BMTC-134
ALGEBRA

Indira Gandhi National Open University
School of Sciences

Block

4

INTEGRAL DOMAINS

Course Design Committee*

Prof. Rashmi Bhardwaj
G.G.S. Indraprastha University, Delhi

Dr. Sunita Gupta
University of Delhi

Prof. Amber Habib
Shiv Nadar University
Gautam Buddha Nagar

Prof. S. A. Katre
University of Pune

Prof. V. Krishna Kumar
NISER, Bhubaneswar

Dr. Amit Kulshreshtha
IISER, Mohali

Prof. Aparna Mehra
I.I.T., Delhi

Prof. Rahul Roy
Indian Statistical Institute, Delhi

Prof. Meena Sahai
University of Lucknow

Dr. Sachi Srivastava
University of Delhi

Prof. Jugal Verma
I.I.T., Mumbai

Faculty members
School of Sciences, IGNOU

Prof. M. S. Nathawat (Director)

Dr. Deepika

Mr. Pawan Kumar

Prof. Poornima Mital

Prof. Parvin Sinclair

Prof. Sujatha Varma

Dr. S. Venkataraman

* The Committee met in August, 2016. The course design is based on the recommendations of the Programme Expert Committee and the UGC-CBCS template.

Block Preparation Team

Prof. Parvin Sinclair (*Editor and Writer*)
School of Sciences
IGNOU

Course Coordinator: Prof. Parvin Sinclair

Acknowledgement:

i) To **Prof. Parvati Shastri**, Mumbai University, and **Dr. Indrakshi Dutta**, Jesus and Mary College, University of Delhi, for their detailed comments.

ii) To Sh. S. S. Chauhan, for the CRC, of this block.

iii) Some material of the earlier IGNOU undergraduate course, Abstract Algebra (MTE-06), has been used in this block.

BLOCK INTRODUCTION

In this block we will continue our discussion on ring theory. In Unit 14, you will study about two special types of rings, namely, integral domains and fields. Here we will discuss the properties of these special rings in some detail.

Next, in Unit 15, we shall discuss rings whose elements may be familiar to you, namely, polynomials in one indeterminate. We will discuss various properties of polynomials over any commutative ring. Apart from its mathematical interest, the theory of polynomials over a field has several applications. In fact, because of this, linear and quadratic polynomials over $\mathbb{Q}$ were dealt with in considerable depth by the ancient Indian mathematicians Aryabhata I, Sridhar, Bhaskara II and others. Nowadays, this theory is used in coding theory and in mathematical modelling of problems from the social sciences and the physical sciences.

Finally, in Unit 16, the last unit of this course, we shall look at those polynomials over $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ which do not have any non-unit factors. Such polynomials are called irreducible polynomials. In this unit, you will study, and apply, several criteria for a polynomial over these fields to be irreducible.

As in the other blocks, at the end of the block you will find several worked out examples covering the concepts you have studied in this block. There are also several miscellaneous exercises, given after the examples, for you to solve. Please work on these exercises yourself to understand the concepts concerned in a better way.

With this block we come to the end of the course. After you finish studying it, please work on the assignment of the course, which deals with all the blocks of the course.

NOTATIONS AND SYMBOLS (used in Block 4)

Please **review the notations and symbols** given in the previous blocks also.

$\text{char } R$	characteristic of the ring R
$R[x]$	ring of polynomials, in the indeterminate x, over the ring R
$\mathbb{Z}[\sqrt{n}]$	$\mathbb{Z}+\sqrt{n}\mathbb{Z},\ n\in\mathbb{Z}$

UNIT 14

INTEGRAL DOMAINS AND FIELDS

Structure **Page Nos.**

14.1 INTRODUCTION

In Unit 10, we introduced you to rings, and then to special rings, like commutative rings and rings with unity. As you found there, the speciality of these rings lies in the properties of the multiplication defined on them. You also saw that a typical example of such special rings is $\mathbb{Z}$. So, in a sense, these rings are abstractions of $\mathbb{Z}$. Yet, they do not necessarily satisfy an essential property of $\mathbb{Z}$, which is the cancellation property for multiplication. In this unit, you shall study about rings which have this property too. Such rings are called integral domains, and are very important for studying several branches of algebra and its applications.

Throughout this unit, we shall assume the rings to be commutative, unless specified otherwise.

In Sec.14.2, we will begin by discussing what a zero divisor is. This will take you further, to the definition of an integral domain, along with several examples. You will see why many of the rings you have seen so far are examples of integral domains, and why many are not! We will discuss various properties of integral domains also in this section.

In the next section, Sec.14.3, we will focus on a feature that characterises any ring, not necessarily commutative. This is a non-negative integer connected to each ring, called its characteristic. We will focus here on the characteristic of an integral domain, in particular. You will study the reasons for the characteristic of an integral domain being 0 or a prime number.

In Sec.14.4, you will study a common property of rings like $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{Z}_p$ (where p is a prime number). In these rings, the non-zero elements form an abelian group with respect to multiplication. Such a ring is called a field. Fields are very useful algebraic objects, one reason being that every non-zero element of a field is a unit. In this section, you will also study some basic properties of fields.

Next, in Sec.14.5, you will study that given an integral domain, there is a field containing it. You will also see how to construct the smallest field that contains a given integral domain. As you will see, this is essentially the way that $\mathbb{Q}$ is constructed from $\mathbb{Z}$.

Related to integral domains and fields are certain special ideals of rings, called prime ideals and maximal ideals. In Sec.14.6, you will study such ideals and their relationship with integral domains and fields.

As you can see, in this unit you will study several 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 studying it, we hope that you will have attained the following learning objectives.

Objectives

After studying this unit, you should be able to:

- define, and give examples of, a zero divisor in a ring;
- check whether an algebraic system is an integral domain or not;
- obtain the characteristic of a ring, whether commutative or not;
- check whether an algebraic system is a field or not;
- prove, and apply, simple properties of integral domains and fields;
- construct, or identify, the field of quotients of an integral domain;
- define, and identify, prime ideals and maximal ideals of a ring.

14.2 WHAT IS AN INTEGRAL DOMAIN?

Let's begin this discussion with looking at the product of two non-zero integers. You know that this is a non-zero integer, i.e., if $m, n \in \mathbb{Z}$ such that $m \neq 0,\ n \neq 0,$ then $mn \neq 0.$

Now consider the ring $\mathbb{Z}_6$. Here $\overline{2} \neq \overline{0}$ and $\overline{3} \neq \overline{0},$ yet $\overline{2} \cdot \overline{3} = \overline{6} = \overline{0}.$ So, we find that the product of the non-zero elements $\overline{2}$ and $\overline{3}$ is zero in $\mathbb{Z}_6$. This example leads us to the following definition.

Remember that R is commutative.

Definition: A non-zero element r in a ring R is called a **zero divisor** in R if there exists a non-zero element b in R such that $rb = 0.$
(Note that b will be a zero divisor too!)

Now, do you agree that $\overline{2}$ is a zero divisor in $\mathbb{Z}_6$? What about $\overline{3}$ in $\mathbb{Z}_4$? Since $\overline{3} \cdot x \neq \overline{0}$ for every non-zero x in $\mathbb{Z}_4$, $\overline{3}$ is not a zero divisor in $\mathbb{Z}_4$.

The name 'zero divisor' comes from the fact that an element $x \in R$ divides $r \in R$ if $\exists\ y \in R$ s.t. $xy = r.$ The difference, though, is that here $r = 0$ but x

and y are both non-zero. So, in the case of $\overline{2}\cdot\overline{3}=\overline{0}$, $\overline{2}\,\big|\,\overline{0}$ and $\overline{3}\big|\overline{0}$. Thus, both $\overline{2}$ and $\overline{3}$ are zero divisors in $\mathbb{Z}_6$.

Let us consider some more examples of rings with zero divisors.

Example 1: Check whether or not $\mathbb{Z}[\sqrt{3}]\big/ <4>$ has zero divisors.

Solution: Note that $\mathbb{Z}[\sqrt{3}]\big/ <4> =\{a+b\sqrt{3}+<4>\big|\, a,\ b\in\mathbb{Z}\}$, and $<4> =\{4a+4b\sqrt{3}|a,\ b\in\mathbb{Z}\}$.

We need to see if $\exists\ \overline{x},\ \overline{y}\in\mathbb{Z}[\sqrt{3}]\big/<4>$ s.t. $\overline{x}\neq\overline{0},\ \overline{y}\neq\overline{0}$ but $\overline{xy}=\overline{0}$, i.e., if $\exists$ $x,\ y\in\mathbb{Z}[\sqrt{3}]$ s.t. $x,\ y\notin<4>$, but $xy\in<4>$.

Consider $x=2,\ y=2.$ Now $x\notin<4>,\ y\notin<4>$. (Why?)

But $xy=4\in<4>$.

Hence, $\overline{2}$ is a zero divisor in $\mathbb{Z}[\sqrt{3}]\big/<4>$.

You can find several other zero divisors in this ring. In fact, you should try and find at least one more.

***

Example 2: Give an example, with justification, of a zero divisor in $C[0,1]$.

Solution: Consider the function $f\in C[0,1]$, given by

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

Let us define $g:[0,1]\to\mathbb{R}$ by

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

Then, from Calculus, you know that $f,\ g\in C[0,1]$.

Also $f\neq 0,\ g\neq 0$ and $(fg)(x)=f(x)g(x)=0\ \forall\ x\in[0,\ 1]$.

Thus, fg is the zero function.

Hence, f is a zero divisor in $C[0,1]$, and so is g.

***

Example 3: Check whether or not the direct product of two non-trivial rings has zero divisors.

Solution: Let A and B be non-trivial rings. Let $a\in A,\ a\neq 0$, and $b\in B,\ b\neq 0$.

Then $(a,0)\in A\times B$ and $(0,b)\in A\times B$ are both non-zero.

However, $(a,0)(0,b)=(0,0)$.

Hence, $(a,0)$ and $(0,b)$ are zero divisors in $A\times B$.

***

Example 4: Check whether or not $\wp(X)$ has zero divisors, where X is a set with at least two elements.

Solution: Each non-empty proper subset A of X is a zero divisor because $A \cdot A^c = A \cap A^c = \emptyset$, the zero element of $\wp(X)$.

***

Example 5: Let $\bar{x}$ be a zero divisor in $\mathbb{Z}_n$, where $n \in \mathbb{N}$. Show that $(x, n) > 1$.

Solution: Let $\bar{y} \in \mathbb{Z}_n$ s.t. $\bar{y} \neq \bar{0}$ and $\bar{x}\,\bar{y} = \bar{0}$.

So $n \nmid x$, $n \nmid y$, but $n | xy$.

Suppose $(x, n) = 1$. Then $\exists\, m, r \in \mathbb{Z}$ s.t. $mx + nr = 1$.

Then $y = y \cdot 1 = mxy + nry$.

Now $n | xy$ and $n | nry$. Hence, $n | (mxy + nry)$, i.e., $n | y$, a contradiction.

Thus, $(x, n) \neq 1$.

Hence, $(x, n) > 1$.

***

Try solving these exercises now.

E1) List all the zero divisors and all the units in $\mathbb{Z}$, and in $\mathbb{Z}_{10}$. Is there a relationship between the zero divisors and the units of each ring? If so, what is it? (This is linked with E5.)

E2) Prove the converse of what is given in Example 5.

E3) Let R be a ring and $a \in R$ be a zero divisor. Show that every non-zero element of the principal ideal Ra is a zero divisor.

E4) Check whether or not $\wp(X)$ has zero divisors, where $X = \{a\}$.

E5) Let R be a ring with unity and $a \in R$, $a \neq 0$.

i) If a is not a zero divisor, does $a \in U(R)$?

ii) If $a \in U(R)$, can a be a zero divisor in R?

Justify your answers.

So far you have seen several examples of rings with zero divisors. You also know that $\mathbb{Z}$ has no zero divisors. Actually, there are many rings without zero divisors. Let us define such rings.

Definition: A non-trivial ring R is called an **integral domain** if

i) R is commutative,

ii) R is with identity, and

ii) R has no zero divisors.

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

This kind of ring gets its name from the set of integers, one of its best known examples. In fact, integral domains were originally thought of as a generalisation of $\mathbb{Z}$.

Can you think of other integral domains? What about $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$? You should check that they satisfy the conditions in the definition.

Now, from the examples you have studied so far, can you think of rings that are not integral domains? What about $C[0,1]$? In Example 2, you have seen that it has zero divisors. Thus, $C[0,1]$ is not an integral domain.

Before we go further, here is a short remark about terminology.

Remark 1: Several authors often shorten the term 'integral domain' to 'domain'. We will do so too.

Let us now look at $\mathbb{Z}_n$. In E1 you have proved that $\mathbb{Z}_{10}$ is not a domain. Earlier, you have noted that $\mathbb{Z}_6$ and $\mathbb{Z}_4$ are not domains. So, is $\mathbb{Z}_n$ not a domain for any $n \in \mathbb{N}$? Take $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$. Since $\overline{1} \cdot \overline{1} = \overline{1} \neq \overline{0}$, $\mathbb{Z}_2$ is a domain.
What about $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$? You should check that it is a domain.
So, what is it about $\mathbb{Z}_2$ and $\mathbb{Z}_3$ that makes them domains, while $\mathbb{Z}_6$ and $\mathbb{Z}_4$ are not? You may have concluded what we shall now prove.

Theorem 1: $\mathbb{Z}_p$ is an integral domain iff p is a prime number.

Proof: You know that $\mathbb{Z}_n$ is a non-trivial commutative ring with identity $\forall\ n \geq 2$. So, we need to prove that $\mathbb{Z}_p$ has no zero divisors iff p is a prime.

A ring R is **without zero divisors** if for $a, b \in R$, $ab = 0 \Rightarrow a = 0$ or $b = 0$.

First, let us assume that p is a prime number.
Suppose $\overline{a}, \overline{b} \in \mathbb{Z}_p$ satisfy $\overline{a}\,\overline{b} = \overline{0}$.
Then $\overline{ab} = \overline{0}$, i.e., $p \mid ab$.
Since p is a prime number, from Unit 1 you know that $p \mid a$ or $p \mid b$.
Thus, $\overline{a} = \overline{0}$ or $\overline{b} = \overline{0}$.
Thus, we have proved that if $\overline{a} \neq \overline{0}$ and $\overline{b} \neq \overline{0}$, then $\overline{a}\,\overline{b} \neq \overline{0}$ in $\mathbb{Z}_p$.
From Block 1 of the course, Real Analysis, you know that this is equivalent to having proved that $\overline{a}\overline{b} = \overline{0} \Rightarrow \overline{a} = \overline{0}$ or $\overline{b} = \overline{0}$.
Thus, $\mathbb{Z}_p$ is without zero divisors, and hence, is a domain.

Conversely, we are given that $\mathbb{Z}_p$ has no zero divisors.
If $p = 1$, then $\mathbb{Z}_p$ is the trivial ring, which is not a domain.
If $p \neq 1$, let $m \mid p$ for some $m \in \mathbb{N}$. So $p = mr$, for some $r \in \mathbb{N}$.
Then $1 \leq m \leq p$, $1 \leq r \leq p$, and $\overline{m}\,\overline{r} = \overline{mr} = \overline{p} = \overline{0}$ in $\mathbb{Z}_p$.
Since $\mathbb{Z}_p$ is without zero divisors, $\overline{m} = \overline{0}$ or $\overline{r} = \overline{0}$. Thus, $p \mid m$ or $p \mid r$.
This is only possible if $m = p$ or $r = p$.
If $m = p$, $r = 1$. If $r = p$, $m = 1$. Thus, the only factors of p are 1 and p.
Hence, p is a prime. ■

By applying Theorem 1, you can immediately conclude something you have proved earlier, namely, that $\mathbb{Z}_{10}$, $\mathbb{Z}_6$ and $\mathbb{Z}_4$ have zero divisors!

Let us look at another example of a domain now.

Example 6: Show that $R = {}^{(D_1 \times D_2)}\!\big/_{D_1 \times \{0\}}$ is an integral domain, where D_1 and D_2 are domains.

Solution: From Unit 13, you know that ${}^{(D_1 \times D_2)}\!\big/_{D_1 \times \{0\}} \simeq D_2,$ a domain.

Since isomorphic rings have exactly the same algebraic properties, and R is isomorphic to a domain, R must be a domain. Hence the result.

***

An interesting point is brought out by the example above. From Example 4, you know that $D_1 \times D_2$ is not a domain. But a quotient ring of $D_1 \times D_2$ becomes a domain!

Try solving some exercises now.

E6) Which of the following rings are **not** integral domains? Why?
$\mathbb{Z}_{97}, 2\mathbb{Z}, \mathbb{Z}+i\mathbb{Z}, \mathbb{R}\times\mathbb{R}, \{0\}, (\mathbb{Z}\times\mathbb{Z})/(\mathbb{Z}\times\{0\}).$

E7) Must the subring of an integral domain be a domain? Must the quotient ring of a domain be a domain? Give reasons for your answers.

E8) Check whether or not $\mathbb{Q}[\sqrt{n}]$ is an integral domain, where n is a square-free integer.

Now consider a ring $R.$ We know that the cancellation law for addition holds in $R,$ i.e., whenever $a+b=a+c$ in $R,$ then $b=c.$ But, does $ab=ac$ imply $b=c?$ It need not. For example, $0\cdot 1 = 0\cdot 2$ in $\mathbb{Z},$ but $1 \neq 2.$ So, if $a=0,$ $ab=ac$ does 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 $ab=ac$ or $ba=ca,$ then $b=c.$)

Proof: Let us first assume that R has no zero divisors. Assume that $a,b,c\in R$ such that $a\neq 0$ and $ab=ac.$ Then

$a(b-c) = ab-ac,$ by Theorem 1, Unit 10.
$\quad = 0.$

As $a\neq 0$ and R has no zero divisors, we get $b-c=0,$ i.e., $b=c.$
Thus, if $ab=ac$ and $a\neq 0,$ then $b=c.$
Similarly, if $ba=ca$ and $a\neq 0,$ then $b=c.$ (Note that here R is not assumed to be commutative.)

Conversely, assume that the cancellation law for multiplication holds in $R.$
Let $a\in R$ 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, there is no non-zero b s.t. $ab=0.$

Hence, a is not a zero divisor, i.e., R has no zero divisors. ■

Using this theorem, we can immediately conclude that **the cancellation law for multiplication holds in an integral domain**.

Note that Theorem 2 is not true for domains alone. It is also true for any non-domain that is without zero divisors, like $2\mathbb{Z}$.

Let us look at a couple of examples of the use of Theorem 2.

Example 7: Does the cancellation law for multiplication hold for $\mathbb{Z}[i]$?

Solution: Since $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$, it is without zero divisors. Thus, by Theorem 2, the cancellation law holds for $\mathbb{Z}[i]$.

***

Example 8: Let R be a non-trivial finite ring with no zero divisors. Show that R must have identity.

Solution: Let $a \neq 0 \in R$. Then a^i is a non-zero element of $R\ \forall\ i \in \mathbb{N}$.
But R has only finitely many elements.
So $a^r = a^s$ for some $r, s \in \mathbb{N}, r \neq s$.
Let n be the least positive integer s.t. $\exists\ m \in \mathbb{N}$ with $a^m = a^n$, $m \neq n$.
Then $m > n$.
So, for all $x \in R$,
$x \cdot a^m = x \cdot a^n$
$\Rightarrow xa^{m-1} = xa^{n-1}$, applying Theorem 2 and cancelling a.
$\Rightarrow xa^{m-n} = x$, applying the same process $(n-1)$ more times.
Similarly, you can show that $a^{m-n}x = x\ \forall\ x \in R$.
Thus, a^{m-n} is the identity of R.

***

Now, you should use Theorem 2 to solve the following exercises.

E9) Check whether or not the cancellation law for multiplication holds in $\mathbb{Z}[\sqrt{7}]$ and in $5\mathbb{Z}$.

E10) In a domain, show that the only solutions of the equation $x^2 = x$ are $x = 0$ and $x = 1$.

An element r of a ring R is called an **idempotent** if $r^2 = r$.

E11) Prove that 0 is the only nilpotent element (see Example 9 of Unit 12) in a domain.

E12) Let R be a non-trivial finite ring with identity and let $a \in R$, $a \neq 0$. Show that a is either a zero divisor or a is a unit of R.

Now let us introduce a non-negative integer associated with any ring. This will lead us to a particular feature of an integral domain.

14.3 CHARACTERISTIC OF A RING

In this section, we will focus on a non-negative integer that characterises rings. If the ring R is finite, this integer actually turns out to be a divisor of the order of the underlying abelian group $(R, +)$. The purpose of introducing this feature of a ring is that it gives an important property of integral domains, as you will see.

Note that in this section, **we will NOT restrict the discussion only to commutative rings**.

Let us begin with a look at $\mathbb{Z}_4$. Is there an $n \in \mathbb{N}$ s.t. $n \cdot \overline{2} = \overline{0}$ in $\mathbb{Z}_4$? Yes, for example, $2 \in \mathbb{N}$ s.t. $2 \cdot \overline{2} = \overline{0}$. Is there an $n \in \mathbb{N}$ such that $n \cdot \overline{3} = \overline{0}$ in $\mathbb{Z}_4$? What about 4? $4 \cdot \overline{3} = \overline{12} = \overline{0}$ in $\mathbb{Z}_4$, so this works.
Is there an $n \in \mathbb{N}$ s.t. $n \cdot x = \overline{0}\ \forall\ x \in \mathbb{Z}_4$? What about 4?
You know that $4x = \overline{0}\ \forall\ x \in \mathbb{Z}_4$, since $\overline{4} = \overline{0}$. In fact, $8x = \overline{0}$ and $12x = \overline{0}$ also, for any $x \in \mathbb{Z}_4$. But 4 is the least positive integer with this property, that is, 4 is the least element of the set $\{n \in \mathbb{N} \mid nx = \overline{0}\ \forall\ x \in \mathbb{Z}_4\}$. This tells us that 4 is the characteristic of $\mathbb{Z}_4$, 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 the **characteristic of R is defined to be zero**.
The characteristic of R is denoted by $\mathbf{char\ R}$.

So, as you have seen above, $\text{char}\ \mathbb{Z}_4 = 4$. In fact, you should check that $\text{char}\ \mathbb{Z}_n = n$, and $\text{char}\ \mathbb{Z} = 0$.

Let us consider another example.

Example 9: Find $\text{char}\ (m\mathbb{Z})$, where $m \in \mathbb{Z}, m \geq 2$.

Solution: Any element of $m\mathbb{Z}$ is of the form $mn, n \in \mathbb{Z}$. Now, if $r \in \mathbb{Z}$ such that $rmn = 0\ \forall\ n \in \mathbb{Z}$, then $rm = 0$, taking $n = 1$.
Since $m \neq 0$, we conclude $r = 0$.
Hence, $\text{char}\ (m\mathbb{Z}) = 0$.

***

Solving the following exercises will give you a better understanding of the characteristic of a ring.

Remember that in this section the rings need not be commutative.

E13) Give an example, with justification, of a ring R with $\text{char}\ R = 0$, $R \neq m\mathbb{Z}, m \in \mathbb{N}$.

E14) Find $\text{char}\ \wp(X)$, where X is a non-empty set.

E15) Let R be a ring and let $\text{char}\ R = m$. What is $\text{char}\ (R \times R)$?

E16) If R is a finite ring, why must $\text{char}\ R$ be non-zero?

E17) i) Let R be a finite ring, with n elements. Show that $\text{char } R$ divides n.

ii) In particular, what are n and r, for $R = \mathbb{M}_2(\mathbb{Z}_4)$?

iii) Give an example, with justification, of R in (i) above, with $r = n$.

Now let us look at a nice result about the characteristic of a ring with identity. It helps in considerably reducing our labour when we want to obtain the characteristic of such a ring.

Theorem 3: Let m be a positive integer and R be a ring with identity. Then the following conditions are equivalent.

i) $m \cdot 1 = 0.$

ii) $ma = 0$ for all $a \in R.$

Proof: We will prove $(i) \Rightarrow (ii)$ and $(ii) \Rightarrow (i).$

$\mathbf{(i) \Rightarrow (ii):}$ We know that $m \cdot 1 = 0.$
Thus, for any $a \in R,\ ma = m(1 \cdot a) = (m \cdot 1)a = 0 \cdot a = 0,$ i.e., (ii) holds.

$\mathbf{(ii) \Rightarrow (i):}$ If $ma = 0\ \forall\ a \in R,$ then it is certainly true for $a = 1,$ i.e., $m \cdot 1 = 0.$ ■

What Theorem 3 tells us is that **to find the characteristic of a ring $\mathbf{R}$ with identity, we only need to look at the set $\{\mathbf{n} \cdot \mathbf{1} \mid \mathbf{n} \in \mathbb{N}\},$** instead of $nx\ \forall\ x \in R,\ n \in \mathbb{N}.$

Let us look at some examples.

i) $\text{char } \mathbb{Q} = 0,$ since $n \cdot 1 \neq 0$ for any $n \in \mathbb{N}.$

ii) Similarly, $\text{char } \mathbb{R} = 0$ and $\text{char } \mathbb{C} = 0.$

iii) You have already seen that $\text{char } \mathbb{Z}_n = n,$ for $n \geq 2.$ Here $n \cdot \overline{1} = \overline{0},$ and n is the least such natural number.

You have seen several examples of rings and their characteristics. From these examples you may have concluded that the characteristic of an infinite ring is zero. However, consider the following example.

Example 10: Find the characteristic of $\mathbb{Z}_3[x],$ the ring of polynomials in x with coefficients from $\mathbb{Z}_3.$

Solution: Any element of $\mathbb{Z}_3[x]$ is a polynomial in x with coefficients $\overline{0}, \overline{1}$ or $\overline{2}$ in $\mathbb{Z}_3.$ This ring has an identity, namely, $\overline{1}.$
Since 3 is the smallest positive integer such that $n \cdot \overline{1} = \overline{0},\ \text{char } \mathbb{Z}_3[x] = 3,$ by Theorem 3.

***

Note that $\mathbb{Z}_3[x]$ is an infinite ring, since for each $n \in \mathbb{N},$ there is a polynomial of degree $n,$ and all these polynomials are distinct. Thus, $\mathbb{Z}_3[x]$ is an example of an infinite ring with non-zero characteristic.

Why don't you solve some exercises now?

E18) Find $\text{char } \mathbb{M}_n(\mathbb{C}), n \in \mathbb{N},$ and $\text{char } \mathbb{M}_n(\mathbb{Z}_m), n, m \in \mathbb{N}.$

E19) If R is a ring and I an ideal of $R,$ must $\text{char } R = \text{char } (R/I)$? Why, or why not?

E20) If R is a ring and S is a proper subring of $R,$ is $\text{char } S < \text{char } R$ in all cases? Why, or why not?

E21) Is there any ring with characteristic 1? Why, or why not?

E22) Let R and S be isomorphic rings. Find $\text{char } R - \text{char } S.$

Now let us look at what Theorem 1 says. It says $\mathbb{Z}_n$ is a domain iff n is a prime. So, if we connect this with $\text{char } \mathbb{Z}_n,$ we find that $\mathbb{Z}_n$ is a domain iff $\text{char } \mathbb{Z}_n$ is a prime. So, the question arises if there is any domain whose characteristic is not a prime. Isn't $\mathbb{Q}$ one such domain, since $\text{char } \mathbb{Q} = 0,$ not a prime? Can $\text{char } R, R$ a domain, take any other values? The following theorem answers this question.

Theorem 4: The characteristic of an integral domain is either zero or a prime.

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 $m \in \mathbb{N}.$ Then m is the least positive integer such that $m \cdot 1 = 0,$ by Theorem 3.
We will show that m is a prime number, using the method of contradiction, i.e., we will assume m is not prime, and then reach a contradiction. This will show that our assumption was wrong.

So, suppose m is not prime. So $m = st,$ where $s, t \in \mathbb{N}, 1 < s < m$ and $1 < t < m.$
Then $m \cdot 1 = 0 \Rightarrow (st) \cdot 1 = 0 \Rightarrow (s \cdot 1)(t \cdot 1) = 0 \Rightarrow s \cdot 1 = 0$ or $t \cdot 1 = 0,$ since R is without zero divisors.
But, s and t are less than $m.$ So, by Theorem 3, we reach a contradiction to the fact that $m = \text{char } R.$ Therefore, our assumption that m is not prime must be wrong. Thus, m is a prime number. ■

Now, what about the converse of Theorem 4? That is, if R is a ring with characteristic 0 or with prime characteristic, must R be a domain? You can use your understanding of 'characteristic' to answer this, and to solve the other exercises that are given below.

E23) Check whether or not the converse of Theorem 4 is true.
(**Hint:** Does E15 help?)

E24) Let R be an integral domain of characteristic p, p a prime. Prove that

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

ii) $(a+b)^{p^n} = a^{p^n} + b^{p^n}$ for $n \in \mathbb{N}$ and $a, b \in R$.

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

iv) the map $\phi : R \to R : \phi(a) = a^p$ is a monomorphism.

v) if R is a finite integral domain, then ϕ [in (iv) above] is an isomorphism.

E25) Which of the statements in E24 are true if $\text{char } R = 0$? Why?

E26) Show that $(a+b)^6 = a^6 + b^6$ need not be true for a ring R, where $a, b \in R$, and $\text{char } R = 6$.

E27) Let R be a ring with unity 1, and let char $R = m$. Define $f : \mathbb{Z} \to R : f(n) = n \cdot 1$. Show that f is a homomorphism. What is a generator for $\text{Ker } f$?

E28) Find the characteristic of $\mathbb{Z}_3 \times \mathbb{Z}_4$. Use this ring as an example to show why Theorem 4 is only true for integral domains.

By now, you would be familiar with integral domains, and their characteristic. Let us move to a discussion on another algebraic structure. We obtain this structure by imposing certain restrictions on the multiplication of a domain.

14.4 FIELDS

In this section, you will study some special domains, of which $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are examples. Let us see what is extra special about these integral domains.

To understand what we are leading to, take a ring, $(R, +, \cdot)$. You know that $(R, +)$ is an abelian group. You also know that the operation $\cdot$ is associative in R. But $(R, \cdot)$ need not be an abelian group. For instance, $(\mathbb{Z}, \cdot)$ is not an abelian group since, for example, 2 has no multiplicative inverse in $\mathbb{Z}$. Similarly, $(\mathbb{C}, \cdot)$ is not an abelian group since there is no element $a \in \mathbb{C}$ such that $a \cdot 0 = 1$. But $(\mathbb{C}^*, \cdot)$ is an abelian group, as you know. So are $\mathbb{Q}^*$ and $\mathbb{R}^*$ abelian groups with respect to multiplication. These observations lead us to define a new algebraic object.

Definition: A ring $(R, +, \cdot)$ is called a **field** if $(R \setminus \{0\}, \cdot)$ is an abelian group.

Thus, for a system $(R, +, \cdot)$ to be a field it must satisfy the ring axioms $R1$ to $R6$ (of Unit 10) as well as the following axioms:

R7) multiplication is commutative;

R8) R has a non-zero identity (which we denote by 1); and

R9) every non-zero element x in R has a multiplicative inverse, which we denote by x^{-1}, i.e., $U(R) = R \setminus \{0\}$.

Consider the following related piece of information, before we go further.

Remark 2: A ring that satisfies $R8$ and $R9$, but not $R7$, is called a **division ring**, or a **skew field**, or a **non-commutative field.** Such rings are also very important in the study of algebra. (One example is $\mathbb{H}$, the ring of real quaternions that you studied in Unit 10.) However, we will not be discussing division rings in this course.

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

As you have seen, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields. However, $(\mathbb{Z}^*, \cdot)$ is not a group. So, $\mathbb{Z}$ is not a field.

Consider another example of a field, in some detail.

Example 11: Show that $\mathbb{Q}[\sqrt{2}] = \{a + \sqrt{2}b \mid a, b \in \mathbb{Q}\}$ is a field.

Solution: From Unit 10, you know that $F = \mathbb{Q}[\sqrt{2}]$ is a commutative ring with identity, $1 + \sqrt{2} \cdot 0$.

Now, let $a + \sqrt{2}b$ be a non-zero element of F. Using the rationalisation process, we see that

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

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

(Note that $a^2 - 2b^2 \neq 0$, since $\sqrt{2}$ is not rational and at least one of a and b is non-zero.)

Thus, every non-zero element of F has a multiplicative inverse.

Therefore, $F = \mathbb{Q} + \sqrt{2}\mathbb{Q}$ is a field.

***

By now you have noted 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 $F \neq \{0\}$, F is a commutative ring 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 $a \neq 0$. As $a \neq 0$ and F is a field, a^{-1} exists.

Then, as you proved in E5(ii), a is not a zero divisor.

So, F has no zero divisors.

Thus, F is an integral domain. ■

We can use Theorem 5 in many ways. For example, by applying Theorem 5 and Theorem 1, you know that $\mathbb{Z}_{10}$ is not a field, as 10 is not a prime.

Now, is the converse of Theorem 5 true? That is, is every domain a field? Note that $\mathbb{Z}$ is a domain, but not a field.

Now you should solve these related exercises.

E29) Which of the following rings are not fields, and why?
$6\mathbb{Z}, \mathbb{Z}_5, \mathbb{Z}_6, \mathbb{Z}[\sqrt{2}], \mathbb{Q}\times\mathbb{Q}, \wp(\{a\}).$

E30) Is a subring of a field also a field? Why?

E31) Check whether or not $\mathbb{Z}[i]$ and $\mathbb{Q}[i]$ are fields.

E32) Is $\mathbb{Z}[x]/<x^2>$ an integral domain? Is it a field? Give reasons for your answers.

You have noted that not every domain is a field. However, if we restrict ourselves to finite domains, we find that they are fields, as you will now see.

Theorem 6: Every finite integral domain is a field.

Proof: Let $R = \{a_0 = 0,\ a_1 = 1, a_2, \ldots, a_n\}$ be a domain. Then, by definition, R is commutative. To show that R is a field, we must show that $U(R) = R \setminus \{0\}$.

So, let $a = a_i$ be a non-zero element of R (i.e., $i \neq 0$). Consider the elements $aa_1, \cdots, aa_n$. For every $j \neq 0, a_j \neq 0,$ and since $a \neq 0,$ we get $aa_j \neq 0.$
Hence, the set $\{aa_1, ..., aa_n\} \subseteq \{a_1, ..., a_n\}.$

Also, $aa_1, aa_2, \ldots, aa_n$ are all distinct elements of the set $\{a_1, ..., a_n\},$ since $aa_j = aa_k \Rightarrow a_j = a_k,$ by Theorem 2.
Thus, $\{aa_1, ..., aa_n\} = \{a_1, ..., a_n\}.$
In particular, $1 = a_1 = aa_j$ for some $j = 1, \ldots, n.$
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 will now prove a theorem which generates several examples of fields.

Theorem 7: $\mathbb{Z}_n$ is a field if and only if n is a prime number.

Proof: From Theorem 1, you know that $\mathbb{Z}_n$ is a domain if and only if n is a prime number. You also know that $\mathbb{Z}_n$ has only n elements. Now we can apply Theorem 6 to obtain the result. ■

Theorem 7 unleashes infinitely many examples of fields: $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5, \mathbb{Z}_7,$ and so on. They are all examples of what we now define.

Definition: A field whose underlying set is finite is called a **finite field**.

Thus, $\mathbb{Z}_p$ is a finite field for every prime p. Finite fields have many important applications in various areas of science and technology, like cryptography. You can study them in detail at a later stage.

Looking at all the examples of fields, can you say anything about the characteristic of a field? In fact, using Theorems 4 and 5 we can.

Theorem 8: The characteristic of a field is either zero or a prime number.

Proof: Applying Theorems 4 and 5, we get this result. ■

From Theorem 7 and Theorem 8, we see that for each prime p we have a field of characteristic p, namely, $\mathbb{Z}_p$.

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 ask you to check an example of a finite field with 4 elements.

E33) Let $R = \{0, 1, a, 1+a\}$. Define $+$ and $\cdot$ in R as given in the following Cayley tables.

$+$	0	1	a	$1+a$
0	0	1	a	$1+a$
1	1	0	$1+a$	a
a	a	$1+a$	0	1
$1+a$	$1+a$	a	1	0

$\cdot$	0	1	a	$1+a$
0	0	0	0	0
1	0	1	a	$1+a$
a	0	a	$1+a$	1
$1+a$	0	$1+a$	1	a

Show that R is a field. Also find the characteristic of this field.

What E33 tells you is that there are finite fields that have n elements, where n is not a prime. However, as you will see in your higher studies, $n = p^r$ for some prime p and some $r \in \mathbb{N}$. For example, in E33, $n = 2^2$.

Let us now look at the ideals of a field. Consider the examples of fields you have studied so far. In Unit 12, you have seen that $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ have only $\{0\}$ as a proper ideal. Is this true for other fields? The answer is given by the following theorem.

Theorem 9: Let R be a commutative ring with identity. Then R is a field if and only if R and $\{0\}$ 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 2 of Unit 12, $I = R$.
So, the only ideals of R are $\{0\}$ and R.

Conversely, assume that R and $\{0\}$ are the only ideals of R.

Let $a \in R$, $a \neq 0$. Consider the principal ideal $Ra = \{ra \mid r \in R\}$.
This is a non-zero ideal of R, since $a \in Ra$.
Therefore, $Ra = R$.
Now, $1 \in R = Ra$.
Therefore, $1 = ba$ for some $b \in R$, i.e., a^{-1} exists.
Since a was an arbitrary non-zero element of R, we have proved that every such element has a multiplicative inverse.
Therefore, R is a field. ■

From Theorem 9 and Example 11, you know that $\mathbb{Q}[\sqrt{2}]$ has no non-trivial proper ideal. In fact, $\mathbb{Q}[\sqrt{p}]$ has no non-trivial proper ideal, where p is a prime. Similarly, you also now know that $\mathbb{C}$, $\mathbb{R}$ and $\mathbb{Z}_p$ have no proper non-trivial ideals. Thus, Theorem 9 is very useful. You will find that you will be applying it again and again in the rest of this block.

Using Theorem 9, we can obtain some interesting properties of **field homomorphisms**. We ask you to prove them in the following set of exercises.

A **field homomorphism** is a ring homomorphism from one field to another.

E34) Let F and K be fields, and let $f: F \to K$ be a field homomorphism. Show that either f is the zero map or f is 1-1.

E35) Check whether or not

i) a homomorphism from a ring to a field must be 1-1,

ii) a field homomorphism must be the zero map or surjective.

E36) Let R be a ring isomorphic to a field F. Show that R must be a field.

Now that we have discussed integral domains and fields, let us look at a natural way of embedding a domain in a field.

14.5 FIELD OF QUOTIENTS

Let us consider the relationship between $\mathbb{Z}$ and $\mathbb{Q}$. You know that every element of $\mathbb{Q}$ is of the form $\frac{a}{b}$, where $a \in \mathbb{Z}$ and $b \in \mathbb{Z}^*$. Actually, we can also denote $\frac{a}{b}$ by the ordered pair $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$. Let us use this to define a relation in $\mathbb{Z} \times \mathbb{Z}^*$ which mimics the way elements of $\mathbb{Q}$ behave.

Recall that, for any ring R, R^* denotes $R \setminus \{0\}$.

In $\mathbb{Q}$, you know $\frac{a}{b} = \frac{c}{d}$ iff $ad = bc$. Let us put a similar relation, ~, on the elements of $\mathbb{Z} \times \mathbb{Z}^*$, i.e., $(a,b) \sim (c,d)$ iff $ad = bc$.
Then, you should check that ~ is an equivalence relation.

Next, you know that the operations in $\mathbb{Q}$ are given by

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \text{ and } \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \ \forall \ \frac{a}{b}, \frac{c}{d} \in \mathbb{Q}.$$

Keeping these operations in mind, we define binary operations on the equivalence classes in $\mathbb{Z}\times\mathbb{Z}^*$ as follows:

Recall, from Unit 1, that the set of all equivalence classes of $\mathbb{Z}\times\mathbb{Z}^*$ w.r.t. ~ is denoted by $(\mathbb{Z}\times\mathbb{Z}^*)/\sim$.

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

$[(a,b)]\cdot[(c,d)]=[(ac,bd)]\ \forall\ [(a,b)], [(c,d)]\in(\mathbb{Z}\times\mathbb{Z}^*)/\sim$.

It turns out that a ring is formed by the set of these equivalence classes, w.r.t. these operations, and it is a field isomorphic to $\mathbb{Q}$.
Further, there is an inclusion from $\mathbb{Z}$ to this field, so that we can treat $\mathbb{Z}$ as a subring of this field.

Let us generalise this procedure to obtain a field encompassing any given integral domain.

A ring R is **embedded** in a ring S if there is a ring monomorphism from R to S.

Theorem 10: Let R be an integral domain. Then R can be embedded in a field F, where every element of F has the form ab^{-1} for $a,\ b\in R, b\neq 0$.

Proof: Consider the set of ordered pairs, $K=\{(a,b)\mid a,b\in R$ and $b\neq 0\}$.
Let us define a relation ~ in K by '$(a,b)\sim(c,d)$ if $ad=bc$.'

~ is reflexive: $(a,b)\sim(a,b)\ \forall\ (a,b)\in K,$ since R is commutative.
So, ~ is reflexive.

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

~ is transitive: Let $(a,b), (c,d), (u,v)\in K$ such that $(a,b)\sim(c,d)$ and $(c,d)\sim(u,v)$.
Then $ad=bc$ and $cv=du.$
Therefore, $(ad)v=(bc)v=b(cv)=bdu,$ i.e., $avd=bud.$
Since $d\neq 0,$ by the cancellation law for multiplication, we get $av=bu,$ i.e., $(a,b)\sim(u,v).$
Thus, ~ is transitive.

Hence, ~ is an equivalence relation.

Let us denote the equivalence class that contains (a,b) by $[a,b]$.
Thus, $[a,b]=\{(c,d)\mid c,d\in R,\ d\neq 0$ and $ad=bc\}$.
For example, $(2,6)\in[1,3]$ and $(1,2)\notin[1,3]$ in $\mathbb{Z}\times\mathbb{Z}^*,$ since $2\cdot 3=6\cdot 1$ and $1\cdot 3\neq 2\cdot 1.$

Also, note that **for any domain $\mathbf{R}$, $[\mathbf{0},\mathbf{1}]=\{\mathbf{0}\}\times(\mathbf{R}\setminus\{\mathbf{0}\})$.**

Let F be the set of all equivalence classes of K with respect to ~, i.e., $\mathbf{F}=\mathbf{K}/\sim$.
As we did for $(\mathbb{Z}\times\mathbb{Z}^*)/\sim$, let us define $+$ and $\cdot$ in F as follows:
$[a,b]+[c,d]=[ad+bc,bd],$ and
$[a,b]\cdot[c,d]=[ac,bd].$
Do you agree that $+$ and $\cdot$ are binary operations on F? Note that if $b\neq 0$ and

$d \neq 0$ in the integral domain $R,$ then $bd \neq 0.$ So, the right-hand sides of the equations defining the operations are equivalence classes in $F.$ Thus, the sum and the product of two elements in F is again an element in $F.$ But, we still need to make sure that these operations are well-defined.

So, let $[a,b]=[a',b']$ and $[c,d]=[c',d'].$ We have to show that $[a,b]+[c,d]=[a',b']+[c',d']$ and $[a,b]\cdot[c,d]=[a',b']\cdot[c',d'],$

i.e., $[ad+bc,bd]=[a'd'+b'c',b'd']$ and $[ac,bd]=[a'c',b'd'].$

Now, $(ad+bc)\,b'd'-(a'd'+b'c')\,bd$

$$\begin{aligned}&= ab'dd'+cd'bb'-a'bdd'-c'dbb'\\&=(ab'-a'b)\,dd'+(cd'-c'd)\,bb'\\&=(0)\,dd'+(0)\,bb', \text{ since } (a,b)\sim(a',b') \text{ and } (c,d)\sim(c',d').\\&=0.\end{aligned}$$

Hence, $[ad+bc,bd]=[a'\,d'+b'c',b'd'],$ i.e., $+$ is well-defined.

Now, let us check if multiplication is well-defined. Consider

$$\begin{aligned}(ac)\,(b'd')-(bd)\,(a'c') &= ab'cd'-ba'dc'\\&=ba'cd'-ba'cd', \text{ since } ab'=ba' \text{ and } cd'=dc'.\\&=0.\end{aligned}$$

Therefore, $[ac,bd]=[a'c',b'd'].$ Hence, $\cdot$ is well-defined.

Let us now prove that F is a field.

i) $+$ **is associative:** For $[a,b], [c,d], [u,v]\in F,$

$$\begin{aligned}([a,b]+[c,d])+[u,v] &= [ad+bc,bd]+[u,v]\\&=[(ad+bc)v+ubd,bdv]\\&=[adv+b(cv+ud),bdv]\\&=[a,b]+[cv+ud,dv]\\&=[a,b]+([c,d]+[u,v]).\end{aligned}$$

ii) $+$ **is commutative:** For $[a,b],\ [c,d]\in F,$

$$[a,b]+[c,d]=[ad+bc,bd]=[cb+da,db]=[c,d]+[a,b].$$

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

$$[0,1]+[a,b]=[0\cdot b+1\cdot a,1\cdot b]=[a,b].$$

iv) **The additive inverse of $[a,b]\in F$ is $[-a,b]$:**

$$[a,b]+[-a,b]=[ab-ab,b^2]=[0,b^2]=[0,1], \text{ since } (0,1)\sim(0,b^2).$$

We would like you to prove the rest of the requirements for F to be a field (see E37), after which the proof will continue.

E37) Show that $\cdot$ in F is associative, commutative, distributive over $+,$ and $[1,\,1]$ is the multiplicative identity for $F.$
Further, show that $F^* = \{[a,b]\in F \mid a,b\neq 0\},$ and that $U(F)=F^*.$

So, we have put our heads together and **proved that F is a field**.

Now, let us define $f: R \to F: f(a) = [a,1]$. We want to show that f is a monomorphism.

f is well-defined: If $a = b$ in $R, [a,1] = [b,1]$ in F, i.e., $f(a) = f(b)$ in F.

f is a homomorphism: For $a, b \in R$,
$f(a+b) = [a+b,1] = [a,1] + [b,1] = f(a) + f(b)$, and
$f(ab) = [ab,1] = [a,1] \cdot [b,1] = f(a) \cdot f(b)$.

f is 1-1: Let $a, b \in R$ such that $f(a) = f(b)$. Then
$[a,1] = [b,1] \Rightarrow (a,1) \sim (b,1) \Rightarrow a = b$.

Thus, f is a monomorphism.

So, by the Fundamental Theorem of Homomorphism, $\text{Im } f = f(R)$ 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 $a, b \in R, b \neq 0$.
So, F is the required field in which R is embedded. ■

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

Thus, $\mathbb{Q}$ is the field of quotients of $\mathbb{Z}$.

Consider the following remark in this context.

Remark 3: Remember that the elements of the field of quotients of a domain R are actually a product of equivalence classes. When we say that any element of this field F, is of the form ab^{-1}, we actually mean $[a,1][b,1]^{-1}$, for $a, b \in R, b \neq 0$. We are 'loosely' equating R with its isomorphic copy $f(R)$ in F.

Before considering more examples of a field of quotients, we shall prove a basic property of this field. This property will make it easier for you to obtain the quotient field of a domain.

Theorem 11: The field of quotients of an integral domain R is the smallest field containing R.

Proof: To prove this, we shall equate $[a,1]$ (of Theorem 10) with a $\forall\, a \in R$.
Let F be the field of quotients of R.
Then, $R \subseteq F$, as discussed in Theorem 10.
Let K be any other field containing R.
Any element of F is of the form ab^{-1}, where $a, b \in R$ and $b \neq 0$.
Since $a, b \in R$, $a, b \in K$.
Since $b \in K^*$ and K is a field, $b^{-1} \in K$.
Thus, $a, b^{-1} \in K$. Hence, $ab^{-1} \in K$.

Thus, $F \subseteq K$.

Hence, F is the smallest field containing R. ■

Let us now use Theorem 11 to find the field of quotients of a large class of domains.

Example 12: Find the field of fractions of a field F.

Solution: Since F is a field, it is the smallest field containing itself. Thus, F is its own field of fractions.

***

By Example 12, you know that $\mathbb{Z}_p$ is the field of fractions of itself, where p is a prime. Similarly, $\mathbb{Q}$ and $\mathbb{C}$ are their own field of fractions.

Try doing some exercises now.

E38) Is $\mathbb{R}$ the field of quotients of $\mathbb{Z}+\sqrt{2}\mathbb{Z}$? Or, is it $\mathbb{C}$? Or, is it $\mathbb{Q}+\sqrt{2}\mathbb{Q}$? Give reasons for your answers.

E39) At what stage of the construction of the field F in Theorem 10 was it crucial to assume that R is a domain? Why?

E40) Let R be a commutative ring with unity, but not an integral domain. Can R be embedded in a field? Why, or why not?

In this section, you have seen how an integral domain can be naturally embedded in a field. Now let us look at quotient rings that are integral domains or fields, and their corresponding fields of fractions.

14.6 PRIME AND MAXIMAL IDEALS

Let us, again, begin with considering $\mathbb{Z}_p$. You know that $\mathbb{Z}/_{n\mathbb{Z}} \simeq \mathbb{Z}_n$ for $n \in \mathbb{N}$. You also know that $\mathbb{Z}_n$ is an integral domain iff n is a prime. Thus, $\mathbb{Z}/_{n\mathbb{Z}}$ is a domain iff n is a prime. What is this property of a prime p that allows $\mathbb{Z}/_{p\mathbb{Z}}$ to be a domain?

You know that if p is a prime number and p divides the product of two integers a and b, then either p divides a or p divides b. In other words, if $ab \in p\mathbb{Z}$, then either $a \in p\mathbb{Z}$ or $b \in p\mathbb{Z}$. It is this property that makes $p\mathbb{Z}$ a special ideal of $\mathbb{Z}$. More generally, consider the following definition.

Definition: A proper ideal P of a ring R (commutative or not) is called a **prime ideal** of R if whenever $ab \in P$ for $a, b \in R$, then either $a \in P$ or $b \in P$. Thus, $2\mathbb{Z}, 3\mathbb{Z}, 11\mathbb{Z}$ are all prime ideals of $\mathbb{Z}$.

As another example, $\{0\}$ is a prime ideal of $\mathbb{R}$ because it is a proper ideal of $\mathbb{R}$, and

$ab \in \{0\} \Rightarrow ab = 0 \Rightarrow a = 0$ or $b = 0 \Rightarrow a \in \{0\}$ or $b \in \{0\}$, where $a, b \in \mathbb{R}$.

Let us look at other examples of prime ideals.

Example 13: Let R be an integral domain. Show that $I = \{(0,x) \mid x \in R\}$ is a prime ideal of $R \times R$.

Solution: Note that $I = \{0\} \times R.$ In Unit 12, you have seen that I is an ideal of $R \times R.$
Further, it is a proper ideal, since $\{0\} \neq R.$

Now, let us check if I is a prime ideal or not. For this, let $(a_1, b_1), (a_2, b_2) \in R \times R$ such that $(a_1, b_1)(a_2, b_2) \in I.$
Then $(a_1a_2, b_1b_2) = (0, x)$ for some $x \in R.$
$\therefore a_1a_2 = 0,$ i.e., $a_1 = 0$ or $a_2 = 0,$ since R is a domain.
Therefore, $(a_1, b_1) \in I$ or $(a_2, b_2) \in I.$
Thus, I is a prime ideal of $R \times R.$

***

Example 14: Check whether or not the ideal $\wp(Y)$ is a prime ideal of $\wp(X),$ where X is a non-empty set and Y is a proper non-empty subset of $X.$

Solution: Let $A, B \in \wp(X)$ s.t. $AB \in \wp(Y),$ i.e., $A \cap B \subseteq Y.$ Then it is not necessary that $A \subseteq Y$ or $B \subseteq Y,$ i.e., it is not necessary that $A \in \wp(Y)$ or $B \in \wp(Y).$
For instance, let $X = \{1, 2, 3\},$ $Y = \{1\},$ $A = \{1, 2\},$ $B = \{1, 3\}.$ Then $A \cap B \subseteq Y,$ but neither A nor B are subsets of $Y.$
Thus, $\wp(Y)$ is not a prime ideal of $\wp(X).$

***

Try solving the following exercises now. Doing so will help you get used to prime ideals.

E41) Check whether or not the set $I = \{f \in C[0, 1] \mid f(0) = 0\}$ is a prime ideal of $C[0, 1].$

E42) Show that a commutative non-trivial ring R with identity is an integral domain if and only if $\{0\}$ is a prime ideal of $R.$

E43) Find all the prime ideals of $\mathbb{C}.$

E44) Check whether or not $< 6 >$ is a prime ideal of $\mathbb{Z}[\sqrt{5}].$

Now, as you have seen, $\mathbb{Z}/n\mathbb{Z}$ is a domain iff $n\mathbb{Z}$ is a prime ideal of $\mathbb{Z}.$ Is this situation true for prime ideals of $\mathbb{Z}$ only? In fact, the same relationship holds between any integral domain and its prime ideals, as we will now prove.

Theorem 12: An ideal P of a commutative 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 is commutative and has identity, from Unit 12 you know that R/P is commutative and has identity.

Also, since P is a proper ideal of R, $(\mathrm{R}/\mathrm{P}) \neq \{\bar{0}\}$.
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. ■

Let us consider some examples to understand how useful Theorem 12 is.

Example 15: Find all the prime ideals of $\mathbb{Z}_{45}$.

Solution: You know that $\mathbb{Z}_{45} = \mathbb{Z}/45\mathbb{Z}$. So, by Theorem 8 of Unit 12, you know that the ideals of $\mathbb{Z}_{45}$ correspond to the ideals of $\mathbb{Z}$ containing $45\mathbb{Z}$.
Thus, the ideals of $\mathbb{Z}_{45}$ are $<\bar{n}>$, where $n \mid 45$. So $n = 1, 3, 5, 9, 15, 45$.
Hence, $<\bar{n}>$ is $\mathbb{Z}_{45}, <\bar{3}>, <\bar{5}>, <\bar{9}>, <\overline{15}>, <\bar{0}>$, respectively.
Since a prime ideal is a proper ideal, $\mathbb{Z}_{45}$ is not a prime ideal.
Since $\bar{3}\cdot\bar{3} \in <\bar{9}>$, but $\bar{3} \notin <\bar{9}>, <\bar{9}>$ is not a prime ideal.
Similarly, you should show why $<\overline{15}>$ is not a prime ideal.
Since 45 is not a prime, $\mathbb{Z}_{45}$ is not a domain. Hence, $<\bar{0}>$ is not a prime ideal.
Now, $\mathbb{Z}_{45}/<\bar{3}> \simeq \mathbb{Z}_3$, by the isomorphism theorems; and $\mathbb{Z}_3$ is a field. Hence, $\mathbb{Z}_{45}/<\bar{3}>$ is a field. So by Theorem 12, $<\bar{3}>$ is a prime ideal of $\mathbb{Z}_{45}$.
Similarly, show that $<\bar{5}>$ is a prime ideal of $\mathbb{Z}_{45}$.
Note that $<3>$ and $<5>$ are the only prime ideals of $\mathbb{Z}$ containing $45\mathbb{Z}$.
Thus, the prime ideals of $\mathbb{Z}_{45}$ correspond to the prime ideals of $\mathbb{Z}$ containing $45\mathbb{Z}$, i.e., $p\mathbb{Z}$, where $p \mid 45$, p a prime.
That is, the only prime ideals of $\mathbb{Z}_{45}$ are
$<\bar{5}> = \{\bar{0}, \bar{5}, \overline{10}, \overline{15}, \overline{20}, \overline{25}, \overline{30}, \overline{35}, \overline{40}\}$, and
$<\bar{3}> = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}, \overline{12}, \overline{15}, \overline{18}, \overline{21}, \overline{24}, \overline{27}, \overline{30}, \overline{33}, \overline{36}, \overline{39}, \overline{42}\}$.

In E48 you will see that the prime ideals of $\mathbb{Z}_n$ correspond to the prime ideals of $\mathbb{Z}$ that contain $n\mathbb{Z}$.

***

Example 16: Show that $<x+5>$ is a prime ideal of $\mathbb{R}[x]$. Also find the quotient field of $\mathbb{R}[x]/<x+5>$.

Solution: First, let us use the Fundamental Theorem of Homomorphism to prove that $\mathbb{R}[x]/<x+5> \simeq \mathbb{R}$.

Define the evaluation function $\phi : \mathbb{R}[x] \to \mathbb{R} : \phi(f(x)) = f(-5)$.

You know, from E2 of Unit 13, that ϕ is a well-defined ring epimorphism. Also

$\text{Ker } \phi = \{f(x) \in \mathbb{R}[x] \mid (-5)$ is a root of $f(x)\}$

$= \{f(x) \in \mathbb{R}[x] \mid (x+5)$ divides $f(x)\}$, as you know from Block 1 of Calculus.

$= < x+5 >$.

Hence, by the Fundamental Theorem of Homomorphism, $\mathbb{R}[x] \big/ < x+5 > \simeq \mathbb{R}$.

Since $\mathbb{R}$ is a field, it is a domain.

Hence, $\mathbb{R}[x] \big/ < x+5 >$ is a domain.

Thus, $< x+5 >$ is a prime ideal of $\mathbb{R}[x]$, applying Theorem 12.

Further, as $\mathbb{R}[x] \big/ < x+5 > \simeq \mathbb{R}$, a field, $\mathbb{R}[x] \big/ < x+5 >$ is a field. Hence, it is its own quotient field.

***

Along the lines of Example 16, you should prove that $< x+r >$ is a prime ideal of $\mathbb{R}[x] \; \forall \; r \in \mathbb{R}$.

Now, let us consider another example of the use of the isomorphism theorems, and Theorem 12, for checking the primeness of an ideal.

Example 17: Check whether or not $< \overline{7} >$ is a prime ideal of $\mathbb{Z}_{49}$.

If it is, find the field of fractions of $\mathbb{Z}_{49} / < \overline{7} >$.

If it is not, give a ring in which $\mathbb{Z}_{49} / < \overline{7} >$ is embedded.

Solution: We will apply the third isomorphism theorem, which you have proved in Unit 13. Here, note that $49\mathbb{Z}$ is an ideal of $7\mathbb{Z}$, which is an ideal of $\mathbb{Z}$. Now,

$$\mathbb{Z} \big/ 7\mathbb{Z} \simeq (\mathbb{Z}/49\mathbb{Z}) \big/ (7\mathbb{Z}/49\mathbb{Z}) \simeq \mathbb{Z}_{49} \big/ < \overline{7} >.$$

Since you have seen that $\mathbb{Z} \big/ 7\mathbb{Z}$ is a domain, so is $\mathbb{Z}_{49} \big/ < \overline{7} >$.

Hence, $< \overline{7} >$ is a prime ideal of $\mathbb{Z}_{49}$.

Note that the required field of fractions is $\mathbb{Z}_7$. (Why?)

***

Try solving some related exercises now.

E45) Check whether or not $< x+20 >$ is a prime ideal of $\mathbb{Z}[x]$.

E46) Let R be a commutative ring with unity such that R/I is a domain for some ideal I of R. Will R be a domain? Why?

E47) Find all the prime ideals of $\mathbb{Z}_{30}$.

Now, in $\mathbb{Z}$ you have seen that a prime ideal is generated by a prime number. Can this be generalised to other domains?
For this, let us first talk about divisibility and prime elements in a domain. Recall, from E29, Unit 10, that we generalised the definition of $'a$ divides b' in $\mathbb{Z}$ to any commutative ring, R. You studied that an element a **divides** an element b in R (denoted by $\mathbf{a}|\mathbf{b}$) if $b = ra$ for some $r \in R$.

In this case, we also say that a is a **factor** of b, or that a is a **divisor** of b.

Thus, $\bar{3}$ divides $\bar{6}$ in $\mathbb{Z}_7$, since $\bar{3} \cdot \bar{2} = \bar{6}$.

Similarly, for $X = \{1, 2, 3\}$, $A = \{1, 2\}$, $B = \{1\}$, $A|B$ in $\wp(X)$ because $\exists\ C = \{1, 3\} \subseteq X$ s.t. $A \cap C = B$.

Note that if R is a ring with unity, then $a|a\ \forall a \in R$. (Why?)

Given this definition of 'divisor' generalised to any commutative ring, let us generalise the concept of a prime integer. We will see what a prime element is in any domain.

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

i) p is not a unit, and

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

Thus, the prime elements of $\mathbb{Z}$ are precisely the prime numbers and their negatives. You also know that a prime element in $\mathbb{Z}$ generates a prime ideal. Is this true for other domains? The following theorem answers this question.

Theorem 13: Let R be an integral domain. Then p is a prime element of R if and only if Rp is a prime ideal of R.

Proof: Let us first assume that p is a prime element of R.
Since p does not have a multiplicative inverse, $1 \notin Rp$.
Thus, Rp is a proper ideal of R.

$x \in R$ has a multiplicative inverse iff $Rx = R$.

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

Conversely, assume that Rp is a prime ideal of R. Then $Rp \neq R$, by definition. 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 $p|b$.
Thus, p is a prime element in R. ■

Theorem 13 is very useful for checking whether an element is a prime element or not, or for finding out when a principal ideal is a prime ideal. For example, Theorem 13 and E42 tell us that **$\mathbf{0}$ is a prime element of $\mathbf{R}$ iff $\mathbf{R}$ is a domain**.

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

Remember that all rings here are assumed to be commutative.

E48) Let $f : R \to S$ be a ring epimorphism with kernel N. Show that

i) if J is a prime ideal in S, then $f^{-1}(J)$ is a prime ideal in R.

ii) if I is a prime ideal of R containing N, then $f(I)$ is a prime ideal of S.

iii) the map ϕ between the set of prime ideals of R that contain N and the set of prime ideals of S, given by $\phi(I) = f(I)$, is a bijection.

E49) Give an example of a ring homomorphism f from R to S such that P is a prime ideal of R, but $f(P)$ is not a prime ideal of S.

E50) Let P_1 and P_2 be distinct prime ideals of a ring R.

i) Must $P_1 \cap P_2$ be a prime ideal of R?

ii) Will $P_1 + P_2$ be a prime ideal of R in all cases?

iii) Will P_1P_2 be a prime ideal of R in all cases?

Give reasons for your answers.

E51) Find two distinct prime ideals of $\mathbb{Z} \times \mathbb{Z}$.

Let us now define a particular kind of prime ideal. This will actually connect a ring to a field as its quotient ring.

Let us begin, again, with $\mathbb{Z}$ as an example. Consider the ideal $2\mathbb{Z}$ of $\mathbb{Z}$. Suppose the ideal $n\mathbb{Z}$ in $\mathbb{Z}$ is such that $2\mathbb{Z} \subseteq n\mathbb{Z} \subseteq \mathbb{Z}$. Then $n|2$. Therefore, $n = \pm 1$ or $n = \pm 2$, so that $n\mathbb{Z} = \mathbb{Z}$ or $n\mathbb{Z} = 2\mathbb{Z}$.
What this tells us is that no ideal of $\mathbb{Z}$ can lie between $2\mathbb{Z}$ and $\mathbb{Z}$. That is, $2\mathbb{Z}$ is maximal among the proper ideals of $\mathbb{Z}$ that contain it. This leads us to the following definition.

Definition: A proper ideal M of a ring R (commutative or not) 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 $I = R$.

Thus, a proper ideal M is a maximal ideal if there is no proper ideal of R which contains it.

An example that may come to your 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. You have also seen earlier that $\{0\}$ is a prime ideal of F.

In the case of fields, you have just seen that a maximal ideal is a prime ideal. Is this true for rings in general? Is there a connection between a prime ideal and a maximal ideal of a ring? To answer this, consider the following characterisation of maximal ideals.

Theorem 14: Let R be a commutative 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. You already know that R/M is a commutative ring with identity. So, it is enough to prove that R/M has no non-trivial proper ideals (see Theorem 9).

So, let I be an ideal of R/M. Consider the canonical homomorphism $\eta : R \to R/M : \eta(r) = r + M.$

Then, from Unit 13, you know that $\eta^{-1}(I)$ is an ideal of R containing $M,$ the kernel of η.

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

Therefore, $I = \eta(\eta^{-1}(I))$ is either $\eta(M)$ or $\eta(R)$.

That is, $I = \{\bar{0}\}$ or $I = R/M.$

Thus, R/M 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, $\eta(I) = \{\bar{0}\}$ or $\eta(I) = R/M.$

$\therefore I = \eta^{-1}(\eta(I))$ is M or $R.$

Therefore, M is a maximal ideal of $R.$ ■

There is an immediate consequence of Theorem 14 (and a few other theorems too).

Corollary 1: Every maximal ideal of a commutative ring with identity is a prime ideal. ■

We ask you to prove the corollary as an exercise (see E52).

Notice that Corollary 1 is a one-way statement. What about its converse? That is, is every prime ideal maximal? What about the zero ideal in $\mathbb{Z}$? Since $\{0\} \subsetneq 2\mathbb{Z} \subsetneq \mathbb{Z}, \{0\}$ is not a maximal ideal. However, since $\mathbb{Z}$ is an integral domain, $\{0\}$ is a prime ideal of $\mathbb{Z}.$

Now let us use the powerful characteristion in Theorem 14 to get some examples of maximal ideals.

Example 18: Show that an ideal $m\mathbb{Z}$ of $\mathbb{Z}$ is maximal iff m is a prime number.

Solution: From Theorem 7, you know that $\mathbb{Z}_m$ is a field iff m is a prime number. You also know that $\mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}_m.$

Thus, by E36, $\mathbb{Z}/m\mathbb{Z}$ is a field iff m is prime.

Hence, by Theorem 14, $m\mathbb{Z}$ is maximal in $\mathbb{Z}$ iff m is a prime number.

***

Example 19: Show that $\overline{2}\mathbb{Z}_{12}$ is a maximal ideal of $\mathbb{Z}_{12}$, whereas $\overline{4}\mathbb{Z}_{12}$ is not.

Solution: You know that $\mathbb{Z}_{12} \simeq \mathbb{Z}/12\mathbb{Z}$ and $\overline{2}\mathbb{Z}_{12} \simeq 2\mathbb{Z}/12\mathbb{Z}$. Thus, by the third isomorphism theorem in Unit 13, we see that $\mathbb{Z}_{12}/\overline{2}\mathbb{Z}_{12} \simeq (\mathbb{Z}/12\mathbb{Z})/(2\mathbb{Z}/12\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}_2$, which is a field. Therefore, $\overline{2}\mathbb{Z}_{12} = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}\}$ is maximal in $\mathbb{Z}_{12}$.

Now, $\overline{4}\mathbb{Z}_{12} \subsetneq \overline{2}\mathbb{Z}_{12} \subsetneq \mathbb{Z}_{12}$.
Therefore, $\overline{4}\mathbb{Z}_{12} = \{\overline{0}, \overline{4}, \overline{8}\}$ is not maximal in $\mathbb{Z}_{12}$.

***

Try solving the following exercises now.

E52) Prove Corollary 1.

E53) Show that $\{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}\}$ is maximal in $\mathbb{Z}_{10}$.

E54) Check whether or not $< x - \pi >$ is maximal in $\mathbb{C}[x]$.

E55) Show that $\{f \in C[0,1] \,\big|\, f\left(\frac{1}{2}\right) = 0\}$ is maximal in $C[0,1]$.

So, let us see what you have studied in this section. You were first introduced 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 you studied about 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.

We end this discussion on integral domains here. Let us now briefly summarise all the ideas you have studied in this unit.

14.7 SUMMARY

In this unit, we have discussed the following points.

1. The definition, and examples, of a zero divisor in a ring.
2. The definition, and examples, of an integral domain.
3. $\mathbb{Z}_n$ is a field iff n is a prime number.
4. The cancellation law for multiplication holds in an integral domain.
5. The definition, and examples, of the characteristic of a ring.
6. The characteristic of an integral domain is either zero or a prime number.
7. The definition, and examples, of a field.
8. Every field is a domain, but the converse is not true.

9. A finite domain is a field.

10. The characterstic of a field is either zero or a prime number.

11. The construction of the field of quotients of an integral domain.

12. The quotient field of a domain is the smallest field containing the domain.

13. The definition, and examples, of prime and maximal ideals.

14. The proof and use of the result that a proper ideal I of a ring R with identity is prime (respectively, maximal) iff R/I is an integral domain (respectively, a field).

15. Every maximal ideal is a prime ideal, but the converse is not true.

16. An element p of an integral domain R is prime iff the principal ideal pR is a prime ideal of R.

14.8 SOLUTIONS / ANSWERS

E1) $\mathbb{Z}$ has no zero divisors since $\mathrm{m} \neq 0,\ \mathrm{n} \neq 0 \Rightarrow \mathrm{mn} \neq 0\ \forall\ \mathrm{m},\ \mathrm{n} \in \mathbb{Z}.$
In Block 3, you have also seen that $\mathrm{U}(\mathbb{Z}) = \{-1, 1\}.$

Now, let us consider the zero divisors in $\mathbb{Z}_{10}.$
$\overline{\mathrm{m}} \in \mathbb{Z}_{10}$ is a zero divisor
$\Leftrightarrow \exists\ \overline{\mathrm{n}} \in \mathbb{Z}_{10}$ s.t. $\overline{\mathrm{m}} \cdot \overline{\mathrm{n}} = \overline{0},\ \overline{\mathrm{m}} \neq \overline{0},\ \overline{\mathrm{n}} \neq \overline{0}.$
$\Leftrightarrow \overline{\mathrm{m}} = \overline{2}$ or $\overline{\mathrm{m}} = \overline{5}.$
Thus, the zero divisors of $\mathbb{Z}_{10}$ are $\overline{2},\ \overline{5}.$
Also, in Block 3, you have seen that
$\mathrm{U}(\mathbb{Z}_{10}) = \{\overline{\mathrm{m}} \in \mathbb{Z}_{10} \mid (\mathrm{m}, 10) = 1\} = \{\overline{1},\ \overline{3},\ \overline{7},\ \overline{9}\}.$

From these two examples, a possible conclusion we can reach about $\mathrm{A},$ the set of zero divisors, and $\mathrm{B},$ the set of units, in a ring is that $\mathrm{A} \cap \mathrm{B} = \emptyset.$ However, for rings in general, this is only a conjecture. It needs to be proved, or disproved.

E2) The statement you need to prove is: For $\mathrm{n} \in \mathbb{N},$ if $\mathrm{x} \in \mathbb{Z}_{\mathrm{n}}$ s.t. $(\mathrm{x}, \mathrm{n}) > 1,$ then $\overline{\mathrm{x}}$ is a zero divisor in $\mathbb{Z}_{\mathrm{n}}.$

To prove it, suppose $\overline{\mathrm{x}}$ is not a zero divisor in $\mathbb{Z}_{\mathrm{n}}.$
Then show that $\mathbb{Z}_{\mathrm{n}} = \{\overline{\mathrm{m}}\,\overline{\mathrm{x}} \mid \overline{\mathrm{m}} \in \mathbb{Z}_{\mathrm{n}}\} = <\overline{\mathrm{x}}>.$
Thus, $(\mathrm{x}, \mathrm{n}) = 1,$ which is a contradiction to what is given to us, namely, $(\mathrm{x}, \mathrm{n}) > 1.$
Hence, $\overline{\mathrm{x}}$ must be a zero divisor in $\mathbb{Z}_{\mathrm{n}}.$

E3) Let $\mathrm{b} \neq 0$ be in R such that $\mathrm{ab} = 0.$
Then, for any $\mathrm{r} \in \mathrm{R},$
$(\mathrm{ra})\mathrm{b} = \mathrm{r}(\mathrm{ab}) = 0.$
Thus, every non-zero element of Ra is a zero divisor.

E4) $\wp(X) = \{\emptyset, X\}, X \neq \emptyset.$

Since $X \cdot X = X \cap X = X \neq \emptyset, \wp(X)$ has no zero divisors.

E5) i) No. For example, $2 \in \mathbb{Z}$ is not a zero divisor. Also, $2 \notin U(\mathbb{Z}).$

ii) No, let us prove this.
If $a \in U(R), \exists\ b \in R$ s.t. $ab = 1.$
Suppose a were a zero divisor in R. Then $\exists\ c \neq 0$ in R s.t. $ac = 0.$
Thus, $acb = 0,$ i.e., $(ab)c = 0,$ since R is commutative.
$\therefore c = 0,$ a contradiction.
Hence, if $a \in U(R), a$ is not a zero divisor in R.

E6) $\mathbb{Z}_{97}$ is a domain, by Theorem 1, since 97 is a prime.

$2\mathbb{Z}$ is not a domain, since $1 \notin 2\mathbb{Z}.$

$\mathbb{Z} + i\mathbb{Z}$ is a non-trivial commutative ring with identity.
Now, let $a + ib \in \mathbb{Z}[i]$ s.t. $\exists\ c + id \in \mathbb{Z}[i], c + id \neq 0,$ and
$(a + ib)(c + id) = 0.$
Then $ac - bd = 0,$ and …(1)
$ad + bc = 0.$ …(2)
(1) gives $b(c^2 + d^2) = 0$ in $\mathbb{Z},$ using (2).
$\therefore b = 0$ or $c^2 + d^2 = 0.$
$c^2 + d^2 = 0 \Rightarrow c = 0$ and $d = 0,$ which is not possible, since $c + id \neq 0.$
$\therefore b = 0.$
Then (1) gives $ac = 0,$ and (2) gives $ad = 0.$
If $a \neq 0,$ then $ac = 0,$ so that $c = 0;$ and $ad = 0 \Rightarrow d = 0.$
This is not possible, again since $c + id \neq 0.$
So, $a = 0$ also.
Thus, $a + ib = 0.$
Hence, $\mathbb{Z}[i]$ has no zero divisors, and hence, it is a domain.

As in Example 4, $\mathbb{R} \times \mathbb{R}$ is not a domain.

$\{0\}$ is trivial, and hence, is not a domain.

As in Example 6, $(\mathbb{Z} \times \mathbb{Z}) / (\mathbb{Z} \times \{0\}) \simeq \mathbb{Z},$ which is an integral domain.

Hence, $(\mathbb{Z} \times \mathbb{Z}) / (\mathbb{Z} \times \{0\})$ is a domain.

E7) No, for example, you have seen that $2\mathbb{Z}$ is not a domain, though $\mathbb{Z}$ is.
The quotient ring need not be a domain. For example, you know that $\mathbb{Z}$ is a domain, but $\mathbb{Z} / 6\mathbb{Z} = \mathbb{Z}_6$ is not.

E8) From Unit 10, you know that $\mathbb{Q}[\sqrt{n}\,]$ is a commutative ring with identity.
Since $\mathbb{Q}[\sqrt{n}\,]$ is a subring of $\mathbb{C},$ and $\mathbb{C}$ has no zero divisors, $\mathbb{Q}[\sqrt{n}\,]$ has no zero divisors. Hence, it is a domain.

E9) Note that $\mathbb{R}$ is an integral domain. Since $\mathbb{Z}[\sqrt{7}]$ is a subring of $\mathbb{R}$, it is also without zero divisors. Hence, the cancellation law for multiplication holds in $\mathbb{Z}[\sqrt{7}]$.

Since $5\mathbb{Z}$ is a subring of $\mathbb{Z}$, and $\mathbb{Z}$ is without zero divisors, so is $5\mathbb{Z}$. Hence, the cancellation law holds for $5\mathbb{Z}$.

E10) $x^2 = x \Rightarrow x(x-1) = 0$

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

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

E11) Let R be a domain and $x \in R$ be nilpotent.

Then $x^n = 0$ for some $n \in \mathbb{N}$.

If $n = 1$, $x = 0$.

If $n > 1$, then $x \cdot x^{n-1} = 0$.

Since R has no zero divisors, $x = 0$ or $x^{n-1} = 0$. We can apply the same argument again and again, till we reach $x^2 = 0$.

$\therefore x \cdot x = 0$, i.e., $x = 0$.

E12) Let $R = \{x_1, \ldots, x_n\}$.

Suppose a is not a zero divisor.

Now $ax_i \in R \ \forall \ i = 1, \ldots, n$.

Also, since a is not a zero divisor, $ax_i = ax_j$ iff $x_i = x_j$ for $i, \ j = 1, \ldots, n$.

Thus, $R = \{ax_1, \ldots, ax_n\}$.

Since $1 \in R$, $1 = ax_i$ for some $i = 1, \ldots, n$.

Hence, a is a unit in R.

E13) For example, consider $R = \mathbb{Q}$. Let $r = \text{char } \mathbb{Q}$.

Then $r \cdot \frac{m}{n} = 0 \ \forall \ \frac{m}{n} \in \mathbb{Q}$.

In particular, $r \cdot 1 = 0$, since $1 \in \mathbb{Q}$.

This is possible only if $r = 0$.

E14) We will show that $2A = \emptyset \ \forall \ A \subseteq X$, and that 2 is the least such natural number.

Firstly, for any $A \subseteq X$,

$2A = A \,\Delta\, A = (A \setminus A) \cup (A \setminus A) = \emptyset$.

Also, since $X \neq \emptyset$, $1 \cdot X \neq \emptyset$. Thus, $\text{char } \wp(X) \neq 1$.

$\therefore \text{char } \wp(X) = 2$.

E15) Let $\text{char}(R \times R) = n$.

We know that $mr = 0 \ \forall \ r \in R$, and m is the least such non-negative integer.

Now, let (r, s) be any element of $R \times R$.

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

Thus, $n \le m$. …(3)

On the other hand, if $r \in R$, then $(r, 0) \in R \times R$.

$\therefore n(r, 0) = (0, 0)$,

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

i.e., $nr = 0$.

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

$\therefore\ m \le n.$ $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\ldots(4)$

Thus, (3) and (4) show that $m = n$, i.e., $\text{char } R = \text{char } (R \times R)$.

E16) $(R, +)$ is a finite group. If $o(R) = n$, then r is the ℓ.c.m of the orders of $x\ \forall\ x \in R$.

Also, $o(x)$ is a factor of n for each x in R. Thus, $r \ne 0$.

E17) i) $(R, +)$ is a group of order n s.t. $rx = 0\ \forall\ x \in R$, where $r = \text{char } R$.

By E16, $r \ne 0$.

Hence, $o(x) \mid r\ \forall\ x \in R$, and r is the least such positive integer.

Hence, from Unit 4, you know that $r \mid n$.

ii) When $R = \mathbb{M}_2(\mathbb{Z}_4)$, $n = 2^4$. So $r = 2, 2^2, 2^3$ or 2^4. In fact, $r = 4$ since $4\begin{bmatrix} \bar{x}_1 & \bar{x}_2 \\ \bar{x}_3 & \bar{x}_4 \end{bmatrix} = \begin{bmatrix} 4\bar{x}_1 & 4\bar{x}_2 \\ 4\bar{x}_3 & 4\bar{x}_4 \end{bmatrix} = \mathbf{0}$, where $\bar{x}_1, \bar{x}_2, \bar{x}_3, \bar{x}_4 \in \mathbb{Z}_4$;

and $2\begin{bmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{0} \end{bmatrix} = \begin{bmatrix} \bar{2} & \bar{0} \\ \bar{0} & \bar{0} \end{bmatrix} \ne \mathbf{0}$.

iii) For example, $\mathbb{Z}_n, n \in \mathbb{N}$. Here $o(\mathbb{Z}_n, +) = n = \text{char } \mathbb{Z}_n$.

E18) Here the identity is $I = \begin{bmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & & \vdots \\ \vdots & \vdots & & 0 \\ 0 & 0 & \ldots & 1 \end{bmatrix} \in \mathbb{M}_n(\mathbb{C})$.

For any $r \in \mathbb{N}$, $r \cdot I = \begin{bmatrix} r & 0 & \ldots & 0 \\ 0 & r & \ldots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \ldots & r \end{bmatrix} \ne \mathbf{0}$.

Hence, $\text{char } \mathbb{M}_n(\mathbb{C}) = 0$.

The identity in $\mathbb{M}_n(\mathbb{Z}_m)$ is $I = \begin{bmatrix} \bar{1} & \bar{0} & \ldots & \bar{0} \\ \bar{0} & \bar{1} & \ldots & \bar{0} \\ \vdots & \vdots & & \vdots \\ \bar{0} & \bar{0} & \ldots & \bar{1} \end{bmatrix}$.

$\therefore\ mI = \begin{bmatrix} \bar{m} & \bar{0} & \ldots & \bar{0} \\ \bar{0} & \bar{m} & \ldots & \bar{0} \\ \vdots & \vdots & & \vdots \\ \bar{0} & \bar{0} & \ldots & \bar{m} \end{bmatrix} = \mathbf{0}$, and m is the least such positive integer.

$\therefore\ \text{char } \mathbb{M}_n(\mathbb{Z}_m) = m.$

E19) No; e.g., $\text{char } \mathbb{Z} = 0$ and $\text{char}(\mathbb{Z}/2\mathbb{Z}) = \text{char } \mathbb{Z}_2 = 2$.

E20) No; e.g., $\mathbb{Z} \subsetneq \mathbb{Q}$, but char $\mathbb{Z} = $ char $\mathbb{Q} = 0$.

E21) Let R have characteristic 1.
Then, for any $r \in R$, $1 \cdot r = 0$, i.e., $r = 0$.
Hence, only the trivial ring has characteristic 1.

E22) Since $R \simeq S$, they have exactly the same algebraic properties. Hence, char $R = $ char S. Hence, char $R - $ char $S = 0$.

E23) Let D be a domain. Then char D is 0 or a prime. So, by E15, char $(D \times D)$ is 0 or a prime.
But, from Example 4, $D \times D$ is not a domain.
Thus, the converse of Theorem 4 is not true.

E24) i) By the binomial expansion (see E16 of Unit 10),
$(a+b)^p = a^p + {}^pC_1\, a^{p-1}b + \cdots + {}^pC_{p-1}\, ab^{p-1} + b^p$.

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

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

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

You can, similarly, show that $(a-b)^p = a^p - b^p$. Here, note that in a ring of characteristic 2, $(-1) = 1$, since $2 = 0$.

ii) You should prove this by induction, taking $P(m)$ to be the predicate, $'(a+b)^{p^m} = a^{p^m} + b^{p^m}, \; a,\, b \in R'$, for $m \in \mathbb{N}$.
In (i), you have proved $P(1)$ is true. Now assume $P(k)$ is true for some $k \in \mathbb{N}$, and then prove that $P(k+1)$ is true.
Then, $P(n)$ will be true $\forall\; n \in \mathbb{N}$.

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

Firstly, $S \neq \emptyset$, since $R \neq \emptyset$.

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

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

Thus, S is a subring of R.

iv) You must first check that ϕ is well-defined.

Next, $\phi(a+b) = (a+b)^p = a^p + b^p = \phi(a) + \phi(b)$, and
$\phi(ab) = (ab)^p = a^p b^p = \phi(a)\,\phi(b)$.
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 (i).
$\Rightarrow a - b = 0$, since R is without zero divisors.
$\Rightarrow a = b$.

v) We have to show that if R is finite, then ϕ is surjective.

Let R have n elements. Since ϕ is $1\text{-}1$, $\operatorname{Im}\phi$ also has n elements.
Also $\operatorname{Im}\phi \subseteq R$. Thus, $\operatorname{Im}\phi = R$.
Hence, ϕ is surjective.

E25) While showing that none of the statements hold true, you will need to use the facts that 0^0 is not defined (see the course 'Calculus') and $a^0 = 1 \ \forall \ a \in R, \ a \neq 0$ (since R is a domain).

E26) Consider $\mathbb{Z}_6$, and $\overline{2}, \overline{3} \in \mathbb{Z}_6$.
Now, $\overline{2}^6 = \overline{4}$ and $\overline{4}^6 = \overline{4}$.
So $\overline{2}^6 + \overline{4}^6 = \overline{8} = \overline{2}$ in $\mathbb{Z}_6$.
Also, $(\overline{2} + \overline{4})^6 = \overline{0}^6 = \overline{0}$.
Thus, $(\overline{2} + \overline{4})^6 \neq \overline{2}^6 + \overline{4}^6$.

E27) You should check that f is a well-defined function.

Next, for $m, n \in \mathbb{Z}$, $f(m+n) = (m+n)\cdot 1$
$= m\cdot 1 + n\cdot 1$, by LI 2(i), Sec.10.3, Unit 10
$= f(m) + f(n)$.
Also, $f(mn) = (mn)\cdot 1 = (mn)(1\cdot 1) = (m\cdot 1)(n\cdot 1)$, from LI 2(v).
So f is a ring homomorphism.

$\operatorname{Ker} f = \{n \in \mathbb{Z} \mid n\cdot 1 = 0\}$ is an ideal of $\mathbb{Z}$.
So, $\operatorname{Ker} f = r\mathbb{Z}$, for some $r \in \mathbb{Z}$, where $r\cdot 1 = 0$.
Since char $R = m$, $m\cdot 1 = 0$.
So $m\mathbb{Z} \subseteq r\mathbb{Z}$, i.e., $r \mid m$.
But $m = \text{char } R$. So $r \geq m$.
Thus, $r = m$, i.e., $\operatorname{Ker} f = m\mathbb{Z}$.

E28) Show that $\text{char }(\mathbb{Z}_3 \times \mathbb{Z}_4) = 12$.
Thus, the characteristic of $\mathbb{Z}_3 \times \mathbb{Z}_4$ is neither 0 nor a prime.
Note that $\mathbb{Z}_3 \times \mathbb{Z}_4$ is not a domain, as you have seen in Example 4.

E29) $6\mathbb{Z}$ is not, since $6\mathbb{Z}$ is without unity.

$\mathbb{Z}_6$ is not, since it is not a domain.

$\mathbb{Z}[\sqrt{2}]$ is not, since not every non-zero element in it is invertible.

$\mathbb{Q} \times \mathbb{Q}$ is not, since it is not a domain.

$\mathbb{Z}_5$ is a field, since it is a domain, by Theorem 1, and $(\mathbb{Z}_5^*, \cdot)$ is a group.

$\wp(\{a\}) = \{\emptyset, \{a\}\}$ is a field since it satisfies $R1\text{-}R9$ (see E4).

E30) No. For example, $\mathbb{Z}$ is a subring of $\mathbb{Q}$, $\mathbb{Q}$ is a field, but $\mathbb{Z}$ is not.

E31) From Unit 10, you know that $U(\mathbb{Z}[i]) = \{\pm 1, \pm i\} \neq (\mathbb{Z}[i])^*$.

Hence, $\mathbb{Z}[i]$ is not a field.

$\mathbb{Q}[i] = \{a + ib \mid a,\, b \in \mathbb{Q}\}$ is a commutative ring with unity. Does every non-zero element in it have a multiplicative inverse? Check this along the lines of Example 11.

E32) Note that $\overline{x} = x + \mathbb{Z}[x] \neq \overline{0}$, since $x \notin < x^2 >$. (Why?)

But $\overline{x} \cdot \overline{x} = \overline{x^2} = \overline{0}$.

Hence, $\mathbb{Z}[x] \big/ < x^2 >$ is not a domain.

Thus, by Theorem 5, it is not a field.

E33) From the tables, you can see that $+$ and $\cdot$ are binary operations on R.
Further, R satisfies $R1$-$R6$ (of Unit 10).
Next, R is commutative with identity and every non-zero element has an inverse, i.e., R satisfies $R7$-$R9$.
Thus, R is a field.
Here, $2x = 0 \; \forall \; x \in R$ and $1 \cdot x \neq 0$ for some $x \in R$ (e.g., $x = 1$).
Thus, char $R = 2$.

E34) $\text{Ker } f$ is an ideal of F. Thus, by Theorem 9,
$\text{Ker } f = \{0\}$ or $\text{Ker } f = F$.
If $\text{Ker } f = \{0\}$, then f is 1-1.
If $\text{Ker } f = F$, then $f = \mathbf{0}$.

E35) i) It need not. For example, consider

$$\pi : \mathbb{Z} \to \mathbb{Z}\big/2\mathbb{Z} : \pi(m) = \begin{cases} \overline{0}, & \text{if } m \text{ is even,} \\ \overline{1}, & \text{if } m \text{ is odd.} \end{cases}$$

Check that π is a ring homomorphism that is not 1-1.
You also know that $\mathbb{Z}\big/2\mathbb{Z} = \mathbb{Z}_2$, a field.

ii) Consider the inclusion homomorphism from $\mathbb{Q}$ to $\mathbb{R}$.
This is neither $\mathbf{0}$ nor surjective.

E36) Since $R \simeq F$, and isomorphic rings satisfy exactly the same algebraic properties, R is a field.

E37) You should prove all these properties by using the corresponding properties of R. Keeping $\mathbb{Q}$ in mind may help you too.

E38) Firstly, from E29, you know that $\mathbb{Z}[\sqrt{2}]$ is not a field. Thus, it can't be its own field of fractions.

Next, any element of the field of quotients F, of $\mathbb{Z}[\sqrt{2}]$, is of the form $\dfrac{a + b\sqrt{2}}{c + d\sqrt{2}}$, where $c + d\sqrt{2} \neq 0$, $a, b, c, d \in \mathbb{Z}$.

Now,

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

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

Note that $\mathbb{Q}+\sqrt{2}\mathbb{Q}$ is a field, as you studied in Example 11.

Also, any element of $\mathbb{Q}+\sqrt{2}\mathbb{Q}$ is of the form

$\frac{a}{b}+\sqrt{2}\frac{c}{d}$, a, b, c, d $\in \mathbb{Z}$, b $\neq 0$, d $\neq 0$.

Now, $\frac{a}{b}+\sqrt{2}\frac{c}{d}=\frac{ad+bc\sqrt{2}}{bd}=\frac{ad+bc\sqrt{2}}{bd+0\sqrt{2}}$, with $ad, bc, bd \in \mathbb{Z}, bd \neq 0.$

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

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

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

Note that $\mathbb{C} \supsetneq F$ (e.g., $i \notin F$), and hence, is not the field of fractions of $\mathbb{Z}[\sqrt{2}].$ Similarly, $\mathbb{R}$ is not the quotient field of $\mathbb{Z}[\sqrt{2}].$ (For example, $\sqrt{3} \in \mathbb{R}$ but $\sqrt{3} \notin \mathbb{Q}[\sqrt{2}].$ Why? Let's see.

Suppose $\sqrt{3} \in \mathbb{Q}[\sqrt{2}].$

Then $\exists\, m \in \mathbb{Z}$ s.t. $m\sqrt{3}=a+b\sqrt{2}, a, b \in \mathbb{Z}.$

So $3m^2=a^2+2b^2+2ab\sqrt{2}.$

Therefore, $a^2+2b^2=3m^2$ and $2ab=0.$ So $a=0$ or $b=0.$

If $a=0, m\sqrt{3}=b\sqrt{2} \Rightarrow m\sqrt{6} \in \mathbb{Z},$ a contradiction.

Similarly, $b=0$ leads to a contradiction.)

E39) If R is not a domain, the relation ~ need not be transitive, and hence, F is not defined.

E40) Let R be a commutative ring with unity. Suppose it is embedded in a field $F.$ Then F is without zero divisors, and R is a subring of $F.$ Thus, R has to be without zero divisors, i.e., R has to be a domain.

E41) Firstly, I is an ideal of $C[0, 1],$ as you know from Unit 12.

Secondly, since any non-zero constant function (e.g., the map $h:[0, 1] \to \mathbb{R}: h(x)=1$) is in $C[0, 1] \setminus I, I$ is a proper ideal.

Finally, let $fg \in I,$ where $f, g \in C[0, 1].$

Then $(fg)(0)=0,$ i.e., $f(0)\cdot g(0)=0$ in $\mathbb{R}.$

Since $\mathbb{R}$ is a domain, this gives us $f(0)=0$ or $g(0)=0,$ i.e., $f \in I$ or $g \in I.$

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

E42) R is a commutative ring with identity. Thus, we need to show that R is without zero divisors 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.

Thus, $\{0\}$ is a prime ideal in R iff R is an integral domain.

E43) Since $\mathbb{C}$ is a field, its only ideals are $\{0\}$ and $\mathbb{C}.$ Since $\mathbb{C}$ is a domain, $\{0\}$ is a prime ideal of $\mathbb{C},$ by E42. Hence, $\{0\}$ is the only prime ideal of $\mathbb{C}.$

E44) It is not. For example, $2 \cdot 3 \in < 6 >$.

Now, if $2 \in < 6 >$, then $\exists\, a + b\sqrt{5} \in \mathbb{Z}[\sqrt{5}]$ s.t. $6(a + b\sqrt{5}) = 2$, i.e., $6a = 2,\ b = 0.$

But there is no $a \in \mathbb{Z}$ s.t. $6a = 2.$ Hence, $2 \notin < 6 >$.

Similarly, $3 \notin < 6 >$.

E45) As in Example 16, prove that $\mathbb{Z}[x] / < x + 20 > \simeq \mathbb{Z}$, a domain. Hence, $< x + 20 >$ is a prime ideal of $\mathbb{Z}[x].$

E46) No. For example, $\mathbb{Z} \times \mathbb{Z}$ is not a domain, but $(\mathbb{Z} \times \mathbb{Z}) / (\mathbb{Z} \times \{0\}) \simeq \mathbb{Z}$, a domain. Hence, $(\mathbb{Z} \times \mathbb{Z}) / (\mathbb{Z} \times \{0\})$ is a domain.

E47) You can do this along the lines of Example 15.

The prime ideals of $\mathbb{Z}_{30}$ are $< \bar{p} >$, where $p \mid 30$, p a prime.

Thus, these are $\bar{2}\mathbb{Z}_{30}$, $< \bar{3} >$ and $< \bar{5} >$.

E48) i) From Theorem 4 of Unit 13, you know that $f^{-1}(J)$ is an ideal of $R.$ Since f is surjective and $J \neq S, f^{-1}(J) \neq R.$

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 of $R.$

ii) Firstly, since f is onto, you know (from Theorem 4, Unit 13) that $f(I)$ is an ideal of $S.$

Also, since $1 \notin I$ and $f^{-1}(f(I)) = I$ (from Theorem 5, Unit 13 as $I \supseteq N$), $f(1) \notin f(I).$ 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 $f(ab) = f(a)f(b) = xy \in f(I)$, i.e., $ab \in f^{-1}(f(I)) = I.$

$\therefore a \in I$ or $b \in I$, since I is a prime ideal.

So, $x \in f(I)$ or $y \in f(I).$

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

iii) **ϕ is 1-1:** $\phi(I) = \phi(J)$

$\Rightarrow f(I) = f(J)$

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

$\Rightarrow I = J$, as both I and J contain $N.$

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 13).

Thus, $J \in \text{Im } \phi.$

E49) Consider the inclusion map $i : \mathbb{Z} \hookrightarrow \mathbb{Q}$ and $P = 2\mathbb{Z}$. Then $i(P) = 2\mathbb{Z}$ is not an ideal of $\mathbb{Q}$ since the only ideals of $\mathbb{Q}$ are $\{0\}$ and $\mathbb{Q}$. Hence, $2\mathbb{Z}$ is not a prime ideal of $\mathbb{Q}$.

E50) i) Let P_1 and P_2 be prime ideals of a ring R s.t. $\exists\ x \in P_1 \setminus P_2$ and $y \in P_2 \setminus P_1$.
Then $xy \in P_1$ and $xy \in P_2$, since P_1 and P_2 are ideals.
$\therefore\ xy \in P_1 \cap P_2$.
But $x \notin P_1 \cap P_2$ and $y \notin P_1 \cap P_2$.
Thus, $P_1 \cap P_2$ is not prime.

ii) No. For example, $2\mathbb{Z} + 3\mathbb{Z} = \mathbb{Z}$, since $(2, 3) = 1$. Here, $2\mathbb{Z}$ and $3\mathbb{Z}$ are prime ideals of $\mathbb{Z}$, but $\mathbb{Z}$ is not prime in $\mathbb{Z}$. (Why?)

iii) No. e.g., $(2\mathbb{Z})(3\mathbb{Z}) = 6\mathbb{Z}$, which is not prime in $\mathbb{Z}$.

E51) As you know from Unit 12, $m\mathbb{Z} \times n\mathbb{Z}$ is an ideal of $\mathbb{Z} \times \mathbb{Z}$, where $m, n \in \mathbb{Z}$.

Now, $\mathbb{Z} \times \mathbb{Z} \big/ (m\mathbb{Z} \times n\mathbb{Z}) \simeq \mathbb{Z}_m \times \mathbb{Z}_n$, which is a domain only if $(m = 1$ and n is a prime or n is $0)$ or if $(n = 1$ and m is a prime or m is $0)$.
Thus, $\mathbb{Z} \times 2\mathbb{Z}$ and $\mathbb{Z} \times 3\mathbb{Z}$ are two prime ideals of $\mathbb{Z} \times \mathbb{Z}$.
Note that they are distinct because, for example, $(1, 2) \in \mathbb{Z} \times 2\mathbb{Z}$ but $(1, 2) \notin \mathbb{Z} \times 3\mathbb{Z}$.

E52) M is maximal in R
$\Rightarrow R/M$ is a field, by Theorem 14.
$\Rightarrow R/M$ is a domain, by Theorem 5.
$\Rightarrow M$ is prime in R, by Theorem 12.

E53) $\{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\} = \bar{2}\mathbb{Z}_{10}$ and $\mathbb{Z}_{10} \big/ \bar{2}\mathbb{Z}_{10} \simeq \mathbb{Z}_2$, a field.
Thus, $\{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\}$ is maximal in $\mathbb{Z}_{10}$.

E54) As in Example 16, show that $\mathbb{C}[x] \big/ < x - \pi > \simeq \mathbb{C}$, a field.
Hence, $< x - \pi >$ is maximal in $\mathbb{C}[x]$.

E55) In Unit 13, you have seen that this ideal is the kernel of the onto homomorphism $\phi : C[0, 1] \to \mathbb{R} : \phi(f) = f\left(\frac{1}{2}\right)$.

$\therefore\ C[0,1]/\text{Ker}\ \phi \simeq \mathbb{R}$, a field.
Thus, $\text{Ker}\ \phi$ is maximal in $C[0,1]$.

UNIT 15

POLYNOMIAL RINGS

Structure **Page Nos.**

15.1 INTRODUCTION

So far you have studied about many rings, includings rings with special properties. You have also studied about polynomials over $\mathbb{R}$ in some detail in Block 1 of 'Calculus'. In the previous units of this course, you studied several examples related to various rings of polynomials. In this unit, we aim to put all your earlier studies of polynomials together, and take them a little further.

In Sec.15.2, you will study about sets whose elements are polynomials of the type $a_0 + a_1x + \cdots + a_nx^n$, where $a_0, a_1, \ldots, a_n$ are elements of a ring R. You will see that this set, denoted by $R[x]$, is a ring also.

In Sec.15.3, you will see why we are discussing polynomial rings in a block on domains and fields. You will study several properties of $R[x]$ in this connection. In particular, you will see that if R is an integral domain, so is $R[x]$.

Taking the discussion further, in Sec.15.4, you will see that the ring of polynomials over a field behaves quite a bit like $\mathbb{Z}$. It satisfies a division algorithm, which is similar to the one satisfied by $\mathbb{Z}$ (see Unit 1). We will prove this property, and some of its consequences, in this section.

In the next section, Sec.15.5, the focus will be on ideals of $F[x]$, where F is a field. You will find out why every ideal in $F[x]$ is a principal ideal, just as for $\mathbb{Z}$. You will also see why this fact is so important.

In the next unit, we will continue our discussion on polynomials. What you study in this unit, and the next, is very basic for your study in any branch of mathematics. So study this unit carefully. Do every exercise in it as you come to the exercise. This will help you ensure that you have achieved the following expected learning outcomes of studying this unit.

Objectives

After studying this unit, you should be able to:

- Define, and give examples of, polynomials over a given ring;
- prove, and use, the result that the set of polynomials over a commutative ring R is the ring $(R[x], +, \cdot)$;
- relate certain properties of $R[x]$ to those of R;
- prove, and apply, the division algorithm for $F[x]$, where F is a field;
- prove, and apply, the result that every ideal in $F[x]$ is a principal ideal, where F is a field.

15.2 RING OF POLYNOMIALS

You have seen several polynomials like $1+x,\ 2+3x+4x^2,\ x^5-1,\ 0,$ and so on. These are examples of polynomials over $\mathbb{R}$, as their coefficients are in $\mathbb{R}$. But they are also polynomials over $\mathbb{Z}$, as their coefficients lie in $\mathbb{Z}$. Does this brief discussion suggest to you what a polynomial over any ring R is? Let's define this object, and terms immediately related to it.

Definitions: Let R be a ring, and let x be an **indeterminate**.

An 'indeterminate' is a formal symbol. It is **not** a variable.

i) A **polynomial over $\mathbf{R}$**, in x, is an expression of the form
$a_0x^0 + a_1x^1 + a_2x^2 + \cdots + a_nx^n,$
where n is a non-negative integer and $a_0, a_1, \ldots, a_n \in R$.

ii) For $i = 0, 1, \ldots, n,\ a_ix^i$ is called a **term** of the polynomial in (i) above.
If $a_0 \neq 0,\ a_0x^0$ is called **the constant term** of this polynomial.

iii) $a_0, a_1, \ldots, a_n$ are called the **coefficients** of the polynomial in (i) above.
If $a_n \neq 0,\ a_n$ is called the **leading coefficient** of this polynomial, and n is called the **degree** of the polynomial. We denote this fact by
$\mathbf{deg}\ (\mathbf{a_0x^0} + \cdots + \mathbf{a_nx^n}) = \mathbf{n}.$

iv) If $a_0 \neq 0$, the polynomial a_0x^0 is called a **constant polynomial**.

v) If $a_i = 0\ \forall\ i = 0, 1, \ldots, n$, the polynomial obtained is 0, called the **zero polynomial.** By definition, **it has no leading coefficient**.
Further, **the degree of the zero polynomial is undefined**.

For example, for any ring R and any $r \in R,\ rx^0$ is a constant polynomial (if $r \neq 0$) or the zero polynomial (if $r = 0$).

Note that in the matter of writing polynomials, we will observe the **following conventions**.

i) We will not write x^0, so that we will only write a_0 for a_0x^0.

ii) We will write x^1 as x.

iii) We will write x^m instead of $1\cdot x^m$ (i.e., when $a_m = 1$), and write $-ax^m$ if $a_m = (-a) \in R$.

iv) We will omit terms of the type $0\cdot x^m$.

Thus, the polynomial $2x^0 + 0\cdot x^1 + 3x^2 + (-1)x^3$ over $\mathbb{Z}$ will be written as $2 + 3x^2 - x^3$, with (-1) as its leading coefficient and 2 as its constant term.

As an example, $\frac{1}{2} - \pi x^5 + \sqrt{2}x^{11}$ is a polynomial over $\mathbb{R}$, where

$a_0 = \frac{1}{2}$, $a_5 = -\pi$, $a^{11} = \sqrt{2}$ and $a_i = 0$ for $i = 1,\ldots,10$, $i \neq 5$. Similarly,

$-\frac{1}{2} + \pi x^5 - \sqrt{2}x^{11}$ is a polynomial over $\mathbb{R}$.

Also, $Ax + Bx^4$, where $A = \begin{bmatrix} 2 & 1 \\ -0.5 & \pi \end{bmatrix}$, $B = \begin{bmatrix} \sqrt{3} & 0 \\ \sqrt{2} & 3 \end{bmatrix}$, is a polynomial of degree 4 over $\mathbb{M}_2(\mathbb{R})$, with B as its leading coefficient and with no constant term.

Henceforth, **whenever we will use the word ‘polynomial’, we will mean a polynomial in the indeterminate x**. We will also often use the shorter notation $\sum_{i=0}^{n} a_i x^i$ for the polynomial $a_0 + a_1x + \cdots + a_nx^n$.

Recall that Σ is the capital Greek letter ‘sigma’, and denotes ‘sum’.

Here is a remark to explain the use of the indeterminate.

Remark 1: As noted above, x is used here as a symbol, called an indeterminate. The symbols $x^0, x^1, x^2, \ldots$ are there as placeholders. So, instead of writing the polynomial over R as $a_0 + a_1x + \cdots + a_nx^n$, we could as well have written it as an infinite sequence with only finitely many non-zero entries, as $(a_0, a_1, \ldots, a_n, 0, 0, \ldots)$ (recall your study of sequences from ‘Real Analysis’). Similarly, a polynomial of degree m can be written as $(b_0, b_1, \ldots, b_m, 0, 0, \ldots)$, $b_i \in R$, or as $b_0 + b_1x + \cdots + b_mx^m$.
Note that $(0, 0, 2, 1, 5, 7, 9, 11, \ldots)$ is not a polynomial, as it does not have only finitely many non-zero entries.

Let us consider some more examples of polynomials in x.

i) $5 + 4x + 3x^2$ is a polynomial of degree 2, whose coefficients belong to $\mathbb{Z}$. Its leading coefficient is 3.

ii) $\overline{8} + \overline{6}x + x^2 + \overline{2}x^4$ is a polynomial of degree 4, with coefficients in $\mathbb{Z}_{10}$. Its leading coefficient is $\overline{2}$.

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

Notation: R[x] will denote **the set of all polynomials over a ring R**.

(Note the use of the square brackets [ ] here. Do not use any other kind of brackets because $R[x]$ and $R(x)$ denote different sets, as you will see a little later.)

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

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

Thus, an example of an element from $\mathbb{Z}_4[x]$ is $f(x) = \overline{1} + \overline{3}x + \overline{2}x^4.$

Here deg $f(x) = 4,$ and the leading coefficient of $f(x)$ is $\overline{2}.$

Before going further, let us see when two polynomials are equal. (Recall, from the course ‘Real Analysis’ the condition for two sequences to be equal.)

Definition: Let R be a ring, and let $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ and $g(x) = b_0 + b_1 x + \cdots + b_m x^m$ be in $R[x].$ We say that $f(x)$ and $g(x)$ are **equal**, denoted by $\mathbf{f(x) = g(x)},$ if $a_i = b_i \; \forall \; i = 0, 1, \ldots, n.$

Thus, if **two polynomials are equal they have** the same leading coefficients, and hence, **the same degree.** Is the converse true? No.

For example, $2x + 3x^4$ and $5 + 3x^4$ are both of degree 4 in $\mathbb{Z}[x],$ though they are not equal. This is because the coefficients corresponding to the places x^0 and x^1 are different in both.

To check your understanding of what you have studied so far, you should solve the following exercises now.

E1) Identify the polynomials from among the following expressions. Which of these are elements of $\mathbb{Z}[x]$?

i) $1 + x + x^2 + x^4 + x^6,$ ii) $\frac{2}{x^2} + \frac{1}{x} + x + x^2,$

iii) $\sqrt{2}x + \sqrt{3}x^2,$ iv) $1 + \frac{1}{2}x + \frac{1}{3}x^2 + \frac{1}{4}x^3,$

v) $x^{1/2} + x + x^2,$ vi) $-5,$

vii) $\sum_{i=0}^{\infty} i x^i,$ viii) $0.$

E2) If $a_0 + 5x^2 + \sqrt{3}x^3 = \frac{1}{2} + b_1 x + b_2 x^2 + b_3 x^3 + b_4 x^{11}$ in $\mathbb{R}[x],$ find $a_0, b_1, b_2, b_3, b_4.$

E3) Determine the degree and the leading coefficient of each of the following polynomials in $\mathbb{R}[x].$

i) $7 + \sqrt{2}x,$ ii) $1 + 3x - 7x^3,$ iii) $1 + x^3 + x^4 + 0 \cdot x^5,$

iv) $\frac{1}{3}x + \frac{1}{5}x^2 + \frac{1}{7}x^3,$ v) $0.$

Now, for any ring $\mathrm{R},$ let us see how we can define addition and multiplication in $\mathrm{R}[\mathrm{x}]$ so that they are well-defined binary operations on $\mathrm{R}[\mathrm{x}].$ To start with, consider the addition of polynomials.

Definition: Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$ and $g(x) = b_0 + b_1x + \cdots + b_mx^m$ be in $\mathrm{R}[\mathrm{x}].$ Let us assume that $m \ge n.$ (An analogous definition holds if $n > m.$) Then we define **addition in $\mathbf{R[x]}$** by

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n + b_{n+1}x^{n+1} + \cdots + b_mx^m$$

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

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

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

Note that $p(x) + q(x) \in \mathbb{Z}[x],$ and that

$\deg\ (p(x) + q(x)) = 3 = \max\ (\deg\ p(x),\ \deg\ q(x))$ in this case.

From the definition given above, it seems that

$\deg\ (f(x) + g(x)) = \max(\deg\ f(x), \deg\ g(x)).$ Is this true? Let’s see.

Consider $p(x) = 1 + x^2$ and $q(x) = 2 + 3x - x^2$ in $\mathbb{Z}[x].$

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

Here $\deg\ (p(x) + q(x)) = 1;$ but $\max(\deg p(x),\ \deg\ q(x)) = \max(2, 2) = 2.$

Thus, $\deg\ (p(x) + q(x)) < \max(\deg\ p(x),\ \deg\ q(x))$ in this case.

So, what we can say is that

$\mathbf{deg\ (f(x) + g(x)) \le max\,(deg\ f(x),\ deg\ g(x))}\ \ \forall\ f(x),\ g(x) \in \mathrm{R}[x].$

Now let us define multiplication in $\mathrm{R}[\mathrm{x}].$

Definition: Let R be a ring. For $f(x) = a_0 + a_1x + \cdots + a_nx^n$ and $g(x) = b_0 + b_1x + \cdots + b_mx^m$ in $\mathrm{R}[x],$ we define **multiplication in $\mathbf{R[x]}$** by

$f(x) \cdot g(x) = c_0 + c_1x + \cdots + c_{m+n}x^{m+n},$

where $c_i = a_ib_0 + a_{i-1}b_1 + \cdots + a_0b_i\ \forall\ i = 0,1,\ldots,m+n.$

(Here 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 $\mathbb{Z}[x]$:

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

Here $m = 3, n = 2,$ so that $m + n = 5.$ Now

$a_0 = 1,\ a_1 = -1,\ a_2 = 0,\ a_3 = 2,\ a_4 = 0 = a_5,$

$b_0 = 2,\ b_1 = 5,\ b_2 = 7,\ b_3 = 0 = b_4 = b_5.$

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

$c_0 = a_0b_0 = 2,$

$c_1 = a_1b_0 + a_0b_1 = 3,$

$c_2 = a_2b_0 + a_1b_1 + a_0b_2 = 2,$

$c_3 = a_3b_0 + a_2b_1 + a_1b_2 + a_0b_3 = -3,$

$c_4 = a_4b_0 + a_3b_1 + a_2b_2 + a_1b_3 + a_0b_4 = 10,$

$c_5 = a_5b_0 + a_4b_1 + a_3b_2 + a_2b_3 + a_1b_4 + a_0b_5 = 14.$

So $p(x)\cdot q(x) = 2 + 3x + 2x^2 - 3x^3 + 10x^4 + 14x^5.$

Note that $p(x)\cdot q(x) \in \mathbb{Z}[x],$ and $\deg\ (p(x)\cdot q(x)) = 5 = (\deg\ p(x) + \deg\ q(x)).$

As another example, consider

$p(x) = \overline{1} + \overline{2}x,\ q(x) = \overline{2} + \overline{3}x^2 \in \mathbb{Z}_6[x].$

Then, $p(x)\cdot q(x) = \overline{2} + \overline{4}x + \overline{3}x^2 + \overline{6}x^3 = \overline{2} + \overline{4}x + \overline{3}x^2,$ since $\overline{6} = \overline{0}.$

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

So, what we can say is that

$\mathbf{deg\ (f(x)\cdot g(x)) \le deg\ f(x) + deg\ g(x)}$.

We need to check that addition and multiplication in $R[x],$ as defined, are closed in $R[x].$ First, let us see if $+$ is well-defined. If

$f(x) = \sum_{i=0}^{n} a_i x^i,\ f'(x) = \sum_{i=0}^{m} a_i' x^i,\ g(x) = \sum_{i=0}^{r} b_i x^i,\ g'(x) = \sum_{i=0}^{s} b_i' x^i$ are in $R[x]$ s.t.

$f(x) = f'(x)$ and $g(x) = g'(x),$ then

$n = m,\ r = s,\ a_i = a_i',\ b_j = b_j'\ \forall\ i = 0,\ldots,n,\ j = 0,\ldots,r.$

So $f(x) + g(x) = \sum_{i=0}^{\max(n,r)} (a_i + b_i)x^i = \sum_{i=0}^{\max(m,s)} (a_i' + b_i')x^i = f'(x) + g'(x).$

Thus, $+$ is well-defined.

You should similarly show that multiplication is well-defined.

For the rest, do E4 below. Also solve the other exercises below. Doing this will help you get used to these operations on polynomials.

E4) Explain why addition and multiplication are binary operations on $R[x].$

E5) Calculate the following:

i) $(2 + 3x^2 + 4x^3) + (5x + x^3)$ in $\mathbb{Z}[x],$

ii) $(\overline{6} + \overline{2}x^2) + (\overline{1} - \overline{2}x + \overline{5}x^3)$ in $\mathbb{Z}_7[x],$

iii) $(1 + x)\cdot(1 + 2x + x^2)$ in $\mathbb{Z}[x],$

iv) $(\overline{1} + x)\cdot(\overline{1} + \overline{2}x + x^2)$ in $\mathbb{Z}_3[x],$

v) $(2 + x + x^2)\cdot(5x + x^3)$ in $\mathbb{Q}[x].$

A polynomial having only one term is called a **monomial**.

E6) Explain why each term of the polynomial $a_0 + a_1x + \cdots + a_nx^n \in R[x],\ R$ a ring, is also a polynomial over $R.$ Thus, $\sum_{i=0}^{n} a_i x^i$ is the sum of n polynomials over $R.$

By now you must have got used to the addition and multiplication of polynomials. You have also seen that $+$ and $\cdot$ are binary operations over $R[x]$. The question now is whether or not $(R[x], +, \cdot)$ is a ring. Let's see.

Theorem 1: If R is a ring, then so is $R[x]$, where x is an indeterminate.

Proof: We need to establish the axioms $R1 - R6$ (of Unit 10) for $(R[x], +, \cdot)$.

R1 (Addition is commutative): Let $p(x) = a_0 + a_1x + \cdots + a_nx^n$ and $q(x) = b_0 + b_1x + \cdots + b_mx^m$ be in $R[x]$.

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

where $t = \max(m, n)$ and $c_i = a_i + b_i \ \forall \ i = 0, 1, \ldots, t.$

Similarly,

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

where $s = \max(n, m) = t$, and $d_i = b_i + a_i \ \forall \ i = 0, 1, \ldots, t.$

Since addition is commutative in R, $c_i = d_i \ \forall \ i \geq 0.$

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

R2 (Addition is associative): By using the associativity of addition in R, you should check that for $p(x), q(x), s(x) \in R[x]$,

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

R3 (Additive identity): The zero polynomial is the additive identity in $R[x]$. This is because, for any $p(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$,

$$\begin{aligned} 0 + p(x) &= (0 + a_0) + (0 + a_1)x + \cdots + (0 + a_n)x^n \\ &= a_0 + a_1x + \cdots + a_nx^n \\ &= p(x). \end{aligned}$$

R4 (Additive inverse): For $p(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$, consider the polynomial $q(x) = -p(x) = -a_0 - a_1x - \cdots - a_nx^n, -a_i$ being the additive inverse of a_i in R. Then

$$\begin{aligned} p(x) + q(x) &= (a_0 - a_0) + (a_1 - a_1)x + \cdots + (a_n - a_n)x^n \\ &= 0 + 0 \cdot x + 0 \cdot x^2 + \cdots + 0 \cdot x^n \\ &= 0. \end{aligned}$$

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

R5 (Multiplication is associative): Let $p(x) = a_0 + a_1x + \cdots + a_nx^n$, $q(x) = b_0 + b_1x + \cdots + b_mx^m$, and $t(x) = d_0 + d_1x + \cdots + d_rx^r$ be in $R[x]$.

Then

$p(x) \cdot q(x) = c_0 + c_1x + \cdots + c_sx^s$, where $s = m + n$ and

$c_k = a_kb_0 + a_{k-1}b_1 + \cdots + a_0b_k \ \forall \ k = 0, 1, \ldots, s.$

Therefore,

$\{p(x) \cdot q(x)\} \cdot t(x) = e_0 + e_1x + \cdots + e_tx^t$,

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

$$\begin{aligned} e_k &= c_kd_0 + c_{k-1}d_1 + \cdots + c_0d_k \\ &= (a_kb_0 + \cdots + a_0b_k)d_0 + (a_{k-1}b_0 + \cdots + a_0b_{k-1})d_1 + \cdots + a_0b_0d_k. \end{aligned}$$

Similarly, you should check that the coefficient of x^k (for any $k \geq 0$) in $p(x)\cdot\{q(x)\cdot t(x)\}$ is

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

$= e_k$, by using the properties of $+$ and $\cdot$ in R.

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

R6 (Multiplication distributes over addition): Let $p(x) = a_0 + a_1x + \cdots + a_nx^n$, $q(x) = b_0 + b_1x + \cdots + b_mx^m$ and $t(x) = d_0 + d_1x + \cdots + d_rx^r$ be in $R[x]$. For any $k \geq 0$, the coefficient of x^k in $p(x)\cdot(q(x)+t(x))$ is

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

Also the coefficient of x^k in $p(x)\cdot q(x) + p(x)\cdot t(x)$ is

$(a_kb_0 + a_{k-1}b_1 + \cdots + a_0b_k) + (a_kd_0 + a_{k-1}d_1 + \cdots + a_0d_k)$

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

$= c_k$.

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

Similarly, you can prove that

$\{q(x)+t(x)\}\cdot p(x) = q(x)\cdot p(x) + t(x)\cdot p(x)$.

Thus, $R[x]$ is a ring. ■

What Theorem 1 tells us is that apart from the examples of polynomial rings you have worked with earlier, $C[0,1][x]$, $(3\mathbb{Z})[x]$, $\mathbb{M}_n(\mathbb{Z})[x]$, $\mathbb{H}[x]$ are all rings.

Also note that, since $(R[x], +)$ is abelian, and using E6, we see that $a_0 + a_1x + \cdots + a_nx^n$ can be written as $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$, or $a_nx^n + a_0 + a_{n-1}x^{n-1} + a_1x + \cdots$.

So, for example, $-\pi + 5x + 5x^3 \in \mathbb{R}[x]$ is the same as $5x - \pi + 5x^3$ or $5x + 5x^3 - \pi$.

Let us consider an example of $R[x]$ in detail.

Example 1: Is $\mathbb{Z}_6[x]$ finite? Why?

Solution: $\mathbb{Z}_6$ has 6 elements.

$\mathbb{Z}_6[x] = \{a_0 + a_1x + \cdots + a_nx^n \mid a_i \in \mathbb{Z}_6 \ \forall\ i = 0, 1, \ldots, n,\ n \in \mathbb{N}\cup\{0\}\}$.

So, a_0 can take any of the values $\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}$.

Similarly, each a_i can take any one of 6 values.

So, $\overline{0}$ is the zero polynomial, and there are 5 constant polynomials. Now, there are $6\times5=30$ polynomials of degree 1, as a_0 can take 6 values but $a_1 \neq \overline{0}$ (as we have already counted $\overline{0}$) so that a_1 can take 5 values.

Similarly, there are $6\times6\times5$ polynomials of degree 2 over $\mathbb{Z}_6$, and so on.

Since n can take infinitely many values, there are infinitely many polynomials over $\mathbb{Z}_6$.

***

Before going further, let us define some commonly used terms related to polynomials. You may already be familiar with them from your earlier studies.

Definition: i) A polynomial of degree 1 is called a **linear polynomial**.

ii) A polynomial of degree 2 is called a **quadratic polynomial**.

iii) A polynomial of degree 3 is called a **cubic polynomial**.

iv) A polynomial of degree 4 is called a **bi-quadratic** (or **quartic**) polynomial.

v) A polynomial with leading coefficient 1 is called a **monic polynomial**.

So, for example $3+5x^3 \in \mathbb{Z}[x]$ is a cubic polynomial, and $\frac{3}{5}+x^3$ is a cubic monic polynomial over $\mathbb{Q}$.

Try solving some exercises now.

E7) Which of the following statements are true? Give reasons for your answers.

i) The product of two linear polynomials in $R[x]$ can be a linear polynomial, where R is a ring.

ii) The product of two quadratic polynomials in $\mathbb{Q}[x]$ is a quartic polynomial.

iii) The sum of two quadratic polynomials in $\mathbb{C}[x]$ is a quadratic polynomial.

iv) If $p(x)$ is a monic polynomial in $R[x]$, where R is a ring with unity, then $p(x)+q(x)$ is monic $\forall\ q(x) \in R[x]$.

E8) Give two distinct elements of positive degree in $\mathbb{M}_2(\mathbb{C})[x]$, with justification.

E9) Check whether or not R is

i) a subring of $R[x]$,

ii) an ideal of $R[x]$.

E10) List all the quadratic polynomials in $\mathbb{Z}_4[x]$.

E11) Let R be a ring and let $\wp_n = \{f(x) \in R[x] \mid \deg f(x) \le n\} \cup \{0\}$, for $n \in \mathbb{N}$. Check whether or not $\wp_n$ is a subring of $R[x]$.

E12) Let R be a ring and $A = \left\{ \sum_{i=0}^{n} a_i x^i \in R[x] \,\middle|\, a_i = 0 \text{ if } i \text{ is odd} \right\}$. Is A a subring of $R[x]$? Why, or why not?

Note that the definitions and theorem in this section are true for **any ring.** But, the case that we are really interested in is when R is a domain. In the next section, our discussion will progress towards this case.

15.3 SOME PROPERTIES OF POLYNOMIAL RINGS

While studying the previous section, you would have realised some properties of $\mathrm{R}[x]$. For instance, from Example 1, you may have realised that given any finite non-trivial ring R, $\mathrm{R}[x]$ is an infinite ring. Have you also thought about the intimate relationship between the operations on a ring R and the operations on $\mathrm{R}[x]$? Of course, while proving Theorem 1, you have seen this relationship. You will now see further evidence of the relationship pertaining to the multiplications in R and in $\mathrm{R}[x]$.

Theorem 2: Let R be a commutative ring with identity. Then $\mathrm{R}[x]$ is also a commutative ring with identity.

Proof: First we shall show that $\mathrm{R}[x]$ is commutative.

Let $p(x) = a_0 + a_1x + \cdots + a_nx^n$ and $q(x) = b_0 + b_1x + \cdots + b_mx^m$ be in the ring $\mathrm{R}[x]$.

Then $p(x)\cdot q(x) = c_0 + c_1x + \cdots + c_sx^s$, where $s = m + n$, and

$c_k = a_kb_0 + a_{k-1}b_1 + \cdots + a_0b_k$

$= b_ka_0 + b_{k-1}a_1 + \cdots + b_1a_{k-1} + b_0a_k$, since both addition and multiplication are commutative in R.

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

Thus, for every $i \geq 0$, the coefficient of x^i in $p(x)\cdot q(x)$ and $q(x)\cdot p(x)$ are equal.

Hence, $p(x)\cdot q(x) = q(x)\cdot p(x)$, i.e., $\mathrm{R}[x]$ is commutative.

Next, we know that R has identity 1. We will prove that the constant polynomial 1 is the identity of $\mathrm{R}[x]$.

Take $p(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathrm{R}[x]$.

Then $1\cdot p(x) = c_0 + c_1x + \cdots + c_nx^n$ (since $\deg 1 = 0$),

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

Thus, $1\cdot p(x) = p(x)$.

Hence, 1 is the identity of $\mathrm{R}[x]$. ■

From Theorem 2, we know that $\mathbb{Z}[x]$ is a commutative ring with identity. Similarly, $F[x]$ is a commutative ring with identity, for any field F.

What about the converse of Theorem 2? This is what the following exercises are about.

E13) If R is a ring such that $\mathrm{R}[x]$ is commutative and has identity, then

i) must R be commutative?

ii) must R have identity?

Give reasons for your answers.

E14) Let R be a commutative ring with identity. Show that $U(R[x]) = U(R)$.

Henceforth, we will assume that the rings are commutative and with identity.

Now let us see if R and $R[x]$ behave the same way regarding zero divisors. For this, we shall first prove a result we had mentioned when we defined the multiplication of polynomials. You also used this implicitly while solving E7(ii).

Theorem 3: Let R be a ring, and let $f(x)$ and $g(x)$ be two non-zero elements of $R[x]$. Then
$\deg(f(x)g(x)) \le \deg f(x) + \deg g(x)$,
with equality iff R is without zero divisors.

Proof: Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$, $a_n \ne 0$,
and $g(x) = b_0 + b_1x + \cdots + b_mx^m$, $b_m \ne 0$.
Then $\deg f(x) = n$, $\deg g(x) = m$.
So, $f(x) \cdot g(x) = c_0 + c_1x + \cdots + c_{m+n}x^{m+n}$, where
$c_k = a_kb_0 + a_{k-1}b_1 + \cdots + a_0b_k$, $k = 0, 1, \ldots, m+n$.
Since $a_{n+1}, a_{n+2}, \ldots, a_{n+m}$ and $b_{m+1}, b_{m+2}, \ldots, b_{m+n}$ are all zero,
$c_{m+n} = a_nb_m$.
Thus, $\deg(f(x)\cdot g(x)) \le n + m = \deg f(x) + \deg g(x)$.

Now, if R is without zero divisors, then $a_nb_m \ne 0$, since $a_n \ne 0$ and $b_m \ne 0$.
Thus, in this case,
$\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$.

Conversely, let $\deg(f(x)g(x)) = \deg f(x) + \deg g(x)\ \forall\ f(x), g(x) \in R[x]\setminus\{0\}$.
We shall prove, by contradiction, that R is without zero divisors.
Suppose, to the contrary, that R has zero divisors, say $ab = 0$, where
$a \ne 0$, $b \ne 0$ in R.
Let $f(x) = a_0 + ax$ and $g(x) = b_0 + bx$ be in $R[x]$.
Then $f(x)g(x) = a_0b_0 + (ab_0 + a_0b)x + abx^2 = a_0b_0 + (ab_0 + a_0b)x$.
In this case, $\deg(f(x)g(x)) = 1 < 2 = \deg f(x) + \deg g(x)$, and we reach a contradiction.
Thus, R is without zero divisors. ■

Theorems 2 and 3 lead us to the following important result.

Theorem 4: $R[x]$ is an integral domain $\Leftrightarrow R$ is an integral domain.

Proof: From Theorem 2 and E13, you 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 $p(x)$ and $q(x)$ be in $R[x]$, of degree n and m, respectively.
Then, from Theorem 3, you know that $\deg(p(x)q(x)) = m + n \ge 0$.

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. Since R is a subring of $R[x]$, R is also without zero divisors.

So, we have proved the theorem. ■

In this section, so far, you have seen that many properties of the ring R carry over to $R[x]$, and vice-versa. Thus, if F is a field, you may expect $F[x]$ to be a field also. Let us see if this is so.

Example 2: Let F be a field. Show that $F[x]$ is not a field.

Solution: Since F is a field, it is an integral domain. So $F[x]$ is an integral domain, by Theorem 4.

Suppose $F[x]$ is a field. Then $U(F[x]) = F[x]^*.$

But, from E14 you know that $U(F[x]) = U(F) = F^* \neq F[x]^*.$

So we reach a contradiction.

Thus, $F[x]$ is not a field.

***

Why don't you solve the following exercises now? Doing so will help you understand $R[x]$ better, for some rings R.

E15) Which of the following polynomial rings are without zero divisors?

i) $R[x]$, where $R = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$,

ii) $\mathbb{Z}_7[x]$,

iii) $\mathbb{M}_2(\mathbb{Q})[x]$,

iv) $R[x]$, where $R = C[0, 1]$,

v) $\wp(X)[x]$, where X is a set with at least two elements.

E16) If I is an ideal of a ring R, show that $I[x] = \left\{ \sum_{i=0}^{n} a_i x^i \middle| a_i \in I,\, n \in \mathbb{N} \cup \{0\} \right\}$ is an ideal of $R[x]$. Further, show that $\left(R/I\right)[x] \simeq R[x]/I[x]$.

E17) Show that $< x >$ is a proper ideal of $R[x]$, where R is a non-trivial commutative ring. Hence, show that **not** every ideal of $R[x]$ is of the form $I[x]$, where I is an ideal of R.

E18) Let R be a domain. Show that $\text{char } R = \text{char } R[x]$.

E19) Let $f : R \to S$ be a ring homomorphism. Show that $\phi : R[x] \to S[x] : \phi(a_0 + a_1 x + \cdots + a_n x^n) = f(a_0) + f(a_1)x + \cdots + f(a_n)x^n$ is a ring homomorphism.

Further, if f is an isomorphism, will ϕ be an isomorphism? Why, or why not?

E20) Let R and S be rings. Define

$$\phi:(R\times S)[x]\to R[x]\times S[x]:\phi\left(\sum_{i=0}^{n}(a_i,b_i)x^i\right)=\left(\sum_{i=0}^{n}a_ix^i,\sum_{i=0}^{n}b_ix^i\right).$$ Check whether or not ϕ is a ring homomorphism. Is ϕ onto? Is ϕ 1-1?

You have seen that if R is a domain so is $R[x]$; but if F is a field, $F[x]$ is not a field. However, $F[x]$ is a domain. So, the question arises if there is any connection between F and the field of quotients of $F[x]$. To answer this, let us consider the following definition first.

Definition: A **rational function** in an indeterminate x over a field F is a quotient $p(x)/q(x)$, with $p(x), q(x)\in F[x], q(x)\neq 0.$
The set of rational functions in x over F is denoted by $\mathbf{F(x)}$. (Note the use of the round brackets here.)

$F[x]\neq F(x)$. Note the use of the different kinds of brackets to denote the different rings.

For example, $\mathbb{Q}(x)=\{f(x)/g(x)\mid f(x), g(x)\in\mathbb{Q}[x], g(x)\neq 0\}.$

Now, let us move towards answering the question we raised above.

Theorem 5: Let F be a field. Then $F(x)$ is the field of fractions of $F[x]$.

Proof: From Unit 14, you know that the field of fractions of the integral domain $F[x]$ is $\{p(x)[q(x)]^{-1}\mid p(x), q(x)\in F[x], q(x)\neq 0\}=F(x),$ by definition. ■

Thus, **for any field F, $F(x)$ is a field**, and is called the **field of rational functions**, in one indeterminate, over F.

For example, $\mathbb{Q}(x)$ is the field of rational functions in x over $\mathbb{Q}$.

Now consider a domain R. You know that $R[x]$ is a domain. If F is the quotient field of R, will $F(x)$ be the quotient field of $R[x]$? Let us try and find an answer, through an example.

Example 3: Find the field of fractions of

i) $\mathbb{Q}[x]$, ii) $\mathbb{Z}[x]$.

Solution: i) By Theorem 5, $\mathbb{Q}(x)$ is the field of quotients of $\mathbb{Q}[x]$.

ii) You know that the field of fractions of a domain is the smallest field containing it. You also know that the field of quotients of $\mathbb{Z}$ is $\mathbb{Q}$. We will use these facts to find F, the field of fractions of $\mathbb{Z}[x]$.
Since F is a field containing $\mathbb{Z}[x]$, it contains $\mathbb{Z}$.
So $F\supseteq\mathbb{Q}$.

Also, for any $f(x)=\frac{r_0}{s_0}+\frac{r_1}{s_1}x+\cdots+\frac{r_n}{s_n}x^n\in\mathbb{Q}[x], s_0s_1\ldots s_nf(x)\in\mathbb{Z}[x].$

Thus, given any $f(x)\in\mathbb{Q}[x]$, $\exists\, m\in\mathbb{Z}$ s.t. $mf(x)\in\mathbb{Z}[x]$.

Now, let ${f(x)}/{g(x)}\in\mathbb{Q}(x)$, where $f(x), g(x)\in\mathbb{Q}[x]$, with $g(x)\neq 0$.

If $f(x)=0$, then $\frac{f(x)}{g(x)} \in F$.

If $f(x) \neq 0$, then $mf(x)$ and $ng(x)$ are in $\mathbb{Z}[x]$ for some $m, n \in \mathbb{Z}$, $m, n \neq 0$.

So $f(x)\big/g(x) = \left(\frac{n}{m}\right)\frac{mf(x)}{ng(x)} \in F$, since $\mathbb{Q} \subseteq F$ and F is the field of quotients of $\mathbb{Z}[x]$.

Hence, $\mathbb{Q}(x) \subseteq F$.

Also, for any $p(x) \in \mathbb{Z}[x]$, $p(x) \in \mathbb{Q}[x] \subseteq \mathbb{Q}(x)$.

Now $\mathbb{Q}(x)$ is a field containing $\mathbb{Z}[x]$ and it is contained in F, the quotient field of $\mathbb{Z}[x]$. Therefore, $\mathbb{Q}(x) = F$.

Thus, the field of quotients of $\mathbb{Z}[x]$ is the same as the field of quotients of $\mathbb{Q}[x]$. Note that we have used the fact that $\mathbb{Q}$ is the field of quotients of $\mathbb{Z}$.

***

On the same lines as in the example above, let us answer the question raised before Example 3.

Theorem 6: Let D be an integral domain, with F being its field of fractions. Then the field of fractions of $D[x]$ is $F(x)$, the field of rational functions over F.

Proof: Firstly, $D \subseteq F \subseteq F(x)$. So $D[x] \subseteq F[x] \subseteq F(x)$.

Also, $F(x)$ is the smallest field containing $F[x]$.

Let K be any field containing $D[x]$.

Then $K \supseteq D$, and hence $K \supseteq F$.

Also, any polynomial in $F[x]$ is of the form $f(x) = \frac{a_0}{b_0} + \frac{a_1}{b_1}x + \cdots + \frac{a_n}{b_n}x^n$,

$a_i, b_j \in D, b_j \neq 0$ for $i, j = 1, \ldots, n$.

Then, as in Example 3(ii), $\exists\, d \in D^*$ s.t. $df(x) \in D[x]$.

$\therefore f(x)$ lies in K, since every polynomial in $D[x]$ lies in K.

Thus, $K \supseteq F[x]$.

Hence, $K \supseteq F(x)$.

Thus, $F(x)$ is the smallest field containing $D[x]$, i.e., it is the field of fractions of $D[x]$. ■

Why don't you solve some related exercises now?

E21) Find the field of fractions of the following domains:

i) $\mathbb{Z}[i][x]$, ii) $\mathbb{Q}[\sqrt{11}][x]$, iii) $\mathbb{Z}_p[x]$, p a prime.

E22) Give two distinct non-trivial elements of the field of quotients of $\mathbb{C}[x]$, with justification.

E23) Find an infinite field of characteristic p, for each prime p.

In this section you have seen several ways in which the properties of $R[x]$ mirror the properties of R. You have also seen that there are some properties that do not match. For example, F is a field, but $F[x]$ is not. However, $F[x]$ is a very interesting algebraic object in its own right. It has several interesting properties which are similar to those of $\mathbb{Z}$. In the next section, we shall discuss some such properties related to divisibility.

15.4 DIVISIBILITY IN POLYNOMIAL RINGS

In Unit 1, you studied various properties of divisibility in $\mathbb{Z}$. In particular, you studied the division algorithm for integers. We will now discuss divisibility, and the division algorithm, for polynomials over a field F. Before going further, why don't you revise Theorem 4, Unit 1, and the related examples? This may help you see the parallels between the properties satisfied by the integers and by polynomials over F.

Let us begin with an example in $\mathbb{Q}[x]$. Let us use long division to find out what happens on dividing $3x^3+4$ by $2x^2+x$.

$$\begin{array}{r l}
 & \frac{3}{2}x-\frac{3}{4} \quad \longleftarrow \text{quotient} \\
2x^2+x \,\big) & \overline{3x^3+4 \qquad\quad} \\
 & 3x^3+\frac{3}{2}x^2 \\
 & \overline{\qquad -\frac{3}{2}x^2+4} \\
 & \qquad -\frac{3}{2}x^2-\frac{3}{4}x \\
 & \qquad \overline{\qquad\quad \frac{3}{4}x+4} \quad \longleftarrow \text{remainder}
\end{array}$$

So, what did we do in the division above? We continued subtracting different multiples of $(2x^2+x)$ till we reached 0 or a polynomial of degree less than $\deg\,(2x^2+x)$. This polynomial, $\frac{3}{4}x+4$, is the remainder. The sum of the multiples of $(2x^2+x)$, i.e., $\frac{3}{2}x-\frac{3}{4}$, is the quotient. This is essentially what is done in the division algorithm, as you will now see.

Theorem 7 (Division Algorithm): Let F be a field. Let $f(x)$ and $g(x)$ be polynomials in $F[x]$, with $g(x) \neq 0$. Then

i) there exist polynomials $q(x)$ and $r(x)$ in $F[x]$ such that $f(x) = q(x)g(x) + r(x)$, where $r(x) = 0$ or $\deg r(x) < \deg g(x)$, and

ii) the polynomials $q(x)$ and $r(x)$ are unique.

Proof: i) If $\deg f(x) < \deg g(x)$, we can choose $q(x) = 0$.
Then $f(x) = 0 \cdot g(x) + f(x)$, where $\deg f(x) < \deg g(x)$.
So, in this case, $r(x) = f(x)$ and $q(x) = 0$.

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

Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$, $a_n \neq 0$, and

$g(x) = b_0 + b_1x + \cdots + b_mx^m$, $b_m \neq 0$, with $n \geq m$.

We shall apply the strong form of the principle of mathematical induction (see Unit 1) on $\deg f(x)$, i.e., n.

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

So, $f(x) = a_0$ and $g(x) = b_0$ are in F.

Hence, $f(x) = (a_0b_0^{-1})b_0 + 0 = q(x)g(x) + r(x)$, where $q(x) = a_0b_0^{-1}$ and $r(x) = 0$.

So the algorithm is true when $n = 0$.

Let us assume that the algorithm holds for all polynomials of degree less than n, and then see if it is true for $f(x)$.

Consider the polynomial

$f_1(x) = f(x) - a_nb_m^{-1}x^{n-m}g(x)$

$= (a_0 + a_1x + \cdots + a_nx^n) - (a_nb_m^{-1}b_0x^{n-m} + a_nb_m^{-1}b_1x^{n-m+1} + \cdots + a_nb_m^{-1}b_mx^n)$.

We have chosen to multiply the term $a_nb_m^{-1}x^{n-m}$ with $g(x)$ to make the coefficient of x^n in $f_1(x)$ zero.

So $\deg f_1(x) \leq n - 1$.

By the induction hypothesis, there exist $q_1(x)$ and $r(x)$ in $F[x]$ such that $f_1(x) = q_1(x)g(x) + r(x)$, where $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

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

$f(x) - a_nb_m^{-1}x^{n-m}g(x) = q_1(x)g(x) + r(x)$,

i.e., $f(x) = \{a_nb_m^{-1}x^{n-m} + q_1(x)\}g(x) + r(x)$

$= q(x)g(x) + r(x)$, where $q(x) = a_nb_m^{-1}x^{n-m} + q_1(x)$ and $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

Therefore, (i) is true for $f(x)$.

Hence, by the principle of induction, (i) is true for all polynomials in $F[x]$.

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

Let $f(x), g(x) \in F[x], g(x) \neq 0$.

If possible, let $q_1(x), q_2(x), r_1(x), r_2(x)$ be in $F[x]$ such that

$f(x) = q_1(x)g(x) + r_1(x)$, where $r_1(x) = 0$ or $\deg r_1(x) < \deg g(x)$, and

$f(x) = q_2(x)g(x) + r_2(x)$, where $r_2(x) = 0$ or $\deg r_2(x) < \deg g(x)$.

Then

$q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x)$, so that

$\{q_1(x) - q_2(x)\}g(x) = r_2(x) - r_1(x)$. …(1)

If $r_1(x) = r_2(x)$, then $q_1(x) = q_2(x)$, by (1), since $g(x) \neq 0$.

So, assume $r_1(x) - r_2(x) \neq 0$. Then $q_1(x) \neq q_2(x)$.

So $\deg \{q_1(x) - q_2(x)\} \geq 0$, and hence,

$\deg [\{q_1(x) - q_2(x)\}g(x)] \geq \deg g(x)$. …(2)

On the other hand,

$\deg \{r_2(x) - r_1(x)\} < \deg g(x)$, …(3)

since $r_1(x) - r_2(x) \neq 0$, and hence, $r_1(x) \neq 0$ or $r_2(x) \neq 0$.

From (2) and (3), we get a contradiction to (1).

Hence, (1) will remain valid only if $r_2(x) - r_1(x) = 0$. And then,

$q_1(x) - q_2(x) = 0$.

i.e., $q_1(x) = q_2(x)$ and $r_1(x) = r_2(x)$.
Thus, we have proved the uniqueness of $q(x)$ and $r(x)$ in the expression $f(x) = q(x)g(x) + r(x)$. ■

The algorithm in Theorem 7 requires us to define some terms, just as in the case of $\mathbb{Z}$.

Definitions: i) The polynomial $q(x)$ in Theorem 7 is called the **quotient**, and $r(x)$ is called the **remainder**, obtained on dividing $f(x)$ by $g(x)$.

ii) If $r(x) = 0,$ then $f(x) = g(x)q(x).$ In this case, we say that $g(x)$ **divides** $f(x),$ or that $g(x)$ is a **factor** of $f(x),$ or that $f(x)$ is **divisible** by $g(x).$ We write $\mathbf{g(x)} \mid \mathbf{f(x)}$ for '$g(x)$ divides $f(x)$', and $\mathbf{g(x)} \nmid \mathbf{f(x)}$ for '$g(x)$ does not divide $f(x)$'.

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

Example 4: Find the quotient and remainder obtained on dividing $x^4 + x^3 + 5x^2 - x$ by $(x^2 + x + 1)$ in $\mathbb{Q}[x]$.

Solution: We will apply long division of polynomials to solve this problem.
Here $f(x) = x^4 + x^3 + 5x^2 - x$ and $g(x) = x^2 + x + 1$.

$$\begin{array}{r l l}
 & x^2 \qquad + 4 & \leftarrow \text{quotient } q(x)\\
(x^2+x+1) & \overline{)\,x^4 + x^3 + 5x^2 - x} & \\
 & \underline{x^4 + x^3 + x^2\qquad} & \leftarrow x^2g(x)\\
 & \qquad\qquad 4x^2 - x & \leftarrow (f(x) - x^2g(x))\\
 & \qquad\qquad \underline{4x^2 + 4x + 4} & \leftarrow 4g(x)\\
 & \qquad\qquad\qquad -5x - 4 & \leftarrow (f(x) - x^2g(x) - 4g(x))
\end{array}$$

Now, since $\deg(-5x-4) = 1 < \deg(x^2 + x + 1),$ we stop the process. So, the remainder $r(x) = -5x - 4.$ So, we get
$x^4 + x^3 + 5x^2 - x = (x^2 + x + 1)(x^2 + 4) - (5x + 4).$
Here the quotient is $x^2 + 4$ and the remainder is $-(5x + 4)$.

***

Example 5: Check whether or not $(x^2 + 2)$ divides $(3x^4 + 2x^2 + 2)$ in $\mathbb{R}[x]$, and $(x^2 + \overline{2})$ divides $(\overline{3}x^4 + \overline{2}x^2 + \overline{2})$ in $\mathbb{Z}_5[x]$.

Solution: Let us first divide in $\mathbb{R}[x]$.

$$\begin{array}{r l}
 & 3x^2 - 4\\
(x^2+2) & \overline{)\,3x^4 + 2x^2 + 2}\\
 & \underline{3x^4 + 6x^2\qquad}\\
 & \qquad -4x^2 + 2\\
 & \qquad \underline{-4x^2 - 8}\\
 & \qquad\qquad 10
\end{array}$$

Thus, in $\mathbb{R}[x]$, $3x^4 + 2x^2 + 2 = (x^2 + 2)(3x^2 - 4) + 10.$ …(4)

Since the remainder is not zero, $(x^2+2) \nmid (3x^4+2x^2+2)$ in $\mathbb{R}[x]$.

Now, let us look at the question for $\mathbb{Z}_5[x]$. Note that the polynomials are the same as the earlier ones in $\mathbb{R}[x]$. Also note that (4) is true in $\mathbb{Z}[x]$ too. So, if we look at (4) in $\mathbb{Z}_5[x]$, we get

$\overline{3}x^4+\overline{2}x^2+\overline{2} = (x^2+\overline{2})(\overline{3}x^2+\overline{1})$, since $-\overline{4}=\overline{1}$ and $\overline{10}=\overline{0}$ in $\mathbb{Z}_5$.

So $(x^2+\overline{2}) \mid (\overline{3}x^4+\overline{2}x^2+\overline{2})$ in $\mathbb{Z}_5[x]$.

***

Why don't you apply the division algorithm for some cases now?

E24) Express $f(x)$ as $g(x)q(x)+r(x)$, where $r(x)=0$ or $\deg r(x) < \deg g(x)$, in each of the following cases.

i) $f(x)=x^4+1, g(x)=\frac{1}{7}-x^3$ in $\mathbb{Q}[x]$,

ii) $f(x)=x^3+\overline{2}x^2-x+\overline{1}, g(x)=\overline{2}x+\overline{1}$ in $\mathbb{Z}_3[x]$,

iii) $f(x)=x^3-3\sqrt{3}, g(x)=x-\sqrt{3}$ in $\mathbb{R}[x]$.

In which of these cases does $g(x)$ divide $f(x)$?

Let us now prove some properties of the relation 'divides' in $F[x]$. (Keep noting the similarity with $\mathbb{Z}$, while you are studying them. While doing so, you can replace 'degree' by 'absolute value' in the case of integers.)

Theorem 8: Let F be a field, and let $f(x), g(x), h(x) \in F[x]$, with $f(x) \neq 0$.

i) If $f(x) \mid g(x)$, where $g(x) \neq 0$, then $\deg f(x) \le \deg g(x)$.

ii) $f(x) \mid f(x)$.

iii) If $f(x) \mid g(x)$ and $a \in F^*$, then $af(x) \mid ag(x)$.

iv) If $g(x) \neq 0$ is s.t. $f(x) \mid g(x)$ and $g(x) \mid h(x)$, then $f(x) \mid h(x)$.

v) If $g(x) \neq 0$ is s.t. $f(x) \mid g(x)$ and $g(x) \mid f(x)$, then $f(x)=ag(x)$ for some $a \in F^*$.

vi) If $f(x) \mid g(x)$ and $f(x) \mid h(x)$, then $f(x) \mid (g(x)+h(x))$.

vii) If $f(x) \mid g(x)$, then $f(x) \mid g(x)h(x)$.

Proof: We will prove (i) and (v) here, and leave the rest for you to prove, as an exercise (see E25).

i) If $f(x) \mid g(x)$, then $\exists\, q(x) \in F[x]$ s.t. $f(x)q(x)=g(x)$.

So $\deg f(x) + \deg q(x) = \deg g(x)$.

Since $g(x) \neq 0$, $q(x) \neq 0$.

Hence, $\deg q(x) \geq 0$.

Hence, $\deg f(x) \leq \deg g(x)$.

v) Let $f(x)q(x) = g(x)$ and $g(x)r(x) = f(x)$ for some $q(x), r(x) \in F[x]$, with $q(x) \neq 0$, $r(x) \neq 0$.

Then $g(x)r(x)q(x) = g(x)$.

So, $r(x)q(x) = 1$, since cancellation holds in $F[x]$.

Thus, $r(x) \in U(F[x]) = U(F) = F^*$, as you have proved in E14.

Hence, $r(x) = r_0 \in F^*$.

Thus, $f(x) = r_0 g(x)$, $r_0 \in F^*$. ■

The proof of the theorem above will be complete once you do the following exercise.

E25) Prove Theorem 8, except for (i) and (v).

Let us now see if, based on Theorem 8, we can define an equivalence relation analogous to Example 3 of Unit 1.

Example 6: Let F be a field and let $h(x) \in F[x]$, $h(x) \neq 0$. Consider the relation $R = \{(f(x), g(x)) \mid h(x) \text{ divides } [f(x) - g(x)],\ f(x), g(x) \in F[x]\}$. Check whether or not R is an equivalence relation on $F[x]$. If it is, find two distinct elements in the equivalence class of 0. If it is not, define an equivalence relation on $F[x]$.

Solution: Note that R is the relation ~ given by '$f(x) \sim g(x)$ iff $h(x) \mid [f(x) - g(x)]$ in $F[x]$'.

R is reflexive: For any $f(x) \in F[x]$, $f(x) \sim f(x)$, since $h(x) \mid 0$.

R is symmetric: Let $f(x) \sim g(x)$. Then $\exists\ r(x) \in F[x]$ s.t. $f(x) - g(x) = h(x)r(x)$.

So, $g(x) - f(x) = h(x)[-r(x)]$, and $-r(x) \in F[x]$.

Hence, $g(x) \sim f(x)$.

R is transitive: Let $f(x) \sim g(x)$ and $g(x) \sim s(x)$ in $F[x]$.

Then $h(x) \mid [f(x) - g(x)]$ and $h(x) \mid [g(x) - s(x)]$.

Thus, by Theorem 8(vi), $h(x) \mid [f(x) - g(x) + g(x) - s(x)]$, i.e., $h(x) \mid [f(x) - s(x)]$.

Hence, $f(x) \sim s(x)$.

So, we have proved that R is an equivalence relation. Hence, R partitions $F[x]$ into equivalence classes, as you know from Sec.1.3, Unit 1.

$$[0] = \{f(x) \in F[x] \mid h(x) \text{ divides } [f(x) - 0]\} = \{f(x) \in F[x] \mid h(x) \text{ divides } f(x)\}$$
$$= \{h(x)g(x) \mid g(x) \in F[x]\}$$
$$= \langle h(x) \rangle.$$

Thus, two elements of $[0]$ are $h(x)$ and $xh(x)$, for example. They are distinct, as they have different degrees.

***

Why don't you check your understanding of divisibility in $F[x]$ now?

E26) In Theorem 8, if $F[x]$ is replaced by $R[x]$, where R is an integral domain, which statements remain true, and why?

E27) Show that if R is a domain and $f(x), g(x) \in R[x]$ are monic polynomials such that $f(x) \mid g(x)$ and $g(x) \mid f(x)$, then $f(x) = g(x)$.

E28) Let F be a field. Check whether or not the relation ~ in $F[x]$, given by $'f(x) \sim g(x)$ iff $f(x) \mid g(x)'$ is an equivalence relation.

E29) Let F be a field and let $f(x), g(x), h(x) \in F[x]$ s.t. $f(x) \neq 0$ and $f(x) \mid g(x)$, $f(x) \mid h(x)$. Show that $f(x) \mid [g(x)r(x) + h(x)s(x)]$ for any $r(x), s(x) \in F[x]$.

Let us now move to another property of $\mathbb{Z}$, and see if it holds true for $F[x]$. You have seen, in Unit 1, that any two non-zero integers a and b have a greatest common divisor d, and $d = an + bm$ for some n, m in $\mathbb{Z}$. Can we define the g.c.d of any two non-zero polynomials in $F[x]$ similarly? Can the concept of 'relatively prime' also be thought of in $F[x]$? Let's see.

Take any two polynomials, say $x^2 + 3x$ and $x^3 + 27$ in $\mathbb{Q}[x]$. Now, $x^2 + 3x = x(x+3)$ and $x^3 + 27 = (x+3)(x^2 - 3x + 9)$.
So $x + 3$ divides $x^2 + 3$ as well as $x^3 + 27$. Thus, $x + 3$ is a common divisor of both these polynomials, according to the definitions given below.

Definitions: Let F be a field, and let $f(x), g(x)$ be non-zero elements of $F[x]$.

i) $h(x) \in F[x]$ is called a **common divisor** of $f(x)$ and $g(x)$ if $h(x) \mid f(x)$ and $h(x) \mid g(x)$.

ii) $d(x) \in F[x]$ is called the **greatest common divisor** (**g.c.d,** in short) of $f(x)$ and $g(x)$, and denoted by **(f(x), g(x))**, if
D1) $d(x)$ is a common divisor of $f(x)$ and $g(x)$;
D2) whenever $h(x)$ is a common divisor of $f(x)$ and $g(x), h(x) \mid d(x)$;
D3) $d(x)$ is a monic polynomial.

iii) $f(x)$ and $g(x)$ are called **coprime**, or **relatively prime**, if $(f(x), g(x)) = 1$.

For example, $(x^2 + 3x,\ x^3 + 27) = (x + 3)$ in $\mathbb{Q}[x]$, by looking at their factors.

Consider the following remark about the uniqueness of the g.c.d.

Remark 2: Suppose $d(x)$ and $d'(x)$ are two g.c.ds of $f(x)$ and $g(x)$ in $F[x]$, F a field. Then, by $D2$, $d(x)\mid d'(x)$ and $d'(x)\mid d(x)$.

Hence, by Theorem 8, $d(x) = ad'(x)$ for some $a \in F^*$. So if we want $d(x)$ to be unique, we need $a = 1$. This is ensured, by E27, if the condition $D3$ is satisfied. Hence, $D3$ is an essential condition for the g.c.d to be unique.

Now, in the case of $\mathbb{Z}$, you know that any two non-zero integers have a g.c.d. Do any two non-zero polynomials in $F[x]$ have a g.c.d? Let's see.

Theorem 9: Let F be a field. Any two non-zero polynomials over F have a g.c.d. Further, for $f(x), g(x) \in F[x]\setminus\{0\}$,
$(f(x), g(x)) = f(x)r(x) + g(x)s(x)$, for some $r(x), s(x) \in F[x]$.

Proof: Let $f(x), g(x)$ be two non-zero polynomials in $F[x]$. Let S be the set of all **monic** polynomials in $F[x]$ of the form $f(x)r(x) + g(x)s(x)$, with $r(x), s(x) \in F[x]$.

Let a_n be the leading coefficient of $f(x)$.

Then $a_n^{-1}f(x)$ is monic, and $a_n^{-1}f(x) = a_n^{-1}\cdot f(x) + 0\cdot g(x) \in S$.

Thus, $S \neq \emptyset$.

Now consider $A = \{n \in \mathbb{N}\cup\{0\} \mid n = \deg h(x)$ for some $h(x) \in S\}$.

Then $A \neq \emptyset$, since $S \neq \emptyset$. So, by the well-ordering principle, that you studied in Unit 1, A has a least element, say m.

Let $d(x) \in S$ s.t. $\deg d(x) = m$.

Since $d(x) \in S$, $d(x)$ is a monic polynomial and $\exists\ \alpha(x), \beta(x) \in F[x]$ s.t.

$d(x) = f(x)\alpha(x) + g(x)\beta(x)$. …(5)

Now, by the division algorithm applied to $f(x)$ and $d(x)$, $\exists\ q(x)$ and $r(x)$ in $F[x]$ s.t.

$f(x) = d(x)q(x) + r(x)$, …(6)

with $r(x) = 0$ or $\deg r(x) < \deg d(x)$.

Now, suppose $r(x) \neq 0$. Then

$r(x) = f(x) - d(x)q(x)$, from (6).

$= f(x) - [f(x)\alpha(x) + g(x)\beta(x)]q(x)$, from (5).

$= f(x)[1-\alpha(x)q(x)] + g(x)[-\beta(x)q(x)]$.

Let a be the leading coefficient of $r(x)$. Then

$a^{-1}r(x) = f(x)[a^{-1} - a^{-1}\alpha(x)q(x)] + g(x)[-a^{-1}\beta(x)q(x)]$.

Thus, $a^{-1}r(x) \in S$ and $\deg a^{-1}r(x) = \deg r(x) < \deg d(x)$.

This is a contradiction to the way $d(x)$ was chosen.

Therefore, our assumption that $r(x) \neq 0$ must be wrong.

Thus, $r(x) = 0$.

Hence, from (6), $d(x)\mid f(x)$.

Similarly, you can show that $d(x)\mid g(x)$.

Thus, $d(x)$ satisfies $D1$ and $D3$ of the definition of g.c.d.

Now, let $h(x)$ be a common divisor of $f(x)$ and $g(x)$. Then, by E29, $h(x)\,|\,d(x)$. So $d(x)$ satisfies $D2$ of the definition also.

Hence, $d(x)=(f(x),\ g(x))$.

Thus, by (5), $(f(x),\ g(x))=f(x)\alpha(x)+g(x)\beta(x)$, for some $\alpha(x),\ \beta(x)\in F[x]$. ■

In this context, consider the following remark.

Remark 3: Theorem 9 says that $(f(x),\ g(x))$ is that **linear combination** of $f(x)$ and $g(x)$ in $F[x]$ which is monic and of least degree among all such combinations.

Note that not every linear combination of $f(x)$ and $g(x)$ is $(f(x),\ g(x))$. For example, consider (x^3-1) and (x^2+2) in $\mathbb{Q}[x]$. By the division algorithm, $x^3-1=(x^2+2)x+(-2x-1)$.

So $-2x-1=(x^3-1)-x(x^2+2)$, a linear combination of (x^3-1) and (x^2+2) in $\mathbb{Q}[x]$. But $-2x-1$ is neither a divisor of (x^3-1), nor of (x^2+2), in $\mathbb{Q}[x]$.

As in the case of $\mathbb{Z}$, if $f(x)$ and $g(x)$ are relatively prime, we have the following corollary to Theorem 9.

Corollary 2: Let F be a field and let $f(x),\ g(x)\in F[x]\setminus\{0\}$. Then $f(x)$ and $g(x)$ are relatively prime **if and only if** $1=f(x)r(x)+g(x)s(x)$ for some $r(x),\ s(x)\in F[x]$.

Proof: We leave the proof to you (see E30). ■

Theorem 9 tells us that any two non-zero polynomials have a g.c.d. Let us consider an example.

Example 7: Find $(x-5,\ 2x+1)$ in $\mathbb{R}[x]$.

Solution: Since $2(x-5)-(2x+1)=-11$,

$$1=\frac{(-2)}{11}(x-5)+\frac{1}{11}(2x+1).$$

Hence, by Corollary 2, $(x-5,\ 2x+1)=1$.

Thus, $(x-5)$ and $(2x+1)$ are relatively prime in $\mathbb{R}[x]$.

***

Note that the definition of g.c.d can be extended to that of n polynomials.

Definition: Let F be a field and $f_1(x),\ f_2(x),\ldots,f_n(x)$ be non-zero elements of $F[x]$. The **monic** polynomial $g(x)\in F[x]$ is called **the greatest common divisor** of $f_1(x),\ldots,f_n(x)$ if

i) $g(x)\,|\,f_i(x)\ \forall\ i=1,\ldots,n,$ and

ii) whenever $h(x)\,|\,f_i(x)\ \forall\ i=1,\ldots,n,$ then $h(x)\,|\,g(x)$.

Further, as in Theorem 9, the **g.c.d of $\mathbf{f_1(x),\ldots,f_n(x)}$** exists and **is of the form $\sum_{i=1}^{n}\mathbf{f_i(x)h_i(x)}$** for some $h_i(x)\in F[x],\ i=1,\ldots,n$.

For example, the g.c.d of $2x^2 + x(2\sqrt{3}+\sqrt{2}) + \sqrt{6}$, $x^3 + 3\sqrt{3}$ and $7x^4 + 7\sqrt{3}x^3 + 5x^2 + 5\sqrt{3}x \in \mathbb{R}[x]$ is $x+\sqrt{3}$, as $x+\sqrt{3}$ is a common divisor which is monic, and the only other common divisors are elements of $\mathbb{R}^*$.

Now, as in the case of $\mathbb{Z}$, relatively prime polynomials have very useful properties. Let us prove some of them.

Theorem 10: Let F be a field, and let $f(x) \in F[x]$, $f(x) \neq 0$. If $g(x), h(x) \in F[x]$ are relatively prime and both are divisors of $f(x)$, then $g(x)h(x)$ divides $f(x)$.

Proof: We know that $1 = g(x)\alpha(x) + h(x)\beta(x)$ for some $\alpha(x), \beta(x) \in F[x]$.
So $f(x) = f(x)g(x)\alpha(x) + f(x)h(x)\beta(x)$. …(7)
Since $g(x) \mid f(x)$, and $h(x) \mid f(x)$, $f(x) = g(x)r(x)$ and $f(x) = h(x)s(x)$ for some $r(x), s(x) \in F[x]$.
Thus, substituting these values of $f(x)$ in (7), we get

$$\begin{aligned} f(x) &= h(x)s(x)g(x)\alpha(x) + g(x)r(x)h(x)\beta(x) \\ &= g(x)h(x)[s(x)\alpha(x) + r(x)\beta(x)]. \end{aligned}$$

Hence, $g(x)h(x) \mid f(x)$ in $F[x]$. ■

Why don't you prove some related properties now?

E30) Prove Corollary 2.

E31) Prove that if F is a field with $a, b \in F$, $a \neq b$, then $x+a$ and $x+b$ are coprime in $F[x]$.

E32) Give an example, with justification, of a cubic polynomial and a quartic polynomial in $\mathbb{Z}_{13}[x]$ which are coprime.

E33) Let F be a field, and let $f(x), g(x), h(x) \in F[x]$. Prove that

i) if $f(x)$ and $g(x)$ are relatively prime, and $f(x)$ and $h(x)$ are relatively prime, then $f(x)$ and $g(x)h(x)$ are relatively prime.

ii) if $f(x) \neq 0, f(x) \mid g(x)h(x)$ and $(f(x), g(x)) = 1$, then $f(x) \mid h(x)$. (This is analogous to the property for $\mathbb{Z}$ given in Theorem 6, Unit 1.)

Now, if you are asked to find the g.c.d of $(3x^5 - \frac{1}{3}x^4 + 5x^2 + x + \frac{7}{5})$ and $(\frac{2}{7}x^3 - 3x^2 + 1)$ in $\mathbb{Q}[x]$, how would you go about doing it? You may look for common divisors, which won't be easy at all. But, remember the Euclidean Algorithm for $\mathbb{Z}$ in Unit 1? There is a similar algorithm for $F[x]$ too, based on applying the division algorithm multiple times. Let's see what it is, through a simple example, to give you an idea of the method.

Example 8: Find the g.c.d of $(x^3 - 1)$ and $(x^2 - x)$ in $\mathbb{Q}[x]$.

Solution: First, we apply the division algorithm to $(x^3 - 1)$ and $(x^2 - x)$. We get

$$x^3 - 1 = (x^2 - x)(x+1) + (x-1). \qquad \ldots(8)$$

Now we apply the division algorithm to $(x^2 - x)$ and the remainder in (8), i.e., $(x-1)$. We get

$$x^2 - x = (x-1)x + 0. \qquad \ldots(9)$$

We have reached a stage where the remainder is zero. Thus, the divisor polynomial at this stage, i.e., $(x-1)$ is the g.c.d. Note that this polynomial is monic.

***

Note that if the divisor polynomial at the last step in Example 8 had not been monic, we would have multiplied it by the inverse of its leading coefficient to make it monic, and this polynomial would have been the g.c.d.

Now keep this example in mind while going through the following algorithm, which we shall not prove in this course.

Euclidean Algorithm: Let F be a field, and let $f(x)$ and $g(x)$ be two non-zero elements of $F[x]$. Apply the division algorithm in $F[x]$ to $f(x)$ and $g(x)$, then to $g(x)$ and $r_1(x)$, and then to $r_1(x)$ and $r_2(x)$, and so on, till a zero remainder is obtained, as follows:

$f(x) = g(x)q_1(x) + r_1(x)$, with $\deg r_1(x) < \deg g(x)$;

$g(x) = r_1(x)q_2(x) + r_2(x)$, with $\deg r_2(x) < \deg r_1(x)$;

$r_1(x) = r_2(x)q_3(x) + r_3(x)$, with $\deg r_3(x) < \deg r_2(x)$;

$\vdots$

$r_{n-2}(x) = r_{n-1}(x)q_n(x) + r_n(x)$, with $\deg r_n(x) < \deg r_{n-1}(x)$;

$r_{n-1}(x) = r_n(x)q_{n+1}(x)$.

Then $a^{-1}r_n(x)$ is the g.c.d of $f(x)$ and $g(x)$, where a is the leading coefficient of $r_n(x)$. ■

Now that you have some idea of what the Euclidean algorithm is, let us consider some more examples of its application.

Example 9: Find $(f(x), g(x))$, where $f(x) = x^4 + \overline{2}x^3 + x + \overline{2}$ and $g(x) = \overline{2}x^2 + \overline{1}$ in $\mathbb{Z}_3[x]$.

Solution: First, $x^4 + \overline{2}x^3 + x + \overline{2} = (\overline{2}x^2 + \overline{1})(\overline{2}x^2 + x + \overline{2}) + \overline{0}$.

We have obtained $\overline{0}$ as the remainder right in the first step, and the quotient is $\overline{2}x^2 + \overline{1}$. So the g.c.d is $\overline{2}^{-1}(\overline{2}x^2 + \overline{1})$ in $\mathbb{Z}_3[x]$.

Since $\overline{2}^{-1} = \overline{2}$, the g.c.d is $\overline{2}(\overline{2}x^2 + \overline{1})$, i.e., $x^2 + \overline{2}$.

***

Example 10: Find the g.c.d of $f(x) = 2x^5 - 3x + 1$ and $g(x) = 2x^3 + 1$ in $\mathbb{Q}[x]$.

Solution: We apply the division algorithm to $f(x)$ and $g(x)$, and get

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

Next, we apply the division algorithm to $2x^3+1$ and $(-x^2-3x+1)$. We get $2x^3+1=(-x^2-3x+1)(-2x+6)+(20x+7)$.

In this way, we continue applying the division algorithm, as follows.

$$-x^2-3x+1=(20x+7)\left(-\frac{1}{20}x-\frac{53}{400}\right)+\frac{771}{400},$$

$$20x+7=\frac{771}{400}\left(\frac{8000}{771}x+\frac{2800}{771}\right).$$

$\therefore$ The g.c.d is $\left(\frac{771}{400}\right)\left(\frac{771}{400}\right)^{-1}$, as it has to be a monic.

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

***

Why don't you work out the g.c.d in some cases yourself now?

E34) Find the g.c.d of $x^{10}-3x^9+3x^8-11x^7+11x^6-11x^5+19x^4-13x^3+8x^2-9x+3$ and $x^6-3x^5+3x^4-9x^3+5x^2-5x+2$ in $\mathbb{Q}[x]$.

E35) Find the g.c.d of $\overline{4}x^4+\overline{2}x^2-\overline{4}x+\overline{2}$ and $\overline{2}x^2+\overline{2}x-\overline{1}$ in $\mathbb{Z}_5[x]$.

Let us now discuss another property of $F[x]$, akin to a property of $\mathbb{Z}$.

15.5 IDEALS IN POLYNOMIAL RINGS

Let us now discuss the algebraic structure of ideals in $F[x]$, where F is a field. You know that any ideal in $\mathbb{Z}$ is a principal ideal. You also know that this is true for any field. Is the same true for $F[x]$, where F is a field? The answer is yes, as you will now see.

Theorem 11: Every ideal of $F[x]$ is a principal ideal, where F is a field.

Proof: Let I be an ideal of $F[x]$. If $I=\{0\}$, then $I=<0>$, a principal ideal.
So, let $I\neq\{0\}$.
Let $S=\{n\in\mathbb{N}\cup\{0\} \mid \deg f(x)=n$ for some $f(x)\in I\}$.
Since $I\neq\{0\}$, $S\neq\emptyset$. So, by the well-ordering principle, S has a least element, say m, and $\deg g(x)=m$ for some $g(x)\in I$.
So $<g(x)>\subseteq I$.

We will show that $I=<g(x)>$.
For this, let $f(x)\in I$. Then, by the division algorithm, $\exists\ q(x), r(x)\in F[x]$ s.t.
$f(x)=g(x)q(x)+r(x)$, where $r(x)=0$ or $\deg r(x)<\deg g(x)$.
Suppose, if possible, $r(x)\neq 0$. Then
$r(x)=f(x)-g(x)q(x)\in I$, since $f(x), g(x)\in I$.
But $\deg r(x)<\deg g(x)$, which contradicts the way $g(x)$ has been chosen.
Hence, $r(x)\neq 0$ is not possible.
Thus, $r(x)=0$.
Hence, $f(x)\in<g(x)>$, i.e., $I\subseteq<g(x)>$.

Thus, $I = <g(x)>$. ■

Regarding Theorem 11, you must note the important point brought out in it.

Remark 4: Any ideal I in $F[x]$ is generated by a polynomial in it of least degree.

Let us now consider some examples of ideals in $F[x]$.

Example 11: Let S be the set of polynomials over $\mathbb{R}$ with zero constant term. Check whether or not S is a maximal ideal of $\mathbb{R}[x]$.

Solution: Firstly, you should check that $S \neq \emptyset$.
Next, you should check that S is a subring of $\mathbb{R}[x]$. Here, note that for any $f(x) \in S$, $f(x) = a_1x + a_2x^2 + \cdots + a_nx^n = x(a_1 + a_2x + \cdots + a_nx^{n-1})$. Thus, $f(x) \in <x>$.
$\therefore S \subseteq <x>$.

Now, for any $f(x) \in S$ and $g(x) \in \mathbb{R}[x]$,
$f(x)g(x) = x(a_1 + a_2x + \cdots a_nx^{n-1})g(x)$ has no constant term.
Hence, $f(x)g(x) \in S$.
Thus, S is an ideal of $\mathbb{R}[x]$.
Also, $x \in S$, so that $<x> \subseteq S$.

Thus, $S = <x>$.

Next, define $\phi : \mathbb{R}[x] \to \mathbb{R} : \phi\left(\sum_{i=0}^{n} a_ix^i\right) = a_0$.

Then, you should check that ϕ is a well-defined ring homomorphism, $\text{Im}\,\phi = \mathbb{R}$ and $\text{Ker}\,\phi = <x>$.

Thus, by the Fundamental Theorem of Homomorphism, $\mathbb{R}[x]/<x> \simeq \mathbb{R}$, which is a field.
Hence, by Theorem 14 of Unit 14, $<x>$ is a maximal ideal of $\mathbb{R}[x]$, i.e., S is a maximal ideal of $\mathbb{R}[x]$.

***

Example 12: Give an example, with justification, of an ideal in $F[x]$ (F a field), which is

i) a prime ideal but not a maximal ideal;

ii) not a prime ideal.

Solution: i) Does $<0>$ fit the bill? To answer this, check whether or not $F[x]/<0>$ is a domain and/or a field. Here you need to recall, from Unit 13, that $R/<0> \simeq R$ for any ring R.

ii) Consider $I = <x(x+1)>$.
Suppose $x \in I$. Then $x = x(x+1)f(x)$ for some $f(x) \in F[x]$.
So, by cancellation, $(x+1)f(x) = 1$.
Comparing degrees on both sides, we get
$1 + \deg f(x) = 0$.

But $\deg f(x) \geq 0.$ So we reach a contradiction. So $x \notin I.$

Similarly, you should show that $x+1 \notin I.$

Thus, $x(x+1) \in I$ but $x \notin I,\ x+1 \notin I.$

Hence, I is not a prime ideal of $F[x].$

***

Now, you may wonder if Theorem 11 is true for polynomial rings over a domain which is not a field. Consider an example.

Example 13: Show that the ideal $< x, 2 >$ in $\mathbb{Z}[x]$ is not a principal ideal.

Not every ideal in $\mathbb{Z}[x]$ is a principal ideal.

Solution: You know that $\mathbb{Z}[x]$ is a domain, since $\mathbb{Z}$ is a domain. We will show that $< 2, x > \neq < f(x) >$ for any $f(x) \in \mathbb{Z}[x],$ by contradiction.

So, suppose $\exists\, f(x) \in \mathbb{Z}[x]$ such that $< 2, x > = < f(x) >$.

Since $2 \in < f(x) >,\ f(x) \neq 0.$

Also, $\exists\, g(x), h(x) \in \mathbb{Z}[x]$ such that

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

Thus, $\deg f(x) + \deg g(x) = \deg 2 = 0,$ and …(10)

$\deg f(x) + \deg h(x) = \deg x = 1.$ …(11)

(10) shows that $\deg f(x) = 0,$ i.e., $f(x) \in \mathbb{Z}^*,$ say $f(x) = n.$

Then (11) shows that $\deg h(x) = 1.$ Let $h(x) = ax + b,$ with $a, b \in \mathbb{Z},\ a \neq 0.$

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 $\mathbb{Z},$ that is, $n = \pm 1.$

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

$1 = x(a_0 + a_1 x + \cdots + a_r x^r) + 2(b_0 + b_1 x + \cdots + b_s x^s),$ where

$a_i,\ b_j \in \mathbb{Z}\ \forall\ i = 0, 1, \ldots, r$ and $j = 0, 1, \ldots, s.$

Now, on comparing the constant term on either side we see that $1 = 2b_0$. This is not possible, since 2 is not invertible in $\mathbb{Z}.$ So we reach a contradiction. Thus, $< x, 2 >$ is not a principal ideal.

***

Now let us consider another property that $\mathbb{Z}$ and $F[x]$ have in common. This is related to Theorem 11.

Theorem 12: Let F be a field and let $f(x), g(x)$ be non-zero elements of $F[x].$ Then $< f(x), g(x) > = < d(x) >,$ where $d(x) = (f(x), g(x)).$

Proof: By Theorem 11, you know that $< f(x), g(x) > = < h(x) >$ for some $h(x) \in F[x].$ So $f(x) \in < h(x) >$ and $g(x) \in < h(x) >,$

i.e., $h(x) \mid f(x)$ and $h(x) \mid g(x).$

$\therefore h(x) \mid d(x).$ …(12)

Further, since $d(x) \mid f(x)$ and $d(x) \mid g(x),\ d(x)$ divides each element of $< f(x), g(x) >,$ by E29.

$\therefore d(x) \mid h(x).$ …(13)

By (12) and (13), $d(x) = ah(x)$, where $a \in F^*$, applying Theorem 8.

$\therefore < f(x), g(x) > = < a^{-1}d(x) > = < d(x) >$. ■

Theorem 12 is very useful. For instance, from Example 8, you now know that $< x^3 - 1, x^2 - x > = < x - 1 >$ in $\mathbb{Q}[x]$.
Similarly, from Example 9, you know that
$< x^4 + \overline{2}x^3 + x + \overline{2}, \overline{2}x^2 + \overline{1} > = < x^2 + \overline{2} >$ in $\mathbb{Z}_3[x]$.

You should solve some exercises now.

E36) Check whether or not $< x^2 + 1 >$ is a maximal ideal of $\mathbb{C}[x]$.

E37) Find a generator of $< 3x + x^2 + 2, -\frac{1}{2}x^3 + x^5 + 1 >$ in $\mathbb{Q}[x]$. Is this ideal a prime ideal of $\mathbb{Q}[x]$? Why, or why not?

E38) Show that $< x, x^2, x^3, \ldots, x^{n-1}, x^n - 1 > = F[x]$, where $n \geq 2$ and F is a field.

E39) Find $f(x)$ and $g(x)$ in $\mathbb{Z}_{11}[x]$, each of degree ≥ 2, s.t. $< f(x), g(x) > = \mathbb{Z}_{11}[x]$.

With this we come to the end of our introductory discussion on polynomial rings. In the next unit, you shall go a little deeper into this area. You will study about roots and factors of polynomials over a field.

Let us now take a pointwise overview of what has been discussed in this unit.

15.6 SUMMARY

In this unit, you have studied the following points.

1) The definition, and examples, of polynomials over a ring.

2) The ring structure of $R[x]$, the set of polynomials over a ring R.

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) Let F be a field. Then

   i) $F[x]$ is not a field,

   ii) $F(x)$ is the field of fractions of $F[x]$.

6) Let D be an integral domain, with F being its field of fractions. Then the field of fractions of $D[x]$ is $F(x)$, the field of rational functions over F.

7) The division algorithm in $F[x]$, where F is a field. This 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 $f(x) = q(x)g(x) + r(x)$, where $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

8) A polynomial $f(x)$ divides a polynomial $g(x)$ in $F[x]$ iff $f(x)h(x) = g(x)$ for some $h(x) \in F[x]$.

9) Let F be a field. Any two non-zero polynomials over F have a unique g.c.d. Further, for $f(x), g(x) \in F[x] \setminus \{0\}$, $(f(x), g(x)) = f(x)r(x) + g(x)s(x)$, for some $r(x), s(x) \in F[x]$.

10) The Euclidean algorithm to find the g.c.d of two non-zero polynomials in $F[x]$, F a field.

11) Every ideal in $F[x]$ is a principal ideal, where F is a field. This is not true for $D[x]$, where D is a domain but not a field.

12) Let F be a field and let $f(x), g(x)$ be non-zero elements of $F[x]$. Then $< f(x), g(x) > = < d(x) >$, where $d(x) = (f(x), g(x))$.

15.7 SOLUTIONS / ANSWERS

E1) The polynomials are (i), (iii), (iv), (vi), (viii).
(ii) and (v) are not polynomials since they involve negative and fractional powers of x; (vii) is not a polynomial since it has infinitely many non-zero terms.
(i), (vi) and (viii) are in $\mathbb{Z}[x]$.

E2) $a_0 = \frac{1}{2}, b_2 = 5, b_3 = \sqrt{3}, b_1 = 0 = b_4.$

E3) The degrees are $1, 3, 4, 3,$ undefined, respectively.

The leading coefficients of the first four are $\sqrt{2}, -7, 1, \frac{1}{7}$, respectively.

0 has no leading coefficient.

E4) You have seen that addition in $R[x]$ is well-defined. Further, If

$$f(x) = \sum_{i=0}^{n} a_i x^i,\ g(x) = \sum_{i=0}^{m} b_i x^i, \text{ then } f(x) + g(x) = \sum_{i=0}^{\max(n, m)} (a_i + b_i) x^i,$$

a finite sum.
Since $a_i, b_i \in R$, $a_i + b_i \in R\ \forall\ i = 0, 1, \ldots, \max(n, m)$.
$\therefore f(x) + g(x) \in R[x]$.

As for addition, if $f(x) = f'(x)$ and $g(x) = g'(x)$ in $R[x]$, show why $f(x) \cdot g(x) = f'(x) \cdot g'(x)$, i.e., multiplication is well-defined.

Then, explain why $f(x) \cdot g(x) \in R[x]$ if $f(x), g(x) \in R[x]$.

E5) i) $2 + 5x + 3x^2 + (4+1)\,x^3 = 2 + 5x + 3x^2 + 5x^3.$

ii) $(\overline{6}+\overline{1})-\overline{2}x+\overline{2}x^2+\overline{5}x^3=-\overline{2}x+\overline{2}x^2+\overline{5}x^3$, since $\overline{7}=\overline{0}$.
$=\overline{5}x+\overline{2}x^2+\overline{5}x^3$, since $-\overline{2}=\overline{5}$.

iii) $(1\cdot 1)+(1\cdot 2+1\cdot 1)x+(1\cdot 1+1\cdot 2+0\cdot 1)x^2=1+3x+3x^2+x^3.$

iv) $\overline{1}+x^3$, since $\overline{3}=\overline{0}$.

v) $10x+5x^2+7x^3+x^4+x^5.$

E6) Each term, a_ix^i, is a finite sum, and $a_i\in R$. Thus, $a_ix^i\in R[x]$.

E7) i) True; for instance, $(\overline{2}x)(\overline{3}x+1)=\overline{0}\cdot x^2+\overline{2}x=\overline{2}x$ in $\mathbb{Z}_6[x]$.

ii) True. Let $f(x)=a+bx+cx^2$ and $g(x)=p+qx+rx^2$ be in $\mathbb{Q}[x]$, where $c\neq 0$, $r\neq 0$. As $\mathbb{Q}$ is a field, $cr\neq 0$.
Also, the highest degree term is crx^4.
Thus, $f(x)g(x)$ is a quartic polynomial.

iii) False; for example, if $f(x)=a+bx+cx^2\in\mathbb{C}[x]$, then $f(x)+(-f(x))=0$, not a quadratic polynomial.

iv) False; for example, if $p(x)=x$ and $q(x)=2x^2$ in $\mathbb{Z}[x]$, then $p(x)$ is a monic polynomial but $p(x)+q(x)$ has leading coefficient 2.

E8) There are infinitely many such pairs. One is $f(x)=\begin{bmatrix}1&0\\0&0\end{bmatrix}x$ and

$g(x)=\begin{bmatrix}1&2\\3&4\end{bmatrix}x$ over $\mathbb{M}_2(\mathbb{C})$.

Since both $f(x)$ and $g(x)$ are linear, with different leading coefficients, they are distinct.

E9) i) R can be thought of as the set of constant polynomials and 0 in $R[x]$. So, $R\subset R[x]$.
Also, both R and $R[x]$ are rings w.r.t. the same operations.
Thus, R is a subring of $R[x]$.

ii) This is not true.
For example, let $R=\mathbb{Z}$ and take $x\in\mathbb{Z}[x]$.
Then $rx\notin\mathbb{Z}$ for any $r\in\mathbb{Z}^*$.
Hence, $\mathbb{Z}$ is not an ideal of $\mathbb{Z}[x]$.

E10) $\mathbb{Z}_4=\{\overline{0},\ \overline{1},\ \overline{2},\ \overline{3}\}$.

Any quadratic polynomial over $\mathbb{Z}_4$ is of the form $a_0+a_1x+a_2x^2$, where $a_0,\ a_1,\ a_2\in\mathbb{Z}_4$.
Thus, there are $4\times 4\times 3=48$ possibilities.
You should list them all for practice in working with such polynomials.

E11) No. For example, let $R=\mathbb{Q}$ and $n=1$.

Then $1+x\in\wp_1$, but $(1+x)^2\notin\wp_1$. Hence, $\wp_1$ is not a ring, and hence, not a subring of $\mathbb{Q}[x]$.

E12) Note that if $f(x)\in A$, then $f(x)=\sum_{i=0}^{n}a_ix^{2i}$, since the coefficient of x^{2i-1} is $0\ \forall\ i\in\mathbb{N}$.

Also, $f(x)\in A\Rightarrow -f(x)\in A$. (Why?)

Now, let $f(x)=\sum_{i=0}^{n}a_ix^{2i}$, $g(x)=\sum_{i=0}^{m}b_ix^{2i}$.

Then you should check that the odd power coefficients of $f(x)-g(x)$ and $f(x)g(x)$ will also be zero.

Hence, $f(x)-g(x)\in A$ and $f(x)g(x)\in A$.

Thus, A is a subring of $R[x]$.

E13) i) R is a subring of $R[x]$. Therefore, multiplication in R is also commutative.

ii) The identity of $R[x]$ is an element of R, and hence, is the identity of R.

E14) Let $f(x)\in R[x]$ be a unit. Then $\exists\ g(x)\in R[x]$ s.t. $f(x)g(x)=1$. So $\deg f(x)+\deg g(x)=\deg 1=0$.

Since $\deg f(x)\geq 0$, $\deg g(x)\geq 0$, we get $\deg f(x)=0$, $\deg g(x)=0$.

So $f(x)\in R$ and is a unit. Thus, $U(R[x])\subseteq U(R)$.

Of course, since R is a subring of $R[x], U(R)\subseteq U(R[x])$.

Thus, $U(R)=U(R[x])$.

E15) (i) and (ii), as $\mathbb{Z}[\sqrt{-5}]$ and $\mathbb{Z}_7$ are domains.

In Unit 14, you have seen that $\mathbb{M}_2(\mathbb{Q})$, $C[0,1]$ and $\wp(X)$ have zero divisors. Hence, the rings in (iii), (iv) and (v) have zero divisors.

E16) Let $f(x)=\sum_{i=0}^{n}a_ix^i$, $g(x)=\sum_{i=0}^{m}b_ix^i\in I[x]$ and $h(x)=\sum_{j=0}^{t}c_jx^j\in R[x]$.

Then $f(x)-g(x)=f(x)+(-g(x))=\sum_{i=0}^{\max(m,\,n)}(a_i-b_i)x^i\in I[x]$, and

$$f(x)h(x)=\sum_{i=0}^{n+t}(a_ic_0+a_{i-1}c_1+\cdots+a_0c_i)x^i\in I[x],$$

since I is an ideal of R.

Similarly, $h(x)f(x)\in I[x]$.

Hence, $I[x]$ is an ideal of $R[x]$.

Let us define $\phi: R[x]\to(R/I)[x]:\phi\left(\sum_{i=0}^{n}a_ix^i\right)=\sum_{i=0}^{n}\bar{a}_ix^i$, where $\bar{a}=a(\text{mod}\, I)\ \forall\ a\in R$.

ϕ is well-defined: Let $\sum_{i=0}^{n}a_ix^i=\sum_{i=0}^{m}b_ix^i$ in $R[x]$. Then $n=m$ and $a_i=b_i\ \forall\ i=0,1,\ldots,n$.

So $\bar{a}_i = \bar{b}_i \ \forall\ i = 0,\ldots,n.$

$$\therefore \sum_{i=0}^{n} \bar{a}_i x^i = \sum_{i=0}^{m} \bar{b}_i x^i \text{ in } (R/I)[x].$$

ϕ **is a ring homomorphism:** Let $f(x) = \sum_{i=0}^{n} a_i x^i,\ g(x) = \sum_{i=0}^{m} b_i x^i.$

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

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

$$= \left(\sum_{i=0}^{n} \bar{a}_i x^i\right) + \left(\sum_{i=0}^{m} \bar{b}_i x^i\right)$$

$$= \phi(f(x)) + \phi(g(x)), \text{ and}$$

$\phi(f(x)g(x)) = \phi\left(\sum_{i=0}^{r} c_i x^i\right)$, where $r = m + n$ and $c_k = \sum_{i=0}^{k} a_i b_{k-i}.$

$$= \sum_{i=0}^{r} \bar{c}_i x^i$$

$$= \sum_{i=0}^{r} (\bar{a}_i \bar{b}_0 + \bar{a}_{i-1} \bar{b}_1 + \cdots + \bar{a}_0 \bar{b}_i) x^i$$

$$= \left(\sum_{i=0}^{n} \bar{a}_i x^i\right)\left(\sum_{i=0}^{m} \bar{b}_i x^i\right)$$

$$= \phi(f(x))\phi(g(x)).$$

ϕ **is onto:** For any $h(x) = \sum_{i=0}^{n} \bar{a}_i x^i \in (R/I)[x],$

$\exists\ f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$ s.t. $\phi(f(x)) = h(x).$

Thus, $\operatorname{Im} \phi = (R/I)[x].$

$$\textbf{Ker } \boldsymbol{\phi} = \left\{ \sum_{i=0}^{n} a_i x^i \in R[x] \,\middle|\, \sum_{i=0}^{n} \bar{a}_i x^i = \bar{0} \right\}$$

$$= \left\{ \sum_{i=0}^{n} a_i x^i \in R[x] \,\middle|\, \bar{a}_i = \bar{0}\ \forall\ i = 0,\ldots,n \right\}$$

$$= \left\{ \sum_{i=0}^{n} a_i x^i \in R[x] \,\middle|\, a_i \in I\ \forall\ i = 0,\ldots,n \right\}$$

$$= I[x].$$

Now apply FTH to get the result.

E17) Let $r \in R^*$. Suppose $r \in \langle x \rangle$. Then $r = xf(x)$ for some $f(x) \in R[x]$. $\therefore 0 = \deg r = \deg x + \deg f(x) \geq 1$, a contradiction. Hence, $\langle x \rangle \neq R[x]$.

Suppose $\langle x \rangle = I[x]$, for some proper ideal I of R.

Let $a \in R \setminus I$. Then $ax \in \langle x \rangle = I[x]$, a contradiction.

Thus, $\langle x \rangle \neq I[x]$.

E18) Let $\text{char } R = n.$ By Theorem 3 of Unit 14, you know that n is the least positive integer such that $n \cdot 1 = 0.$ Since 1 is also the identity of $R[x]$, the same theorem of Unit 14 tells you that $\text{char } R[x] = n = \text{char } R.$

E19) Let $p(x) = a_0 + a_1 x + \cdots + a_n x^n$, $q(x) = b_0 + b_1 x + \cdots + b_m x^m \in R[x].$

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, $\phi(p(x) \cdot q(x)) = \phi\left(\sum_{i=0}^{m+n} c_i x^i\right)$, where $c_i = a_i b_0 + a_{i-1} b_1 + \cdots + a_0 b_i.$

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

$= \sum_{i=0}^{m+n} [f(a_i) f(b_0) + f(a_{i-1}) f(b_1) + \ldots + f(a_0) f(b_i)] x^i,$ since f is a ring homomorphism.

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

Thus, ϕ is a homomorphism.

Now, if f is an isomorphism, then for any $h(x) = \sum_{i=0}^{n} a_i x^i \in S[x],$

$h(x) = \sum_{i=0}^{n} f(b_i) x^i,$ where $a_i = f(b_i) \; \forall \; i$ as f is onto.

$$= \phi\left(\sum_{i=0}^{n} b_i x^i\right).$$

Thus, $\text{Im } \phi = S[x].$

Show that $\text{Ker } \phi = (\text{Ker } f)[x] = \{0\},$ as f is $1\text{-}1.$
Thus, ϕ is an isomorphism.

E20) First, show that ϕ is well-defined.

Next, if $f(x) = \sum_{i=0}^{n} (a_i, r_i) x^i$ and $g(x) = \sum_{i=0}^{m} (b_i, s_i) x^i$ in $(R \times S)[x],$ then

$$\phi(f(x) + g(x)) = \phi\left(\sum_{i=0}^{t} [(a_i, r_i) + (b_i, s_i)] x^i\right), \; t = \max(m, n)$$

$$= \phi\left(\sum_{i=0}^{t} (a_i + b_i, r_i + s_i) x^i\right)$$

$$= \left(\sum_{i=0}^{t} (a_i + b_i) x^i, \sum_{i=0}^{t} (r_i + s_i) x^i \right)$$

$$= \left(\sum_{i=0}^{t} a_i x^i, \sum_{i=0}^{t} r_i x^i \right) + \left(\sum_{i=0}^{t} b_i x^i, \sum_{i=0}^{t} s_i x^i \right)$$

$$= \phi(f(x)) + \phi(g(x)).$$

Similarly, show that $\phi(f(x)g(x)) = \phi(f(x))\phi(g(x))$.

Next, let $(f(x), g(x)) \in R[x] \times S[x]$, where $\deg f(x) = n$ and $\deg g(x) = m$. Suppose $m \geq n$.

Then, $f(x) = \sum_{i=0}^{m} a_i x^i, g(x) = \sum_{i=0}^{m} b_i x^i$, where $a_i = 0$ for $i > n$.

Then $\phi\left(\sum_{i=0}^{m} (a_i, b_i) x^i \right) = (f(x), g(x))$.

Thus, ϕ is onto.

$$\text{Ker } \phi = \left\{ \sum_{i=0}^{n} (a_i, b_i) x^i \in (R \times S)[x] \,\middle|\, a_i = 0 = b_i \;\forall\; i = 0, \ldots, n \right\}$$

$$= \{0\}.$$

Thus, ϕ is an isomorphism.

$\therefore (R \times S)[x] \simeq R[x] \times S[x]$.

E21) i) The quotient field of $\mathbb{Z}[i]$ is $\left\{ \frac{a + ib}{c + id} \,\middle|\, a, b, c, d \in \mathbb{Z}, c + id \neq 0 \right\}$.

Now $\frac{a + ib}{c + id} = \frac{(a + ib)(c - id)}{c^2 + d^2} = p + iq$, for some $p, q \in \mathbb{Q}$.

Thus, the quotient field of $\mathbb{Z}[i]$ is $\mathbb{Q}[i]$.

$\therefore$ The quotient field of $\mathbb{Z}[i][x]$ is $\mathbb{Q}[i](x)$.

ii) $\mathbb{Q}[\sqrt{11}]$ is a field, as you have shown in Unit 14.

$\therefore \mathbb{Q}[\sqrt{11}](x)$ is the required field.

iii) $\mathbb{Z}_p(x)$.

E22) Any element α of $\mathbb{C}[x]$ is also in $\mathbb{C}(x)$. Apart from these elements, there are the elements like

$(a_0 + a_1 x + \cdots + a_n x^n)(b_0 + b_1 x + \cdots + b_m x^m)^{-1}$, where $\sum_{i=0}^{m} b_i x^i \neq 0$,

$a_i, b_j \in \mathbb{C} \;\forall\; i = 1, \ldots n;\; j = 1, \ldots, m$.

Pick any two, and show why they are distinct.

E23) In E18 you have proved that $\text{char } \mathbb{Z}_p[x] = \text{char } \mathbb{Z}_p = p$.

Now consider $\mathbb{Z}_p(x)$. The identity is $\overline{1}$, where $p \cdot \overline{1} = \overline{0}$.

Thus, $\text{char } \mathbb{Z}_p(x) = p$.

Also, $\mathbb{Z}_p(x)$ is infinite, as $\mathbb{Z}_p[x]$ is infinite.

E24) i)

$$\begin{array}{rl}
 & -x \\
-x^3+\frac{1}{7}\,\big) & \overline{x^4+1} \\
 & x^4-\frac{1}{7}x \\
\hline
 & \qquad \frac{1}{7}x+1
\end{array}$$

We stop here since $\deg\left(\frac{1}{7}x+1\right)<\deg\left(-x^3+\frac{1}{7}\right)$.

So $f(x)=(-x)g(x)+\left(\frac{1}{7}x+1\right)$.

Here $q(x)=-x$ and $r(x)=\frac{1}{7}x+1$.

ii)

$$\begin{array}{rll}
 & \bar{2}x^2 \qquad +\bar{1} & \\
\bar{2}x+\bar{1}\,\big) & \overline{x^3+\bar{2}x^2-x+\bar{1}} & \\
 & x^3+\bar{2}x^2 & \text{(since } \bar{4}=\bar{1} \text{ here)} \\
\hline
 & \qquad\qquad -x+\bar{1} & \\
 & \qquad\qquad \bar{2}x+\bar{1} & \\
\hline
 & \qquad\qquad\quad \bar{0} & \text{(since } -\bar{1}=\bar{2} \text{ here)}
\end{array}$$

Thus, $f(x)=(\bar{2}x^2+\bar{1})\,g(x)$.
$\therefore g(x)\,|\,f(x)$.

iii) $f(x)=(x^2+\sqrt{3}x+3)\,g(x)$.
$\therefore g(x)\,|\,f(x)$.

E25) ii) Since $f(x)=1\cdot f(x)$ and $1\in F[x], f(x)\,|\,f(x)$.

iii) $f(x)\,|\,g(x)\Rightarrow \exists\ p(x)\in F[x]$ s.t. $g(x)=f(x)p(x)$

$\Rightarrow ag(x)=af(x)p(x),$ for any $a\in F^*$.

$\Rightarrow af(x)\,|\,ag(x)$.

iv) $g(x)=f(x)p(x)$ and $h(x)=g(x)q(x)$ for some $p(x), q(x)\in F[x]$.
$\therefore h(x)=f(x)p(x)q(x),$ and $p(x)q(x)\in F[x]$.
Thus, $f(x)\,|\,h(x)$.

vi) $g(x)=f(x)p(x)$ and $h(x)=f(x)q(x)$ for some $p(x), q(x)\in F[x]$.
So $g(x)+h(x)=f(x)\,(p(x)+q(x)),$ and $p(x)+q(x)\in F[x]$.
$\therefore f(x)\,|\,(g(x)+h(x))$.

vii) $g(x)=f(x)p(x)$ for some $p(x)\in F[x]$.
$\therefore g(x)h(x)=f(x)p(x)h(x),$ and $p(x)h(x)\in F[x]$.
$\therefore f(x)\,|\,g(x)h(x)$.

E26) The difference between $F[x]$ and $R[x]$ lies in their units. But nowhere in the proofs have we applied the fact that every element of F^* is a unit, except in (v). This can be written as:

'If $g(x)$ is s.t. $g(x) \neq 0,\ f(x) \mid g(x)$ and $g(x) \mid f(x),$ then $f(x) = ag(x),$ for some $a \in U(R)$.'

E27) By E26, $f(x) = ag(x)$ for some $a \in U(R)$.
Thus, $\deg f(x) = \deg g(x)$.
Since the leading coefficients of $f(x)$ and $g(x)$ are $1,\ a = 1$.
Thus, $f(x) = g(x)$.

E28) ~ is not symmetric. For example, $(x-2) \mid (x^2-4)$ in $\mathbb{Q}[x],$ but $(x^2-4) \nmid (x-2)$. (Why?)

E29) Use (vi) and (vii) of Theorem 8 to prove this.

E30) If $f(x)$ and $g(x)$ are relatively prime, $(f(x), g(x)) = 1$. So $1 = f(x)r(x) + g(x)s(x),$ for some $r(x), s(x) \in F[x]$.

Conversely, we know that 1 is a linear combination of $f(x)$ and $g(x)$.
Let $d(x) = (f(x), g(x))$.
Since $d(x) \mid f(x)$ and $d(x) \mid g(x),$
$d(x) \mid (f(x)r(x) + g(x)s(x)),$ i.e., $d(x) \mid 1,$ by E29.
$\therefore \deg d(x) = 0$.
Also, $d(x)$ is monic.
Hence, $d(x) = 1$.

E31) $1 = \frac{1}{(a-b)}(x+a) - \frac{1}{(a-b)}(x+b)$. Hence, by Corollary 2, they are coprime.

E32) e.g., $f(x) = x^3, g(x) = x^4 + \overline{1}$.
Since $(-x)f(x) + g(x) = \overline{1}, (f(x), g(x)) = \overline{1}$.
There can be several other examples. Look for some more.

E33) i) $1 = f(x)r(x) + g(x)s(x)$ …(14)

$1 = f(x)p(x) + h(x)q(x)$ …(15)

for some $r(x), s(x), p(x), q(x) \in F[x]$.
From (15), we get
$g(x) = f(x)g(x)p(x) + g(x)h(x)q(x)$.
So, putting this in (14), we get
$1 = f(x)[r(x) + g(x)p(x)s(x)] + g(x)h(x)q(x)s(x)$
$\therefore (f(x), g(x)h(x)) = 1$.

ii) $1 = f(x)r(x) + g(x)s(x)$ …(16)

for some $r(x), s(x) \in F[x]$.
Also $g(x)h(x) = f(x)p(x)$ …(17)

for some $p(x) \in F[x]$.

Now, from (16), we get

$$h(x) = f(x)h(x)r(x) + g(x)h(x)s(x)$$

$= f(x)h(x)r(x) + f(x)p(x)s(x)$, from (17).

$= f(x)\alpha(x)$, where $\alpha(x) = h(x)r(x) + p(x)s(x) \in F[x]$.

$\therefore f(x) \big| h(x)$.

E34) $x^{10} - 3x^9 + 3x^8 - 11x^7 + 11x^6 - 11x^5 + 19x^4 - 13x^3 + 8x^2 - 9x + 3$

$= (x^6 - 3x^5 + 3x^4 - 9x^3 + 5x^2 - 5x + 2)(x^4 - 2x) + (-x^4 - 3x^3 - 2x^2 - 5x + 3)$.

Then, $x^6 - 3x^5 + 3x^4 - 9x^3 + 5x^2 - 5x + 2$

$= (-x^4 - 3x^3 - 2x^2 - 5x + 3)(-x^2 + 6x - 19) + (-59x^3 - 118x + 59)$.

Next, $-x^4 - 3x^3 - 2x^2 - 5x + 3 = (-59x^3 - 118x + 59)\left(\frac{1}{59}x + \frac{3}{59}\right)$.

$\therefore$ the required g.c.d is $-\frac{1}{59}(-59x^3 - 118x + 59)$, since the g.c.d has to be monic.

Thus, the g.c.d is $(x^3 + 2x - 1)$.

E35) $f(x) = \overline{4}x^4 + \overline{2}x^2 + x + \overline{2}$, $g(x) = \overline{2}x^2 + \overline{2}x + \overline{4}$, since $-\overline{1} = \overline{4}$.

$\overline{4}x^4 + \overline{2}x^2 + x + \overline{2} = (\overline{2}x^2 + \overline{2}x + \overline{4})(\overline{2}x^2 + \overline{3}x + \overline{4}) + (x + \overline{3})$,

$\overline{2}x^2 + \overline{2}x + \overline{4} = (x + \overline{3})(\overline{2}x + \overline{1}) + \overline{1}$,

$(x + \overline{3}) = \overline{1}(x + \overline{3})$.

$\therefore (f(x), g(x)) = \overline{1}$.

E36) $x^2 + 1 = (x + i)(x - i)$ in $\mathbb{C}[x]$.

So $x^2 + 1 \in < x + i > \subsetneq \mathbb{C}[x]$, since $1 \notin < x + i >$.

Suppose $x + i \in < x^2 + 1 >$.

Then $(x + i) = (x^2 + 1)f(x)$, for some $f(x) \in \mathbb{C}[x]$.

So $1 = \deg\,(x + i) = \deg\,(x^2 + 1) + \deg\, f(x) \geq 2$, which is a contradiction.

Thus, $x + i \notin < x^2 + 1 >$.

$\therefore < x^2 + 1 > \neq < x + i >$.

$\therefore < x^2 + 1 > \subsetneq < x + i > \subsetneq \mathbb{C}[x]$.

$\therefore < x^2 + 1 >$ is not a maximal ideal of $\mathbb{C}[x]$.

E37) You should check that $x^2 + 3x + 2$ and $x^5 - \frac{1}{2}x^3 + 1$ are coprime.

$\therefore < 3x + x^2 + 2, -\frac{1}{2}x^3 + x^5 + 1 > = < 1 > = \mathbb{Q}[x]$.

Thus, the given ideal is not a proper ideal, and hence, it is not a prime ideal.

E38) The g.c.d of $x, x^2, \ldots, x^{n-1}$ is x.

$\therefore$ the g.c.d of $x, x^2, \ldots, x^{n-1}, x^n - 1$ is the g.c.d of $x, x^n - 1$, which is 1

(because $x \cdot x^{n-1} - (x^n - 1) = 1$).

$\therefore < x, x^2, \ldots, x^{n-1}, x^n - 1 > = < 1 > = F[x]$.

E39) There can be several answers. Ours is $x^2 + \overline{10},$ and $x^2.$

Here $\overline{1} = (\overline{10})^{-1}(x^2 + \overline{10} - x^2).$

Hence, $x^2 + \overline{10}$ and x^2 are co-prime.

$\therefore < x^2 + \overline{10},\ x^2 > \, = \, < \overline{1} > \, = \mathbb{Z}_{11}[x].$

UNIT 16

ROOTS AND FACTORS OF POLYNOMIALS

16.1 INTRODUCTION

In the previous unit, you have worked with polynomials over different rings. You have also studied the division algorithm in $\mathrm{F}[x]$, where F is a field. In this context, you have worked with quotients, remainders and the idea of one polynomial dividing another. In this unit, we will help you take this understanding further. Note that **throughout this unit, a ring is assumed to be commutative**.

In Sec.16.2, you will study what a root of a polynomial is, and how this is related to a factor of a polynomial. You will also see how the degree of a polynomial is related to the number of roots it has. This follows from the remainder theorem, as you will see.

In the next section, Sec.16.3, you will be introduced to the idea of reducible and irreducible polynomials over a field, F. Here you will see that an irreducible polynomial in $\mathrm{F}[x]$ generates a maximal ideal of $\mathrm{F}[x]$. You will also see that irreducible elements of $\mathrm{F}[x]$ are precisely the prime elements of $\mathrm{F}[x]$.

Next, in Sec.16.4, you will study the criteria for a polynomial over $\mathrm{F}[x]$ to be irreducible, when F is $\mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$. For example, you will discover that an irreducible polynomial over $\mathbb{Q}$ can be of any degree, while over $\mathbb{C}$ it must be of degree 1.

In Unit 15, you have seen that there is much similarity in the properties of integers and the properties of polynomials over a field. In Sec.16.5, we will consider another such similarity, namely, unique factorisation. You will find that irreducible polynomials over a field play the role that prime numbers play in $\mathbb{Z}$. In this section, you will also study some consequences of unique factorisation in $F[x]$.

This unit has been created keeping the following expected learning goals in mind. Please go through it carefully, solving every exercise as you come to it.

Objectives

After studying this unit, you should be able to:

- define, and give examples of, a root (or a zero) of a polynomial over a commutative ring R;
- state, prove and apply the remainder theorem;
- define, and give examples of, a factor of a polynomial corresponding to a root of the polynomial;
- define, and give examples of, irreducible elements and prime elements of $F[x]$, where F is a field;
- apply the various criteria to decide whether a given polynomial over $\mathbb{C}, \mathbb{R}$ or $\mathbb{Q}$ is irreducible or not;
- state, prove and apply the unique factorisation theorem for $F[x]$, where F is a field.

16.2 ROOTS

In Calculus, as well as in school mathematics, you have been finding roots of polynomials. For example, you know that if $x+1=0$, then $x=-1$. So (-1) is a root of the polynomial $x+1$. Similarly, you know that if ax^2+bx+c is a quadratic polynomial over $\mathbb{C}$, then its roots are given by the quadratic formula: $\frac{-b\pm\sqrt{b^2-4ac}}{2a}$. To generalise this concept, let us formally define a term for a process you have used several times before.

Definition: Let R be a ring and let $f(x)=a_0+a_1x+\cdots+a_nx^n\in R[x]$. Then for any $r\in R$, we define $f(r)=a_0+a_1r+\cdots+a_nr^n\in R$ to be the **value of $f(x)$ obtained by substituting r for x**.

Thus, if $f(x)=1+x+x^2\in\mathbb{Z}[x]$, then $f(2)=1+2+4=7$, and $f(0)=1+0+0=1$.

Now let us define a root, in general.

Definition: Let R be a ring. An element r in R is called a **root** (or a **zero**) of $f(x)\in R[x]$ if $f(r)=0$.

For example, if $f(x)=12-2x-2x^2$ in $2\mathbb{Z}[x]$, then $f(2)=12-4-8=0$.

So 2 is a root of $12-2x-2x^2$ in $2\mathbb{Z}$.
Also, since $f(-2)=12+4-8\neq 0$, (-2) is not a root of $12-2x-2x^2$ in $2\mathbb{Z}$.

As another example, if $f(x)=2x^3+(1-2\pi)x^2+(5-\pi)x-5\pi\in\mathbb{R}[x]$, then $f(\pi)=0$. So, π is a zero of $f(x)$ in $\mathbb{R}$.

For polynomials over a field F, the concept of a root is closely related to the division algorithm in $F[x]$. To see how, consider the following important theorem, which is actually a corollary of the division algorithm given in Unit 15.

Theorem 1 (Remainder Theorem): Let F be a field. If $f(x)\in F[x]$ and $b\in F$, then there exists a 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 $g(x)$, there exist unique $q(x)$ and $r(x)$ in $F[x]$, such that

$$\begin{aligned} f(x) &= q(x)g(x)+r(x) \\ &= q(x)(x-b)+r(x), \text{ where } r(x)=0 \text{ or } \deg r(x)<\deg g(x)=1. \end{aligned}$$

So $r(x)=0$ or $r(x)$ is an element of F^*.
Thus, $r(x)=a$, for some $a\in F$.
So, $f(x)=(x-b)q(x)+a$.
Substituting b for x, we get
$f(b)=(b-b)q(b)+a=0\cdot q(b)+a=a$.
Thus, $a=f(b)$.
Therefore, $f(x)=(x-b)q(x)+f(b)$.
Thus, the remainder is the value of $f(x)$ when we substitute b for x. ■

Note that in Theorem 1, $\deg f(x)=\deg\,(x-b)+\deg q(x)=1+\deg q(x)$.
Therefore, $\deg q(x)=\deg f(x)-1$.

An immediate corollary to Theorem 1 is the following.

Corollary 1: Let F be a field and let $f(x)\in F[x]$, with $\deg f(x)\geq 1$. Then $a\in F$ is a root of $f(x)$ iff $(x-a)\mid f(x)$.

Proof: We leave the proof to you as an exercise (see E1). ■

Let's see how Corollary 1 is useful. For example, you now know that $x(x+1)\in\mathbb{Z}[x]$ has 0 and 1 as its only roots since x and $x+1$ are its only linear factors.

As another example, consider $f(x)=6x^2-x-1\in\mathbb{Q}[x]$. By the quadratic formula, you know that its roots are $\frac{1}{2}$ and $\frac{-1}{3}$. Thus, $(x-\frac{1}{2})$ and $(x+\frac{1}{3})$ are factors of $f(x)$, by Corollary 1.

Now, since 2 is a unit in $\mathbb{Q}$, $(x-\frac{1}{2})=(2^{-1})2(x-\frac{1}{2})$. So $2(x-\frac{1}{2})$ is also a factor of $f(x)$, i.e., $(2x-1)$ is a factor of $f(x)$.
Similarly, $(3x+1)$ is a factor of $f(x)$.
Did you notice that both these factors of $f(x)$ are in $\mathbb{Z}[x]$?

Now consider $(x-1)^2(x-2) \in \mathbb{Q}[x]$. Here $(x-1)$ is a double factor. So, 1 is twice a root of this polynomial. This is an example of what we shall now define.

Definition: Let R be a ring and $f(x) \in R[x]$. We say that $a \in R$ is a **root of multiplicity $\mathbf{m}$** of $f(x)$, $m \in \mathbb{N}$, if
$(x-a)^m \mid f(x)$, but $(x-a)^{m+1} \nmid f(x)$.

For example, 3 is a root of multiplicity 2 of the polynomial $(x-3)^2(x+2) \in \mathbb{Q}[x]$, and (-2) is a root of multiplicity 1 of this polynomial.

Now you should solve some exercises.

E1) Prove Corollary 1.

E2) Find the roots of the following polynomials, along with their multiplicities.

i) $\frac{1}{2}x^2 - \frac{5}{2}x + 3 \in \mathbb{Q}[x]$,

ii) $x^2 + x + \overline{1} \in \mathbb{Z}_3[x]$,

iii) $x^4 + \overline{2}x^3 - \overline{2}x - \overline{1} \in \mathbb{Z}_5[x]$,

iv) $(5x+3)^2(\sqrt{2}-4x)^3(ix+1-\sqrt{3}i)^{11} \in \mathbb{C}[x]$.

E3) Give an example of a polynomial over $\mathbb{Z}_{11}$ which has only two distinct roots, of multiplicity 3 and 2, respectively. Justify your choice of example.

E4) 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 map at $\mathbf{a}$**, as you know from Unit 13.) Show that

i) ϕ is an onto ring homomorphism,

ii) $\phi(b) = b \ \forall \ b \in F$,

iii) $\text{Ker } \phi$ is the set of all polynomials in $F[x]$ having a as a zero. Further, find a generator for $\text{Ker } \phi$.

What does the Fundamental Theorem of Homomorphism say in this case?

E5) Let F be a field. Prove that $F[x]/_{<x-a>} \simeq F[x]/_{<x>} \ \forall \ a \in F^*$.

E6) Let F be a field, and let $a \in F^*$ be a root of $a_0 + a_1x + \cdots + a_nx^n \in F[x]$.
Show that a^{-1} is a root of $a_n + a_{n-1}x + \cdots + a_0x^n \in F[x]$.
Will this still be true if F is replaced by a domain D which is not a field? Why?

Let us now look at how we can obtain all the roots of a given polynomial in $F[x]$. As you know, this is possible for a linear, or a quadratic, polynomial. For polynomials of higher degree we may be able to obtain some by trial-and-error, as you have done in E2(iii).

As another example, consider $f(x) = x^5 - 2x + 1 \in \mathbb{R}[x].$ We try replacing x by $1,$ and find $f(1) = 0.$ So, we find that 1 is a zero of $f(x).$ But this method may not give us all the roots of $f(x)$ in $\mathbb{R}.$

Also, note that a polynomial in $F[x]$ may have no zero in $F.$ (For example, $x^2 + 1 \in \mathbb{R}[x]$ has no zero in $\mathbb{R},$ since its zeros are i and $-i,$ both in $\mathbb{C} \setminus \mathbb{R}.$) However, we can give an upper bound for the **number of roots** in F of a polynomial in $F[x].$

Theorem 2: A non-zero polynomial of degree n over a field F has at the most n roots in $F.$

Proof: If $n = 0,$ then any polynomial of degree 0 is a non-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 $n.$
For $n \in \mathbb{N},$ let $P(n)$ be the predicate, 'If $f(x) \in F[x]$ is of degree $n,$ then $f(x)$ has at most n roots in F'.
We will first check whether the statement $P(1)$ is true or not.
If $f(x) \in F[x]$ s.t. $\deg f(x) = 1,$ then $f(x) = a_0 + a_1 x,$ where $a_0,\ a_1 \in F$ and $a_1 \neq 0.$
So $f(x)$ has one root, namely, $(-a_1^{-1} a_0) \in F.$ Can it have more roots? From Corollary 1, you know that it cannot have more roots, since $\deg f(x) = 1 = \deg (x + a_1^{-1} a_0).$
So, for $n = 1,$ $f(x)$ has exactly 1 root, in fact, and it is in $F.$
Thus, $P(1)$ is true.

Now assume that $P(m)$ is true for some $m \in \mathbb{N}.$
We will show that $P(m+1)$ is true.
Let $f(x) \in F[x]$ s.t. $\deg f(x) = m + 1.$ We will show that the number of roots of $f(x)$ in F is at most $m + 1.$
There are two possibilities now – either $f(x)$ has no zero in $F,$ or $f(x)$ has a zero in $F.$
If $f(x)$ has no root in $F,$ then the number of roots of $f(x)$ in F is $0 \leq m + 1.$
Thus, trivially, $f(x)$ has at most $m + 1$ roots in $F.$

Next, suppose $f(x)$ has a root $a \in F.$
Then $f(x) = (x - a)g(x),$ where $\deg g(x) = (m + 1) - 1 = m,$ and $g(x) \in F[x].$
Hence, by the induction hypothesis, $g(x)$ has at most m roots in $F.$ Let $a_1, \ldots, a_s$ be the distinct roots of $g(x)$ in $F,$ where $s \leq m.$
Now, a_i is a root of $g(x)$

$\Rightarrow g(a_i) = 0$

$\Rightarrow f(a_i) = (a_i - a)g(a_i) = 0$

$\Rightarrow a_i$ is a root of $f(x)$ in $F \ \forall\ i = 1, ..., s.$

Thus, each root of $g(x)$ is a root of $f(x).$
Thus, $f(x)$ has at least $s + 1$ roots $a, a_1, \ldots, a_s$ in $F,$ where $s + 1 \leq m.$
Does $f(x)$ have any more roots in F? Let's see.
Now, $b \in F$ is a root of $f(x)$

$\Leftrightarrow f(b) = 0$

$\Leftrightarrow (b-a)g(b)=0$
$\Leftrightarrow b-a=0$ or $g(b)=0,$ since F is an integral domain.
Thus, b is a root of $f(x)$
$\Leftrightarrow b=a$ or b is a root of $g(x)$
$\Leftrightarrow b=a,\ a_1,\ldots,a_s.$
So, the only roots of $f(x)$ are a and $a_1,\ldots,a_s.$
Thus, $f(x)$ has at the most $m+1$ roots in $F.$
$\therefore P(m+1)$ is a true statement.

Hence, $P(n)$ is true $\forall\ n\in\mathbb{N},$ i.e., the theorem is true for all $n\geq 1.$ ■

Here consider an important point about Theorem 2.

Remark 1: Using Theorem 2, you know that $x^3-1\in\mathbb{Q}[x]$ can't have more than 3 roots in $\mathbb{Q}.$ However, it has only one root in $\mathbb{Q},$ i.e., $1.$ The others are $\omega=\dfrac{-1+i\sqrt{3}}{2},$ and $\omega^2,$ in $\mathbb{C}\setminus\mathbb{Q}.$ Thus, it is important to note the significance of 'at the most' in the statement of Theorem 2.

In Theorem 2, we have not spoken about the multiplicity of the roots. This is the point of the following corollary of Theorem 2.

Corollary 2: If $f(x)\in F[x]$ is of degree $n,$ then $f(x)$ has at the most n distinct roots in $F,$ where F is a field. ■

We will use Corollary 2 to prove the following useful theorem.

Theorem 3: Let $f(x)$ and $g(x)$ be non-zero polynomials of degree n over a field $F.$ If there exist $n+1$ distinct elements $a_1,\ldots,a_{n+1}$ in F such that $f(a_i)=g(a_i)\ \forall\ i=1,\ldots,n+1,$ then $f(x)=g(x).$

Proof: Consider the polynomial $h(x)=f(x)-g(x).$
Then $\deg h(x)\leq n,$ but $h(x)$ has $n+1$ distinct roots $a_1,\ldots,a_{n+1}$ in $F.$ (Why?)
By Corollary 2, this is impossible, unless $h(x)$ is the zero polynomial, i.e., $f(x)=g(x).$ ■

Note that Theorem 3 is not true if the a_is are not all distinct. For example, take $f(x)=(x-2)^2(x-3)$ and $g(x)=(x-2)(x-3)^2$ in $\mathbb{R}[x].$ They are both of degree $3,$ but $2,\ 2,\ 3,\ 3$ are 4 elements in $\mathbb{R}$ s.t. $f(x)$ and $g(x)$ have the same value, $0,$ at these points. Also $f(x)\neq g(x).$

Now, by Theorem 2, you know that if you are given a polynomial of degree $25,$ say, over $\mathbb{R},$ then you can find a maximum of 25 zeros of this polynomial in $\mathbb{R}.$ Is the same true for $\mathbb{Z},$ say? Or for a ring that is not a domain? Let us look at an example.

Example 1: Prove that $x^3+\overline{5}x\in\mathbb{Z}_6[x]$ has more than 3 zeros.

Solution: Since $\mathbb{Z}_6$ is finite, it is easy for us to run through all its elements and check which of them are roots of $f(x)=x^3+\overline{5}x.$

So, by substitution we find that
$f(\overline{0}) = 0 = f(\overline{1}) = f(\overline{2}) = f(\overline{3}) = f(\overline{4}) = f(\overline{5})$.

In fact, every element of $\mathbb{Z}_6$ is a zero of $f(x)$. Thus, $f(x)$ has 6 zeros, while $\deg f(x) = 3$. Thus, Theorem 2 (and hence, Theorem 3) is not true for $\mathbb{Z}_6[x]$.

***

From Example 1, you can see that for a ring that is not a domain, Theorem 2 and 3 are not true. However, these theorems are true for a domain too, as you will now see.

Theorem 4: A non-zero polynomial of degree n in $D[x]$, where D is an integral domain, has at the most n roots in D.

Proof: Let $f(x) \in D[x]$ be of degree n. Let F be the field of quotients of D. Then $f(x) \in F[x]$. Hence, $f(x)$ has at the most n roots in F, by Theorem 2. Also, any root of $f(x)$ in D will be a root in F too. Thus, $f(x)$ cannot have more than n roots in D. ■

Try solving the following exercises now.

E7) Prove Corollary 2.

E8) State, and prove, the statement analogous to Theorem 3, replacing a field F by an integral domain D.

E9) Let F be a field and $f(x) \in F[x] \setminus \{0\}$. Show that $f(x)$ can have at most n linear factors in $F[x]$.

E10) Let p be a prime number. Consider $x^{p-1} - \overline{1} \in \mathbb{Z}_p[x]$. Use the fact that $\mathbb{Z}_p$ is a group of order p to show that every non-zero element of $\mathbb{Z}_p$ is a root of $x^{p-1} - \overline{1}$. Thus, show that

i) $x^{p-1} - \overline{1} = (x - \overline{1})\,(x - \overline{2}) \ldots (x - \overline{p-1})$, and

ii) $(p-2)! \equiv 1 (\text{mod } p)$.

E11) The polynomial $x^4 + \overline{4}$ can be factored into linear factors in $\mathbb{Z}_5[x]$. Find this factorisation.

E12) Find all the zeros of $x^n - 1 \in \mathbb{C}[x]$, where $n \in \mathbb{N}$.

In E12, you may have noted that all the zeros of the polynomial over $\mathbb{C}[x]$ lie in $\mathbb{C}$. As you know, this need not be true for polynomials in $F[x]$, for other fields F. For example, this is not true for $F = \mathbb{R}$.

Let us now consider elements of $F[x]$ that have no roots in F. These polynomials are somewhat analogous to prime numbers in $\mathbb{Z}$.

16.3 IRREDUCIBLE POLYNOMIALS

From Unit 1, you know that a prime number is a non-zero, non-unit element of $\mathbb{Z}$ that has no factors other than 1 and itself. You also know that if p is a prime in $\mathbb{Z}$, then $p\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$. So, does a prime element of $F[x]$ satisfy this property too, where F is a field? From Theorem 13, Unit 14, we are assured that a prime element will generate a prime ideal. This may or may not be maximal in $F[x]$. In this section, you will study what these prime elements are. You will also study that they generate maximal ideals in $F[x]$.

Firstly, recall from Unit 15, that the units of $F[x]$ are the elements of F^*. Thus, **the units of $F[x]$ are precisely the constant polynomials in $F[x]$**. So, a non-zero non-unit element of $F[x]$ is a polynomial of degree ≥ 1.

Next, if $f(x) \mid g(x)$ in $F[x]$, then $\deg f(x) \leq \deg g(x)$. So, if $g(x)$ has no factors other than a unit and itself, then $g(x) = af(x)$, for some $a \in F^*$.
This means that $\deg f(x) = \deg g(x)$.
For example, $g(x) = 3x + 5$ has no factor of positive degree, since $\deg g(x) = 1$. Also, $x^2 + 1 \in \mathbb{R}[x]$ has no linear factor in $\mathbb{R}[x]$, by Corollary 1. However, $x^2 - 1$ has $(x-1)$ and $(x+1)$ as factors in $\mathbb{R}[x]$, again by Corollary 1.
With this background, let us define a concept in $F[x]$ that will turn out to have somewhat similar properties to that of a prime number in $\mathbb{Z}$.

Definition: Let F be a field. A non-zero non-unit polynomial $p(x) \in F[x]$ is called

i) **irreducible** in $F[x]$ if whenever $p(x) = f(x)g(x)$ in $F[x]$, then $\deg f(x) = 0$ or $\deg g(x) = 0$.

ii) **reducible** in $F[x]$, if it is **not irreducible** in $F[x]$.

For example, $(x^2 - 1)$ is reducible in $\mathbb{Q}[x]$ as well as in $\mathbb{R}[x]$ as $x^2 - 1 = (x-1)(x+1)$ and $\deg\,(x-1) = 1 = \deg\,(x+1)$.

Let us consider an example of irreducible polynomials in detail. This is actually a class of examples.

Example 2: Let F be a field. Show that any linear polynomial in $F[x]$ is irreducible in $F[x]$.

Solution: Let $f(x) = ax + b \in F[x], a \neq 0$. Suppose $f(x) = g(x)h(x)$, in $F[x]$.
Then $1 = \deg f(x) = \deg g(x) + \deg h(x) \geq 0$.
This is only possible if either $\deg g(x) = 0$ or $\deg h(x) = 0$, i.e., if either $g(x) \in F^*$ or $h(x) \in F^*$.
Thus, by definition, $f(x)$ is irreducible in $F[x]$.

***

So, a linear polynomial is irreducible over F. What about non-linear polynomials in $F[x]$? You have seen that $x^2 - 1$ is reducible over $\mathbb{R}$. Consider the following example.

Example 3: Check whether or not $x^2 + 1 \in \mathbb{R}[x]$ is irreducible.

Solution: Let $x^2 + 1 = f(x)g(x)$ in $\mathbb{R}[x]$. Then $\deg f(x) \leq 2$.

Suppose, if possible, $\deg f(x) = 1.$

Since $f(x)\big|(x^2+1),$ by Corollary 1 we find that x^2+1 has a root in $\mathbb{R}.$

This is a contradiction.
Hence, $\deg f(x) \neq 1.$
$\therefore \deg f(x) = 0$ or $\deg f(x) = 2.$
If $\deg f(x) = 2,$ then $\deg g(x) = 0.$
Hence, (x^2+1) is irreducible.

***

In the following theorem you can see the relationship between irreducibility and roots of non-linear polynomials.

Theorem 5: Let F be a field and let $p(x) \in F[x],$ with $\deg p(x) \geq 2.$ If $p(x)$ is irreducible in $F[x],$ then $p(x)$ has no roots in $F.$

Proof: We shall prove the contrapositive of the statement to be proved, i.e., if $p(x)$ has a root in $F,$ then $p(x)$ is reducible.

Suppose $p(x)$ has a root $a \in F.$ Then, by Corollary 1, $(x-a)\big|p(x).$ So $p(x) = (x-a)g(x)$ in $F[x],$ where $\deg g(x) = \deg p(x) - 1 \geq 1.$
Thus, $p(x)$ is reducible in $F[x].$
Hence, the theorem is proved. ■

Now, is the converse of Theorem 5 true? That is, if $p(x)$ is of degree ≥ 2 and has no root in $F,$ then must $p(x)$ be irreducible in $F[x]$? Let's see.
Consider $f(x) = x^4 + 2x^2 + 1 \in \mathbb{R}[x].$ This is reducible, since $f(x) = (x^2+1)(x^2+1)$ in $\mathbb{R}[x]$ and $\deg(x^2+1) = 2 \neq 0.$ But $f(x)$ has no root in $\mathbb{R},$ since it roots are $\pm\sqrt{-1} \in \mathbb{C} \setminus \mathbb{R}.$
Thus, the converse of Theorem 5 is not true.

In the counterexample above, note that $\deg f(x) = 4.$ So, the question now is — Is the converse of Theorem 5 true if $\deg f(x) = 2$ or 3? This is what the following theorem answers.

Theorem 6: Let F be a field, and let $p(x)$ be a quadratic or a cubic polynomial over $F.$ If $p(x)$ has no roots in $F,$ then $p(x)$ is irreducible in $F[x].$

Proof: We shall prove the contrapositive of the statement to be proved. Thus, we aim to prove that if $p(x)$ is reducible in $F[x],$ then $p(x)$ has a root in $F.$
So, let $p(x) = f(x)g(x)$ in $F[x],$ with $\deg f(x) \geq 1, \deg g(x) \geq 1.$ Now $\deg p(x) = \deg f(x) + \deg g(x),$ and $\deg p(x) = 2$ or $3.$ Therefore, $\deg f(x) = 1$ or $\deg g(x) = 1.$
Suppose $f(x)$ is linear, say $f(x) = ax + b, a \neq 0.$
Then $f(-a^{-1}b) = 0.$ So $p(-a^{-1}b) = 0.$ Thus, $-a^{-1}b \in F$ is a root of $p(x).$

Similarly, if $g(x)$ is linear, then $p(x)$ will have a root in $F.$
Thus, we have proved that if $p(x)$ is reducible, it has a root in $F;$ or equivalently, if $p(x)$ has no root in $F, p(x)$ is irreducible over $F.$ ■

Why don't you solve some exercises now?

E13) Which of the following polynomials are irreducible? Give reasons for your choice.

i) $x^2 - 2x + 1 \in \mathbb{R}[x]$,

ii) $x^2 + x + 1 \in \mathbb{C}[x]$,

iii) $ix + 2 \in \mathbb{C}[x]$,

iv) $x^4 + 3x^2 + 2 \in \mathbb{R}[x]$,

v) $x^2 + a^2 \in \mathbb{R}[x] \ \forall \ a \in \mathbb{R}^*$.

E14) Check whether or not $x^3 + \overline{3}x^2 + \overline{2}$ is irreducible in $\mathbb{Z}_5[x]$.

E15) If $f(x) \in F[x]$ has a root in F, with $\deg f(x) \leq 3$, then $f(x)$ is reducible in $F[x]$. True or false? Why?

E16) Find two prime numbers p s.t. $(x + \overline{2}) \,\big|\, (x^4 + x^3 + x^2 - x + \overline{1})$ in $\mathbb{Z}_p[x]$.

E17) For which $n \in \mathbb{N}$ is $x^n - 1 \in \mathbb{Q}[x]$ irreducible, and why?

So far, you have studied the relationship between $f(x)$ being irreducible in $F[x]$ and the roots of $f(x)$ in F. Let us now come back to what we had suggested at the beginning of this section, i.e., an analogue in $F[x]$ of a prime element in $\mathbb{Z}$. In Unit 14, you saw that if p is a prime number, then $p\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$. You will now see that irreducible elements in $F[x]$, where F is a field, have the same property.

Theorem 7: Let F be a field and let $f(x) \in F[x]$ be irreducible in $F[x]$. The ideal $< f(x) >$ is a maximal ideal of $F[x]$.

Proof: Let I be an ideal of $F[x]$ s.t. $< f(x) > \subseteq I \subseteq F[x]$.
From Sec.15.5, Unit 15, you know that every ideal in $F[x]$ is a principal ideal.
$\therefore I = < g(x) >$ for some $g(x) \in F[x]$.
Then $f(x) \in < g(x) > \Rightarrow \exists\, h(x) \in F[x]$ s.t. $f(x) = g(x)h(x)$.
Since $f(x)$ is irreducible, either $g(x) \in F^*$ or $h(x) \in F^*$.
If $g(x) \in F^*$, say $g(x) = c$, then $< g(x) > = < c > = F[x]$.
If $h(x) \in F^*$, say $h(x) = a$, then $g(x) = a^{-1} f(x) \in < f(x) >$, so that $< g(x) > = < f(x) >$.
Hence, $< f(x) >$ is a maximal ideal of $F[x]$. ■

Two immediate corollaries of Theorem 7 are the following.

Corollary 3: If $f(x) \in F[x]$ is irreducible, then $F[x]/< f(x) >$ is a field.

Proof: Since $< f(x) >$ is a maximal ideal of $F[x]$, $F[x]/< f(x) >$ is a field, by Theorem 14, Unit 14. ■

Corollary 4: If $f(x) \in F[x]$ is irreducible, then $f(x)$ is a prime element of $F[x]$.

Proof: Since $< f(x) >$ is a maximal ideal, it is a prime ideal of $F[x]$. Hence, $f(x)$ is a prime element of $F[x]$, by Theorem 13, Unit 14. ■

Let us consider an example of the use of Theorem 7.

Example 4: Let p be a prime number. Is $\mathbb{Q}[x]/<x^3-p>$ a field? Why, or why not?

Solution: From Theorem 7 you know that for any field F, if $f(x)$ is irreducible in $F[x]$, then $<f(x)>$ is a maximal ideal of $F[x]$.

Now, the roots of x^3-p are $p^{1/3}, p^{1/3}\omega, p^{1/3}\omega^2$, where ω is a cube root of unity in $\mathbb{C}\setminus\mathbb{R}$.. Also $p^{1/3}\in\mathbb{R}\setminus\mathbb{Q}$. Thus, none of the roots of x^3-p lie in $\mathbb{Q}$.

So, by Theorem 6, x^3-p is irreducible.

Therefore, $<x^3-p>$ is a maximal ideal of $\mathbb{Q}[x]$.

Thus, $\mathbb{Q}[x]/<x^3-p>$ is a field.

***

Now let us go back to Corollary 4. In this corollary, you have seen that every irreducible element of $F[x]$ is a prime element. Is the converse true? Let's see.

Theorem 8: Let F be a field and let $f(x)\in F[x]$ be a prime element. Then $f(x)$ is irreducible in $F[x]$.

Proof: Let $f(x)=g(x)h(x)$ in $F[x]$. Then $f(x)\,|\,g(x)h(x)$.

So, by the definition of a prime element, $f(x)\,|\,g(x)$ or $f(x)\,|\,h(x)$.

Suppose $f(x)\,|\,g(x)$.

Since $f(x)=g(x)h(x)$, we see that $g(x)\,|\,f(x)$ also.

So, by Theorem 8, Unit 15, $f(x)=ag(x)$ for some $a\in F^*$.

Thus, $ag(x)=g(x)h(x)$.

So, by the cancellation law, $h(x)=a$, i.e., $\deg h(x)=0$.

Similarly, if $f(x)\,|\,h(x)$, then $\deg g(x)=0$.

Thus, $f(x)$ is irreducible. ■

What do Theorem 8 and Corollary 4 tell you? Don't they say that **$f(x)\in F[x]$ is prime iff it is irreducible**?

Why don't you solve some related exercises now?

E18) Let F be a field, and let $p(x)$ be irreducible in $F[x]$. If $p(x)\,|\,f_1(x)f_2(x)\ldots f_n(x)$, then show that $p(x)\,|\,f_i(x)$ for some $i=1,\ldots,n$, where $f_j(x)\in F[x]\ \forall\ j=1,\ldots,n$.

E19) Which of the following statements are true? Give reasons for your answers.

i) If F_1 and F_2 are fields such that $F_1\subseteq F_2$, and $f(x)\in F_1[x]$ is irreducible over F_1, then $f(x)$ is irreducible over F_2.

ii) $x^3+\bar{2}x^2+\bar{2}$ is a prime element in $\mathbb{Z}_5[x]$.

iii) If $p(x)$ is a prime element of $F[x]$, then $\overline{p(x)}$ is a prime element of $F[x]/I$ for any ideal I of $F[x]$, where F is a field.

By now you would have developed quite a bit of familiarity with the idea of irreducibility over a field. Let us look at this concept in greater depth in the special cases of polynomials over the complex, real and rational fields.

16.4 IRREDUCIBILITY OVER $\mathbb{C}, \mathbb{R}$ AND $\mathbb{Q}$

So far, you have studied irreducibility over any field F. Let us discuss what happens over $\mathbb{C}, \mathbb{R}$ or $\mathbb{Q}$, in particular.

16.4.1 Irreducibility over $\mathbb{C}$ and $\mathbb{R}$

You have seen that a linear polynomial is irreducible in $\mathrm{F}[x]$, for any field F. Hence, linear polynomials over $\mathbb{C}$ are irreducible too. However, for $\mathbb{C}$ we have a much stronger result, which is really basic for algebra.

In 1799, the great mathematician Gauss proved the Fundamental Theorem of Algebra.

Theorem 9 (The Fundamental Theorem of Algebra): A polynomial of degree $n \geq 1$ in $\mathbb{C}[x]$ has all n of its roots in $\mathbb{C}$, where repeated roots are counted with their respective multiplicities. ■

This theorem appears simple, but is very deep. We shall not prove it in this course, as the proof requires some understanding of complex analysis. But let us see what follows immediately from this theorem.

Corollary 5: Every polynomial over $\mathbb{C}$, of degree $n \geq 1$, can be written as a product of n linear polynomials in $\mathbb{C}[x]$. ■

In other words, Corollary 5 says that **the only irreducible polynomials in $\mathbb{C}[x]$ are the linear polynomials**.

Thus, (x^2+1) is not irreducible in $\mathbb{C}[x]$, while it is irreducible in $\mathbb{R}[x]$, as you have seen earlier.

By the Fundamental Theorem of Algebra, you now know that, for example, $(2+3i)x^{10}+(-5+i\sqrt{5})x^7+\pi x^5+i$ has 10 roots in $\mathbb{C}$. These roots may or may not all be distinct, of course.

Next, let us look at irreducible polynomials in $\mathbb{R}[x]$. How do we find out if a given polynomial of degree ≥ 2 in $\mathbb{R}[x]$ is irreducible or not? Well, by Theorems 5 and 6, you know that if the polynomial is of degree 2 or 3, it is irreducible iff it has no root in $\mathbb{R}$. However, we have a more precise result about this, which actually follows from Theorem 9.

Theorem 10: If $p(x) \in \mathbb{R}[x]$ is irreducible, then $p(x)$ is a linear or a quadratic polynomial.

Proof: Let $\deg p(x) = n$. Since $p(x)$ is irreducible in $\mathbb{R}[x]$, it has no real roots.

If $n = 1$, then $p(x)$ is linear, and hence, it is irreducible.

Suppose $n \geq 2$. Note that $p(x) \in \mathbb{R}[x] \subseteq \mathbb{C}[x]$.

So, by Theorem 9, $p(x) = a_n(x-z_1)(x-z_2)\ldots(x-z_n)$, where $a_n \in \mathbb{R}$ and $z_i \in \mathbb{C}\ \forall\ i = 1,\ldots,n$.

Also, $p(x) = a_0 + a_1x + \cdots + a_nx^n$, $a_i \in \mathbb{R}\ \forall\ i = 0,\ldots,n$.

Now, if $p(z) = 0$ for some $z \in \mathbb{C}$, then $a_0 + a_1z + \cdots + a_nz^n = 0$ in $\mathbb{C}$.

So $p(\bar{z}) = a_0 + a_1\bar{z} + \cdots + a_n\bar{z}^n = \overline{p(z)} = 0$ in $\mathbb{C}$, where $\bar{z}$ is the conjugate of z in $\mathbb{C}$. Note that $a_i = \bar{a}_i$, since $a_i \in \mathbb{R}\ \forall\ i = 0, 1, \dots, n.$
So, if $(x - z)$ is a factor of $p(x)$, $(x - \bar{z})$ must also be a factor of $p(x)$ in $\mathbb{C}$, i.e., if z is a root of $p(x)$ in $\mathbb{C}$, then so is $\bar{z}$. Note that $z \neq \bar{z}$, since $z \notin \mathbb{R}$.
Thus, **the non-real complex roots** of $p(x)$ **occur in pairs**.
So, if $p(x) \in \mathbb{R}[x]$ has one non-real complex root, it must have at least two such roots. Similarly, if $p(x)$ has 3 non-real complex roots, then it must have at least four such roots, and so on.

Now two cases arise: $\deg\ p(x)$ is odd, or $\deg\ p(x)$ is even.
If $\deg\ p(x)$ is odd, then $p(x)$ must have at least one real root since any root in $\mathbb{C} \setminus \mathbb{R}$ will occur in pairs. Thus, $p(x)$ is reducible over $\mathbb{R}$ in this case.

Next, suppose $\deg\ p(x)$ is even, say $\deg\ p(x) = 2m,\ m \in \mathbb{N}$, i.e., $n = 2m.$
For each pair of non-real complex conjugate roots $a + ib$ and $a - ib$, of $p(x)$,
$[x - (a + ib)][x - (a - ib)] = x^2 - 2ax + (a^2 + b^2) \in \mathbb{R}[x].$ …(1)
So, for each pair of non-real complex conjugate roots, you get a factor of $p(x)$ of degree 2. Since $p(x)$ has no real roots, and the non-real roots of $p(x)$ occur in pairs, $p(x)$ has m pairs of roots in $\mathbb{C} \setminus \mathbb{R}$. So $p(x)$ has m factors in $\mathbb{R}[x]$ of the form in (1).
Therefore, in this case $p(x)$ can be irreducible only if $m = 1$, i.e., $\deg\ p(x) = 2.$

Thus, we have proved that if $p(x) \in \mathbb{R}[x]$ is irreducible, then $\deg\ p(x) = 1$ or $\deg\ p(x) = 2.$ ■

Why don't you solve some exercises now?

E20) If $p(x)$ is a linear polynomial, or a quadratic polynomial, in $\mathbb{R}[x]$, it is irreducible. True or false? Why?

E21) If $p(x) \in \mathbb{R}[x]$ is of degree 6, how many linear factors does it have in $\mathbb{C}[x]$? And, how many irreducible factors can $p(x)$ have in $\mathbb{R}[x]$?

So, you have seen that irreducibility over $\mathbb{C}$ or $\mathbb{R}$ is pretty clear-cut in terms of the degree of the polynomials. Let us see if this is the case in $\mathbb{Q}[x]$.

16.4.2 Irreducibility over $\mathbb{Q}$

Let us now consider irreducible polynomials over $\mathbb{Q}$. Surprisingly, we find that if $p(x) \in \mathbb{Q}[x]$ is irreducible, we cannot say anything about its degree. To understand the reason for this, we need to first define irreducibility in $\mathbb{Z}[x]$.

Definition: Let $f(x) \in \mathbb{Z}[x],\ f(x) \neq 0, 1, -1.$ $f(x)$ is called **irreducible in $\mathbb{Z}[x]$** if whenever $f(x) = g(x)h(x)$ in $\mathbb{Z}[x]$, then $g(x) = \pm 1$ or $h(x) = \pm 1.$

Recall that $U(\mathbb{Z}[x]) = U(\mathbb{Z}) = \{1, -1\}.$

For example, $x + 9$ is irreducible in $\mathbb{Z}[x]$, but $3x + 9$ is reducible since $3x + 9 = 3(x + 3)$, both factors being non-units in $\mathbb{Z}[x]$.

Related to this is the following comment.

Remark 1: Note that a polynomial that is reducible in $\mathbb{Z}[x]$ can be irreducible in $\mathbb{Q}[x]$ (e.g., $3x+9$).

Now consider any polynomial over $\mathbb{Q}$, say $f(x)=\frac{3}{2}x^3+\frac{1}{5}x^2+3x+\frac{1}{3}.$ If we take the l.c.m of all the denominators, i.e., of $2,5,1$ and 3, which is 30, and multiply $f(x)$ by it, what do we get? We get

$30f(x)=45x^3+6x^2+90x+10$, and this lies in $\mathbb{Z}[x]$.

Using the same process, we can multiply any $f(x)\in\mathbb{Q}[x]$ by a suitable integer d so that $df(x)\in\mathbb{Z}[x]$. In fact, you have used this process while proving Theorem 6, Unit 15. This process will also be used to prove the following theorem.

Theorem 11: If $f(x)\in\mathbb{Z}[x]$ is irreducible in $\mathbb{Z}[x]$, then it is also irreducible in $\mathbb{Q}[x]$. ■

We will not prove this theorem here, as it involves introducing some more concepts and Gauss' Lemma. (If you are interested in learning about this, please do refer to Gauss' Lemma in any of the books we have recommended in the Course Introduction.) But let's see why this theorem is important. What this result says is that to check irreducibility of a polynomial in $\mathbb{Q}[x]$, it is enough to check it in $\mathbb{Z}[x]$. And, for checking it in $\mathbb{Z}[x]$, we have a wonderful test formulated by the German mathematician, Theodor Schönemann (1812-1868), and later proved by the German mathematician Eisenstein in 1850. It is popularly known by Eisenstein's name, and Schönemann's name seems to have gone into the background. We will state this here, but we will not prove it in this course.

Fig.1: Ferdinand Gotthold Max Eisenstein (1823-1852) was a student of Gauss.

Theorem 12 (Eisenstein's Criterion): Let $f(x)=a_0+a_1x+\cdots+a_nx^n\in\mathbb{Z}[x]$. Suppose that for some prime number p,

i) $p\nmid a_n$,

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 $\mathbb{Z}[x]$ (and hence, in $\mathbb{Q}[x]$). ■

Now, putting Theorems 11 and 12 together, you can see that Eisenstein's test tells us when a polynomial in $\mathbb{Z}[x]$ is irreducible in $\mathbb{Q}[x]$. Let us illustrate the use of this criterion.

Example 5: Is $2x^7+3x^5-6x^4+3x^3+12$ irreducible in $\mathbb{Q}[x]$? Why, or why not?

Solution: The given polynomial is of degree 7, in $\mathbb{Z}[x]$. Its coefficients are $a_0=12,\ a_1=0=a_2,\ a_3=3,\ a_4=-6,\ a_5=3,\ a_6=0,\ a_7=2$. By looking at the coefficients, we see that the prime number 3 satisfies the conditions given in Eisenstein's criterion:

i) $3\nmid 2$,

ii) $3\mid 12,\ 3\mid 0,\ 3\mid 3,\ 3\mid(-6)$, and

iii) $3^2\nmid 12$.

Therefore, the given polynomial is irreducible in $\mathbb{Z}[x]$, and hence, in $\mathbb{Q}[x]$.

***

Now let us look at an example of checking the irreducibility of a polynomial, using Theorem 12 indirectly.

Example 6: Let p be a prime number. Show that $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible in $\mathbb{Q}[x]$. ($f(x)$ is called the **pth cyclotomic polynomial**.)

Solution: To start with, note that $f(x) = g(x)h(x)$ in $\mathbb{Z}[x]$ iff $f(x+1) = g(x+1)h(x+1)$ in $\mathbb{Z}[x]$.

Thus, $f(x)$ is irreducible in $\mathbb{Z}[x]$ iff $f(x+1)$ is irreducible in $\mathbb{Z}[x]$.

Now, $(x-1)f(x) = x^p - 1$.

$\therefore [(x+1)-1]f(x+1) = (x+1)^p - 1$,

i.e., $xf(x+1) = x^p + {}^pC_1 x^{p-1} + \cdots + {}^pC_{p-1} x + 1 - 1$ (by the binomial theorem)

$$= x(x^{p-1} + px^{p-2} + {}^pC_2 x^{p-3} + \cdots + {}^pC_{p-2} x + p)$$

$\therefore f(x+1) = x^{p-1} + px^{p-2} + {}^pC_2 x^{p-3} + \cdots + {}^pC_{p-2} x + p$, by cancellation, since $x \neq 0$.

Now apply Eisenstein's criterion, taking p as the prime.

You can see that $f(x+1)$ is irreducible in $\mathbb{Z}[x]$.

Therefore, $f(x)$ is irreducible in $\mathbb{Z}[x]$, and hence, in $\mathbb{Q}[x]$.

***

You should solve the following exercises now.

E22) For any $n \in \mathbb{N}$ and prime number p, show that $x^n - p$ is irreducible in $\mathbb{Q}[x]$.

E23) If $a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Q}[x]$, can you always find a prime p that satisfies the conditions (i), (ii) and (iii) in Theorem 12? Why, or why not?

E24) Which of the following elements of $\mathbb{Z}[x]$ are irreducible over $\mathbb{Q}$?

i) $x^2 - 12$, ii) $8x^3 + 6x^2 - 9x + 24$, iii) $5x + 1$, iv) $5x^2 + 5$.

E25) Show that $x^p + \bar{a} \in \mathbb{Z}_p[x]$ is not irreducible for any $\bar{a} \in \mathbb{Z}_p$.

E26) Check whether or not $x^{n-1} + x^{n-2} + \cdots + x + 1 \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Q}[x] \; \forall \; n \geq 2$.

E27) If $f(x) \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Q}$, then it is irreducible over $\mathbb{Z}$. True, or false? Why?

E28) Is Theorem 7 true for $\mathbb{Z}[x]$? Why?

It is not always easy to find out if a given polynomial in $\mathbb{Q}[x]$ is irreducible or not. Of course, Eisenstein's criterion helps in some cases. But from E23, you know that there are irreducible polynomials in $\mathbb{Q}[x]$ that do not satisfy this criterion. However, there are a couple of other theorems that could be of some help. Let us discuss them now.

Theorem 13 (Rational Root Theorem): Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$, where $a_n \neq 0.$ If $\frac{p}{q} \in \mathbb{Q}$ is a root of $f(x),$ where $(p, q) = 1,$ then $p \mid a_0$ and $q \mid a_n.$

Proof: Since $f(\frac{p}{q}) = 0,$ we see that $a_0 + a_1\frac{p}{q} + \cdots + a_n\frac{p^n}{q^n} = 0.$

So $a_0q^n + a_1pq^{n-1} + \cdots + a_{n-1}p^{n-1}q + a_np^n = 0.$

Now, $q \mid (a_0q^n + \cdots + a_{n-1}p^{n-1}q).$

So $q \mid (-a_np^n).$

Thus, $q \mid a_n,$ as $(p, q) = 1.$

Similarly, since $p \mid (a_1pq^{n-1} + a_2p^2q^{n-2} + \cdots + a_np^n),$ $p \mid a_0.$

Hence the result. ■

Note that if $f(x) \in \mathbb{Z}[x]$ has no root in $\mathbb{Q},$ it could still be irreducible (e.g., $x^2 + 1$). So Theorem 13 has only a very limited role for checking irreducibility of a polynomial of degree ≥ 4.

Let us consider an example of applying Theorem 13.

Example 7: Check whether or not $f(x) = 8x^3 + 9x^2 - 5x - 2$ is irreducible in $\mathbb{Q}[x]$.

Solution: In this case there is no prime number which will help us apply Eisenstein's criterion. So, let's see if $f(x)$ has a rational root.

If $\frac{p}{q}$ is a root, with $(p, q) = 1,$ then by Theorem 13, $p \mid (-2)$ and $q \mid 18.$

So the possibilities for p and q are $p = \pm 1, \pm 2,$ and $q = \pm 1, \pm 2, \pm 3, \pm 6, \pm 9, \pm 18.$

The next step is to use a trial-and-error method. Voila! We find $f\left(-\frac{1}{3}\right) = 0.$

Hence, $\left(x + \frac{1}{3}\right)$ is a factor of $f(x)$ in $\mathbb{Q}[x]$.

$\therefore f(x)$ is not irreducible over $\mathbb{Q}$.

***

As you can see from the example above, applying the rational root theorem is not easy manually. This is because $\frac{p}{q}$ could be one of many possibilities, and each has to be tried out till you hit a possible root – or don't !

Further, if a polynomial has degree $\geq 4,$ then it may have no root in $\mathbb{Q}$ and still be reducible, as you have seen. So, this theorem is not really helpful except in the case of degree 2 or $3,$ and that too when the coefficients a_n and a_0 have only a small number of factors.

Now let's discuss another criterion for irreducibility over $\mathbb{Q}$. Like Theorem 12, this is based on Theorem 11 too.

Theorem 14 ($\text{Mod } p$ Irreducibility Test): Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x].$ If there is a prime p s.t. $p \nmid a_n$ and s.t.

$\overline{f(x)} = \bar{a}_0 + \bar{a}_1 x + \cdots + \bar{a}_n x^n$ is irreducible in $\mathbb{Z}_p[x]$, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Proof: We shall prove this by contradiction. Suppose $f(x)$ is reducible over $\mathbb{Q}$. Then $f(x)$ is reducible over $\mathbb{Z}$, by Theorem 11.
So $f(x) = g(x)h(x)$, with $g(x), h(x) \in \mathbb{Z}[x], g(x) \neq \pm 1, h(x) \neq \pm 1.$
So, in $\mathbb{Z}_p[x]$, we have $\overline{f(x)} = \overline{g(x)} \cdot \overline{h(x)}.$
Here $\deg \overline{g(x)} \leq \deg g(x) < \deg \overline{f(x)}$ and $\deg \overline{h(x)} < \deg \overline{f(x)}.$
This contradicts our assumption that $\overline{f(x)}$ is irreducible over $\mathbb{Z}_p$. So we reach a contradiction.
Therefore, $f(x)$ is irreducible in $\mathbb{Q}[x]$. ■

Let us consider an application of Theorem 14.

Example 8: Is $6x^3 - 7x^2 + 8x + 2$ irreducible in $\mathbb{Q}[x]$? Give reasons for your answer.

Solution: Here there is no prime for which we can apply Eisenstein's criterion. So, let us try Theorem 14.
Let $f(x) = 6x^3 - 7x^2 + 8x + 2.$
Consider $p = 7$, as $7 \nmid 6$. So, we look at $\overline{f(x)}$ in $\mathbb{Z}_7[x]$. We find that
$\overline{f(x)} = \bar{6}x^3 + x + \bar{2}.$
This is reducible iff $\overline{f(x)}$ has a root in $\mathbb{Z}_7$, by Theorem 6.
On substituting $x = \bar{0}, \bar{1}, \ldots, \bar{6}$, you can check that none of these give
$\overline{f(x)} = \bar{0}.$
Hence, $\overline{f(x)}$ is irreducible in $\mathbb{Z}_7[x]$.
Thus, by Theorem 14, $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Check that you can take $p = 5$ in this example too. Why? You will find that $\overline{f(x)}$ is irreducible in $\mathbb{Z}_5[x]$ also.

***

Let us consider an example of a polynomial with degree > 3 also.

Example 9: Let $f(x) = \frac{3}{7}x^4 - \frac{2}{7}x^2 + \frac{9}{35}x + \frac{3}{5} \in \mathbb{Q}[x]$. Check whether or not $f(x)$ is irreducible over $\mathbb{Q}$.

Solution: Note that $g(x) = 35f(x) = 15x^4 - 10x^2 + 9x + 21 \in \mathbb{Z}[x]$.
Also $f(x)$ is irreducible over $\mathbb{Q}$ iff $g(x)$ is irreducible over $\mathbb{Q}$.
Now, take $p = 2$ in Theorem 14. We get $\overline{g(x)} = x^4 + x + \bar{1} \in \mathbb{Z}_2[x]$.
You can check that $\overline{g(x)}$ has no roots in $\mathbb{Z}_2$.
Let us check if it has any quadratic factors.
Any such factor has to be $x^2 + \bar{1}$ or $x^2 + x + \bar{1}$.
Since $x^2 + \bar{1}$ has a zero in $\mathbb{Z}_2$, this cannot be a factor of $\overline{g(x)}$. Also,
$(x^2 + x + \bar{1}) \nmid (x^4 + x + \bar{1})$ in $\mathbb{Z}_2[x]$. (Why?).
So $\overline{g(x)}$ is irreducible in $\mathbb{Z}_2[x]$.

Thus, $g(x)$ is irreducible in $\mathbb{Q}[x]$, by Theorem 14.
Hence, $f(x)$ is irreducible in $\mathbb{Q}[x]$.

***

In spite of Eisenstein's criterion, and Theorems 13 and 14, we don't have enough tools for checking irreducibility over $\mathbb{Q}$. For example, there may be a polynomial that has no root in $\mathbb{Q}$. Or, there may be a polynomial for which an obvious candidate for p is not available for applying Theorem 14. Then, we can fall back on our good old way of inspection in some cases. For example, if you see x^4+4x^2+2, you can look at it and say it is $(x^2+2)^2$, and hence it is reducible over $\mathbb{Q}$.
Also, there are several factorisation algorithms available in Computer Algebra, for testing over a finite field or over $\mathbb{Q}$. You can study some of these in your higher studies.

Why don't you solve some exercises now?

E29) Which of the following statements are true? Justify your answers.

i) $\mathbb{Q}[x] \big/ < x^7+7x^6-14 >$ is a field.

ii) $\mathbb{R}[x] \big/ < x^7+7x^6-14 >$ is a field.

iii) $Q[x] \big/ < 21x^3-3x^2+2x+9 >$ is not a field.

E30) Give an example, with justification, of a polynomial of degree 10, which is irreducible over $\mathbb{Q}$, but when considered in $\mathbb{Z}_{11}[x]$ it is reducible.

E31) Check whether or not the following polynomials are irreducible over $\mathbb{Q}$.

i) $2x^3+3x^2+6x+2$,

ii) $6x^3+x+9$,

iii) x^5+2x+4,

iv) $8x^3-6x+1$ (you can apply the method used in Example 6 here).

Let us now consider why irreducible polynomials are important in $F[x]$.

16.5 UNIQUE FACTORISATION

In Unit 1, you studied the Fundamental Theorem of Arithmetic. As you know, this theorem is the basis on which we say that prime numbers are the atoms that make up any integer. Also, you have seen a parallel between prime numbers and irreducible polynomials in $F[x]$ in many aspects. Let us see if we can think of irreducible polynomials as being the building blocks for any polynomial in $F[x]$, paralleling the Fundamental Theorem of Arithmetic.

Now, from the Fundamental Theorem of Algebra, you know that if $f(x) \in \mathbb{C}[x]$ s.t. $\deg f(x) = n \geq 1$, then $f(x) = p_1(x)p_2(x)\ldots p_n(x)$, where $p_i(x)$ is a linear polynomial in $\mathbb{C}[x]$ $\forall$ $i = 1, \ldots, n.$ Thus, $f(x)$ is completely factorised as a product of irreducible polynomials in $\mathbb{C}[x].$ For example, $x^3 - 1 = (x-1)(x-\omega)(x-\omega^2),$ where ω is a non-real cube root of unity.

Now, in $\mathbb{R}[x]$ you have seen that the irreducible polynomials are of degree 1 or degree $2.$ Can we completely factorise any polynomial in $\mathbb{R}[x]$ as a product of irreducible polynomials? The following theorem tells us we can, and more!!

Theorem 15 (Unique Factorisation): Let F be a field, and let $f(x) \in F[x]$ s.t. $\deg f(x) = n \geq 1.$

i) There exist irreducible polynomials $p_1(x), p_2(x), \ldots, p_m(x)$ in $F[x]$ such that $f(x) = p_1(x)p_2(x)\ldots p_m(x).$

ii) If $f(x) = q_1(x)q_2(x)\ldots q_r(x)$ also, where $q_i(x) \in F[x]$ is irreducible $\forall$ $i = 1, \ldots, r,$ then $m = r$ and each $p_i = c_i q_j$ for some $j = 1, \ldots, m$ and $c_i \in F^*.$ ■

Theorem 15 can be proved by using Corollary 4, and then applying induction on $m.$ However, we shall not prove it in this course, but will apply it in several situations. Let us consider an example.

Example 10: Write $f(x) = x^5 - 4x$ as a product of irreducible polynomials in $\mathbb{R}[x],$ and in $\mathbb{C}[x].$

Solution: Now $f(x) = x^5 - 4x = x(x^4 - 4) = x(x^2-2)(x^2+2)$

$$= x(x-\sqrt{2})(x+\sqrt{2})(x^2+2). \qquad \ldots(2)$$

Since x^2+2 has no real roots, $f(x) = x(x-\sqrt{2})(x+\sqrt{2})(x^2+2)$ is a factorisation in $\mathbb{R}[x],$ as required.

However, in $\mathbb{C}[x],$ $x^2+2 = (x+i\sqrt{2})(x-i\sqrt{2}).$

So (2) gives us $f(x) = x(x-\sqrt{2})(x+\sqrt{2})(x+i\sqrt{2})(x-i\sqrt{2}),$ as a product of irreducible polynomials in $\mathbb{C}[x].$

***

You should solve the following exercises now.

E32) Show that $\bar{3}x^2 + \bar{4}x + \bar{3} \in \mathbb{Z}_5[x]$ factors as $(\bar{3}x+\bar{2})(x+\bar{4})$ and as $(\bar{4}x+\bar{1})(\bar{2}x+\bar{3}).$ Does this contradict Theorem 15(ii)? Give reasons for your answer.

E33) Write $2x^4 + x^3 + 4x^2 + x + 2$ as a product of irreducible polynomials in $\mathbb{Q}[x].$

E34) Write $2x^4 - 3x^3 - 8x^2 + 9x + 6$ as a product of irreducible polynomials in $\mathbb{R}[x].$

E35) If $f(x) \in \mathbb{R}[x]$ such that $\deg f(x) = 5,$ how many real roots can $f(x)$ have? Give examples to justify your answer.

E36) Show that the factorisation in Theorem 15 need not be unique, upto order, in $\mathbb{Z}_8[x]$. Note that $\mathbb{Z}_8$ is not a field.

(Thus, Theorem 15 need not be true if F is not a field.)

With this we come to the end of our discussion on factorisation and irreducibility in $F[x]$, where F is a field. Let us summarise what we have discussed in this unit.

16.6 SUMMARY

In this unit, you have studied the following points.

1. The definition of a root (or a zero), and the multiplicity of a root, of a polynomial over a ring R.

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

3. Let F be a field and let $f(x) \in F[x]$, with $\deg f(x) \geq 1$. Then $a \in F$ is a root of $f(x)$ iff $(x-a) \mid f(x)$.

4. A non-zero polynomial of degree n over a field F has at the most n roots in F.

5. A non-zero polynomial of degree n in $D[x]$, where D is an integral domain, has at the most n roots in D.

6. Let $f(x)$ and $g(x)$ be two non-zero polynomials of degree n over a field F (respectively, a domain D). If there exist $n+1$ distinct elements $a_1, \ldots, a_{n+1}$ in F (respectively, D) such that $f(a_i) = g(a_i)\ \forall\ i = 1,\ldots, n+1$, then $f(x) = g(x)$.

7. The definition, and examples, of an irreducible polynomial over a field F, and over $\mathbb{Z}$.

8. Let F be a field and let $p(x) \in F[x]$, with $\deg p(x) \geq 2$. If $p(x)$ is irreducible in $F[x]$, then $p(x)$ has no roots in F.

9. Let F be a field, and let $p(x)$ be a quadratic or a cubic polynomial over F. If $p(x)$ has no roots in F, then $p(x)$ is irreducible in $F[x]$.

10. **Fundamental Theorem of Algebra:** A polynomial of degree $n \geq 1$ in $\mathbb{C}[x]$ has all of its roots in $\mathbb{C}$, counted with their respective multiplicities.

11. If $p(x) \in \mathbb{R}[x]$ is irreducible, then $p(x)$ is a linear or a quadratic polynomial.

12. If $f(x) \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Z}[x]$, then it is irreducible in $\mathbb{Q}[x]$.

13. **Eisenstein's Criterion:** Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$. Suppose that for some prime number p,

    i) $p \nmid a_n$,

ii) $p\,|\,a_0, p\,|\,a_1,\ldots,p\,|\,a_{n-1},$ and

iii) $p^2 \nmid a_0.$

Then $f(x)$ is irreducible in $\mathbb{Z}[x]$ (and hence, in $\mathbb{Q}[x]$).

14. Let F be a field and let $f(x) \in F[x]$ be irreducible. Then $< f(x) >$ is a maximal ideal of $F[x]$.

15. Let F be a field and let $f(x) \in F[x]$ be a prime element. Then $f(x)$ is irreducible in $F[x]$.

16. **Rational root theorem:** Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x], a_n \neq 0.$ If $\frac{p}{q} \in \mathbb{Q}$ is a root of $f(x),$ where $(p, q) = 1,$ then $p\,|\,a_0$ and $q\,|\,a_n.$

17. **(Mod p Irreducibility Test):** Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x].$ If there is a prime p s.t. $p \nmid a_n$ and s.t. $\overline{f(x)} = \bar{a}_0 + \bar{a}_1x + \cdots + \bar{a}_nx^n$ is irreducible in $\mathbb{Z}_p[x],$ then $f(x)$ is irreducible in $\mathbb{Q}[x].$

18. **Unique factorisation:** Let F be a field, and let $f(x) \in F[x],$ $\deg f(x) = n \geq 1.$

i) There exist irreducible polynomials $p_1(x), p_2(x),\ldots, p_m(x)$ in $F[x]$ such that $f(x) = p_1(x)p_2(x)\ldots p_m(x).$

ii) If $f(x) = q_1(x)q_2(x)\ldots q_r(x)$ also, where $q_i(x) \in F[x]$ is irreducible $\forall\ i = 1,\ldots, r,$ then $m = r$ and each $p_i = c_iq_j$ for some $j = 1,\ldots, m$ and $c_i \in F^*.$

16.7 SOLUTIONS / ANSWERS

E1) $a \in F$ is a root of $f(x) \in F[x]$
iff $f(a) = 0$
iff $f(x) = (x - a)q(x),$ for some $q(x) \in F[x],$ by Theorem 1.
Iff $(x - a)\,|\,f(x),$ by definition.

E2) i) By the quadratic formula, the roots are 3 and $2,$ each with multiplicity $1.$ Thus, the given polynomial is the same as $\frac{1}{2}(x - 3)(x - 2) \in \mathbb{Q}[x].$ You should check this.

ii) $x^2 + x + \bar{1} = (x - \bar{1})^2$, since $-\bar{2} = \bar{1}$ in $\mathbb{Z}_3.$
Thus, $\bar{1}$ is the only zero. Its multiplicity is 2 since $(x - \bar{1})^2$ is a factor, and $(x - \bar{1})^3$ is not a factor, of the given polynomial

iii) By trial-and-error, one zero is $\bar{1}$. 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 $x^3 + \bar{3}x^2 + \bar{3}x + \bar{1}.$

Applying long division, we see that $x^3+\bar{3}x^2+\bar{3}x+\bar{1}=(x+\bar{1})^3$.

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

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

iv) Note that $5x+3=5(x+\frac{3}{5})$, $\sqrt{2}-4x=(-4)(x-\frac{1}{2\sqrt{2}})$ and $(ix+1-i\sqrt{3})=i[x-(\sqrt{3}+i)]$.

So $\frac{-3}{5}$, $\frac{1}{2\sqrt{2}}$ and $(\sqrt{3}+i)$ are the roots of the given polynomial.

Since the polynomial is given as a product of these linear polynomials, you can see that their multiplicities are $2, 3, 11$, respectively.

E3) For example, $x^3(x-\overline{10})^2 \in \mathbb{Z}_{11}[x]$.

Here $\bar{0}$ has multiplicity 3 and $\overline{10}$ has multiplicity 2, and these are the only roots. There can be several other examples.

E4) i) Prove this as you have done in Unit 13.

ii) Since b is a constant polynomial, its value doesn't change by substituting a for x.

iii) $f(x) \in \text{Ker } \phi$ iff $\phi(f(x))=0$ iff $f(a)=0$ iff a is a zero of $f(x)$.

Now, by Corollary 1, $f(x) \in \text{Ker } \phi$

iff $(x-a)\,\big|\,f(x)$

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

Thus, $\text{Ker } \phi = \, < x-a >$.

The Fundamental Theorem of Homomorphism says that $(F[x]/ < x-a >) \simeq F$.

E5) By E4, $F[x]\big/ < x-a > \;\simeq F$ and $F[x]\big/ < x > \;\simeq F$. Hence the result.

E6) Let $f(x)=a_0+a_1x+\cdots+a_nx^n$.

Then $a_0+a_1a+\cdots+a_na^n=0$, as $a \in F^*$ is a root of $f(x)$.

So $a^n(a_0a^{-n}+a_1a^{-(n-1)}+\cdots+a_n)=0$.

Since $a^n \neq 0$ and F is a domain,

$a_n+a_{n-1}a^{-1}+\cdots a_1(a^{-1})^{n-1}+a_0(a^{-1})^n=0$, noting that $a^{-m}=(a^{-1})^m \; \forall \; m \in \mathbb{Z}$.

$\therefore a^{-1}$ is a root of $a_n+a_{n-1}x+\cdots+a_1x^{n-1}+a_0x^n \in F[x]$.

No, as a^{-1} may not lie in D. For example, 2 is a root of $x^2-4 \in \mathbb{Z}[x]$. But $4x^2-1 \in \mathbb{Z}[x]$ has no root in $\mathbb{Z}$.

E7) By Theorem 2, $f(x)$ has at most n roots in F. Hence, $f(x)$ has at most n distinct roots in F.

E8) **Statement:** Let $f(x)$ and $g(x)$ be two non-zero polynomials of degree n over an integral domain D. If there exist $n+1$ distinct elements $a_1,\ldots,a_{n+1}$ in D such that $f(a_i)=g(a_i) \; \forall \; i=1,\ldots,n+1$, then $f(x)=g(x)$.

Proof: Follow the reasoning in the proof of Theorem 3, applying Theorem 4 and E7 to get the result.

E9) Show how this follows from Corollary 1 and Theorem 2.

E10) i) You know that $(\mathbb{Z}_p^*, \cdot)$ is a group, and $o(\mathbb{Z}_p^*) = p-1.$

Thus, from Unit 4, you know that $x^{p-1} = \overline{1} \ \forall \ x \in \mathbb{Z}_p^*,$

i.e., each of the $p-1$ elements of $\mathbb{Z}_p^*$ is a root of $x^{p-1} - \overline{1}$.

Therefore, $(x-\overline{1})....(x-\overline{p-1}) \Big| (x^{p-1} - \overline{1})$.

Since $x^{p-1} - \overline{1}$ can have at most $p-1$ roots in $\mathbb{Z}_p$ (by Theorem 2), we find that the $(p-1)$ elements of $\mathbb{Z}_p^*$ are the only roots of $x^{p-1} - \overline{1}$.

Now, comparing the leading coefficients and degrees of $x^{p-1} - \overline{1}$ and $\prod_{i=1}^{p-1}(x-\overline{i}),$ we see that $x^{p-1} - \overline{1} = (x-\overline{1})(x-\overline{2})\ldots(x-\overline{p-1}).$

ii) Substituting $\overline{0}$ for x in (i), we get $-\overline{1} = (-1)^{p-1}\overline{(p-1)!},$ i.e.,

$\overline{p-1} = (-1)^{p-1}\overline{(p-1)!},$ since $\overline{p-1} = -\overline{1}$ in $\mathbb{Z}_p.$

i.e., $(-1)^{p-1}(p-2)! \equiv 1 (\operatorname{mod} p).$

Now, $(-1)^{p-1} \equiv 1 (\operatorname{mod} p),$ for every prime $p.$ (Why?)

Hence, we get the result.

E11) The polynomial $x^4 + \overline{4}$ is the same as $x^4 - \overline{1}$ in $\mathbb{Z}_5[x],$ since $\overline{4} = -\overline{1}$.

Thus, applying the result in E10, we get

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

E12) Recall, from your study of group theory, the group $U(n)$ of the $n\text{th}$ roots of unity. Each $n\text{th}$ root of unity is a zero of $x^n - 1$ in $\mathbb{C}.$ Also, $x^n - 1$ has at most n zeros in $\mathbb{C}.$ Hence, the elements of $U(n)$ are all the zeros of $x^n - 1$ in $\mathbb{C}.$

E13) i) No, since $x^2 - 2x + 1 = (x-1)(x-1).$

ii) No, since $x^2 + x + 1 = (x-\omega)(x-\omega^2),$ where ω is a non-real cube root of unity.

iii) Yes, by Example 2.

iv) No, since $x^4 + 3x^2 + 2 = (x^2+1)(x^2+2).$

v) No, by Theorem 6.

E14) Let $f(x) = x^3 + \overline{3}x^2 + \overline{2}.$ Since $f(x)$ is a cubic, by Theorem 6 you need to see if $f(a) = \overline{0}$ for any $a \in \mathbb{Z}_5.$ You will find that $f(a) \neq \overline{0} \ \forall \ a \in \mathbb{Z}_5.$

Thus, $f(x)$ is irreducible over $\mathbb{Z}_5.$

E15) False. For example, a linear polynomial over F is irreducible, and its root is in $F.$ However, it is true for the other cases, by Theorem 5.

E16) Let $f(x) = x^4 + x^3 + x^2 - x + 1$ in $\mathbb{Z}[x].$

Then $f(-2) = 16 - 8 + 4 + 2 + 1 = 15.$

Thus, $f(-\overline{2}) = \overline{0}$ in $\mathbb{Z}_p[x]$ for $p = 3$ or $p = 5.$

$\therefore (x+\overline{2}) \Big| f(x)$ in $\mathbb{Z}_p[x]$ if $p = 3$ or $p = 5.$

E17) $x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1) \; \forall \; n \geq 2.$

Thus, $x^n - 1$ is reducible $\forall \; n \geq 2.$

However, for $n = 1,$ $x - 1$ is irreducible, by Example 2.

E18) Since $p(x)$ is irreducible over $F,$ it is prime in $F[x],$ by Corollary 4.

You need to prove $P(n)$ is true $\forall \; n \in \mathbb{N},$ where

$P(n):$ if $p(x) \mid f_1(x) \ldots f_n(x),$ then $p(x) \mid f_i(x)$ for some $i = 1, \ldots, n.$

$P(1)$ is trivially true. (Why?)

Assume that the statement $P(m)$ is true for some $m \in \mathbb{N}.$

You should prove that $P(m+1)$ is true. (You can write $f_1(x) \ldots f_{m+1}(x) = [f_1(x) \ldots f_m(x)] f_{m+1}(x),$ and use the definition of a prime element.)

Hence, $P(n)$ is true $\forall \; n \in \mathbb{N}.$

E19) i) e.g., take $x^3 - 5$ in $\mathbb{Q}[x],$ and in $\mathbb{R}[x].$ Use Example 4 and Theorem 6 to show why the statement is false.

ii) This is false. Since $\overline{1}$ is a zero in $\mathbb{Z}_5,$ the given polynomial is reducible, and hence, not prime in $\mathbb{Z}_5[x].$

iii) Not true; e.g., x is a prime element of $F[x],$ but $\overline{x}$ is zero in $F[x]/< x >,$ and hence, not a prime element.

E20) If $p(x)$ is linear, it is irreducible. However, if it is quadratic it need not be irreducible. e.g., $x^2 - 1$ is quadratic and reducible in $\mathbb{R}[x].$

E21) By Theorem 9, $p(x)$ has 6 linear factors in $\mathbb{C}[x],$ not necessarily distinct.

For $p(x) \in \mathbb{R}[x],$ we have the following cases.

i) All the roots of $p(x)$ are in $\mathbb{R}.$ Then $p(x)$ has 6 irreducible (linear) factors in $\mathbb{R}[x].$

ii) $p(x)$ has 4 roots in $\mathbb{R}$ and 2 in $\mathbb{C} \setminus \mathbb{R}.$ Then $p(x)$ has 5 irreducible factors in $\mathbb{R}[x],$ 4 linear and 1 quadratic, as in Theorem 10.

iii) $p(x)$ has 2 roots in $\mathbb{R}$ and 4 in $\mathbb{C} \setminus \mathbb{R}.$ Then $p(x)$ has 4 irreducible factors in $\mathbb{R}[x],$ 2 linear and 2 quadratic.

iv) $p(x)$ has no real roots, and 6 roots in $\mathbb{C} \setminus \mathbb{R}.$ Then $p(x)$ has 3 irreducible factors in $\mathbb{R}[x],$ all of them being quadratic.

E22) The coefficients in $x^n - p$ are $a_n = 1,$ $a_{n-1} = 0 = \cdots = a_1,$ $a_0 = -p.$

$\therefore p \mid a_i$ for $i = 0, 1, \ldots, n-1,$ $p \nmid a_n$ and $p^2 \nmid a_0.$

Hence, by Eisenstein's criterion, $x^n - p$ is irreducible in $\mathbb{Z}[x],$ and hence, in $\mathbb{Q}[x].$

E23) Not so; $(x^2 + 1)$ is a counterexample. (Why?)

E24) i) It is irreducible, since its roots are not in $\mathbb{Q}$ (or show this by using Eisenstein's criterion with $p = 3$).

ii) This is irreducible, using Eisenstein's criterion with $p = 3$.

iii) This is irreducible, since it is a linear polynomial.

iv) Note that this is reducible over $\mathbb{Z}$, since it is $5(x^2 + 1)$. It is irreducible over $\mathbb{Q}$ as it has no roots in $\mathbb{Q}$.

E25) Since $(\mathbb{Z}_p^*, \cdot)$ is a group of order $p - 1$,

$\bar{a}^{p-1} = \bar{1} \ \forall \ \bar{a} \in \mathbb{Z}_p^*$.

$\therefore \bar{a}^p = \bar{a} \ \forall \ \bar{a} \in \mathbb{Z}_p^*$.

Also $\bar{0}^p = \bar{0}$.

$\therefore \bar{a}^p = \bar{a} \ \forall \ \bar{a} \in \mathbb{Z}_p$.

So $\overline{p-a}^{\,p} + \bar{a} = \overline{p-a} + \bar{a} = \bar{p} = \bar{0} \ \forall \ \bar{a} \in \mathbb{Z}_p$.

Thus, $\overline{p-a}$ is a zero of $x^p + \bar{a}$ in $\mathbb{Z}_p$.

$\therefore x^p + \bar{a}$ is reducible over $\mathbb{Z}_p$.

E26) From Example 6, you know that if n is a prime, this is irreducible in $\mathbb{Q}[x]$.

However, if you take an odd composite integer, say $n = 9$, then $\sum\limits_{i=0}^{9} x^i$ has (-1) as a root.

$\therefore$ It is reducible in $\mathbb{Q}[x]$.

E27) False. For example, $3(x + 5)$ is irreducible over $\mathbb{Q}$, but not over $\mathbb{Z}$.

E28) x is irreducible over $\mathbb{Z}$. However, $\mathbb{Z}[x] \big/ < x > \simeq \mathbb{Z}$, which is not a field.

Hence, $< x >$ is not maximal in $\mathbb{Z}[x]$.

E29) i) Show that by Eisenstein's criterion, $x^7 + 7x^6 - 14$ is irreducible over $\mathbb{Z}[x]$, and hence, over $\mathbb{Q}[x]$.

$\therefore < x^7 + 7x^6 - 14 >$ is maximal in $\mathbb{Q}[x]$.

Hence, the given quotient ring is a field.

ii) By Theorem 10, $x^7 + 7x^6 - 14$ is reducible in $\mathbb{R}[x]$.

Hence, $< x^7 + 7x^6 - 14 >$ is not maximal in $\mathbb{R}[x]$.

Hence, the given quotient ring is not a field.

iii) False. Use the Mod p Irreducibility Test, with $p = 2$, to show that $21x^3 - 3x^2 + 2x + 9$ is irreducible over $\mathbb{Q}$.

E30) Take, for example, $x^{10} - 11$. Explain why this example works.

E31) i) Eisenstein's criterion can't be applied here. Let's apply Theorem 14 for $p = 3$. We get the polynomial $\bar{2}x^3 + \bar{2}$ over $\mathbb{Z}_3[x]$.

But this has a root, $\bar{2}$.

So taking $p = 3$ doesn't help.

Let us try $p = 5$. Then the polynomial we get is

$\bar{2}x^3 + \bar{3}x^2 + x + \bar{2} \in \mathbb{Z}_5[x]$.

You should check that this has no zero in $\mathbb{Z}_5$. Thus, it is irreducible over $\mathbb{Z}_5$.

Hence, by Theorem 14, $2x^3+3x^2+6x+2$ is irreducible over $\mathbb{Q}[x]$.

ii) Similarly, apply Theorem 14 here, with $p=5$.

iii) Apply Theorem 14, with $p=3$, to conclude that this has no linear factors in $\mathbb{Z}_3[x]$. Then check for quadratic factors.

Suppose $x^2+\bar{a}x+\bar{b}\in\mathbb{Z}_3[x]$ is such a factor.

Then it should not have a zero in $\mathbb{Z}_3$. So the only possibility for such factors are x^2+1, $x^2+x+\overline{2}$ and $x^2+\overline{2}x+\overline{2}$.

By long division, you should check that none of these divide $x^5+\overline{2}x+\overline{1}$ in $\mathbb{Z}_3[x]$.

$\therefore\ x^5+\overline{2}x+\overline{1}$ is irreducible in $\mathbb{Z}_3[x]$.

Therefore, the given polynomial is irreducible over $\mathbb{Q}$.

iv) If $p(x)=8x^3-6x+1$, then you can show this is irreducible over $\mathbb{Q}$ by using Eisenstein's criterion on $p(x+1)$. You can also use Theorem 14, with $p=5$, to prove this.

E32) You should check that

$$(\overline{3}x+\overline{2})(x+\overline{4})=\overline{3}x^2+\overline{4}x+\overline{3}=(\overline{4}x+\overline{1})(\overline{2}x+\overline{3}).$$

Also note that $x+\overline{4}=\overline{4}(\overline{4}x+\overline{1})$ and $\overline{3}x+\overline{2}=\overline{4}(\overline{2}x+\overline{3})$, where $\overline{4}\in\mathbb{Z}_5^*$. Hence, this exemplifies Theorem 15(ii); it doesn't contradict the theorem.

E33) Inspection works here. You should check that the given polynomial is $(2x^2+x+2)(x^2+1)$, as a product of irreducible polynomials over $\mathbb{Q}$.

E34) By trial-and-error, using Theorem 13 as an aid, we get $(x-2)$ as a linear factor.

Then, by long division, you will get

$$\begin{aligned}2x^4-3x^3-8x^2+9x+6&=(x-2)(2x^3+x^2-6x-3)\\&=(x-2)(2x+1)(x-\sqrt{3})(x+\sqrt{3}),\end{aligned}$$

applying Theorem 13 again, or by inspection.

This is the required factorisation.

E35) All 5 can be real, as in $\prod_{i=1}^{5}(x-a_i)$, $a_i\in\mathbb{R}$.

It can have 3 real roots and 2 non-real roots, as in $(x^2+1)(x+1)^3$, or it can have only 1 real root, as in $(x^2+1)^2(x+1)$.

E36) For instance, $(\overline{2}x+\overline{3})(\overline{4}x+\overline{1})=\overline{3}(\overline{2}x+\overline{1})$.

Here $\overline{3}$ is a unit in $\mathbb{Z}_8$, since $(3,8)=1$.

So the LHS is a product of two irreducible polynomials, while the RHS has only one irreducible polynomial.

MISCELLANEOUS EXAMPLES AND EXERCISES

As in the previous blocks, the few examples and exercises, given below cover the concepts and processes you have studied in this block. Studying the examples, and solving the exercises, will give you a better understanding of the concepts concerned. This will also give you more practice in solving such problems.

Example 1: Find all the prime ideals, and maximal ideals, of $\mathbb{Z}_{16}$.

Solution: The ideals of $\mathbb{Z}_{16}$ are of the form $\overline{m}\mathbb{Z}_{16}$, where $m|16$.

So $m = 1, 2, 4, 8, 16$.

Thus, the proper ideals are $\{0\}, <\overline{2}>, <\overline{4}>, <\overline{8}>$.

Since 16 is not a prime, $\mathbb{Z}_{16}$ is not a domain. So $\{\overline{0}\}$ is not a prime ideal.

Next, by the isomorphism theorems, $\mathbb{Z}_{16}\big/_{<\overline{2}>} \simeq \mathbb{Z}_2$, a field.

So $<\overline{2}>$ is a maximal ideal of $\mathbb{Z}_{16}$, and hence a prime ideal of $\mathbb{Z}_{16}$.

Now, let us consider $<\overline{4}>$. Since $\overline{4} \in <\overline{4}>$ is s.t. $(\overline{4})^2 = \overline{16} = \overline{0}$, and $\overline{4} \neq \overline{0}$, $<\overline{4}>$ is not a prime ideal of $\mathbb{Z}_{16}$.

Similarly, show why $<\overline{8}>$ is not a prime ideal of $\mathbb{Z}_{16}$.

Thus, the only prime ideal of $\mathbb{Z}_{16}$ is $<\overline{2}>$, which is also the only maximal ideal.

***

Example 2: Prove that the prime ideals of $\mathbb{Z}_n$ correspond to the prime ideals of $\mathbb{Z}$ containing $n\mathbb{Z}$, where $n \in \mathbb{N}$.

Solution: We have the natural epimorphism $\pi : \mathbb{Z} \to \mathbb{Z}_n : \pi(m) = m + n\mathbb{Z} = \overline{m}$.
Here $\text{Ker}\,\pi = n\mathbb{Z}$.
By E47(iii), Unit 14, you get the result now.

***

Example 3: If R and S are two rings and $f : R \to S$ is a homomorphism, then $f(M)$ is a maximal ideal of S for every maximal ideal M of R. True, or false? Why?

Solution: Consider the natural map $\pi : \mathbb{Z} \to \mathbb{Z}\big/_{6\mathbb{Z}}$.

Now, $5\mathbb{Z}$ is maximal in $\mathbb{Z}$, but $\pi(5\mathbb{Z}) = \mathbb{Z}\big/_{6\mathbb{Z}}$, since $(5, 6) = 1$.

Hence, $\pi(5\mathbb{Z})$ is not a proper ideal. Thus, it is not a maximal ideal of $\mathbb{Z}/6\mathbb{Z}$.
Thus, the given statement is false.

***

Example 4: If R is a commutative ring with unity, can $R[x]$ be a field? Why, or why not?

Solution: Suppose $R[x]$ is a field. Then $x^{-1} \in R[x]$, say $x^{-1} = f(x) \in R[x]$.
So $xf(x) = 1$. …(1)

Also, since $R[x]$ is without zero divisors, R is without zero divisors.
Thus, by (1), $1 + \deg f(x) = 0$, a contradiction.
Thus, $R[x]$ is not a field.

***

Example 5: Prove that if a ring has characteristic zero, then it must be infinite.

Solution: Let R be a ring with characteristic zero.
If there is an $a \in R$ s.t. $o(a)$ is infinite, then $\{na \mid n \in \mathbb{Z}\}$ is an infinite subset of R. Thus, R must be infinite.

Now consider the case that every element of R has finite order. Suppose, if possible, that R is finite, say $R = \{a_1, a_2, \ldots, a_n\}$.
Let $o(a_i) = m_i \forall\ i = 1, \ldots, n.$
Then, for $m = m_1 m_2 \ldots m_n$, $ma_i = 0\ \forall\ i = 1, \ldots, n.$
So $\text{char } R$ is finite, a contradiction to our hypothesis.
Hence, R must be infinite.

***

Example 6: Construct a field with 8 elements, using an appropriate irreducible polynomial over $\mathbb{Z}_2$.

Note that the field in Example 6 has p^r elements, where $p = 2$ and $r = 3$.

Solution: We are looking for a field with 2^3 elements. So we use Theorem 6 and Corollary 3 of Unit 16, and look for an irreducible **cubic** polynomial over $\mathbb{Z}_2$.
Let us consider $f(x) = x^3 + x + 1$.
You should check that $f(x)$ is irreducible over $\mathbb{Z}_2$.
Hence, $\mathbb{Z}_2[x] \big/ < x^3 + x + 1 > = \{ax^2 + bx + c + < x^3 + x + 1 > \mid a, b, c \in \mathbb{Z}_2\}$ is a field.
Since each of a, b, c can take 2 values, the number of elements in this field is 8.
Hence, this is the required field.

***

Example 7: Let F be a field and $f(x) \in < x >$. Let $K = \{\alpha \in F \mid f(\alpha) = 0\}$. Is K a subring of F? Give reasons for your answer.

Solution: Consider $f(x) = x(x-1) \in \mathbb{R}[x]$. Here $K = \{0, 1\}$. So K is not a subring of $\mathbb{R}$.

***

Miscellaneous Exercises

E1) If R and S are rings with identity, and $f : R \to S$ is a monomorphism, show that $\text{char } R = \text{char } S$.

E2) Let F be a field and R be a ring s.t. $f : F \to R$ is a ring homomorphism. Show that f is the zero map or f is 1-1.

E3) Let R be a domain. Show that $o(r)=o(s)\ \forall\ r, s \in R,$ where $o(x)$ denotes the order of x as an element of $(R, +).$

E4) Let R be a commutative ring s.t. the order of $(R, +)$ is $10.$ Can R be an integral domain? Why, or why not?

E5) Let R be an integral domain. If $\text{char } R = 0,$ show that the order of every non-zero element is infinite. If $\text{char } R = p,$ show that every non-zero element has order $p.$

E6) Is $3x^5+15x^4-20x^3+10x+20$ irreducible over $\mathbb{Q}[x]?$ Is it irreducible over $\mathbb{R}[x]?$ Give reasons for your answers.

E7) Let F be a field, $f(x) \in F[x]$ and $a \neq 0, a \in F.$

i) If $af(x)$ is irreducible over $F,$ prove that $f(x)$ is irreducible over $F.$

ii) If $f(ax)$ is irreducible over $F,$ prove that $f(x)$ is irreducible over $F.$

iii) If $f(x+a)$ is irreducible over $F,$ prove that $f(x)$ is irreducible over $F.$

E8) Construct a field of with 25 elements.

E9) Check whether the following polynomials are irreducible or not.

i) $\frac{5}{2}x^5+\frac{9}{4}x^4+\frac{15}{4}x^3+\frac{3}{5}x^2+\frac{6}{7}x+\frac{3}{10}$ over $\mathbb{Q},$

ii) x^2+x+4 over $\mathbb{Z}_{11},$

iii) x^4+1 over $\mathbb{Z}_{11},$

iv) x^4+15x^3+7 over $\mathbb{Q},$

v) $x^3+(5m+1)x+(5n+1)$ over $\mathbb{Z},$ where $m, n \in \mathbb{Z}.$

E10) Let $f(x) \in F[x], F$ being a field. Show that for any $a \in F,$ $(x-a)\big|[f(x)-f(a)].$

E11) Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial. Let $\alpha \in \mathbb{Q}$ s.t. $f(\alpha)=0.$ Show that $\alpha \in \mathbb{Z}.$

E12) Let F be a finite field. Find a polynomial over F which has no root in $F.$

SOLUTIONS / ANSWERS

E1) Let $f : R \to S$ be a monomorphism, and let $\text{char } R = m, \text{char } S = n.$
Now, m is the least positive integer s.t.
$m \cdot 1 = 0$ in $R.$ …(2)
Also $f(1)$ is the identity in S. Hence, by definition, n is the least positive integer s.t.
$n \cdot f(1) = 0$ in $S.$ …(3)
(2) gives us $m \cdot f(1) = f(0) = 0,$ in $S.$ …(4)
From (3) and (4), we get $m \geq n.$
Similarly, you should see why $n \geq m.$
Thus, $m = n.$

E2) Let $f \neq \mathbf{0}$. Since $\text{Ker } f$ is an ideal of $F,$ and $\text{Ker } f \neq F,$ we get $\text{Ker } f = \{0\}.$ Thus, f is $1\text{-}1.$

E3) Let $o(r) = m, o(s) = n.$
Then $mr = 0, ns = 0,$ and m and n are the least such positive integers.
Now, $mr = 0 \Rightarrow (mr)s = 0$
$\Rightarrow r(ms) = 0$
$\Rightarrow ms = 0,$ since $r \neq 0$
$\therefore n \mid m.$ …(5)
Similarly, you should show that $m \mid n.$ …(6)
(5) and (6) give us $m = n,$ i.e., $o(r) = o(s).$

E4) Since 2 and 5 are primes dividing $10,$ by Cauchy's theorem for finite abelian groups (see Unit 7), we have $a, b \in R$ s.t.
$o(a) = 2$ and $o(b) = 5.$
Now, $o(a) = 2 \Rightarrow 5a = a \neq 0.$
Also, $o(b) = 5 \Rightarrow 2b \neq 0.$
But $(5a)(2b) = 10ab = 0,$ since $o(R) = 10.$
Thus, $5a$ and $2b$ are zero divisors in $R.$
Hence, R is not an integral domain.

E5) By E3, $o(r) = o(1) \; \forall \; r \in R^*.$ …(7)
If $\text{char } R = 0,$ then $o(1)$ is infinite.
So, by (7), $o(r)$ is infinite $\forall \; r \in R^*.$

If $\text{char } R = p,$ then by (7), $o(1) = p = o(r) \; \forall \; r \in R^*.$

E6) Let $p(x) = 3x^5 + 15x^4 - 20x^3 + 10x + 20.$
Now 5 divides each of the coefficients of $x^4, x^3, x^2, x^1, x^0,$ i.e., $15, -20, 0, 10, 20.$
Also $5 \nmid 3,$ the leading coefficient, and $5^2 \nmid 20,$ the constant term.
Hence, by Eisenstein's criterion, $p(x)$ is irreducible over $\mathbb{Q}.$

Since $\deg p(x) > 2,$ it is reducible over $\mathbb{R}.$

E7) i) Suppose, to the contrary, that $f(x)$ is reducible over F.
Then $f(x)=g(x)h(x)$ in $F[x]$, where $\deg g(x)\geq 1$, $\deg h(x)\geq 1$.
$\Rightarrow af(x)=[ag(x)]h(x)$, with $\deg ag(x)\geq 1$ and $\deg h(x)\geq 1$.
Thus, $af(x)$ is reducible in $F[x]$, a contradiction.

You can solve (ii) and (iii) along the same lines as (i).

E8) Note that $25=5^2$. So we can look for an irreducible quadratic polynomial over $\mathbb{Z}_5$, to construct a field of order 25. You can see Example 6 for completing the solution.

E9) i) Let $f(x)$ be the given polynomial, and $g(x)=140f(x)$.
Then $g(x)=350x^5+315x^4+525x^3+84x^2+120x+42$.
Now, taking $p=3$ and applying Eisenstein's criterion, you should be able to conclude that $g(x)$ is irreducible over $\mathbb{Q}$.
Hence, $f(x)$ is irreducible over $\mathbb{Q}$ (using E7(i)).

ii) You should check that none of the elements of $\mathbb{Z}_{11}$ is a root of the given polynomial. Hence, it is irreducible.

iii) Again, as in (ii), show that this is irreducible.

iv) Using the $\bmod\ p$ test, for $p=3$, you should show that this is irreducible.

v) Apply the $\bmod\ p$ test for $p=5$, and prove this.

E10) Let $g(x)=f(x)-f(a)\in F[x]$. Then $g(a)=0$, i.e., a is a root of $g(x)$.
Hence, $(x-a)\mid g(x)$. Hence the result.

E11) Let $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in\mathbb{Z}[x]$, and let $\alpha=\frac{p}{q}$, with

$(p,q)=1$.
Then $p^n+a_{n-1}p^{n-1}q+\cdots+a_1pq^{n-1}+a_0q^n=0$.
If $q=\pm1$, then $\alpha\in\mathbb{Z}$.
Suppose $q\neq\pm1$, and let r_1 be a prime dividing q. Then r_1 divides $[-q(a_{n-1}p^{n-1}+\cdots+a_1pq^{n-2}+a_0q^{n-1})]=p^n$.
Hence, $r_1\mid p$ (see Unit 1).
We reach a contradiction because $(p,q)=1$.
Hence, q has no prime factors.
Hence, $q=\pm1$, i.e., $\alpha\in\mathbb{Z}$.

E12) Let $F=\{a_1,a_2,\ldots,a_n\}$. Then

$$f(x)=1+\prod_{i=1}^{n}(x-a_i)\in F[x].$$

Also $f(a_i)=1\ \forall\ i=1,\ldots,n$.
Thus, no element of F is a root of $f(x)$.
Hence, $f(x)$ fits the given constraints.