iff (x-a) | f(x) iff f(x) $\in$ <x-a>

Thus, Ker ϕ = <x-a>
The Fundamental Theorem of Homomorphism says that

F[x]/<x-a> $\underset{\sim}{}$ F.

13. $(Z_p^*,.)$ *is a group and* $o(Z_p^*) = p-1)$

Thus, by E 8 of Unit 4, $x^{p-1} = \bar{1} \forall\ x \in Z_p^*$,

i.e., each of the p-1 elements of Z_p^* is a root of $x^{p-1}-\bar{1}$

Therefore, $(x-\bar{1}) \ldots (x-\overline{p-1}) \mid (x^{p-1}-\bar{1})$.

Since, $x^{p-1}-\bar{1}$ can have at most p-1 rots in Z_p, we find that the (p-1) elements of Z_p^* are yjr only rooyd of $x^{p-1}-\bar{1}$.

Thus, $x^{p-1}-\bar{1} = (x-\bar{1})\ldots(x-\overline{p-1})$.

14. The polynomial $x^4 + \bar{4}$ is the same as $x^4 - \bar{1}$ in $Z_5[x]$,

since $\bar{4} = -\bar{1}$. Thus, applying the result in E 13, we get,

$x^4 + \bar{4} = (x-\bar{1})(x-\bar{2})(x-\bar{3})(x-\bar{4})$

7.0 REFERENCES/FURTHER READING

Ansa B. E. (2010). Modern Algebra Ethereal Bliss Publisher. Calabar.

Kiku, A. O. (1992). Abtract Algebra Ibadan. Ibadan University, Press

Ilori, S. A. & Akinyele, O. (1986). Elementary Abstract and Linear Algebra. Ibadan University, Press.

Ilori, S. A. & Ajayi D. O. (2000). University Mathematics Series 2. Algebra Books (A Division of Ass Book Markers Nig. Ltd Ibadan).

Lipschuty, S. (2004). Schaum's Outlines Series on Set Theory and Related Topics. MAcGraw – Hill, NY.

Osisiogu, U. A. (1998). An Introduction to Real Analysis with Special Topic on Functions of Several Variables and Method of Languages Multipliers, Bestsoft Educational Books Nigeria.

UNIT 3 SPECIAL INTEGRAL DOMAINS

CONTENTS

1.0 INTRODUCTION

In this unit we shall look lit 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 6 you saw that the division algorithm holds for F[x] where F is a field. In Unit 1 you saw that it holds for **Z**. Actually, there are lots of other domains for which this algorithm is true. Such integral domains are called Euclidean domains. We shall discuss their properties in Sec. 7.2

In the next section we shall look at some domains which are algebraically very similar to 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.

2.0 OBJECTIVES

At the end of 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.

3.0 MAIN CONTENT

3.1 Euclidean Domain

In this course you have seen that 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: $R \setminus \{0\} \rightarrow N \cup \{0\}$ is
A **Euclidean valuation** on R if !.he 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: $Z \rightarrow N \cup \{0\}$: d(n) = | n |
Then, for any a,b $\in$ Z\{0},

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

= d(a),

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

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

i.e., a = bq+r,. where r= 0 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\.{0}, is a Euclidean domain.

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

d: F[x] \ {0} $\rightarrow$ **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 too, 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 \ {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\ {0}. Thus, the units of F[x] are the non-zero element of F. That is, the units of F and F[x] coincide.

Example 3

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

Solution

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

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

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

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

⇨ $ac-5bd = 1$ and $bc+ad = 0$

⇨ $abc-5b^2d = b$ and $bc+ad = 0$

⇨ $a(-ad)-5b^2d = b$, substituting be $=-ad$.

⇨ $(a^2+5b^2)d = -b$

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) **Z,** b) $\mathbf{Z}_6$, c) $\mathbf{Z}+i\mathbf{Z}$.

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 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(d) d(1) can't happen.

Conversely, assume that is a unit in R. Let be 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 $n \in \mathbf{Z}$ is a unit in **Z** iff |n| = |1| = 1. Thus, the only unit 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 Euclidean 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 = Ra, 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 $I \subseteq$ Rand 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) < q(b) is not possible.

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

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

From (I) and (2) we get

1= Rb.

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

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

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

3.2 Principal Ideal Domain (PID)

In the previous section you have proved 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.

Thus, **Z** is a PID. Can you think of another example of a PID? What about **Q** and **Q**[x]? In fact, by Theorem 2 all Euclidean domains are PlDs. 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 $\in$ Z, is a principal ideal domain, but not it Euclidean domain. The proof of this 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 Z[x] is not a PID.

Solution

You know that **Z**[x] is a domain, since **Z** is one. We will show that all its ideals are not principal. Consider the ideal of 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) $\in$ **Z**[x].

On the contrary, suppose that $\exists$ f(x) $\in$ Z[x] such that <2,x> = <f(x)>. Clearly, f(x) $\neq$ 0. Also, $\exists$ g(x), h(x) $\in$ **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 h(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$\in$ < f(x)> = <x,2>. Thus, we can write

1 = x $(a_0+a_1x^4+a_1x^r)$ + $2(b_0+b_1x+\ldots+b_sx^s)$, where $a_1,b_j \in Z \forall$ i = 0, 1…..r and j = 0, 1,…….,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, <x,2> is not a principal ideal.

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

Now, try the following exercise.

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 $a,b \neq 0$, then a **divides** b if there exists $c \in R$ such that $b = ac$.

Now we would like to generalize 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, $c \mid d$.

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, then d=ud`, for some unit u. For this we need a result that you can prove in the following exercise.

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 to 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 **Q**[x] find the g.c.d of

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

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

Solution

By the quadratic formula, we know that the roots of p(x) are 2 and – 5, and the roots of q(x) are 2 and – 1 / 3

Therefore, p(x) = (x-2) (x+5) 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 **Z** / <8>
b) x^2+8x15 and $x^2+12x+35$ in **Z**[x].
c) x^3-2x^2+6x-5 and x^2-2x+1 in **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 dieal <a,b>. Since R is a PID, this ideal must be principal also. Let d $\in$ R such that <a,b> = <d>. we will show that the g.c.d of a and b is d.

Since a $\in$ <d>, d | a, Similarly, d | b.

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

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

Since c | a and c | b, c | (ax+by), i.e., c | 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 a.

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) $\in$ F[x].

For example, in 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 | bc. Show that if (a,b) = 1, then a | c.

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

Let us now discuss a concept related 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 **E**9(x), i.e., the irreducible polynomials over **R** and **C.** Consider the following important theorem about polynomials in **C**[x]. You have already come across this in the Linear Algebra course.

Theorem 5 (Fundamental Theorem of Algebra)

Any non-constant polynomial in **C**[x] has a rot 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 **C**[x] iff it is linear

Theorem 6

Any irreducible polynomial in **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 betwee9 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 | ab, where $a,b \in R$. Suppose $x \times a$. Then (x,a) = 1, since the only factor of x is itself, up to units. Thus, by E 11, x | 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 | ab. If p | 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 primness) over **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 l0 of Unit 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

$I_1 \subseteq I_2 \subseteq \ldots$. r an ass(

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

Proof

Consider the set $I = I_1 \cup I_2 \cup \ldots \bigcup_{n=1}^{\infty}$. We will prove that I is 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 n ideal of R. Since R is a PID, I = <a> 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, $I_m = I_{m+2}$, and so on. Thus, $I_m=I_{m+1} = 1_{m+2}$=…

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 < p > 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 PIP. An ideal < a > is a maximal ideal of R iff a is a prime element of R.

Proof

If <a> 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 < a > ~ I. Since R is a PID, I = <b> for some b e R. We will show that b is a unit in R; and hence, by E 4, <b>=R, i.e., I = R.

Now, <a> $\subseteq$ <b> $\Rightarrow$ a = bc for some c $\in$ R. Since a is irreducible, either is an associate of a or b is a unit in R. But if b is an associate of a, then <b> = <a>, a contradiction. Therefore, b is a unit in R. Therefore, 1= R.

Thus, <a> is a maximal ideal of R.

What Theorem 9 says is ~hat the prime ideals and maximal ideals coincide in a PID.

Try the following exercise now.

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

a) < 5 > in Z,
b) $< x^2-1 >$ in Q [
c) $<x^2+x+1 >$ in R[x],
d) < x > in 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 ID and a be a non-zero non-invertible element of R. then there is some prime element p in R such that p|a.

Proof

If a is prime, take p = a. otherwise, we write a = a_1b_1, where neither a_1 nor b_1 is an associate of a. Then $<a> \subset_{\times} < a_1 >$. If a_1 is prime take p = a_1. Otherwise, we can write a_1 = a_2b_2, where neither a_2 nor b_2 is an associate of a_1. Then $<a_1> \subset_{\times} <a_2>$. Continuing in this way we get an increasing chain

$<a> \subset_{\times} <a_1> \subset_{\times} <a_2> \subset_{\times} \ldots$

By Theorem 8, this chain stops with some $<a_n>$. Then a_n with be prime, since it doesn't have any non-trivial factors. Take p = a_n, 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 = $p_1p_2\ldots p_r$, where $p_1,p_2,\ldots,p_r$, are prime elements of R.

Proof

If a is a prime element, there is nothing to prove. If not, then p_1 | a for some prime p_1 in R, by Theorem 10. Let a = p_1a_1. If a_1 is a prime, we are through. Otherwise $p_2|a_1$ for some prime p_2 in R. Let a_1 = p_2a_2. Then a = $p_1p_2a_2$. 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, $<a> \subset_{\times} <a_1>$. Similarly, $<a_1> \subset_{\times} <a_2>$. So, as the process continues we get an increasing chain of ideals,

$<a> \subset_{\times} <a_1> \subset_{\times} <a_2> \subset_{\times}$

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

Hence, the process stops after m steps, i.e., we can write $a = p_1p_2\ldots p_m$, where p_i is a prime element of R $\forall$ i = 1,…, m.

Thus, any non-zero non-invertible element in a PID can be factorised into a product of Primes. What is interesting about this factorization 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 $a = P_1P_2...P_n = q_1q_2...q_m$, 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 Rand if $p|a_1a_2... a_n$ (where $a_1,a_2,\ldots, a_n \in R$), then p_i for some i= 1,2,...,n.

Now let us start the proof of Theorem 12.

Proof

Since $p_1p_2\ldots p_n = q_1q_2\ldots q_m$, $p_1|p_1p_2\ldots q_m$.

Thus, by E 15, $p_1|q_j$ for some j = 1,……,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 $q_1 = p_1u_1$. Since q_1 is irreducible, u_1 must be a unit in R. So p_1 and q_1 are associates. New we have

$P_1p_2\ldots p_n = (p_1u_1)\, q_2\ldots q_m$

Canceling p_1 from both sides, we get

$p_2p_3\ldots p_n = u_1q_2\ldots q_m$.

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

Then we will get

$1 = u_1u_2\ldots u_n\, q_{n+1}\ldots qm$.

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_i, and vice versa.

What Theorem 12 says is that **any two prime factorizations 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 $[\frac{1}{2}(x+1)]$ $[2(x-1)]$ in $\mathbf{R}[x]$.

Now you can try the following exercise.

E 16) Give the prime factorization 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 oilier domains also. Let us discuss such rings now.

3.3 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 $a = p_1p_2\ p_n = q_lq_2 \ldots\ q_m$ be two factorisations into irreducible, then n = m and each p_i is am 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 Theorem 11 and 12 help? Of course! In them we have proved that **every PID 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 filed 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 $\mathbf{Z}[\sqrt{-5}] = \{a+b\sqrt{-5} \mid a,b \in \mathbf{Z}\}$ is not a UFD.

Solution

Let us define a function

$f: \mathbf{Z}[\sqrt{-5}] \rightarrow NU\ \{0\}$ 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

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

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

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

In Example 3, you have already shown that the only units of $\mathbf{Z}[\sqrt{-5}]$ 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 $\alpha,\beta \in \mathbf{Z}[\sqrt{-5}]$.
Applying the function f we see that

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

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

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

So, if $\alpha = a+b\sqrt{-5}$, 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 $\mathbf{Z}$. 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 factorization of 9 as a product of irreducible elements is not unique. Therefore, $\mathbf{Z}[\sqrt{-5}]$ 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 $2+\sqrt{+5} \chi 3$. 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 $\mathbf{Z}[\sqrt{+5}]$.

Now let us discuss some properties of a UFO. 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 any element a in a UFD R can be written as

$A = p_1^{r1} p_2^{r2} \ldots p_n^{rn}$

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 $\in$ R.

Let $a = p_1^{r1}p_2^{r2}\ldots p_n^{rn}$ and $b = p_1^{S1}p_2^{S2}\ldots p_n^{Sn}$

Where $p_1,p_2,\ldots, p_n$ are distinct irreducible elements of R and r_i and spare non-negative integers $\forall$ i = 1,2,…,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 $20 = 2^2x3^0\ x.5^1$ and $15 = 2^0\ x3^1x.5^1$)

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

Then $d = p_1^{t1}p_2^{t2}\ldots p_n^{tn}$ divides a as well as b, since $t_i \leq r_i$ and $t_i \leq s_i\ \forall$ I = 1,2,….,n.

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

Thus, $c = p_1^{m1}p_2^{m2}\ldots p_n^{mn}$ where $m_i \leq r_i$ and $m_i \leq s_i\ \forall$I = 1,2,…,n. Thus, $m_i \leq t_i\ \forall$

Therefore, c | 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 elemnt. 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 EI3 We know that every prime in R is irreducible. So let us prove the converse.

Let a $\in$ R be irreducible and let a | bc, where b,c$\in$ R.

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

If(a,b) = a, a | b.

If (a,b) = 1, then a $\nmid$b. Let bc = ad, where d $\in$ R.

Let b = p_1^{r1} p_2^{r2}…p_m^{rm} and c = $q_1^{S1}q_2^{S2}$…q_n^{Sn}, be irreducible factorizations of b and c. Since bc = ad and a is irreducible, a must be one of the p_is or one of the q_is. Since aχb, a $\neq p_i$ for any i. Therefore, a = q_j for some j. That is, a|c.

Thus, If (a,b) =1 , then a |c

So, we have shown that a | bc a | b or a | c.

Hence, a is prime.

For the final property of UFDs that we are going to state, let us go back of Example 4 for a moment. Over there we gave you an example of a PID R, for which 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. Y 011 can use it to solve the following exercises.

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

E21) If p is an irreducible clement 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.

4.0 CONCLUSION

5.0 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 arc 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 roots1n 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 an~ F[x] are UFDs, for any field F

11) In a UFD (and hence, in a PID) an clement is prime iff it is irreducible

12) Any two elements In a UFD have a g.c.d.

13) If Ris a UFD, then so is R [x]

ANSWER TO SELFASSESSMENT EXERCISE

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.

2. In Unit. 13, you have seen that

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

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

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

b) Let $\bar{m}\ m \in \mathbf{Z}_6$ 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

$(a+ib)\,(c+id) = 1$,
$\Rightarrow$ $(ac-bc)+(ad+bc)I = 1$
$\Rightarrow$ $ac-bd = 1$ and $ad+bc = 0$
$\Rightarrow$ $b = 0$, as in Example 3.

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

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.

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

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

Then $2 \in S$, $3 \in S$ but $2-3 \notin S$ since $|2-3| = 1$.

Thus, S is not even a subring of R,

7. For example, $\mathbf{Z}[x]$ is a subring of $\mathbf{Q}[x]$, which is a PID. But $\mathbf{Z}$[xl is not a PID.

8. $\mathbf{Z}$ is it,PID. But $\mathbf{Z}/6\mathbf{Z}$ is not even a domain. Thus, it is not a P1D.

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

b. $a \mid b$ and $b \mid a$

=> $b = ac$ and $a = bd$ for some $b,d \in R$.
=> $b = bdc$
=> $b = 0$ 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 $b \mid a$.
Also, let $v \in R$ such that $uv = 1$. Then $av = buv = b$.
Thus, $a \mid b$.

10a. $\bar{2}$.

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.

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

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

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

12. (c) is, because of Theorem

(a) is not, since it is $(x-1)^2$
(b) is not, because of Theorem 5'.
(d) is not, because of Theorem 6.

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.

14(a), (c), since 5 and x^2+x+1 are irreducible in **Z** and **R**[x], respectively.
(b) is not, using Theorem 9.
(d) is not, since **Z**[x]/ $\langle x \rangle \simeq$ **Z**, which is not a field.

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

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

Since p is a prime element, we find that $p \mid a_1 a_2 ... a_{n-1}$ or $p \mid a_n$

If $p \mid a_1 a_2 ... a_{n-1}$, then $p \mid a_i$ for some i = 1,…,n-l 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,….,

So, our result is true for n.

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

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 po1ynonlial is linear, and hence, irreducible over $\mathbf{Z}_2$

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

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 $g_l(x) = f_2(x)g_2(x)$. Then deg $g_2(x)$ < deg $g_l(x)$. 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 $f_1(x)$ is prime in F[x].

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

18. 10 = 2 x 5 = x 2.

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 $\mathbf{Z}[\sqrt{-5}]$.

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

21. No. For example, x is irreducible in **Z**[x]; but $\bar{x}$ is zero in **Z**[x]/< x > $\underline{\sim}$ **Z**.
22. The quotient ring of a domain need not be a domain. For example, **Z** is a UFD, but **Z**/<4> is not.

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

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

6.0 TUTOR-MARKED ASSIGNMENT

7.0 REFERENCES/FURTHER READING

Ansa B. E. (2010). Modern Algebra Ethereal Bliss Publisher. Calabar.

Kiku, A. O. (1992). Abtract Algebra Ibadan. Ibadan University, Press

Ilori, S. A. & Akinyele, O. (1986). Elementary Abstract and Linear Algebra. Ibadan University, Press.

Ilori, S. A. & Ajayi D. O. (2000). University Mathematics Series 2. Algebra Books (A Division of Ass Book Markers Nig. Ltd Ibadan).

Lipschuty, S. (2004). Schaum's Outlines Series on Set Theory and Related Topics. MAcGraw – Hill, NY.

Osisiogu, U. A. (1998). An Introduction to Real Analysis with Special Topic on Functions of Several Variables and Method of Languages Multipliers, Bestsoft Educational Books Nigeria.

UNIT 4 IRREDUCIBILITY AND FIELD EXTENSIONS

CONTENTS

1.0 INTRODUCTION

In the previous unit we discussed various kinds of integral domains, including unique factorization domains. Over there you saw that **Z**[x] and **Q**[x] are UFDs. Thus, the prime and irreducible elements coincide in these rings; In this unit we will give you a method for obtaining the prime (or irreducible) elements of **Z**[x] and **Q**[x]. This is the Eisenstein criterion, which can also be used for obtaining the irreducible elements of any polynomial ring over a UFD.

After this we will introduce you to field extensions and subfields. We will use irreducible polynomials for obtaining field extensions of a field F from F[x]. We will also show you that every field it; a field extension of **Q** or **Z**p for some prime p. Because of this we call Q and the $\mathbf{Z}_p^S$ prim fields. We will discuss these fields briefly.

Fig. 1: Evariste Galois (1811 – 1832)

Finally, we wil1.look at finite fields. These fields were introduced by the young French mathematician Evariste Galois (Fig. l) while he was exploring number theory. We will discuss some properties of finite fields which will show us how to classify them.

Before reading this unit we suggest that you go through the definitions of irreducibility from Unit l4. We also suggest that you

go through Units 3 and 4 of the Linear Algebra course if you want to understand the proof of Theorem 7 of this unit. We have kept the proof optional. But once you know what a vector space and its basis are, then the proof IS very.

2.0 OBJECTIVES

At the end of this unit, you should be able to:

- prove and use Eisenstein's criterion for irreducibility in **Z**[x] and **Q**[x]
- obtain field cxten5ionsof a field F from F[x]
- obtain the prime field of any field
- use the fact that finite field F has p^n elements, where char F = p and $\dim_{Z_p} F = n$.

3.0 MAIN CONTENT

3.1 Irreducibility in Q[x]

In Module 3 Unit 4 we introduced you to irreducibility irredt1clble polynomials in F[x], where F is a field. We also stated the Fundamental Theorem of Algebra, which said that a polynomial over **C** is irreducible iff it is linear. You also learnt that if a polynomial over **R** is irreducible, it must have degree l or degree 2. Thus, anypo1ynomial over **R** of degree more than 1 is reducible. And. using the quadratic formula, we know which quadratic polynomials over **R** are irreducible.

Now let us look at polynomials over **Q**. Again, as for any field F, a linear polynomial over **Q** is irreducible. Also, by using the quadratic formula we can explicitly obtain the roots of any quadratic polynomial over **Q** and hence figure out whether it is irreducible or not. But, can you tell whether $2x^7+3x^5 – 6x^4 + 3x^3 + 12$ is irreducible over **Q** or not? In two seconds we can tell you that it is irreducible, by using the Eisenstein criterion. This criterion was will build up the theory for proving this useful criterion.

Let us start with a definition.

Definition

Let $f(x) = a_0 + a_1x +...+ a_nx^n \in \mathbf{Z}[x]$. We define the content of f[x] to be the g.c.d of the integers $a_0, a_l,\ldots,$ an,

We say that f(x) is **primitive** if the content of f(x) is 1

For example, the content of $3x^2 + 6x + 12$ is the g.c.d. of 3,6 and 12, i.e., 3. Thus, this polynomial is not primitive. But $x^5 + 3x^2 + 4x - 5$ is primitive, since the g.c.d of 1,0,0,3,4,-5 is 1.

You may like to try the following exercises now.

E 1) What are the contents of the following polynomials over **Z**?

a) $1 + x + x^2 + x^3 + x^4$

b) $7x^4 - 7$

c) $5(2x^2 - l)(x + 2)$

E 2) Prove that any Polynomial $f(x) \in \mathbf{Z}[x]$ can be written as $dg(x)$, where d is the conter t

We will now prove that the product of primitive polynomials is a primitive polynomial. This result is well known as **Gauss' lemma.**

Theorem 1

Let f(x) and g(x) be primitive polynomials. Then so is f(x) g(x).

Proof

Let $f(x) = a_0 + a_l x + \ldots a_n x^n \in \mathbf{Z}[x]$ and

$g(x) = b_0 + b_l x + \ldots + b_m x^m \in \mathbf{Z}[x]$.where the

g.c.d of $a_0, a_1, \ldots, a_n$ is 1 and the g.cd of $b_0\ b_1, \ldots, b_m$ is 1. Now

$f(x)\ g(x) = c_0 + c_1 x + \ldots + c_{m+n} x^{m+n}$

where $c_k = a_0 b_k + a_l b_{k-1} + \ldots + a_k b_0$.

To prove the result we shall assume that it is false and then reach a contradiction. So, suppose that f(x) g(x) is not primitive. Then the g.c.d of $c_0, c_1, \ldots, c_{m+n}$ is greater than 1, and hence some prime p must divide it. Thus, $p \mid c_i \ \forall\ i = 0, 1, \ldots, m+n$. Since f(x) is primitive, p does not divide some a_i. Let r be the least integer such that $p \nmid a_r$. Similarly, let s be the least integer such that $p \nmid b_s$.

Now consider

$c_{r+s} = a_0b_{r+s}+a_lb_{r+s1} + ...+ a_rb_s + ...+a_{r+s}\, b_0$

$= a_rb_s + (a_0b_{r+s} + a_lb_{r+s-l}+ \ldots + a_{r-l}\, b_{s+1} + a_{r+1}b_{s-1}+\ldots+ a_{r+s}b_0)$

By our choice Of r and s, $p \mid a_0,\ldots, p \mid a_1$, $P \mid a_{r-1}$, and $p \mid b_0$, $p \mid b_l,\ldots, p \mid b_{s-l}$. Also $p \mid c_{r+s}$

Therefore, $p \mid c_{r+s} - (a_0b_{r+s} +... + a_{r-1}\, b_{s+1} + a_{r+1}\, b_{s-l}+ ...+ a_{r+s}b_0)$

i.e., $p \mid a_r\, b_s$

$\Rightarrow p \mid a_r$ or $p \mid b_s$ since p is a prime.

But $p \nmid ar$ and $p \nmid b_s$. So we reach a contradiction. Therefore, our supposition is false. That is, our theorem is true.

Let us shift our attention to polynomials over Q now.

Consider any polynomial over **Q**, say f(x) = $\frac{3}{2}x^3 + \frac{1}{5}x^2 + 3x + \frac{1}{3}$. If we take the kcm of all the denominators, i.e., of 2,5, 1 and 3, i.e., 30 and multiply f(x) by it what do we get?

$30f(x) = 45x^3 + 6x^2 + 90x + 10 \in \mathbf{Z}[x]$

Using the same process, we can multiply any $f(x) \in \mathbf{Q}[x]$ by a suitable integer d so that $df(x) \in \mathbf{Z}[x]$. We will use this fact while relating irreducibility in $\mathbf{Q}[x]$ with irreducibility in $\mathbf{Z}[x]$.

Theorem 2

If $f(x) \in \mathbf{Z}[x]$ is irreducible in $\mathbf{Z}[x]$, then it is irreducible in $\mathbf{Q}[x]$.

Proof

Let us suppose that f(x) is not irreducible over $\mathbf{Q}[x]$. Then we should reach a contradiction. So let f(x) = g(x) h(x) in $\mathbf{Q}[x]$, where neither g(x) nor h(x) is a unit, i.e., deg g(x) > 0, deg h(x) > 0. Since $g(x) \in \mathbf{Q}[x]$, $\exists\ m \in \mathbf{Z}$ such that $mg(x) \in \mathbf{Z}[x]$. Similarly, $\exists\ n \in \mathbf{Z}$ such that $n\, h(x) \in \mathbf{Z}[x]$.

Then,

$mnf(x) = mg(x)\, nh(x)$ ……(1)

Now, let us use E2. By E2, $f(x) = rf_1(x)$, $mg(x) = sg_1(x)$, $nh(x) = th_1(x)$, where r, s and t are the contents of f(x), mg (x) and nh (x) and $f_1(x)$, $g_1(x)$, $h_1(x)$ are primitive polynomials of positive degree.

Thus, (1) gives us

$Mnrf_1(x) = stg_1(x)\, h_1(x)$ ……(2)

Since $g_1(x)$ and $h_1(x)$ are primitive, Theorem 1 says that $g_1(x)\, h_1(x)$ is primitive. Thus, the content of the right hand side polynomial in (2) is st. But the content of the left hand side polynomial in (2) is mnr. Thus. (2) says that mnr = st.

Hence, using the cancellation law in (2), we get $f_1(x) = g_1(x)\, h_1(x)$.

Therefore, $f(x) = rf_1(x) = (rg_1(x))\, h_1(x)$ in $\mathbf{Z}[x]$, where neither $rg_1(x)$ nor $h_1(x)$ is a unit. This contradicts the fact that f(x) is irreducible in $\mathbf{Z}[x]$.

Thus, our supposition is false. Hence, f(x) must be irreducible in $\mathbf{Q}[x]$.

What this result says is that to check irreducibility of a polynomial in $\mathbf{Q}[x]$, it is enough to check it in $\mathbf{Z}[x]$. And. for checking it in $\mathbf{Z}[x]$ we have the terrific Eisenstein's criterion that we mentioned at the beginning of this section.

Theorem 3 (Eisenstein's Criterion)

Let $f(x) = a_0 + a_1x + ... + a_nx^n \in \mathbf{Z}[x]$ Suppose that for some prime number p,

i) $f \nmid a_n$,

ii) $p \mid a_0\ p \mid a_1, \ldots, p \mid a_{n-1}$, and

iii) $p^2 \nmid a_0$

Then f(x) is irreducible in $\mathbf{Z}[x]$ (and hence in $\mathbf{Q}[x]$)

Proof

Can you guess our method of proof? By contradiction, once again! So suppose f(x) is reducible in **Z**[x].
Let f(x) = g(x) h(x),

Where $g(x) = b_0 + b_1 x + ... + b_m x^m$, m> 0 and

$h(x) = c_0 + c_1 x + \ldots + c_r x^r$, $r > 0$.

Then n = deg f = deg g + deg h = m + r, and

$a_k = b_0 c_k + b_1 c_{k-1} + \ldots + b_k c_0 \; \forall \; k = 0, 1 \ldots, n.$

Now $a_0 = b_0 c_0$. We know that $p \mid a_0$. Thus, $p \mid b_0 c_0 \therefore p \; b_0$ or $p \mid c_0$. Since $p^2 \nmid a_0$, p cannot divide both b_0 and c_0. Let us suppose that $p \mid b_0$ and $p \nmid c_0$.

Now let us look at $a_n = b_m c_r$. Since $p \nmid a_n$, we see that $p \nmid b_m$ and $p \nmid c_r$. Thus, we see that for some I, $p \nmid b_i$. Let k be the least integer such that $p \nmid b_k$. Note that $0 < k \leq m < n$.

Therefore, $p \mid a_k$.

Now, $a_k = (b_0 c_k + \ldots + b_{k-1} c_1) + b_k c_0$.

Since $p \mid a_k$ and $p \mid b_0, \ldots, p \mid b_{k-1}$, we see that $p \mid a_k - (b_0 c_k + \ldots + b_{k-1} c_1)$, i.e., $p \mid b_k c_0$. But $p \nmid c_0$. So we reach a contradiction.

Thus, f(x) must be irreducible in **Z**[x].

Let us illustrate the use of this criterion.

Example 1

Is $2x^7 + 3x^5 - 6x^4 + 3x^3 + 12$ irreducible in **Q**[x]?

Solution

By looking at the coefficients we see that the prime number 3 satisfies the conditions given in Eisenstein's criterion. Therefore, the given polynomial is irreducible in Q[x]

Example 2

Let p be a prime number. Is $Q[x]/\langle x^3 - p \rangle$ a field?

Solution

From Unit 14 you know that for any field F, if f(x) is irreducible in F[x], then $\langle f(x) \rangle$ is a maximal ideal of F[x].

Now, by Eisenstein's criterion, $x^3 - p$ is irreducible since p satisfies the conditions given in Theorem 3. Therefore, $\langle x^3 - p \rangle$ is a maximal Ideal of **Q**[x].

From Unit 12 you also know that if R is a ring, and M is a maximal ideal of **R**. then **R/M** is a field.

Thus, $\mathbf{Q}[x] / \langle x^3 - p \rangle$ is a field.

In this example we have brought out an important fact. We ask you to prove it in the following exercise.

E 3) For any $n \in N$ and prime number p, show that $x^n - p$ is irreducible over **Q**[x].note that this shows us that we can obtain irreducible polynomials of any degree over **Q**[x].

Now let us look at another example of an irreducible polynomial. While solving this we will show you how Theorem 3 can be used indirectly.

Example 3

Let p be a prime number. Show that

$f(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$ is irreducible in **Z**[x]. f(x) is called the **pth cyclotomic polynomial.**

Solution

To start with we would like you to note that f(x) = g(x) h(x) in **Z**[x] iff f(x+1) = g(x+1) h(x+1) in **Z**[x]. Thus, f(x) is irreducible in **Z**[x] iff f(x+1) is irreducible in **Z**[x].

Now, $f(x) = \dfrac{x^p - 1}{x - 1}$

$\therefore$ f(x+1) = $\frac{x+1^p-1}{x}$

= $\frac{1}{x}(x^p + {}^pC_1\, x^{p-1} + ... + {}^pC_{p-1}\, x + 1 - 1)$, (by the binomial theorem)

= $x^{p-1} + px^{p-2} + {}^pC_2x^{p-3} + \ldots + {}^pC_{p-2}\, x + p$.

Now apply Eisenstein's criterion taking p as the prime. We find that f(x+1) is irreducible. Therefore, f(x) is irreducible.

You can try these exercises now.

E 4) If $a_0 + a_1x + \ldots + a_n x^n \in \mathbf{Z}[x]$ is irreducible in $\mathbf{Q}[x]$, can you always find a prime p that satisfies the conditions (i), (ii) and (iii) of Theorem 3?

E 5) Which of the following elements of $\mathbf{Z}[x]$ are irreducible over $\mathbf{Q}$?

a) x^2-12 ..

b) $8x^3 + 6x^2 - 9x + 24$.

c) $5x + 1$

E 6) Let p be a prime integer. Let a be a non-zero non-unit square-free integer, i.e., $b^2 \neq a$ for any $b \in \mathbf{Z}$. Show that $\mathbf{Z}[x]/\langle x^p + a \rangle$ is an integral domain.

E 7) Show that $x^P + \bar{a} \in \mathbf{Z}$plx] is not irreducible for any it" E Zp' (**Hint:** Does E 13 of Unit 13 help?)

So far we have used the fact that if f(x) E Z[x] IS irreducible over. Z. then it is also irreducible over **Q**, Do you think we can have a similar relationship between irreducibility in $\mathbf{Q}[x]$ and R[x]? To answer this consider $f(x) = x^2 - 2$. This is irreducible in $\mathbf{Q}[x]$, but $f(x) = (x - \sqrt{2})\ (x + \sqrt{2})$) in $\mathbf{R}[x]$. Thus, we cannot extend irreducibility over **Q** to irreducibility over **R**.

But we can generalise the fact that irreducibility in $\mathbf{Z}[x]$ implies irreducibility in Q[x]. This is not only true for **Z** and **Q**; it is true for any UFD R and its field of quotients F (see Sec. 12.5). Let us state this relationship explicitly.

Theorem 4

Let R be a UFD with field of quotients F.

i) If $f(x) \in \mathbf{R}[x]$ is an irreducible primitive polynomial, then it is also irreducible in F[x].

ii) (**Eisenstein's Criterion**) Let $f(x) = a_0 + a_1x + \ldots + a_n x^n \in R[x]$ and $p \in R$ be a prime element such that $p \nmid a_n$, $p^2 \nmid a_0$ and $p \mid a_i$ for $0 \leq i < n$. Then f(x) is irreducible in F[x].

The proof of this result is on the same lines as that of Theorems 2 and 3. We will not be doing it here. But if you are interested, you should try and prove the result yourself.

Now, we have already pointed out that if F is a field and f(x) is irreducible over F, then $F[x]/\langle f(x)\rangle$ is a field. How is this field related to F? That is part of what we will discuss in the next section.

3.2 Field Extensions

In this section we shall discuss subfields and field extensions. To start with let us define these terms. By now the definition may be quite obvious to you.

Definition

A non-empty subset S of a field F is caned a **subfield** of F if it is a field with respect to the operations on F. If $S \neq F$, then S is called a **proper subfield** of F.

A field K is called a **field extension** of F if F is a subfield of K. Thus, **Q** is a subfield of **R** and **R** is a field extension of **Q**. Similarly, **C** is a field extension of **Q** as well as of **R**.

Note that a non-empty subset S of a field F is a subfield of F iff

i) S is a subgroup of (F,+), and .
ii) The 'set of all non-zero elements of S forms a subgroup of the group of non-zero elements of F under multiplication.

Thus, by Theorem 1 of Unit 3, we have the following theorem.

Theorem 5

A non-empty subset S of a field F is a subfield of F if and only if

i) $a \in S, b \in S \Rightarrow a-b \in S$, and

ii) $a \in S, b \in S, b \neq 0\ ab^{-1} \in S$.

Why don't you use Theorem 5 to do the following exercise now.

E 8) Show that

a) **Q** + i**Q** is a subfield of **C**
b) **Z** + $\sqrt{2}$ **Z** is not a subfield or **R**.

Now, let us look at a particular field extension of a field F. Since F[x] is an integral domain, we can obtain its field of quotients (see Module 3 Unit 2). We denote this field by F(x). Then F is a subfield of F(x). Thus, F(x) is a field extension of F. Its elements are expressions of the form $\frac{f(x)}{g(x)}$, where f(x), g(x) ∈ F[x} and g(x) ≠ o.

There is another way of obtaining a field extension of a field F from F[x]. We can look at quotient rings of F[x] by its maximal ideals. You know that an ideal is maximal in F[x] iff it is generated by an irreducible polynomial over F. So, F[x]/<f(x), 1s a field iff f(x) is irreducible over F.

Now, given any f(x) ∈ F[x], such that deg f(x) > 0, we will show that there is a field monomorphism from F into F[x]/<f(x). This will show that F[x)/<f(x» contains an isomorphic copy of F; and hence, we can say that it contains F.

So, let us define ϕ: F→ F[x]/<f(x)>: ϕ(a) = a + <f(x».

Then, ϕ (a+b) = ϕ (a) + ϕ (b), and

ϕ (ab) = ϕ (a) ϕ (b)

Thus, ϕ is a ring homomorphism.

What is Ker ϕ ?).

Ker ϕ = {a $\in$ F | a + <f(x)> = <f(x)>}

= {a $\in$ F | a + $\in$ <f(x)>}

= {a $\in$ F | f(x) | a}

= {0}, since deg f > 0 and deg a $\leq$ 0.

Thus, ϕ is 1-1, and hence an inclusion.

Hence, F is embedded in F[x]/<f(x)>
Thus, if f(x) is irreducible in F[x], then F[x]/<f(x)> is a field extension of F.

Now for a related exercise!

E 9) Which of the following rings are field extension of **Q**?

a) **Q**[x]/<x^3 + 10>,
b) **R**[x]/<x^2 + 2>,
c) **Q**,
d) **Q**[x]/<x^2-5x + 6>.

Well, we have looked at field extensions of any field F. Now let us look at certain fields, one of which F will be an extension of.

3.2.1 Prime Fields

Let us consider any field F. Can we say anything about what its subfields look like? Yes, we can say something about one of its subfields. Let us prove this very startling and useful fact. Before goi1lg into the proof we suggest that you do a quick revision of Theorems 3. 4 al1d 8 of Unit 12. Well, here's the result.

Theorem 6

Every field contains a subfield isomorphic to Q or to Z_p, for some prime number p.

Proof

Let F be a field. Define a function

f : **Z** $\rightarrow$ F : f(n) = n.1 = 1 + 1 + … + 1 (n times).

In E 11) of Module 3 Unit 2 you have shown that f is a ring homomorphism and Ker f = p**Z**, where p is the characteristic of F.

New, from Theorem 8 of Unit 12 you know that char F = 0 or char F = p, a prime. So let us look at these two cases separately.

Case 1

(Char F – 0): In this case f is one-one, ∴ **Z** = f(**Z**). Thus, f(**Z**) is an integral domain contained in the field F. Since F is a field, it will also contain the field of quotients of f(**Z**). This will be isomorphic to the field of quotients of **Z**, i.e., **Q**. Thus, F has a subfield which is isomorphic to **Q**.

Case 2

(Char F = p, for some prime p) :

Since,p1s a prime number, **Z**/p**Z** is a field.

Also, by applying the Fundamental Theorem of Homomorphism to f, we get **Z**/p**Z** $\underset{\sim}{}$ f(Z).

Thus, f(Z) is isomorphic to **Z**p and is contained in F. Hence, F has subfield isomorphic to **Z**p.

Let us reword Theorem 6 slightly. What it says is that :

Let F be a field.

i) If char F = 0, then F has a subfield isomorphic to Q.
ii) If char F = p, then F has a subfield isomorphic to Z_p.

Because of this property of **Q** and $\mathbf{Z}_p$ (where p is a prime number) we call these fields **prime fields.**

Thus, the prime fields are **Q**, $\mathbf{Z}_2$, $\mathbf{Z}_3$, $\mathbf{Z}_5$ etc.

We call the subfield isomorphic to a prime field (obtained in Theorem 6), the **prime subfield** of the given field.

Now, suppose a field F is an extension of a field K. Are the prime subfields of K and F isomorphic or not? To' answer this let us look at char K and char F. We want to know if char K = char F or not. Since F ~s a field extension of K, the unity of F and K is the same, namely, 1. Therefore, the least positive integer "such that n.l = 0 is the same for F

as well as K. Thus, char K = char-F. Therefore, the prime subfields of K and F are isomorphic.

So, now can you do the following exercises?

E 10) Show that the smallest subfield of any field is its prime subfield.

E 11) Let F be a field which has no proper subfields. Show that F is isomorphic to a prime field.

E 12) Obtain the prime subfields of **R**, **Z**s and the field given in E 15 of Unit 12.

E 13) Show that given any field, if we know its characteristic then we can obtain its prime subfield and vice versa.

A very important fact brought out by E 10 and E 11 is that: **a field is a prime field iff it has no proper subfields.**

Now let us look at certain field extensions of the fields $\mathbf{Z}_p$.

You have dealt a lot with the finite fields $\mathbf{Z}_p$. Now we will look at field extensions of these fields. You know that any finite F has characteristic p, for some prime p. And then F is an extension of $\mathbf{Z}_p$. Suppose F contains q elements. Then q must be a power of p. That is what we will prove now.

Theorem 7

Let F be a finite field having q elements and characteristic p. Then $q = p^n$, for some positive integer n.

The proof of this result uses the concepts of a vector space and its basis. These are discussed in Block 1 of the Linear Algebra course. So, if you want to go through the proof, we suggest that you quickly revise Units 3 and 4 of the Linear Algebra course. If you are not interested in the proof, you may skip it.

Proof of Theorem 7

Since char F = p, F has a prime subfield which is isomorphic to **Z**p. We lose nothing if we assume 1hat the prime subfield is Z_p. We first show that F is a vector space over **Z**p with finite dimension.

Recall that a set V is a vector space over a field K if

i) we can define a binary operation + on V such that (V. +) is an abelian group,

ii) we can define a 'scalar multiplication' : K x V $\rightarrow$ V such that $\forall$ a, b $\in$ K and v,w $\in$ V,

a. (v + w) = a.v +a.w

(a + b). v =a.v + b.v

(ab). V = a. (b. v)

1.v = v.
Now, we know1hat (P, +)'is an abelian group. We also know that the multiplication in F will satisfy till the conditions that the scalar multiplication should satisfy. Thus, F is a vector space over $\mathbf{Z}_p$. Since F is a finite field, it has a finite dimension over $\mathbf{Z}_p$. Let $\dim_{Z_p}$ F = n. Then we can find $a_l,\ldots, a_n \in F$ such that

$F = Z_p a_l + Z_p a_2 + ..+ Z_p a_n$.
We will show that F has p^n elements.

Now, any element of F is of the form

$b_l a_l + b_2 a_2 +...+ b_n a_n$, where $b_l,..., b_n \in \mathbf{Z}_p$,

Now, since $o(\mathbf{Z}_p) = p$, b_1 can be anyone of its p elements.

Similarly, each of b_2, b_3, ... , b_n has p choices. And, corresponding to each of these choices we get a distinct element of F. Thus, the number of elements in F is p x p x…xp(n times) = p^n.

The utility of this result is something similar to that of Lagrange's theorem. Using this result we know that, for instance, no field of order 26 exists. But does a field of order 25 exist? Does Theorem 7 answer this question? It only says that a field of order 25 **can** exist. But it does not say that it **does** exist. The following exciting result, the proof of which is beyond the scope of this course, gives us the required answer. This result was obtained by the American mathematician E.H. Moore in 1893.

Theorem 8

For any prime number p and n$\in$ **N**, there exists Ii field with p^n elements. Moreover, any two finite fields having the same number of elements, are isomorphic

Now, you call utilize your knowledge of finite fields to solve tile following exercises. The first exercise is a generalization of E 13 in Unit 13.

E 14. Let F be a finite field with p^n elements. Show that $a^{p^n} = a \; \forall \in F$. And hence,

show that $x^{p^n} - x = \prod_{a_i \in F} (x-a_i)$.

(**Hint**: Note that (F \ {0},.) is a group of order p^n-l.)

E 15) Let F be a finite field with p^n elements. Define $f : F \to F : f(a) = a^P$. Show that f is anutomorphism of F of order n; i e., f is an isomorphism such that f n = I, and $f^r \neq 1$ for r < n.

E 16) Let F be a field such that a $\in$ F iff a is a root of $x^{27} - x \in$

a) What is char F?
b) Is **Z** $\subset$ F?
c) Is **Q** $\subseteq$ F?
d) Is F $\subseteq$ **Q**? Why?

E 11) Any two infinite fields are isomorphic. True or false? Why? Remember that isomorphic structures must have the same algebraic properties.

We close our discussion on field extensions now. Let us go over the points that we have covered in this unit.

4.0 CONCLUSION

5.0 SUMMARY

We have discussed the following points in this unit.

1) Gauss; lemma, i.e., the 'product of primitive polynomials is primitive.

2) Eisenstein's criterion for polynomials over **Z** and **Q**. This states that if $f(x) = a_0 + a_1 x + ... + a_n x^n \in \mathbf{Z}[x]$ and there is a prime $p \in Z$ such that

i) $p \mid a_i \ \forall\ i = 0,.1, ..., n-1.$

ii) $p \nmid a_n$, and

iii) $p^2 \nmid a_0$,

then f(x) is irreducible over **Z** (and hence over **Q**)

3) For any $n \in N$, we can obtain an irreducible polynomial over **Q** of degree n.

4) Definitions and examples of subfields and field extensions

5) Different ways of obtaining field extensions of a field F from F[x].

6) Every field contains a subfield isomorphic to a prime field.

The prime fields are **Q** or $\mathbf{Z}_p$, for some prime p.

7) The number of elements in a finite field F is p^n, where char F = p and $\dim_{Z_p} F = n$.

8) Given a prime number p and $n \in \mathbf{N}$, there exists a field containing p^n elements. Any two finite fields with the same number of elements are isomorphic.

9) If F is a finite field with p^n elements, then $xp^n - x$ is a product of p^n linear polynomials over F.

Now we have reached the end of this unit as well as this course. We hope that we have been able to give you a basic understanding of the nature of groups, rings and fields. We also hope that you enjoyed going through this course.

ANSWER TO SELFASSESSMENT EXERCISE

1. a) 1, b) 7, c) 5

2. Let $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ and let the content of f(x) be d. Let $a_i = db_i \ \forall\ I = 0, 1, \ldots, n$. Then the g.c.d of $b_0, b_1, \ldots, b_n$ is 1. Thus, $g(x) = b_0 + b_1 x + \ldots + b_n x^n$ is primitive. Also, $f(x) = db_0 + db_1 x + \ldots + db_n x^n = d(b_0 + b_1 x + \ldots + b_n x^n) = d\, g(x)$.

3. $f(x) = x^n - P = a_0 + a_l x + \ldots + a_n x^n$,

where $a_0 = p$, $a_l = 0 = \ldots = a_{n-1}$, $a_n = 1$

Thus, $p \mid a_i \; \forall \; i = 0, 1, \ldots, n - l$, $p^2 \nmid a_0$, $p \nmid a_n$.

So, by the Eisenstein criterion, f(x) is' irreducible over **Q**.

4. Not necessarily

For example, there is no p that satisfies the conditions for f(x) in Example 3.

5. All of them (a) and (b), because of Eisenstein's criterion; and (c), because any linear polynomial is irreducible.

6. Since $a \neq 0, \pm 1, \exists$ a prime q such that $q \mid a$. Also $q^2 \nmid a$, since a is square-free. Then, using q as the prime, we can apply Eisenstein's criterion to find that $x^p + a$ is irreducible in **Z**[x]. Thus, it is a prime element of **Z**[x]. Hence, $\langle x^P + a \rangle$ is a prime ideal of **Z**[x].

   Hence the result,

7. By E 13 of Unit 13 we know that $\bar{a}^P = \bar{a} \; \forall \; \bar{a} \in \mathbf{Z}p$. Now consider

   $X^p + \bar{a} \in \mathbf{Z}_p[x]$

   $\overline{p - a}$ is a zero of this polynomial, since

   $(\overline{p - a})^p + \bar{a} = \overline{p - a} + \bar{a} = \bar{p} = \bar{0} \; Z_p$

Thus, $x_P + \bar{a}$ is reducible over **Z**p.

8a. **Q** + i**Q** is a non-empty subset of **C**.

Now, let a + ib and c + id be in **Q**+i**Q**.

Then (a + ib) -(c + id) = (a – c) + i (b – d) $\in$ **Q** + i**Q**.

Further, let $c + id \neq 0$, so that $c^2 + d^2 \neq 0$.

Then $(c + id)^{-1} = \dfrac{c - id}{c^2 + d^2}$

Thus, $(a + ib)(c + id)^{-1} = (a + ib)\ \frac{(c - id)}{c^2 + d^2}$

$$= \frac{(ac - bd)}{c^2 + d^2} + i\frac{(ac - bd)}{c^2 + d^2} \in \mathbf{Q} + i\,\mathbf{Q}.$$

Thus, $\mathbf{Q} + i\mathbf{Q}$ is a subfield of **C.**

b.) $2 \in \mathbf{Z} + \sqrt{2}\,\mathbf{Z}$ but $2^{-1} \notin \mathbf{Z} + \sqrt{2}\,\mathbf{Z}$. Therefore,
$\mathbf{Z} + \sqrt{2}\,\mathbf{Z}$ is not a field, and hence not a subfield of R.

9. (a), (b) and (c).

10. Let F be a field ~d K be a subfield of F. Then, .we have just seen that both K and F have isomorphic prime subfields.

Thus, K contains the prime subfield of F.

Thus, we have shown that every subfield of F must contain its prime subfields. Hence, this is the smallest subfield of F.

11. F must contain a prime subfield. But it contains no proper subfield be its own prime subfield. That is, F must be isomorphic to a prime field.

12. $\mathbf{Q}$, $\mathbf{Z}_5$, $\mathbf{Z}_2$, since their characteristic's are 0,5 and 2, respectively.

13. F be a field. Firstly, let us assume that char F = p is known. Then, by Theorem 6, we know the prime subfield of F. Conversely, let K be the prime subfield of F. Then we know char K, and as shown before E 10, char F = char K. So we know char F.

14. Since $(F\setminus\{0\},.)$ is a group of order $p^n - 1$, $a^{P^n} - 1 = 1$

$\forall\ a \in F \setminus \{0\}$.

$\therefore\ ap^n = a\ \forall\ a \in F\setminus\{0\}$. Also $0^{P^n} = 0$.

Thus, $a^{P^n} = a\ \forall\ a \in F$.

Now, $x^{P^n} - x \in F[x]$ can have at the most p^n roots in F (by Theorem 7 of Unit 13).

Also, each of the p^n elements of F is a root. Thus, these are all the roots of x^{P^n} - x.

$\therefore\ x^{P^n} - x = \prod_{a_i \in F} (x - a_i)$

15. $f(a + b) = (a + b)P = a^P + b^P$ (using E 10 of Unit 12)

$= f(a) + f(b)$.

$f(ab) = (ah)P = a^P b^P = f(a)\, f(b)$.

f is 1 – 1, by E 10(c) of Unit 12.

Hence, Im f has the same number of elements as the domain of f, i.e., F. Further, Im $1 \subseteq$ F $\therefore$ Im f = F, i.e., f is onto.

Hence, f is an automorphism.

Now, $f^n(a) = [f(a)]^n = (a^p)^n = a^{P^n} = a\ \forall\ a \in F$.

$\therefore\ f^n = I$.

Also, for $r < n$, $f^r(a) = a^{P^r}$

Now, we can't have $a^{P^r} = a\ \forall\ a \in F$, because this would mean that the polynomial $x^{P^n} - x \in F[x]$ has more than pf roots. This would contradict Theorem 7 of Unit 13. Thus, $f^r(a) \neq a$ for some $a \in F$. $\therefore f^r \neq I$ if $r < n$.

Hence, o(f) = n.

E 16) $a \in F$ iff $a^{27} = a$, i.e., $a^{33} = a$

a) Char F = 3.
b) No, since char $Z_2 \neq$ char F.
c) No.
e) No, since $F \subseteq \mathbf{Q} \Rightarrow$ char F = char **Q** = 0.

17. False.

For example, **Q** and **R** are both infinite, but **Q** has no proper subfields, while **R** does. Thus, **Q** and **R** are not isomorphic.

6.0 TUTOR-MARKED ASSIGNMENT

7.0 REFERENCES/FURTHER READING

Ansa B. E. (2010). Modern Algebra Ethereal Bliss Publisher. Calabar.

Kiku, A. O. (1992). Abtract Algebra Ibadan. Ibadan University, Press

Ilori, S. A. & Akinyele, O. (1986). Elementary Abstract and Linear Algebra. Ibadan University, Press.

Osisiogu, U. A. (1998). An Introduction to Real Analysis with Special Topic on Functions of Several Variables and Method of Languages Multipliers, Bestsoft Educational Books Nigeria.