DIRECTORATE OF DISTANCE EDUCATION

UNIVERSITY OF NORTH BENGAL

MASTERS OF SCIENCE-MATHEMATICS

SEMESTER -I

ABSTRACT ALGEBRA

DEMATH-1 CORE-1

BLOCK-2

UNIVERSITY OF NORTH BENGAL

Postal Address:

The Registrar,

University of North Bengal,

Raja Rammohunpur,

P.O.-N.B.U.,Dist-Darjeeling,

West Bengal, Pin-734013,

India.

Phone: (O) +91 0353-2776331/2699008

Fax:(0353) 2776313, 2699001

Email: regnbu@sancharnet.in ; regnbu@nbu.ac.in

Wesbsite: www.nbu.ac.in

First Published in 2019

FOREWORD

The Self-Learning Material (SLM) is written with the aim of providing simple and organized study content to all the learners. The SLMs are prepared on the framework of being mutually cohesive, internally consistent and structured as per the university's syllabi. It is a humble attempt to give glimpses of the various approaches and dimensions to the topic of study and to kindle the learner's interest to the subject

We have tried to put together information from various sources into this book that has been written in an engaging style with interesting and relevant examples. It introduces you to the insights of subject concepts and theories and presents them in a way that is easy to understand and comprehend.

We always believe in continuous improvement and would periodically update the content in the very interest of the learners. It may be added that despite enormous efforts and coordination, there is every possibility for some omission or inadequacy in few areas or topics, which would definitely be rectified in future.

We hope you enjoy learning from this book and the experience truly enrich your learning and help you to advance in your career and future endeavours.

ABSTRACT ALGEBRA

BLOCK-1

BLOCK-2

BLOCK-2 ABSTRACT ALGEBRA

Introduction to the block

Abstract algebra begins with the observation that several sets that occur naturally in mathematics, such as the set of integers, the set of rationals, the set of 2×2 matrices with entries in the reals, the set of functions from the reals to the reals, all come equipped with certain operations that allow one to combine any two elements of the set and come up with a third element. These operations go by different names, such as addition, multiplication, or composition (you would have seen the notion of composing two functions in calculus). Abstract algebra studies mathematics from the point of view of these operations, asking, for instance, what properties of a given mathematical set can be deduced just from the existence of a given operation on the set with a given list of properties. We will be dealing with some of the more rudimentary aspects of this approach to mathematics in this book.

In unit 8, So far we have studied group which is an algebraic structure equipped with one binary operation. In this chapter we shall study ring which is an algebraic structure equipped with two binary operations. we will discuss various properties of those functions between rings which preserve the algebraic structure of their domain rings. These functions are called ring Homomorphisms.

After understanding the concept of ring isomorphism's. In unit 9, we have introduced ideals. Ideal is an important algebraic structure will be useful in further study and we will also discuss the different algebra of ideals.

In unit 10, we will discuss prime and reducible elements. We are all quite familiar with the ring I of integers. Also our familiar set Q of rational numbers is nothing but the set of quotients of the elements of I. Taking motivation from these facts, we now proceed to construct the quotient field of an arbitrary integral domain.

In unit 11, we will discuss Euclidean rings or Euclidean domains. We will also discuss the various properties of Euclidean domain. Every field is a Euclidean ring. Every Euclidean ring is a principal ideal domain. We have also discussed fundamental theorem of Arithmetic.

In unit 12, we will discuss the concept of Unique Factorization Domain. We will discuss various properties of Unique Factorization Domain. We have discussed polynomial ring over unique factorization domain.

In unit 13, we will introduce the concept of principal ideal domain. We will discuss various properties of principal ideal domain. Every Euclidean ring is a principal ideal domain. Every field is a principal ideal ring. We have given examples of PID that are not Euclidean.

In unit 14, we will discuss rings of polynomials. We will discuss various properties of rings of polynomials and study different types of rings of polynomials. If F is a field, then the set F [x] of all polynomials over F is an integral domain.

UNIT – 8: RING HOMOMORPHISM

STRUCTURE

8.0 OBJECTIVES

After studying this unit, you should be able to:

- Explain the concept of homomorphism
- Describe Isomorphism

8.1 INTRODUCTION

So far we have studied group which is an algebraic structure equipped with one binary operation. In this chapter we shall study ring which is an algebraic structure equipped with two binary operations. we will discuss various properties of those functions between rings which preserve the algebraic structure of their domain rings. These functions are called ring Homomorphisms.

8.2 HOMOMORPHISMS

Let us start our study with definition of ring. . .

Definition: Suppose R is a non-empty set equipped with two binary operation called addition and multiplication and denoted by '+' and '.' respectively i.e. for all a, b ∈ R we have a + b ∈ R and a.b ∈ R Then this algebraic structure (R, +, .) is called a ring, if the following postulates are satisfied:

1. Addition is associative, i.e.

$(a + b) + c = a + (b + c)$; $\forall a, b, c \in R$.

2 Addition is commutative, i.e., $a + b = b + a$, $\forall a, b \in R$

3 There exists an element denoted by 0 in R such that

$0 + a = a$; $\forall a \in R$

4 To each element a in R there exists an element-a In R such that

$(-a) + a = 0$.

5. Multiplication is associative, I.e.,

$a . (b . c) = (a . b) . c$; $\forall a, b, c \in R$

6. Multiplication is distributive with respect to addition

for all $a, b, c \in R$

$a . (b + c) = a . b + a . c$ Left distributive law

and $(b + c) . a = b . a + c . a$ Right distributive law

Definition: If in a ring R, the multiplication composition is also commutative i.e, if we have ab=ba for all a, b in R, Then R is called a commutative ring.

Definition: A non-zero element of a ring is called a zero divisor or a divisor of zero if there exists an element $b \neq 0$ in R such that either $a . b = 0$ or $b . a = 0$.

Rings without zero divisors: A ring R is without zero-divisors, if the product of no two non-zero elements of R is zero.

Definition: A ring is called an integral domain if it (i) Is commutative, (ii) has unit element, (iii) is without zero divisors.

Definition: A ring R with at least two elements is called a field if it (i) is commutative, (ii) has unity, (iii) is such that each non zero element possesses multiplicative inverse.

Definition: A ring R with at least two elements is called a division ring or a skew field if it (i) has unity, (ii) is such that each non-zero element possesses multiplicative inverse.

Definition: A ring R with at least two elements is called a field if it (i) is commutative, (ii) has unity, (iii) is such that each non zero element possesses multiplicative inverse.

Definition : The characteristic of a field, F, denoted char (F) , is defined to be the smallest positive integer p such that p.F = 0 if such a p exists and is defined to be 0 otherwise .

Definition: A map f : R→ S between rings is called a ring homomorphism if f (x + y) = f (x) + f (y) and f (x y) = f (x) f (y) for all x, y ∈ R.

Note: The word 'homomorphism' is derived from two Greek words 'homos', meaning 'link', and 'morphe', meaning 'form'.

Example: The map from $\mathbf{Z}$ to $\mathbf{Z}_n$ given by $x \mapsto x \bmod n$ is a ring homomorphism.

Let us define two sets related to a given homomorphism.

Definition: Let a mapping f : R→ S between rings be a ring homomorphism. Then we define

(i) the image of f to be the set

{ s ∈ S | there exists an r ∈ R such that f(r) = s }

(ii) the kernel off to be the set

Ker f = { r □ R | f (r) = 0_s }

Note that Im f □ S, and Ker f □ R.

Definition: (a) Left Ideal

A non-empty subset S of a ring is said to be a left Ideal of R if:

(i) S is a subgroup of R with respect to addition

(ii) r s ∈ S for all r ∈ R and s ∈ S.

(b) Right Ideal

A non-empty subset S of a ring R is said to be a right ideal of R if:

(i) S is a subgroup of R under addition

(ii) s r ∈ S for all r ∈ R and s ∈ S

(c) Ideal .

A non - empty subset S of a ring R is said to be an ideal (also a two sided ideal) if and only if it is both a left ideal and a right ideal . Thus a non-empty subset of a ring R is said to be an Ideal of R if :

(i) S is a subgroup of R under addition i.e., S is a subgroup of the additive group of R.

(ii) r s ∈ S and s r ∈ S for every r in R and for every s in S.

Note: Every ring R always possesses two improper ideals: one R itself and the other consisting of 0 only. These are respectively known as the unit ideal and the null ideal.

Definition : Let R be a ring and I an ideal of R . Then the quotient ring of R by I , denoted R / I is the ring defined by the following binary operations :

(r + I) + (s + I) = (r + s) + I and (r + I) × (s + I) = (r s+ I) ∀ r , s ∈ R .

Theorem 1 : Composition of two ring homomorphisms is a ring homomorphism.

Proof : Let φ : R → S and ψ : S → T be two ring homomorphisms . We need to show that ψ∘φ (defined by ψ (φ (r))) is a ring homomorphism. First , we check that 1 is sent to 1 : ψ (φ (1)) = ψ (1) = 1 , the first equality because φ is a ring homomorphism , the second equality because ψ is a ring homomorphism . Second, choose r1, r2 ∈ R. We check that the composition preserves addition: ψ (φ (r1 + r2)) = ψ (φ (r1) + φ (r2)) = ψ (φ (r1)) + ψ (φ (r2)) . Again, the first

equality holds because φ is a ring homomorphism, the second equality because ψ is a ring homomorphism. The reason that multiplication is preserved is similar : ψ (φ (r1 ·r2)) = ψ (φ (r1) ·φ (r2)) = ψ (φ(r1))·ψ (φ (r2)) .

Theorem 2 : A ring homomorphism φ : R → S is 1-1 ⇐⇒ kerφ = {0}.

Proof : Suppose φ is 1 - 1 and let x ∈ ker φ (x could be anything in ker φ) . Then φ (0) = 0 = φ (x) . Since φ is 1 - 1 this forces 0 = x . So anything that is in ker φ must be 0, so ker φ = { 0 } . Suppose that ker φ = { 0 } and let x , y ∈ R be such that φ (x) = φ (y) . We need to show that x must equal y. But φ (x) = φ (y) implies φ (x – y) = φ (x) – φ (y) = 0 , so x − y ∈ ker φ, and so x − y = 0 . . .

Lemma : Suppose f : R → S is a ring homomorphism and the only two sided ideals of R are {0} and R. Then f is injective.

Proof : Since Ker f is a two - sided ideal of R , then either Ker f = { 0 } or Ker f = R. But Ker f ≠ R since f (1) = 1 by definition (in words, Ker f is a proper ideal). . .

At this point , it may be worth already noticing the analogy between on the one hand rings and their two - sided ideals , and on the other hand groups and their normal subgroups .

• Two - sided ideals are stable when the ring acts on them by multiplication , either on the right or on the left, and thus r a r−1 ∈ I , a ∈ I , r ∈ R , while normal subgroups are stable when the groups on them by conjugation g h g−1 ∈ H , h ∈ H , g ∈ G (H ≤ G) .

• Groups with only trivial normal subgroups are called simple . We will not see it formally here , but rings with only trivial two - sided ideals as in the above lemma are called simple rings .

• The kernel of a group homomorphism is a normal subgroup , while the kernel of a ring homomorphism is an ideal .

• Normal subgroups allowed us to define quotient groups . We will see now that two - sided ideals will allow to define quotient rings .

Example : Let R and S be commutative rings , and let φ : R → S be a ring homomorphism.

(a) Does φ map idempotent elements to idempotent elements ?

Solution : Yes ; if e2 = e, then (φ (e))2 = φ (e2) = φ (e) .

(b) Does φ map nilpotent elements to nilpotent elements ?

Solution : Yes ; if xn = 0, then (φ (x)) n = φ(x n) = φ(0) = 0 .

(c) Does φ map zero divisors to zero divisors ?

Solution : No ; let π : Z2 ⊕Z2 → Z2 be given by φ ((x , y)) = x. Then π maps the zero divisor (1 , 0) to 1 , which is definitely not a zero divisor .

Theorem 3: Let f : R → S be a ring homomorphism. Then

(1) f (0_R) = 0_S,

(2) f (− r) = − f (r) for all r ∈ R,

(3) if r ∈ R * then f (r) ∈ S * and f (r^{-1}) = f (r) $^{-1}$, and

(4) if R' ⊂ R is a subring, then f (R ') is a subring of S.

Proof: $0_R + 0_R = 0_R$, f (0_R) + f (0_R) = f (0_R). Then since S is a ring, f (0_R) has an additive inverse, which we may add to both sides. Thus we obtain f (0_R) = f (0_R) + f (0_R) + − f (0_R) = f (0_R) + − f (0_R) = 0_S , as desired.

Let r ∈ R. Since r + − r = − r + r = 0_R, we have f (r) + f (− r) = f (− r) + f (r) = f (0_R) = 0_S, where the last equality comes from (1). Thus f (− r) = − f (r) as additive inverses are unique.

Now let r ∈ R *. Then there exists r^{-1} ∈ R such that r .· r^{-1} = r^{-1} . r = 1_R. Then since f is a ring homomorphism we have . . . .

f (r) . f (r^{-1}) = f (r^{-1}) f (r) = f (1_R) = 1_S.

Thus f (r) has a multiplicative inverse and it is f (r^{-1}) .

Lastly, let R' ⊂ R be a subring.

To show that f (R ') is a subring we must show that 1_S ∈ f (R ') and for all s_1, s_2 ∈ f (R '), s_1–s_2 and $s_1 s_2$ are also in f (R '). Since s_1, s_2 ∈ f (R ') , there exists r_1, r_2 ∈ R ' such that f (r_1) = s_1 and f (r_2) = s_2. Thus s_1–s_2 = f (r_1) – f (r_2) = f (r_1) + f (− r_2) = f (r_1 – r_2) , and $s_1 s_2$ = f (r_1) f (r_2) = f ($r_1 r_2$). Since R ' is a subring , r_1 – r_2 and r_1 r_2 are contained in R ' . Hence s_1 – s_2 and $s_1 s_2$ are in f (R ') .

Furthermore, 1_R ∈ R ' so 1_S = f (1_R) ∈ f (R ') . Therefore, f (R ') is a subring of S . . .

Check Your Progress-1

1. A Ring is said to be commutative if it also satisfies the property

(a) No zero divisors (b) Multiplicative Identity

(c) Multiplicative Inverse (d) Commutativity of multiplication

2. gof (x, y) is equal to:

(a) gof(x) . gof(y) (b) gof(x) + gof(y)

(c) $gof(x^{-1})$. $gof(y^{-1})$ (d) $gof(x)$. $gof(y^{-1})$

8.3 ISOMORPHISMS

Definition: Let R and S be two rings. A homomorphism f : R □□ S is called an isomorphism if f is 1-1 and onto .

An isomorphism of a ring R onto itself is called an automorphism of R . For example , the identity' function I_R : R □ R : I_R (x) = x is an automorphism .

Note: The word ' isomorphisms ' is derived from the Greek word ' ISOS ' meaning' equal ' .

Let us look at another example of an isomorphism . . .

Example: The map from **C** to ring of 2 × 2 real matrices given by $a + bi \mapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ is a ring isomorphism .

Theorem 4 : (Fundamental Theorem for Homomorphisms) . Let φ : R → S be a ring homomorphism , where R is a commutative ring. Use φ (R) to denote the image of φ (everything that is φ (r) for some r). Then φ (R) ≅ R / ker φ .

Proof : One should note that φ (R) is itself a ring . Check this . Let I = ker φ which is an ideal . Define ψ : R / ker φ → φ (R) by setting ψ (r + I) = φ (r) . Check that ψ is a well-defined homomorphism .

Also, it is clear that ψ is onto. Lastly, consider the ker ψ:

Ker ψ = { r + I | φ (r) = 0}

= { r + I | r belongs to ker φ }

= { r + I | r belongs to I }

Since I is the zero of R/I, this means that ψ is 1-1.

Example : Let R be a commutative ring, with identity 1.

(a) Show that if e is an idempotent element of R, then 1 − e is also idempotent.

Solution: We have (1 – e) 2 = (1 – e) (1 – e) = 1 – e – e + e2 = 1 – e – e + e = 1 − e.

(b) Show that if e is idempotent, then R ≅ Re ⊕ R (1 – e) .

Solution: Note that e (1 – e) = e − e2 = e − e = 0 . Define φ : R → Re ⊕ R (1 – e) by φ (r) = (re , r (1 − e)) , for all r ∈ R. Then φ is one-to-one since if φ (r) = φ (s) , then re = se and r (1 − e) = s (1 – e) , and adding the two equations gives r = s. Furthermore, φ is onto, since for any element (ae , b (1− e)) we have (a e , b (1 – e)) = φ (r) for r = a e +b (1 – e). Finally, it is easy to check that φ preserves addition , and for any r , s ∈ R we have φ (rs) = (rs e, r s (1 – e)) and φ (r) φ (s) = (r e , r (1 –e)) (s e , s (1 – e)) = (rs e 2 , r s (1 − e) 2) = (rs e , r s (1 − e)) . It is clear that φ (1) = (e ,1 − e) , which is the multiplicative identity of Re⊕R(1−e).

Example : Find the kernel of the evaluation map from R[x] into C

Solution: A polynomial with real coefficients that has i as a root must also have −i as a root. Therefore for f(x) ∈ R[x] we have f(i) = 0 if and only if x−i and x + i are both factors of f(x). That is, if and only if x2 + 1 is a factor of f(x). The kernel of the evaluation mapping is $< x^2 + 1 >$

Theorem 5 : If ϕ : R → S is a ring homomorphism, then ker (ϕ) is an ideal of R .

Proof : We know that ker (ϕ) is a subgroup of (R , +) . If r ∈ R and n ∈ ker (ϕ) , then ϕ (rn) = ϕ (r) ϕ (n) = ϕ (r) 0 = 0 and ϕ (n r) = ϕ (n) ϕ (r) = 0 ϕ (r) = 0, which shows that r n and n r ∈ ker (ϕ) for all r ∈ R and n ∈ ker (ϕ) .

Theorem 6 : If $\phi : R \to R$ is a ring homomorphism, then ϕ is either the zero or the identity homomorphism .

Proof : If $t = \phi(1)$, then as above, $t2 = t$, i.e. $t(t-1) = 0$. Since R is a field this implies that $t = 0$ or $t = 1$. If $t = 0$, then for all $a \in R$, $\phi(a) = \phi(a \cdot 1) = \phi(a)\phi(1) = \phi(a) \cdot 0 = 0$, I .e . ϕ is the zero homomorphism. So we may now assume that $t = 1$. If $t = 1$, $\phi(n) = \phi(n \cdot 1) = n \cdot \phi(1) = n \cdot 1 = n$ for all $n \in Z$. Therefore for $n \in N \setminus \{0\}$ and $m \in Z$, $m = \phi(m) = \phi n \cdot m\, n = \phi(n)\phi m\, n = n\phi m\, n$ from which it follows that $\phi(m/n) = m/n$. Thus we now know that $\phi|Q$ is the identity. Since $\ker(\phi) \neq R$, we must have $\ker(\phi) = \{0\}$ so that ϕ is injective. In particular $\phi(b) \neq 0$ for all $b \neq 0$. Moreover if $a > 0$ in R and $b := \sqrt{a}$, then $\phi(a) = \phi b\, 2 = [\phi(b)]\, 2 > 0$.

So if $y , x \in R$ with $y > x$, then $\phi(y) - \phi(x) = \phi(y - x) > 0$, i.e. ϕ is order preserving. Finally, let $a \in R$ and choose rational numbers $xn, yn \in Q$ such that $x\,n < a < y\,n$ with $xn \uparrow a$ and $yn \downarrow a$ as $n \to \infty$. Then $x\,n = \phi(x\,n) < \phi(a) < \phi(yn) = yn$ for all n. Letting $n \to \infty$ in this last equation then shows, $a \leq \phi(a) \leq a$, i.e. $\phi(a) = a$. Since $a \in R$ was arbitrary, we may conclude that ϕ is the identity map on R.

Example: If R is a ring with unity, while R ' is a ring without unity . It is impossible to exist a surjective ring homomorphism from R to R ' . For example , no surjective homomorphism from Z to nZ for $n > 2$. Actually , there is no non trivial ring homomorphism from Z to nZ since any non trivial subring of nZ has no unity .

Example : If both R , R ' are rings with unity , and is some isomorphism from R to R ' . Then $\varphi(1) = 1$ ' . In particular , if R is a cyclic group , this already determines the isomorphism . For example , construct an isomorphism between Zab and $Za \to Zb$, for a , b are positive integers and $\gcd(a , b) = 1$. The unity of Zab is (1) and the unity of Za and Zb is (1,1). The isomorphism must be $(1) = (1 , 1)$. Then any $(n) = (n \cdot 1) = n(1) = (n , n)$.

Example : Show that the ring $Z[\sqrt{2}]$ has precisely two automorphisms.

Solution: The first automorphism is the identity mapping. $\varphi : Z[\sqrt{2} \to Z[\sqrt{2}]$ defined by $\varphi(m+n\sqrt{2}) = m-n\sqrt{2}$ is also an automorphism. (You

should check this.) Why are these the only possible automorphisms? By definition, for any automorphism we must have φ(1) = 1, and therefore φ (m) = m and φ (n) = n for m + n √2. Furthermore, φ (√2) φ (√2) = φ (√2 √2) = φ (2) = 2, which forces φ (√2) = ± √2. This shows that we have in fact found all possible automorphisms of Z [√ 2] .

Example : Let R be a commutative ring with char (R) = 2. Define φ : R → R by φ (x) = x 2 , for all x ∈ R .

(a) Show that φ is a ring homomorphism .

Solution : Let a , b ∈ R . Remember that 2 x = 0 for x ∈ R , since char (R) = 2 . Then φ (a + b) = (a + b) 2 = a2 + 2ab + b2 = a2 + b2 = φ (a) + φ (b) , and φ (a b) = (a b) 2 = a b b2 = φ (a) φ(b) , so φ respects addition and multiplication . Finally , φ (1) = 12 = 1 .

(b) Find an example of such a ring in which φ is an automorphism .

Solution : Let R be any Boolean ring . We know that it has characteristic 2 , and on such a ring φ is just the identity mapping .

(c) Find an example of such a ring in which φ is not onto .

Solution : The polynomial ring Z2[x] has characteristic 2 , and in the image of φ every polynomial has even degree , so φ is not onto .

Theorem 7 : (First isomorphism theorem) Let R and S be rings and let f : R → S be a homomorphism . Then :
(1) The kernel of f is an ideal of R ,
(2) The image of f is a subring of S ,
(3) The map F : R / ker f → im f ⊂ S, r + ker f → f (r) is a well-defined isomorphism.

Proof: The image of f is a subring by Theorem 1. Let us prove that ker f is an ideal. By Theorem 1, f (0) = 0 , so 0 ∈ ker f and hence the kernel is nonempty. Let a,b ∈ ker f and let r ∈ R. Then since f is a homomorphism we have

f (a + b) = f (a) + f (b) = 0 + 0 = 0 ,
f (r a) = f (r) f (a) = f (r) . 0 = 0 ,
f (a r) = f (a) f (r) = 0 . f (r) = 0 .

Thus a + b, r a and a r are in ker f and so ker f is an ideal .

Consider the map f. We first show that it is well-defined . Let r , r ' ∈ R be such that r – r ' ∈ ker f, i.e., such that r + ker f = r ' + ker f. Then,

$f(r) = f(r' + (r - r')) = f(r') + f(r - r') = f(r') + 0 = f(r')$,

so f is well defined. Let $r_1 + I$, $r_2 + I \in R / I$. Then since f is a homomorphism we have :

$F(r_1 + I + r_2 + I) = F(r_1 + r_2 + I) = f(r_1 + r_2) = f(r_1) + f(r_2) = F(r_1 + I) + F(r_2 + I)$

$F((r_1 + I)(r_2 + I)) = f(r_1 r_2 + I) = f(r_1 r_2) = f(r_1) f(r_2) = F(r_1 + I) F(r_2 + I)$

$F(1 + I) = f(1) = 1$.

Therefore F is a homomorphism.

Let us prove that F is bijective . If r + ker f ∈ ker F, then F (r + I) = f (r) = 0 and so r ∈ ker f or equivalently r + ker f = ker f. Thus ker F is trivial and so, F is injective. Let s ∈ im f. Then there exists an r ∈ R such that f (r) = s or equivalently that F (r + ker f) = s. Thus s ∈ im f and so F is surjective . Hence F is an isomorphism as desired .

Definition: Let R be a ring. A non-empty subset S of the set R is said to be subring of R if S is closed with respect to the operations of addition and multiplication in R and S itself is a ring for these operations.

Theorem 8 : (Second isomorphism theorem) Let R be a ring, let $S \subset R$ be a subring, and let I be an ideal of R . Then :
(1) $S + I := \{ s + a : s \in S , a \in I \}$ is a subring of R,
(2) $S \cap I$ is an ideal of S, and
(3) (S + I) / I is isomorphic to S / (S ∩ I).

Proof: (1): S is a subring and I is an ideal so 1 + 0 ∈ S + I.

Let $s_1 + a_1$ and $s_2 + a_2$ be elements of S + I. Then

$(s_1 + a_1) - (s_2 + a_2) = (s_1 - s_2) + (a_1 - a_2) \in S + I$

and $(s_1 + a_1)(s_2 + a_2) = s_1 s_2 + (s_1 a_2 + a_1 s_2 + a_1 a_2) \in S + I$.

Hence S + I is a subring of R.

(2): The intersection $S \cap I$ is no nempty since 0 is contained in I and S. Let $a_1, a_2 \in S \cap I$ and let $s \in S$. Then $a_1 + a_2 \in S \cap I$ since S and I are both closed under addition. Furthermore $s a_1$ and $a_1 s$ are in $S \cap I$ since I is closed under multiplication from $R \supset S$ and S is closed under multiplication. Therefore $S \cap I$ is an ideal of S.

(3): Consider the map $f : S \rightarrow (S + I)/ I$ which sends an element s to s + I. This is a ring homomorphism by definition of addition and multiplication in quotient rings. We claim that it is surjective with kernel $S \cap I$, which would complete the proof by the first isomorphism theorem. Consider elements $s \in S$ and $a \in I$. Then $s + a + I = s + I$ since $a \in I$, so $s + a + I \in$ im f and hence f is surjective. Let $s \in S$ be an element of ker f. Then $s + I = I$ which holds if and only if $s \in I$ or equivalently if $s \in S \cap I$. Thus ker $f = S \cap I$

Theorem 9 : (Third isomorphism theorem) Let R be a ring and let $J \subset$ I be ideals of R. Then I/J is an ideal of R / J and $(R / J) /(I / J) \cong R/I$.

Proof: Since I and J are ideals, they are nonempty and so $I/J = \{ a + J : a \in I \}$ is also nonempty. Let $a_1, a_2 \in I$ and let $r \in R$. By definition of addition and multiplication of cosets, we have

$(a_1 + J) + (a_2 + J) = (a_1 + a_2) + J,$

$(r + J) (a_1 + J) = r a_1 + J$, and

$(a_1 + J) (r + J) = a_1 r + J.$

Since I is an ideal, $a_1 + a_2$, $r a_1$, and $a_1 r$ are contained in I so I / J is an ideal of R / J.

Consider the map $f : R/J \rightarrow R/I$ that sends r + J to r + I. We claim that this is a well-defined surjective homomorphism with kernel equal to I / J . Then (R / J) / (I / J) is isomorphic to R/I by the first isomorphism theorem.

Properties of isomorphism of rings:

If f is an isomorphism of a ring R onto a ring R ' ,then

(i) the image of the zero of R is the zero of R . . .

(ii) the image of the negative of an element of R is the negative of the image of that element i.e. $f (- a) = - f (a)$ for all a in R . . .

(iii) If R Is commutative ring , then R ’ is also a commutative ring . . .

(iv) If R is without zero divisors , then R’ is also without zero divisors . . .

(v) If R is with unit element , then R ’ is also with unit element . . .

(vi) If R is a field , then R ’ is also a field . . .

(vil) If R is a skew field , then R ’ is also a skew field . . .

Proof: (i) Let $a \in R$. Then $f(a) \in R'$, Let 0 ’ denote the zero element of R ’ . To prove that $f(0) = 0'$.

We have $f(a) + 0' = f(a) = f(a + 0) = f(a) + f(0)$. By cancellation law for addition in R ' , we get from $f(a) + 0' = f(a) + f(0)$, the result that $0' = f(0)$.

(ii) We have $f(a) + f(-a) = f[a + (-a)) = f(0) = 0'$.

Therefore, f (- a) is the additive inverse of f (a) in R'.

Thus $f(-a) = -f(a)$.

(iii) Let f (a) and f (b) be any two elements of R’ . Then $a , b \in R$.

We have $f(a) f(b) = f(ab) = f(ba) = f(b) f(a)$

Therefore, R’ is also commutative . . .

(iv) We have $f(0) = 0'$. Also f is one-one. Therefore 0 is the only element of R whose f-image is 0 ’ .

Let f (a) , f (b) be two non-zero elements of R ' . Then $f(a) \neq 0'$, $f(b) \neq 0'$ implies $a \neq 0, b \neq 0$. Since R is without zero divisors, therefore $a \neq 0, b \neq 0 \rightarrow ab \neq 0 \rightarrow f(ab) \neq f(0)$

$\rightarrow f(a) f(b) \neq 0' \rightarrow$ R is without zero divisors . . .

(v). Let 1 be the unit element of R. Then $f(1) \in R'$. If f (a) is any element of R ' , we have

$f(l) f(a) = f(la) = f(a)$ and $f(a) f(1) = f(al) = f(a)$.

Therefore, f (1) is the unit element of R ’.

(vi) If R is a field, then R is commutative, with unity and each non-zero element of R will possess multiplicative inverse.

Now as proved in (iii) and (v) , R ' will be commutative and will also have the unit element i.e, f (l) .

Let f (a) be any non-zero element of R'. Then

$f(a) \neq 0' \rightarrow a \neq 0 \rightarrow a^{-1}$ exists.

Now $f(a^{-1}) \in R'$ and we have

$f(a^{-1}) f(a) = f(a^{-1} a) = f(1)$

$f(a^{-1})$ is the multiplicative inverse of f (a) .

Hence R ' is a field . . .

(vii) As shown in (v) R' will be with unit element i . e . , f (1) and as shown in (vi) cach non-zero element of R ' will be inversible .

Therefore R ’ is a skew-field .

Definition : An ideal M in an arbitrary ring R is called a maximal ideal if $M \neq R$ and the only ideals containing M are M and R .

Definition : Assume R is a commutative ring . An ideal P is called a prime ideal if $P \neq R$ and whenever the product a b of two elements $a , b \in R$ is an element of P , then at least one of a and b is an element of P .

Theorem 10 : . Assume R is a commutative ring . Then R is a field if and only if its only ideals are 0 and R . , .

Theorem 11: . Assume R is a commutative ring . The ideal M is a maximal ideal if and only if the quotient ring R / M is a field .

Proof : This follows from the Lattice Isomorphism Theorem for Rings along with theorem 10 . The ideal M is maximal if and only if there are no ideals I with $M \subset I \subset R$. By the Lattice Isomorphism Theorem the ideals of R containing M correspond bijectively with the ideals of R / M , so M is maximal if and only if the ideals of R / M are 0 and R / M . By Theorem 10 we see that M is a maximal ideal if and only if R / M is a field . .

Check Your Progress-2

3. An isomorphism of a ring R onto itself is called an _____of R.

a. automorphism

b. isomorphic

c. homomorphism

d. None of the above

4. If f : R □ R' is an isomorphism of rings, then f^{-1} : R' □ R is also an _____.

a. automorphism

b. isomorphic

c. homomorphism

d. None of the above

8.4 LET US SUM UP

In this unit we have discussed the definition and example of a ring homomorphism. The definition and examples of a ring isomorphism. Two rings are isomorphic if they have exactly the same algebraic structure.

8.5 KEYWORDS

1. ***Homomorphism:*** Homomorphism is derived from two Greek words 'homos', meaning 'link', and 'morphe', meaning 'form'.
2. ***Inclusion Map:*** Let S be a subring of a ring R and map i: H □ G, i(h) = h is a homomorphism. This function is called the **inclusion map.**

8.6 QUESTIONS FOR REVIEW

1. Let F be a field and let a ∈ F. Prove that ϕ: F[x] → F, ϕ(f(x)) = f(a) is a ring homomorphism.
2. Let R and S be rings and let φ: R → S be a homomorphism. Prove that φ is injective if and only if ker φ = {0}.
3. Let n ∈Z be a positive integer. Prove that ϕ: Z→Z, ϕ(a) = na is not a ring homomorphism.

4. Let R be a ring and let I be an ideal. Prove that ϕ: R $\rightarrow$ R/I, ϕ(r) = r + I is a ring homomorphism

8.7 SUGGESTED READINGS AND REFERENCES

1. Thomas W Judson (2013). *Abstract Algebra: Theory and Applications*. Orthogonal Publishing.
2. Paul B. Garrett (2007). *Abstract Algebra*. Chapman and Hall/CRC.
3. Vijay K Khanna (2017).*A Course in Abstract Algebra Fifth Edition*. Vikas Publishing House
4. LALJI PRASAD (2016). *Modern Abstract Algebra*. Paramount Publication
5. Stephen Lovett (2016). *Abstract Algebra: Structures and Applications*. Chapman and Hall/CRC

8.8 ANSWERS TO CHECK YOUR PROGRESS

1. (d) (answer for Check your Progress-1 Q.1)
2. (a) (answer for Check your Progress-1 Q.2)
3. (a) (answer for Check your Progress-2 Q.3)
4. (b) (answer for Check your Progress-2 Q.4)

UNIT – 9: IDEALS

STRUCTURE

9.0 OBJECTIVES

After studying this unit, you should be able to:

- Identify ideals
- Solve different algebra of ideals

9.1 INTRODUCTION

After understanding the concept of ring isomorphism's. In this unit we have introduced ideals. Ideal is an important algebraic structure will be useful in further study and we will also discuss the different algebra of ideals.

9.2 IDEALS

Definition: (a) Left Ideal

A non-empty subset S of a ring is said to be a left Ideal of R if:

(i) S is a subgroup of R with respect to addition

(ii) r s $\in$ S for all r $\in$ R and s $\in$ S.

(b) Right Ideal

A non-empty subset S of a ring R is said to be a right ideal of R if:

(i) S is a subgroup of R under addition

(i i) s r ∈ S for all r ∈ R and s ∈ S

(c) Ideal.

A non-empty subset S of a ring R is said to be an ideal (also a two sided ideal) if and only if it is both a left ideal and a right ideal. Thus a non-empty subset of a ring R is said to be an Ideal of R if:

(iii) S is a subgroup of R under addition i.e., S is a subgroup of the additive group of R.

(iv) rs ∈ S and sr ∈ S for every r in R and for every s in S.

Note: Every ring R always possesses two improper ideals: one R itself and the other consisting of 0 only. These are respectively known as the unit ideal and the null ideal.

Any other ideals of Rare called proper ideals. A ring having no proper ideals is called a simple ring.

Definition : Let I and J be ideals of R. (1) Define the sum of I and J by I + J ={ a + b | a ∈ I , b ∈ J } . (2) Define the product of I and J , denoted by I . J, to be the set of all finite sums of elements of the form a . b with a ∈ I and b ∈ J .

Definition : An ideal M in an arbitrary ring R is called a maximal ideal if M ≠ R and the only ideals containing M are M and R.

Example: If m is a fixed integer, the set P of Integers given by P= {xm: x is an integer} is an ideal of the ring R of all integers.

Solution: Let x_1m and x_2m be any two elements of P. Then x_1 and x_2 are some integers.

We have x_1m - x_2m =(x_1 - x_2) m ∈ P since x_1-x_2 is also an integer.

Therefore P is a subgroup of R Under addition.

Now let r be any integer i.e., r be any element of R and xm be any element of P. Then r (xm) = (rx) m ∈ P since rx is also an integer.

Therefore P is a left ideal of R. But R is a commutative ring. Hence P is an ideal of R.

Example: The set of integers I is only a subring but not an ideal of the ring of rational numbers (Q , + , .)

Solution: The product of a rational number and an integer is not necessarily an integer.

For example $3 \in I$, $2/5 \in Q$ but $(2/5).3=6/5$ does not belong to I.

Therefore, I is not an ideal of the ring of rational numbers.

Definition : An ideal M in an arbitrary ring R is called a maximal ideal if $M \neq R$ and the only ideals containing M are M and R .

Definition : Assume R is a commutative ring . An ideal P is called a prime ideal if $P \neq R$ and whenever the product a b of two elements $a , b \in R$ is an element of P , then at least one of a and b is an element of P .

Example : Here are a few examples. Checking the details is left as an exercise .

(1) In Z, all the ideals are of the form nZ for $n \in Z^{+}$. The maximal ideals correspond to the ideals pZ, where p is prime .

(2) Consider the integral domain Z [x] . The ideals (x) (i . e . , the subring containing polynomials with 0 constant term) and (2) (i . e , the set of polynomials with even coefficients) are not maximal since both are contained in the proper ideal (2 , x) . However, as we shall see soon , (2 , x) is maximal in Z [x] . . .

(3) The zero ring has no maximal ideals . . .

(4) Consider the abelian group Q under addition . We can turn Q into a trivial ring by defining ab = 0 for all $a , b \in Q$. In this case, the ideals are exactly the additive subgroups of Q . However, Q has no maximal subgroups, and so Q has no maximal ideals . . .

Note. The notion of a prime ideal is a generalization of “prime” in Z. Suppose $n \in Z^{+} \setminus \{1\}$ such that n divides ab. In this case, n is guaranteed to divide either a or b exactly when n is prime. Now, let nZ be a proper ideal in Z with $n > 1$ and suppose $ab \in Z$ for $a,b \in Z$. In order for nZ to

be a prime ideal, it must be true that n divides either a or b. However, this is only guaranteed to be true for all a,b ∈ Z when p is prime. That is, the nonzero prime ideals of Z are of the form pZ, where p is prime. Note that in the case of the integers, the maximal and nonzero prime ideals are the same . . .

Prime ideals

Definition : An ideal Pin R is prime if P ≠ R and whenever ab ∈ P, then a ∈ P or b ∈ P

Theorem 1 : . Assume R is a commutative ring . Then R is a field if and only if its only ideals are 0 and R . , .

Theorem 2: . Assume R is a commutative ring . The ideal M is a maximal ideal if and only if the quotient ring R / M is a field .

Proof : This follows from the Lattice Isomorphism Theorem for Rings along with theorem 1 . The ideal M is maximal if and only if there are no ideals I with M ⊂ I ⊂ R. By the Lattice Isomorphism Theorem the ideals of R containing M correspond bijectively with the ideals of R / M , so M is maximal if and only if the ideals of R / M are 0 and R / M . By Theorem 1 we see that M is a maximal ideal if and only if R / M is a field . .

Examples :

(1) The prime ideals of Z are (0) , (2) , (3) , (5) , . . . ; these are all maximal except (0) .

(2) If A = C [x] , the polynomial ring in one variable over C then the prime ideals are (0) and (x − λ) for each λ ∈ C ; again these are all maximal except (0) .

(3) If A = Z [x] , the polynomial ring in one variable over Z and p is a prime number, then (0) , (p) , (x) , and (p , x) = { a p + b X | a, b ∈ A } are all prime ideals of A . Of these , only (p , x) is maximal .

(4) If A is a ring of R-valued functions on a set for any integral domain R then
I = { f ∈ A | f (x) = 0 } is prime .

Check your Progress-1

1. Let R be a ring, U ⊆ R is ideal of R then A:U is a subgroup of R under addition B: for all u ∈ U and r ∈ R ; ur , ru ∈ U

(a) A and B both are true

(b) Only A is true

(c) Only B is true

(d) Both A and B are false

2. Which of the following structure is not a field

(a) (R , + , .)

(b) (C , + , .)

(c) (E , + , .)

(d) (Q , + , .)

9.3 ALGEBRA OF IDEALS

Let us start discussing the algebra of ideals

Theorem 3 : If f : A → B is a ring homomorphism and P is a prime ideal of B , then f^{-1} (P) is a prime ideal of A .

Proof : Notice that f induces a ring homomorphism g from A to B/P by post composing with the natural projection map B → B/P . Now a ∈ ker g if and only if f (a) ∈ P , so using the first isomorphism theorem we see that g induces an isomorphism from A /f^{-1} (P) to a subring of B/P . Since the latter is an integral domain, A / f^{-1} (P) must be an integral domain too . . .

Theorem 4 : Let a commutative ring R not be the zero ring . Then R is a field if and only if its only ideals are (0) and (1) .

Proof : In a field , every nonzero element is invertible, so an ideal in the field other than (0) contains 1 and thus is (1) . Conversely , if the only ideals are (0) and (1) then for all a ≠ 0 in R we have (a) = (1), and that

implies 1 = ab for some b, so a has an inverse . Therefore all nonzero elements of R are invertible , so R is a field . . .

Theorem 5 : Every ideal in a ring R is the kernel of some ring homomorphism out of R .

Proof : Since I is an additive subgroup we have the additive quotient group (of cosets) R / I = { r + I : r ∈ R } . Denote r + I as r. Under addition of cosets , the identity is 0 and the inverse of r is −r. Define multiplication on R/I by r · r ‘ = rr’ for r, r ‘ ∈ R / I. We need to check that this is well-defined: say r1 = r2 and r’ 1 = r’ 2 . Then r1 − r2 = x ∈ I and r’ 1 – r’ 2 = y ∈ I. So to show r1 r’ 1 = r2 r’ 2 ,

r1 r’ 1 − r2 r’ 2 = (r1 − r2 + r2) r’ 1 − r2 r’ 2 = (r1 − r2) r1 + r2 (r’ 1 – r’ 2) = x r’1 + r2 y ∈ I + I = I.

Checking the rest of the conditions to have R/I be a ring is left to you. The reduction mapping R → R/I by r 7→ r = r + I is not just an additive group homomorphism but a ring homomorphism too. Indeed, r1 + r2 = r1 + r2, r1r2 = r1r2, 1 = multiplicative identity in R/I The kernel of R → R/I is r ∈ R : r = 0 = {r : r + I = I} = I, so we have constructed an example of a ring homomorphism out of R with prescribed kernel I. This is analogous to the role of the canonical reduction homomorphism G → G/N in group theory that proves every normal subgroup N of a group G is the kernel of some group homomorphism out of G . . .

Theorem 6 : If R is an integral domain in which all ideals are principal then every nonzero prime ideal in R is maximal.

Proof : Write a nonzero prime ideal of R as (p) for some p ∈ R (the ideal is principal by hypothesis) . To prove (p) is maximal, let I be an ideal with (p) ⊂ I ⊂ R. We will show I = (p) or I = R. By hypothesis, I = (a) for some a ∈ R. Then the condition (p) ⊂ I says (p) ⊂ (a) , so p ∈ (a) . Thus p = ab for some b ∈ R, so ab ≡ 0 mod (p) . Since (p) is a prime ideal , R / (p) is an integral domain and therefore a ≡ 0 mod (p) or b ≡ 0 mod (p) . We will show one of these cases leads to (a) = (p) and the other leads to (a) = R. If a ≡ 0 mod (p) then a = p a’ for some a’ ∈ R, so p = ab = pa’ b. Since R is an integral domain, 1 = a’ b , so b is a unit . Thus (a) = (a b) = (p) . If b ≡ 0 mod (p) then b = pb’ for

some b' ∈ R, so p = a b = p a b' . As before we can cancel p, getting 1 = a b' , so a is a unit. Thus (a) = (1) = R . . .

Zorn's Lemma

If (S, ≤) is a partially ordered set such that every chain C in S has an upper bound in S then for every element x in S there is a maximal element y in S with x ≤ y . . .

Theorem 7 : If A is a ring and I an ideal of A such that I ≠ A , then A contains a maximal ideal m such that I ⊂ m .

Note that if A isn't the zero ring then I = (0) is an ideal not equal to A so it follows from this that there is always at least one maximal ideal .

Proof : Let A be the set of ideals of A not equal to A , ordered by inclusion . We must show that whenever C is a chain in A it has an upper bound in A , since then the result follows immediately from Zorn. So let's take such a chain C. Let I = ∪ J. Now suppose x1, x2 are in I. Then there are J1, J2 in C such that xi ∈ Ji . Either J1 ⊂ J2 or J2 ⊂ J1 ; WLOG the former . Then x1 ∈ J2, so x1 + x2 ∈ J2 ⊂ I. Also if a ∈ A then a xi ∈ J2 ⊂ I for each i. It follows that I is an ideal. It now just remains to check that I ≠ A. But 1 does not belong J for each J ∈ C, so 1 does not belong I and I ≠ A as required . . .

Theorem 8 : Let R be a ring and let I be an ideal of R , such that I = R . Then R / I is a ring. Furthermore there is a natural ring homomorphism u: R → R / I which sends r to r + I.

Proof : As I is an ideal , and addition in R is commutative , it follows that R / I is a group , with the natural definition of addition inherited from R . Further we have seen that φ is a group homomorphism . It remains to define a multiplication in R / I . Given two left cosets r + I and s+I in R / I , we define a multiplication in the obvious way, (r + I) (s + I) = r s + I. In fact this is forced by requiring that u is a ring homorphism . As before the problem is to check that this is well-defined. Suppose that r' + I = r + I and s' + I = s + I. Then we may find i and j in I ' ' such that r = r + i and s = s + j. We have ' r s' = (r + i) (s + j) = r s + i s + r j + i j. As ' I is an ideal, is + rj + ij ∈ I. It follows that r s' + I = rs + I and multiplication is well-defined. The rest is easy to check . . .

Example : Let X be a set and let R be a ring. Let F denote the set of functions from X to R. We have already seen that F forms a ring, under pointwise addition and multiplication.

Let Y be a subset of X and let I be the set of those functions from X to R whose restriction to Y is zero. Then I is an ideal of F. Indeed I is clearly non-empty as the zero function is an element of I. Given two functions f and g in F, whose restriction to Y is zero, then clearly the restriction of f + g to Y is zero. Finally, suppose that f $\in$ I, so that f is zero on Y and suppose that g is any function from X to R. Then gf is zero on Y . Thus I is an ideal. Now consider F/I. I claim that this is isomorphic to the space of functions G from Y to R. Indeed there is a natural map from F to G which sends a function to its restriction to Y , f $\rightarrow$ f|Y . It is clear that the kernel is I. Thus the result follows by the Isomorphism Theorem. As a special case, one can take X = [0 , 1] and R = R. Let Y = { 1 / 2 } . Then the space of maps from Y to R is just a copy of R . . .

Example : Let ϕ : Z [i] $\rightarrow$ Z_3 [i] be the unique homomorphism such that ϕ (1) = 1 and ϕ (i) = i, i.e. ϕ (a + ib) = a $\cdot$ 1 + b $\cdot$ i = a mod 3 + (b mod 3) i $\in$ Z_3 [i] . Notice that ker (ϕ) = { a + bi : a, b $\in$ < 3 > $\subset$ Z} = < 3 > + < 3 > i. Here is a more interesting example . . .

Example : In Z_{10} we observe that $3^2 = 9 = -1$ and also $7 = -3$ has this property, namely $7^2 = (-3)2 = 3\mathbf{2} = 9 = -1$. Therefore there exists a unique homomorphism, ϕ : Z [i] $\rightarrow$ Z10 such that ϕ (1) = 1 and ϕ (i) = $7 = -3$. The explicit formula is easy to deduce, ϕ (a + bi) = a $\cdot$ 1 + b $\cdot$ 7 = (a $-$ 3b) mod 10 . . .

Example : Let I be an ideal in a ring R with 1. I = R iff I contains a unit.

Proof. If I = R, then 1 $\in$ I is a unit in I. ($\Leftarrow=$) Let u $\in$ I be a unit. Then there exists v $\in$ R with vu = 1. For any r $\in$ R, we get r = r $\cdot$ 1 = r (v u) = (r v) u $\in$ I . . .

Example : A commutative ring R with 1 is a field iff its only two ideals are (0) and R .

Proof. ($=\Rightarrow$) Any nonzero ideal I contains some nonzero element, which is a unit since R is a field. By above example , I = R. ($\Leftarrow=$) Let $0 \neq a \in$ R and let I = (a) . By hypothesis , I = R , so I contains the identity 1 .

Therefore 1 = r a for some r ∈ R , so that r is the inverse of a . Therefore R is a field . . .

Example : Every ideal I in Z is principal.

Proof. Assume I ≠ (0) (which is principal) . Let c be the smallest positive element in I (exists by the well-ordering axiom) . Then (c) ⊆ I. Conversely, let a ∈ I. By the division algorithm, we can write a = c q + r with 0 ≤ r. . .

Theorem 8 : If ϕ : R → S is a ring homomorphism, then ker (ϕ) is an ideal of R .

Proof : We know from last quarter that ker (ϕ) is a subgroup of (R, +). If r ∈ R and n ∈ ker (ϕ), then ϕ (rn) = ϕ (r) ϕ (n) = ϕ (r) 0 = 0 and ϕ (nr) = ϕ (n) ϕ (r) = 0 ϕ (r) = 0, which shows that r n and n r ∈ ker (ϕ) for all r ∈ R and n ∈ ker (ϕ) .

Theorem 9 : Let P be an ideal of a commutative ring with identity. Then P is a prime ideal ⇐⇒ R/P is an integral domain . . .

Proof : P is a prime ideal if and only if a b ∈ P implies a ∈ P or b ∈ P for all a, b ∈ R . . But the statement a b ∈ P ⇒ a ∈ P or b ∈ P in R is equivalent to a b = 0 ⇒ a = 0 or b = 0 for all a, b ∈ R/P. This happens if and only if R / P is an integral domain . . .

Theorem 10 : Let I be an ideal in a ring R. The mapping π : R → R / I given by π (r) = r + I is a surjective ring homomorphism with kernel I.

Proof : The fact that π preserves addition and multiplication follows from the definition of addition and multiplication in R / I . It is surjective since any coset r + I is the image of r ∈ R. Finally, the kernel is the set of all r ∈ R such that π (r) = 0 + I , the zero element of R / I . But r + I =0+ I iff r ≡ 0 (mod I) iff r ∈ I. Thus the kernel is just I . . .

Example : 1. (p(x)) in F[x] is a prime ideal iff p(x) is irreducible. And we have seen that F[x]/(p(x)) is a field iff p(x) is irreducible .

2 . (p) in Z is a prime ideal iff p is prime. And we have seen that Zp is a field iff p is prime .

3 . The zero ideal in an integral domain R is prime .

4 . For a nonprincipal ideal, consider the ideal P = (p, x) in Z[x] where p is prime.

Assume f(x) = Paixi , g(x) = Pbjxj ∈ Z[x] with f(x)g(x) ∈ P. This says the constant term a0b0 is divisible by p. But then either p|a0 (and so f(x) ∈ P) or p|b0 (and so g(x) ∈ P). Therefore P is a prime ideal. In this case, the quotient ring is Zp, a field.

5. Now consider (x) in Z[x]. The quotient ring Z[x]/(x) ∼= Z, an integral domain, but not a field. Is (x) a prime ideal? Assume f (x) = P ai x i , g (x) = Pb j x j ∈ Z [x] with f (x) g (x) ∈ (x). This says the constant term a0b0 is 0, so either a0 = 0 (and so f (x) ∈ (x)) or b0 = 0 (and so g (x) ∈ (x)) .

Theorem 11 : Let P be an ideal in R. P is a prime ideal iff R / P is an integral domain.

Proof : (=⇒) Assume P is prime . Then R / P is a commutative ring with identity . We have R / P ≠ 0 since P ≠ R (or equivalently 1 does not belong P) . Therefore 0 ≠ 1 in R / P . Finally we check for zero divisors : if a b + P = (a + P) (b + P) = 0 + P , then a b ∈ P . Since P is prime , a ∈ P or b ∈ P ; that is, a + P = 0 + P or b + P = 0 + P. Therefore R / P is an integral domain. (⇐=) Now assume that R/P is an integral domain. Since 1 ≠ 0 in R / P , we have P ≠ R. Assume a b ∈ P. Then (a + P) (b + P) = a b + P = 0 + P. Since there are no zero divisors , we know that either a + P = 0 + P or b + P = 0 + P. And so, either a ∈ P or b ∈ P. How much more do we need to assume to have R / P be a field ? Our main example was (4) and (5) above: Z [x] modulo (x) was an integral domain , but modulo the larger ideal (p , x) it was a field . So it helps to have big ideals . . .

Theorem 12 : A commutative ring with zero divisors can be imbedded in a field .

OR Every Integral domain can be imbedded in a field .

Proof: Let D be a commutative ring without zero divisors .

Let D_0 be the set of all non-zero elements of D. Let S = D x D

0

i. e . , let S be the set of all ordered pairs (a , b) where a , b ∈ D and b ≠ 0 . Let us define a relation ~ in S . We shall say that

(a , b) ~ (c , d) if and only if a d = b c

We claim that this relation is an equivalence relation in S

Therefore it will partition S into disjoint equivalence classes . We shall denote the equivalence class containing (a , b) by $\frac{a}{b}$ other notations to denote this equivalence class are (a , b) or [a , b] .

Then $\frac{a}{b}$ = { (c , d) ∈ S : (c , d) ~ (a , b) } .

Obviously $\frac{a}{b} = \frac{c}{d}$ if (a , b) ~ (c , d) i . e . , iff a d = b c .

Also $\frac{a}{b} = \frac{a\,x}{b\,x}$ for all x ∈ D_0 . The reason is that

(a , b) ~ (a x , b x) since a b x = b a x .

These equivalence classes are our quotients. Let F be the set of all such quotients i.e., F= { $\frac{a}{b}$: (a , b) ∈ S }

We now define addition and multiplication operations in F as follows:

$$\frac{a}{b} + \frac{c}{d} = \frac{a\,d + b\,c}{b\,d} \; and \; \frac{a}{b}.\frac{c}{d} = \frac{ac}{bd}$$

Since D is without zero divisors, therefore b ≠ 0 , d ≠ 0 → b d ≠ 0 .

Therefore both $\frac{a\,d+b\,c}{b\,d}$ and $\frac{a\,c}{b\,d}$ are elements of F. Thus F is closed with respect to addition and multiplication. We shall now show that both addition and multiplication in F are well defined.

For this we are to show that if

$\frac{a}{b} = \frac{a'}{b'}$ and $\frac{c}{d} = \frac{c'}{d'}$ then $\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'}$ and $\frac{a}{b}.\frac{c}{d} = \frac{a'}{b'}.\frac{c'}{d'}$

We have $\frac{a}{b} = \frac{a'}{b'}$ → a b ' = b a ' and $\frac{c}{d} = \frac{c'}{d'}$ → c d ’ = d c ’ .

Now to show that $\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'}$

We are to show that $\frac{a\,d+b\,c}{b\,d} = \frac{a'\,d'+b'c'}{b'\,d'}$

i.e. (a d + b c) b ' d ' = b d (a ' d ' + b ' c ') .

Now (a d + b c) b ' d ' = a d b ' d ' + b c b ' d ' = a b ' d d ' + b b ' c d

= b a ' d d ' + b b ' d c ' [since, a b ' = b a ' and c d ' = d c ']

= b d a ' d ' + b d b ' c ' = b d (a ' d ' + b ' c ') , which was desired.

Again to show that $\frac{a}{b}.\frac{c}{d} = \frac{a'}{b'}.\frac{c'}{d'}$ we are to show that

$\frac{a\,c}{b\,d} = \frac{a'c'}{b'\,d'}$ i.e. , a c b ’ d ' = b d a ’ c ’

Now a c b ’ d ' = a b ' c d ' = b a ' d c ’ = b d a ' c ' , which was desired.

Therefore both addition and multiplication are well defined on F. We shall now show that F is a field for these two operations.

For that we will have to prove

i. Associativity of addition.
ii. Commutativity of addition.
iii. Existence of additive identity.
iv. Existence of additive inverse.
v. Associativity of multiplication.
vi. Commutativity of multiplication.
vii. Existence of multiplicative identity.
viii. Existence of multiplicative inverse of non-zero elements of F
ix. Distributivity of multiplication over addition.

Therefore, F is a field under the addition and multiplication as defined above. This field F is called the field of quotients of D.

We shall now show that the field F contains a subset D ' such that D is isomorphic to D ' .

Let D ' = { $\frac{a\,x}{x}$ ∈ F : a , 0 ≠ x ∈ D } Then D ' ⊆ F .

If x ≠ 0, y ≠ 0 are elements of D, then $\frac{a\,x}{x} = \frac{a\,y}{y}$ since a x y = x a y , Therefore if x is any fixed non-zero element of D, we can write D ' = { $\frac{a\,x}{x}$ ∈ F : a , 0 ≠ x ∈ D } .

We claim that the function φ : D → D ' defined by φ (a) = $\frac{a\,x}{x}$ is an isomorphism of D onto D ' .

φ is one-one. We have φ (a) = φ (b) → a = b

φ is onto D ' . If $\frac{a\,x}{x}$ ∈ D ', then a ∈ D. Also we have φ (a) = $\frac{a\,x}{x}$

Thus φ is onto D ' .

Therefore φ is an isomorphism of D onto D'.

Hence, D ≅ D ' . . .

Theorem 13 : The intersection of any two left ideals of a ring is again a left ideal of the ring.

Proof: Let I_1 and I_2 be two left ideals of a ring R . Then I_1 and I_2 are subgroups of R Under addition . Therefore $I_1 \cap I_2$ is also a subgroup of R Under addition.

Now to show that $I_1 \cap I_2$ is a left ideal of R , we are only to show that r ∈ R, S ∈ $I_1 \cap I_2$

→ r s ∈ $I_1 \cap I_2$

We have s ∈ $I_1 \cap I_2$ → s ∈ I_1 , s ∈ I_2

But and are left ideals of R . Therefore

r ∈ R , s ∈ I_1 → r s ∈ I_1 and r ∈ R , s ∈ I_2 → r s ∈ I_2

Now r s ∈ I_1 , r s ∈ I_2 → r s ∈ $I_1 \cap I_2$

Therefore, $I_1 \cap I_2$ is also a left ideal of R . . .

Note. A similar result can be proved for right ideals as well as for ideals.

Theorem 14: An arbitrary intersection of left ideals of a ring is a left ideal of the ring.

Proof: Let R be a ring and let $\{ S_t : t \in T \}$ be any family of left ideals of R . Here T is an index set and is such that for all $t \in T$, S_t is a left ideal of R . Let $S = \cap S_t = \{ x \in R : x \in S_t \text{ for all } t \in T \}$ be the intersection of this family of left ideals of R. Then to prove that S is also a left ideal of R .

Obviously $S \neq \Phi$, since at least 0 is in S_t for all $t \in T$.

Now let a , b be any two elements of S . Then

$A , b \in S \rightarrow a , b \in S_t$ for all $t \in T$

$\rightarrow a - b \in S_t$ for all $t \in T$ [since, S_t is a left ideal of R]

$\rightarrow a - b \in \cap S_t \rightarrow a - b \in S$.

Now let a be any element of S and r be an element of R.

We have $a \in S \rightarrow a \in \cap S_t \rightarrow a \in S_t$ for all $t \in T$

$\rightarrow r a \in S_t$ for all $t \in T$ [since , S_t is a left ideal of R]

$\rightarrow r a \in \cap S_t \rightarrow r a \in S$.

Thus $a , b \in S \rightarrow a - b \in S$ and $r \in R, a \in S \rightarrow r a \in S$

Therefore , S is a left ideal of R . . . .

Theorem 15 : The left Ideal generated by the union $I_1 \cup I_2$ of two left ideals is the set $I_1 + I_2$ consisting of the elements of R obtained on adding any element of I_1 to any element of I_2 .

Proof: Let $a_1 + a_2 , b_1 + b_2 \in I_1 + I_2$.

Then $a_1 , b_1 \in I_1$ and $a_2 , b_2 \in I_2$

Since I_1 , I_2 are left ideals of R , therefore they are subgroups of the additive group of R . Therefore

$a_1 , b_1 \in I_1 \rightarrow a_1 - b_1 \in I_1$ and $a_2 , b_2 \in I_2 \rightarrow a_2 - b_2 \in I_2$

Consequently $(a_1 + a_2) - (b_1 + b_2) = (a_1 - b_1) + (a_2 - b_2) \in I_1 + I_2$

Therefore $I_1 + I_2$ is a subgroup of the additive group of R .

Now let $r \in R$ and $a_1 + a_2 \in I_1 + I_2$. Then $a_1 \in I_1$, $a_2 \in I_2$. We have $r(a_1 + a_2) = r a_1 + r a_2 \in I_1 + I_2$

[since I_1 is a left ideal implies $r a_1 \in I_1$ and similarly $r a_2 \in I_2$]

Therefore $I_1 + I_2$ is a left ideal of R .

Since $0 \in I_2$, therefore $a_1 \in I_1$, can be written as $a_1 + 0$. Thus $a_1 \in I_1 \rightarrow a_1 \in I_1 + I_2$

Therefore $I_1 \subseteq I_1 + I_2$

Similarly $I_2 \subseteq I_1 + I_2$

$I_1 \cup I_2 \subseteq I_1 + I_2$.

Thus $I_1 + I_2$ is a left ideal containing $I_1 \cup I_2$.

Also if any left ideal contains $I_1 \cup I_2$, then it must contain $I_1 + I_2$.

Therefore $I_1 + I_2$ is the smallest left ideal containing $I_1 \cup I_2$

$I_1 + I_2$ = the left ideal generated by $I_1 \cup I_2 \ldots$

Example : If U is an ideal of a ring R with unity and $1 \in U$ prove that U = R.

Solution : We have $U \subseteq R$ since U is an ideal of R . Let x be any element of R . Since U is an ideal of R , therefore

$1 \in U , x \in R \rightarrow 1 x \in U \rightarrow x \in U$.

Therefore $R \subseteq U$

U = R .

Theorem 16 : A commutative ring with unity a field if it has no proper ideals

Proof : Let R be a commutative ring with unity having no proper ideals i.e., the only ideals of Rare (0) and R itself. In order to show that R Is a field, we should show that each non zero element of R possesses multiplicative inverse

Let a be any non-zero element of R .

The set Ra = { r a : r ∈ R } is an ideal of R . (See theorem 2)

Since 1 ∈ R, therefore l a = a ∈ R a .Thus 0 ≠ a ∈ Ra . Therefore the ideal Ra ≠ (0) . Since R has no proper ideals , therefore the only possibility is that R a = R . Thus every element of R is a multiple of a by some element of R . In particular , 1 ∈ R so it can be realised as a multiple of a. Thus there exists an element b ∈ R such that b a = 1 . Therefore a^{-1} = b . Hence each non-zero element of R possesses multiplicative inverse .

Therefore R is a field . . .

Check your Progress-2

3. Let R be any ring. The union of an increasing chain of ideals $I_1 \subseteq I_2 \subseteq$….. is

(a) Not an ideal
(b) An ideal
(c) A field
(d) A ring

4. Let R be a commutative ring with unit element whose only ideals are (0) and R itself then

(a) R is finite integral domain
(b) R is integral domain
(c) Division ring
(d) None of these

9.4 LET US SUM UP

Here we have studied the definition of ideals, which says that A non-empty subset S of a ring R is said to be an ideal (also a two sided ideal) if and only if it is both a left ideal and a right ideal. Thus a non-empty subset of a ring R is said to be an Ideal of R if:

(i) S is a subgroup of R under addition i.e., S is a subgroup of the additive group of R.

(ii) rs ∈ S and sr ∈ S for every r in R and for every s in S.

Then we have studied algebra of ideals.

9.5 KEYWORDS

1. Ideal: A non-empty subset S of a ring R is said to be an ideal (also a two sided ideal) if and only if it is both a left ideal and a right ideal. Thus a non-empty subset of a ring R is said to be an Ideal of R if:

1. S is a subgroup of R under addition i.e., S is a subgroup of the additive group of R.
2. rs ∈ S and sr ∈ S for every r in R and for every s in S.

9.6 QUESTIONS FOR REVIEW

1. If U, V are ideals of a ring R, let U+V={u+v: u ∈ U, v ∈ V}. Prove that U+V is also an ideal of R.

2. Prove that the intersection of two ideals of R is an ideal of R.

3. For any given element a of a ring R, let Ra={xa : x ∈ R}. Prove that Ra is a left ideal of R.

4. If U, V are ideals of a ring R let UV be the set of all those elements of R which can be written as finite sums of elements of the form uv where u ∈ U and v ∈ V. Prove that UV is an ideal of R.

5. The set of rational numbers is only a subring but not an ideal of the ring of real numbers.

9.7 SUGGESTED READINGS AND REFERENCES

6. Thomas W Judson (2013). *Abstract Algebra: Theory and Applications*. Orthogonal Publishing.
7. Paul B. Garrett (2007). *Abstract Algebra*. Chapman and Hall/CRC.

8. Vijay K Khanna (2017).*A Course in Abstract Algebra Fifth Edition*. Vikas Publishing House
9. LALJI PRASAD (2016). *Modern Abstract Algebra*. Paramount Publication
10. Stephen Lovett (2016). *Abstract Algebra: Structures and Applications*. Chapman and Hall/CRC

9.8 ANSWERS TO CHECK YOUR PROGRESS

5. (a) (answer for Check your Progress-1 Q.1)
6. (c) (answer for Check your Progress-1 Q.2)
7. (b) (answer for Check your Progress-2 Q.3)
8. (a) (answer for Check your Progress-2 Q.4)

UNIT – 10: FIELD EXTENSIONS AND IRREDUCIBLITY

STRUCTURE

10.0 OBJECTIVES

After studying this unit, you should be able to:

- Explain the concept of homomorphism
- Describe Isomorphism

10.1 INTRODUCTION

In this unit, we will discuss prime and reducible elements. We are all quite familiar with the ring I of integers. Also our familiar set Q of rational numbers is nothing but the set of quotients of the elements of I. Taking motivation from these facts, we now proceed to construct the quotient field of an arbitrary integral domain.

10.2 PRIME AND REDUCIBLE ELEMENTS

Let us start our study prime and irreducible elements with few examples .

Prime Elements

Definition : Let D be an integral domain with unity element 1 . A non-zero non-unit element $a \in D$, having only trivial divisors , is called a prime or irreducible element of D . An element $0\ b \in D$ having proper divisors is called a reducible or composite element of D .

From this definition it is obvious that if p is a prime element of D and if $p = x\ y$, where $x , y \in D$, then one of x or y must be a unit in D .

Also $0 \neq b \in D$ is a composite element of D if and only if we can find two elements $x, y \in D$ such that $b = x\ y$ and none of x and y is a unit in D.

Greatest Common Divisor

Definition: Let R be a commutative ring. If $a, b \in R$ then $0 \neq d \in R$ is said to be a greatest common divisor of a and b if

(i) $d \mid a$ and $d \mid b$.

(ii) Whenever $c \mid a$ and $c \mid b$ then $c \mid d$ . .

We shall use the notation $d = (a , b)$ to denote that d is a greatest common divisor of a and b .

Now suppose $a , b \in D$ where D is an integral domain with unity element 1. Let a, b possess a greatest common divisor .

If d_1 , d_2 are two greatest common divisors of a and b, we have

$d_1 \mid d_2$, and $d_2 \mid d_1$,

d_1 and d_2 are associates .

Thus in an integral domain with unity in case a greatest common divisor of a and b exists , it is unique apart from the distinction between associates .

Theorem 1 : If R is an integral domain and $a \in R$ is a prime element then a is irreducible .

Proof : Let $a \in R$ be a prime element and let $a = b\ c$. We want to show that either b or c must be a unit in R .

We have a | (b c) , and since a is a prime element it implies that a | b or a | c. We can assume that a | b . Since also b | a, thus we obtain that a ~ b, i.e. a = b u for some unit u ∈ R. Therefore we have b c = a = b u

this gives u = c, and so c is s unit.

Relatively Prime Elements

Definition : Let D be an integral domain with unity element 1 . Two elements a , b ∈ D are said to be relatively prime if their greatest common divisor is a unit of D .

But any associate of a greatest common divisor is a greatest common divisor. Also the unity element is an associate of any unit. Therefore if a, b are relatively prime we may assume that a greatest common divisor of a and b is 1 i . e . , (a , b) = 1 .

Definition:

Suppose R is a non-empty set along with two binary operations addition and multiplication denoted by '+' and '×' respectively i.e. for $a,b\in R$ we have $a+b\in R$ and $a\times b\in R$ such that

1) Addition is associative i.e. $(a+b)+c=a+(b+c),\forall a,b,c\in R$

2) Addition is commutative i.e. $(a+b)=(b+a),\forall a,b\in R$

3) There exists an element denoted by $e=0\in R$ such that $a+0=0+a,\forall a\in R$

4) To each element $a\in R$ there exist an element $-a\in R$ such that $a+(-a)=0$

5) Multiplication is associative i.e. $(a\times b)\times c=a\times(b\times c),\forall a,b,c\in R$

6) Multiplication is distributive over addition

i.e. $a\times(b+c)=(a\times b)+(a\times c)$ and $(b+c)\times a=(b\times a)+(c\times a)\ \forall a,b,c\in R$

Then the algebraic structure is denoted by $(R,+,\times)$ is called a ring.

Or in other words

A ring is an ordered triplet $(R,+,\times)$ where R is a non-empty set and + and $\times$ are two binary operation on R satisfy following axioms.

1) $R_1:(R,+)$ is a commutative group.

2) $a\times(b\times c)=(a\times b)\times c$, for all a,b,c ∈ R i.e. multiplication is associative

3)

$a\times(b+c)=(a\times b)+(a\times c)$ and $(b+c)\times a=(b\times a)+(c\times a)$ $\forall a,b,c\in R$

i.e. Multiplication is distributive over addition

Definition:

A ring R with at least two elements is called a field if

i) it is a commutative ring,
ii) it has unity,
iii) it is such that each non-zero element possess multiplicative inverse.

Field extensions

Definition:

Further information: Glossary of field theory

The notion of a subfield E ⊂ F can also be regarded from the opposite point of view, by referring to F being a field extension (or just extension) of E, denoted by F / E,

and read "F over E".

A basic datum of a field extension is its degree [F : E] , i . e . , the dimension of F as an E-vector space.

[G : E] = [G : F] [F : E] .

Extensions whose degree is finite are referred to as finite extensions. The extensions C / R and F4 / F2 are of degree 2, whereas R / Q is an infinite extension.

Check Your Progress-1

1. GCD of 7 and 8

(a) 1 (b) 7

(c) 56 (d) 8

2. Which of the following pair is relatively prime elements

(a) 5, 9 (b) 3, 9

(c) 3, 6 (d) 2, 8

10.3 QUOTIENT FIELD OF INTEGRAL DOMAIN

We are all quite familiar with the ring I of integers. Also our familiar set Q of rational numbers is nothing but the set of quotients of the elements of I.

Thus $Q = \{ p / q : p \in I, 0 \neq q \in I \}$.

Taking motivation from these facts, we now proceed to construct the quotient field of an arbitrary integral domain.

The field of Quotients

Definition: A ring R can be imbedded in a ring S if S contains a subset S ’ such that R is isomorphic to S ’ .

If D is a commutative ring without zero divisors , then we shall see that it can be imbedded in a field If, there exists a field F which contains a subset D isomorphic to D . We shall construct a field F with the help of elements of D and this field F will contain a subset B' such that D is isomorphic to D ' This field F is called the " field of quotients " of D , or simply the " quotient field " of D

On account of isomorphism of D onto D ' , we can say that D and D ' are abstractly identical . Therefore if we identify D with D , then we can say that the quotient field Of D is a field

containing D . We shall also see that F is the smallest field containing D .

Recall that a field is a set F equipped with two operations, addition (+) and multiplication (·), and two special elements 0, 1, satisfying:

• (F, +) is an abelian group with identity element 0.

• (F* , .) is an abelian group with identity element 1 (here F* denotes F \ {0}).

• For all a ∈ F, 0 . a = a . 0 = 0.

• Distributivity: for all a, b, c ∈ F, we have a . (b + c) = a . b + a . c .

A finite field is a field which is, well, finite.

Example : The simplest example of a finite field is as follows. Take a prime p ∈ Z. Let F_p = Z/pZ (the quotient of the ring Z mod the ideal pZ).

Very explicitly, F_p = {0, 1, . . . , p− 1 } , and the operations are addition and multiplication of integers mod p. To see that this is a field, the main step is to verify that every a ∈ F ∗ p has a multiplicative inverse. Since a ∈ F ∗ p and p is prime, we have that GCD (a , p) = 1, and so by Euclid, we know that there exist integers x, y s.t. a x + p y = 1. Then x mod p is a^{-1} .

Let F be a finite field. For a positive integer r, consider the r-fold sum s_r = 1 + 1 + . . . + 1. Since F is finite, some s_r must equal 0. Let p be the smallest positive p for which s_p equals 0. Observe that if p exists, it must be prime; for if p = a · b with a, b < p, then by distributivity we have 0 = s_p = s_a · s_b, and so one of s_a, s_b must equal 0, contradicting the minimality of p. This p is called the characteristic of the field F. Now observe that the subset {0, s1, s2, . . . , sp−1} ⊆ F is itself a field, isomorphic to

Fp. This is called the prime subfield of F. The key to the full classification of all finite fields is the observation that F is a finite dimensional vector space over F_p. Let $n = \dim_{Fp}(F)$. Then we have $|F| = p^n$. In particular, the cardinality of a finite field must be a prime power .

Field Extensions

Definition : Let F be a field and let $K \subseteq F$ be a subring . Then we say K is a subfield of F if K is a field . In this case we also call F an extension field of K and abbreviate this by saying F/K is a field extension .

Definition : The degree of a field extension K/F, denoted [K : F] , is the dimension of K as a vector space over F . The extension is said to be finite if [K : F] is finite and is said to be infinite otherwise .

Example : The concept of field extensions can soon lead to very interesting and peculiar results . The following examples will illustrate this :

(1) Take the field Q . Now, clearly, we have the polynomial p (x) = $x^2 - 2 \in Q[x]$; however, it should be evident that its roots, $\pm\sqrt{2}$ does not belong to Q. This polynomial is then said to be irreducible over Q. Thus, by considering the quotient ring Q [x] / (x2−2), we find that we obtain another field, denoted Q ($\sqrt{2}$) (or Q ($-\sqrt{2}$) , which just so happens to be isomorphic to Q ($\sqrt{2}$) | this, of course, is no coincidence) .

(2) Take the field R . Again, we may easily find a polynomial , which is irreducible over our field . Choosing p (x) = $x^2 + 1 \in R[x]$, it is obvious that the roots, ±i does not belong to R . Thus , if we consider the quotient ring , R [x] / (x2 + 1) ,we obtain the field R (i) (∼ = C) . Since both of the given examples are of polynomials that are irreducible over the particular fields, it will be of great benefit to examine the subject of irreducible polynomials (and the criteria to label them as irreducible) more closely.

Let now Z be the ring of rational integers and K a field whose unit element we denote by e . The mapping m → m e of Z into K obviously a homomorphism of the ring Z into K . The kernel of the homomorphism is the set of m is Z such that m e = 0 in K . This is an ideal in Z and as Z is a principal ideal domain , this ideal is generated by integer say p . Now p is either zero or else is a prime . In the first case it means that K contains a subring isomorphic to Z and K has characteristic zero . Therefore K contains a subfield isomorphic to the field of rational numbers . In the second case K has characteristic p and since Z / (p) is a finite field of p elements, K contains a subfield isomorphic to Z / (p) .

EXAMPLE : (a) The field of complex numbers C has degree 2 over R (basis { 1 , I }) .

(b) The field of real numbers R has infinite degree over Q : the field Q is countable, and so every finite – dimensional Q - vector space is also countable, but a famous argument of Cantor shows that R is not countable .

(c) The field of Gaussian numbers Q (I) has degree 2 over Q (basis { 1 ; i }) .

(d) The field F [x] has infinite degree over F; in fact, even its subspace FŒX has infinite dimension over F (basis 1;X;X2;:::).

Lemma 1 : If F/K is a field extension, then F is a K vector space .

Proof : By definition, F is an abelian group under addition, so we can define our vector addition to be the addition in F . Also, we can define our scalar multiplication $* : K \times F \to F$ to be given by $k*x = k\ x$ where the second multiplication is just multiplication of elements in F. Then it is easy to check that F satisfies the definition of a vector space with scalars K with these operations .

So if F/K is a field extension, we define [F : K] = dim K (F) , the dimension of F as a K vector space . Therefore , [F : K] is the cardinality of any basis of F as a K-vector space .

Theorem 1 : A commutative ring with zero divisors can be imbedded in a field .

OR Every Integral domain can be imbedded in a field .

Proof: Let D be a commutative ring without zero divisors .

Let D_0 be the set of all non-zero elements of D. Let S = D x D_0

i. e . , let S be the set of all ordered pairs (a , b) where a , b ∈ D and b ≠ 0 . Let us define a relation ~ in S . We shall say that

(a , b) ~ (c , d) if and only if a d = b c

We claim that this relation is an equivalence relation in S

Therefore it will partition S into disjoint equivalence classes . We shall denote the equivalence class containing (a , b) by $\frac{a}{b}$ other notations to denote this equivalence class are (a , b) or [a , b] .

Then $\frac{a}{b}$ = { (c , d) ∈ S : (c , d) ~ (a , b) } .

Obviously $\frac{a}{b} = \frac{c}{d}$ if (a , b) ~ (c , d) i . e . , iff a d = b c .

Also $\frac{a}{b} = \frac{a\,x}{b\,x}$ for all x ∈ D_0 . The reason is that

(a , b) ~ (a x , b x) since a b x = b a x .

These equivalence classes are our quotients. Let F be the set of all such quotients i.e., F= { $\frac{a}{b}$: (a , b) ∈ S }

We now define addition and multiplication operations in F as follows:

$$\frac{a}{b} + \frac{c}{d} = \frac{a\,d + b\,c}{b\,d} \; and \; \frac{a}{b}.\frac{c}{d} = \frac{ac}{bd}$$

Since D is without zero divisors, therefore b ≠ 0 , d ≠ 0 → b d ≠ 0 .

Therefore both $\frac{a\,d+b\,c}{b\,d}$ and $\frac{a\,c}{b\,d}$ are elements of F. Thus F is closed with respect to addition and multiplication. We shall now show that both addition and multiplication in F are well defined.

For this we are to show that if

$\frac{a}{b} = \frac{a'}{b'}$ and $\frac{c}{d} = \frac{c'}{d'}$ then $\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'}$ and $\frac{a}{b}.\frac{c}{d} = \frac{a'}{b'}.\frac{c'}{d'}$

We have $\frac{a}{b} = \frac{a'}{b'} \rightarrow$ a b ' = b a ' and $\frac{c}{d} = \frac{c'}{d'} \rightarrow$ c d ' = d c ' .

Now to show that $\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'}$

We are to show that $\frac{a\,d+b\,c}{b\,d} = \frac{a'd'+b'c'}{b'd'}$

i.e. (a d + b c) b ' d ' = b d (a ' d ' + b ' c ') .

Now (a d + b c) b ' d ' = a d b ' d ' + b c b ' d ' = a b ' d d ' + b b ' c d

= b a ' d d ' + b b ' d c ' [since, a b ' = b a ' and c d ' = d c ']

= b d a ' d ' + b d b ' c ' = b d (a ' d ' + b ' c ') , which was desired.

Again to show that $\frac{a}{b}.\frac{c}{d} = \frac{a'}{b'}.\frac{c'}{d'}$ we are to show that

$\frac{a\,c}{b\,d} = \frac{a'c'}{b'd'}$ i.e. , a c b ' d ' = b d a ' c '

Now a c b ' d ' = a b ' c d ' = b a ' d c ' = b d a ' c ' , which was desired.

Therefore both addition and multiplication are well defined on F. We shall now show that F is a field for these two operations.

For that we will have to prove

x. Associativity of addition.
xi. Commutativity of addition.
xii. Existence of additive identity.
xiii. Existence of additive inverse.
xiv. Associativity of multiplication.

xv. Commutativity of multiplication.

xvi. Existence of multiplicative identity.

xvii. Existence of multiplicative inverse of non-zero elements of F

xviii. Distributivity of multiplication over addition.

Therefore, F is a field under the addition and multiplication as defined above. This field F is called the field of quotients of D.

We shall now show that the field F contains a subset D ' such that D is isomorphic to D ' .

Let D ’ = $\{ \frac{a\,x}{x} \in F : a , 0 \neq x \in D \}$ Then D ' $\subseteq$ F .

If x $\neq$ 0, y $\neq$ 0 are elements of D, then $\frac{a\,x}{x} = \frac{a\,y}{y}$ since a x y = x a y , Therefore if x is any fixed non-zero element of D, we can write D ’ = $\{ \frac{a\,x}{x} \in F : a , 0 \neq x \in D \}$.

We claim that the function φ : D $\rightarrow$ D ' defined by φ (a) = $\frac{a\,x}{x}$ is an isomorphism of D onto D ' .

φ is one-one. We have φ (a) = φ (b) $\rightarrow$ a = b

φ is onto D ' . If $\frac{a\,x}{x} \in$ D ’, then a $\in$ D. Also we have φ (a) = $\frac{a\,x}{x}$

Thus φ is onto D ' .

Therefore φ is an isomorphism of D onto D'.

Hence, D $\cong$ D ’ . . .

In the next theorem we shall show that the quotient field F of D is the smallest field containing D . In other words if D is contained in any other field K , then F will also be contained in K .

Theorem 2 : If K is any field which contains an integral domain D , then K contains a subfield isomorphic to the quotient field F Of D .

In other words the quotient field F of D is the smallest field containing D .

Proof : Let D be a commutative ring without zero divisors .

Let $a \in D$ and $0 \neq b \in D$. Since K is a field containing D , therefore $a \in K , 0 \neq b \in K \rightarrow a b^{-1} \in K$

Let K ' be the subset of containing the elements of the form $a b^{-1}$ where a, b ∈ D with $b \neq 0$. Thus

$K' = \{ a b^{-1} \in K : a , 0 \neq b \in D \}$

We shall show that K ' is a subfield of K and K ' is isomorphic to the quotient field F of D. Let $a b^{-1} \in K' , c d^{-1} \in K'$. Then

$0 \neq b , \ 0 \neq d \in D$

Now $a b^{-1} – c d^{-1} = a d d^{-1} b^{-1} – c b b^{-1} d^{-1} = (a d – b c) d^{-1} b^{-1} = (a d – b c) (b d)^{-1} \in K'$, since $a d – b c \in D$ and $0 \neq b d \in D$.

Further suppose that $0 \neq c d^{-1} \in K'$. Then $c \neq 0$ and we have

$(a b^{-1}) (c d^{-1})^{-1} = a b^{-1} c d^{-1} = a d (c b)^{-1} \in K'$, since $a d \in D$ and $0 \neq c b \in D$

Hence K ' is a subfield of K. We shall now show that the quotient field F of G is isomorphic to K ' . We have

$$F = \left\{ \frac{a}{b} : a \in D, 0 \neq b \in D \right\}$$

Consider the mapping f : F → K ' defined by

$$f \left(\frac{a}{b} \right) = a b^{-1} \ \forall \ \frac{a}{b} \in F$$

The mapping f is one-one because we have

$$f \left(\frac{a}{b} \right) = f \left(\frac{a}{b} \right)$$

$\rightarrow a b^{-1} = c d^{-1} \rightarrow a b^{-1} b d = c d^{-1} b d$

$\rightarrow a\,d = c\,b\,d^{-1}\,d \rightarrow a\,d = b\,c$

$\rightarrow (a, b) \sim (c, d)$

Also f is onto K ' . If $a\,b^{-1}$ is an element of K ' , then $\frac{a}{b} \in F$

and $f\left(\frac{a}{b}\right) = a\ b^{-1}$

Further $f\left(\frac{a}{b} + \frac{c}{d}\right) = f\left(\frac{a\,d + b\,c}{b\,d}\right) = (a\,d + b\,c)\,(b\,d)^{-1}$

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

$= a\,b^{-1} + c\,d^{-1} = f\left(\frac{a}{b}\right) + f\left(\frac{c}{d}\right)$

Also $f\left(\frac{a}{b} \cdot \frac{c}{d}\right) = f\left(\frac{a\,c}{b\,d}\right) = (a\,c)\,(b\,d)^{-1} = (a\,c)\,d^{-1}b^{-1} = (a\,b^{-1})\,(c\,d^{-1}) = f\left(\frac{a}{b}\right) f\left(\frac{c}{d}\right)$

Hence F ≅ K ' . . .

If we identify K ' with F , we see that if D is contained in any field K , then F is also contained in K . Therefore F is the smallest field containing D . . .

Corollary : The quotient field of a finite integral domain coincides with itself.

Suppose D is a finite integral domain. Then D is also a field.

Thus D is the smallest field containing D . The quotient field F of D is also the smallest field containing D . Hence F coincides with D .

Example : What is the quotient field of 2Z , where Z is the ring of integers ?

Theorem 3 : Any two isomorphic integral domains have isomorphic quotient fields .

Proof : Suppose D and D ' are two isomorphic integral domains.

Let f be an isomorphism of D onto D ' . If a , b , c etc . are the elements of then f (a) . f (b) f (c) etc . will be the elements of D ' . Also

f (a + b) = f (a) + f (b) and f (a b) = f (a) f (b) for all a , b in D .

Let F , F ' be the quotient fields of D , D ' respectively . Then F consists of the equivalence classes (quotients) of the form $\frac{a}{b}$ where a , $0 \neq b \in D$ and F ' consists of the equivalence classes of the form $\frac{f(a)}{f(b)}$ where f (a) , f (b) ∈ D ' .

Consider the mapping φ : F → F ' defined by

$$\varphi\left(\frac{a}{b}\right) = \frac{f(a)}{f(b)} \ \forall \ \frac{a}{b} \in F$$

First we shall show that the mapping φ is well defined i . e . , if $\frac{a}{b} = \frac{c}{d}$ then

$$\varphi\left(\frac{a}{b}\right) = \varphi\left(\frac{c}{d}\right)$$

We have $\frac{a}{b} = \frac{c}{d} \rightarrow$ a d = b c

→ f (a d) = f (b c) → f (a) f(d) = f (b) f (c)

$$\rightarrow \frac{f(a)}{f(b)} = \frac{f(c)}{f(d)} \rightarrow \varphi\left(\frac{a}{b}\right) = \varphi\left(\frac{c}{d}\right)$$

Therefore φ is well-defined.

φ is one-one . We have

$$\varphi\left(\frac{a}{b}\right) = \varphi\left(\frac{c}{d}\right) \rightarrow \frac{f(a)}{f(b)} = \frac{f(c)}{f(d)}$$

→ f (a) f (d) = f (b) f (c) → f (a d) = f (b c)

→ a d = b c [f is one – one]

$$\frac{a}{b} = \frac{c}{d}$$

φ is one – one .

Also φ is onto F ' . If $\frac{f(a)}{f(b)} \in F'$, then

$\frac{a}{b} \in F$ and $\varphi\left(\frac{a}{b}\right) = \frac{f(a)}{f(b)}$

Therefore φ is onto F ' .

Further $\varphi\left(\frac{a}{b} + \frac{c}{d}\right) = \varphi\left(\frac{a}{b}\right) + \varphi\left(\frac{c}{d}\right)$

Also $\varphi\left(\frac{a}{b} . \frac{c}{d}\right) = \varphi\left(\frac{a}{b}\right) . \varphi\left(\frac{c}{d}\right)$

Therefore φ is an isomorphism of F onto F ' .

Therefore F ≅ F ' . . .

Check Your Progress-2

3 . A ring R is an integral domain if

a . R is commutative ring

b . R is commutative ring with zero divisor

c . R is commutative ring without zero divisor

d . R is a ring with zero divisor

4 . An integral domain D is of finite characteristic if for all a in D , there exists m , a positive integer such that

a . m a = 1

b . m a = 0

c . m a = a

d . None of these

10.4 PRIME FIELDS

Definition: A field is said to be prime if it has no subfield other than itself

The field of rational numbers is a prime field while the field of real numbers is not a prime field. The field I , is prime for each prime integer p .

A subfield E of a field F is a subset of F that is a field with respect to the field operations of F. Equivalently E is a subset of F that contains 1 , and is closed under addition, multiplication, additive inverse and multiplicative inverse of a nonzero element. This means that $1 \in E$, that for all $a , b \in E$ both $a + b$ and $a \cdot b$ are in E , and that for all $a \neq 0$ in E , both $– a$ and $1 / a$ are in E .

Field homomorphisms are maps $f : E \rightarrow F$ between two fields such that $f(e1 + e2) = f(e1) + f(e2)$, $f(e1e2) = f(e1)f(e2)$, and $f(1E) = 1F$, where e1 and e2 are arbitrary elements of E. All field homomorphisms are injective. If f is also surjective, it is called an isomorphism (or the fields E and F are called isomorphic) .

A field is called a prime field if it has no proper (i.e., strictly smaller) subfields. Any field F contains a prime field. If the characteristic of F is p (a prime number), the prime field is isomorphic to the finite field F_p introduced below. Otherwise the prime field is isomorphic to Q.

A fundamental example of a finite (Galois) field is the set Fp of mod-p remainders, where p is a given prime number. Here, as in Zp, the set of elements is $Rp = \{0 , 1 , \cdots , p – 1 \}$, and the operation $\oplus$ is mod-p addition. The multiplicative operation $*$ is mod-p multiplication; i . e . , multiply integers as usual and then take the remainder after division by p .

The prime subfield of a finite field, and prime field uniqueness

A subfield G of a field F is a subset of the field that is itself a field under the operations of F. For example, the real field R is a subfield of the complex field C. We now show that every finite field F has a subfield that is isomorphic to a prime field Fp. Let F be a finite field with $q = |F|$ elements. By the field axioms, F has an additive identity 0 and a multiplicative identity 1. Consider the single-generator subgroup of the additive group of F that is generated by 1, namely $S (1) = \{ 1 , 1 \oplus 1 , . . . \}$. Let $n = | S (1) |$. By the finite cyclic groups theorem , S (1) is isomorphic to $Zn = \{ 0 , 1 , 2 , . . . , n – 1 \}$ under the correspondence $i1 \in S (1) \subseteq F \leftrightarrow i \in Zn$. The elements of S (1) are called the integers of F .

By the distributive law in F , the product $i*j$ (in F) of two nonzero elements in S(1) is simply the sum of ij ones, which must be the element of S(1) corresponding to ij mod n. Thus the multiplication rule of F must reduce to mod-n multiplication in S(1). It then follows from the prime fields theorem that n must be equal to a prime p in order that S(1) be a field.

Theorem 4 : (Prime fields) The set $Rn = \{0,1,\cdots,n-1\}$ forms a field under mod-n addition and multiplication if and only if n is a prime number p.

Proof : We have already seen that the elements of Rn form an abelian group under addition modulo n, namely the cyclic group Zn. In Zn, the associative, commutative and distributive properties of addition and multiplication modulo n follow from the corresponding properties of ordinary addition and multiplication. Zn has a multiplicative identity, namely 1. If n is not a prime, then n = ab for some integers a,b in the range 1 < a, b < n. The product $a*b$ is therefore equal to 0, modulo n; thus $Zn - \{0\}$ is not closed under mod-n multiplication, which implies that Zn is not a field. On the other hand, suppose that n is equal to a prime p. To see that the nonzero elements of Zp form a group under multiplication, we show that they have the permutation property. By unique factorization, the product of two nonzero integers a, b < p cannot equal 0 mod p. Therefore the nonzero elements of Zp are closed under multiplication mod p. Also, for a , b , $c \neq 0$ and $b \neq c$ we have a (b – c) mod $p \neq 0$. Thus a b $\neq$ a c mod p, which implies $a*b \neq a*c$. Consequently there are no zeroes or repetitions in the set of $p-1$ elements $\{a*1,a*2,...,a*(p-1)\}$, which means they must be a permutation of the nonzero elements of Zp. This prime field with p elements will be denoted by Fp. We will shortly show that Fp is essentially the only field with p elements. . .

Theorem 4 : Every prime field of characteristic 0 is Isomorphic to the field of rational numbers .

Proof : Let F be a prime field of characteristic 0 . For the sake of convenience let us denote the unity element (multiplicative identity) of F

by e . Since F is of characteristic 0 , therefore for any integer n , we have n e = 0 (zero element of F) if and only if n = 0 .

Here ne is an integral multiple of the element e of E .

We have n e in F . Consider a subset F ' of F defined as

F ' = { m e / n e : m , n in the set of integers I with $n \neq 0$ } .

Since $n \neq 0$, $n e \neq 0$, therefore n e is an inversible element of F . So m e / n e = (m e) (n e) $^{-1}$ is definitely an element of F . We claim that F' is a subfield of F .

But F can have no proper subfield because F is a prime field . Therefore we must have F ' = F .

Thus F = { m e / n e : m , n are in I with $n \neq 0$ } .

If Q is the field of rational numbers, then Q = { m / n : m , n E I with n # 0 } ,

Let f be a mapping from F into Q defined as

f (m e / n e) = { m / n : m , n in I with $n \neq 0$. }

f is well-defined .

f is one-one .

f is onto .

f preserves compositions.

Therefore We have F ≅ Q . . .

Theorem 5 : Every field of characteristic 0 contains a subfield isomorphic to the field of rational numbers .

Proof : Let F be any field of characteristic 0 and let e be the unity element of F . Since F is of characteristic 0 , therefore for any integer n, we have n e = 0 if and only if n = 0 .

Consider the subset F of F defined as

F ’ = { m e / n e : m, $0 \neq$ n in I } .

Now prove that F ’ is a subfield of F and F $\cong$ Q where Q is the field of rational numbers .

Theorem 6 : Every prime field of finite characteristic p is isomorphic to the field I_p , of the residue classes of the set of integers modulo p .

Proof: Let F be a prime field of finite characteristic p . Then p must be a prime number . The unit element e of F will be of order p regarded as an element of the additive group of F . The identity element of the additive group of F is the zero element of F . Therefore if n is any integer , then

n e $\neq$ 0 if and only if p is a divisor of n

Consider a subset F ' of F defined as

F ’ = { n e : n in I where I is the set of integers }

F ' is a cyclic subgroup of the additive group of F .

Since F ' is generated by e whose order is p , therefore F ’ constrains p distinct elements . We claim that F ’ is a subfield of F . For this we shall prove that F’ is an integral domain and we know that every finite integral domain is a field .

Let me, ne be any two elements of F ' . Then

m e – n e = (m - n) e $\in$ F ’ since m - n $\in$ I .

Also (m e) (n e) = (m n) e^2 = (m n) e $\in$ F since m n $\in$ I.

Thus F ’ is a subring of F . Since F is without zero divisors , therefore F ’ is also without zero divisors . Therefore F ’ is a commutative ring without zero divisors . Therefore F is an integral domain and so F ’ is a subfield of F . But F can have no proper subfield because F is a prime field . Therefore we must have

F = F ’ = {n e : n $\in$ I } .

Now , we shall prove that

$F \cong I_p$

Let f be a mapping from F into I_p , defined as

f (n e) = the residue class [n] , for all n ∈ I .

f is well defined .

f is one-one .

f is onto .

f preserves compositions.

Hence $F \cong I_p$. . . .

Theorem 7 : Let R be an Integral domain with unity of finite characteristic p . Then R contains a subset isomorphic to the field I_p of the residue classes of the set of integers modulo p .

Proof: Proceed as in theorem 6. If e is the unity element of R, then prove that R ' = { n e : n in I } is isomorphic to I_p .

Theorem 8: Let R be an integral domain with unity of characteristic 0. Then R contains a subset isomorphic to the integral domain of integers.

Proof: If e is the unity element of R, then prove that

R ’ = { n e : n in I }

is isomorphic to the integral domain I of integers. Show that the mapping f from R' into I defined as f (n e) = n for all n in I is an isomorphism of R ’ onto I .

Check Your Progress-3

5. If P is a prime. The ring Z of integers modulo P is

a. Ring

b. Field

c. Group

d. Subgroup

6. The number of elements in finite field is always a

a. Even number

b. Prime number

c. Odd number

d. Number=p^m where m > 0 and p is a prime number

10.5 LET US SUM UP

In this unit we have discussed prime and reducible elements. We are all quite familiar with the ring I of integers. Also our familiar set Q of rational numbers is nothing but the set of quotients of the elements of I. Taking motivation from these facts, we have constructed the quotient field of an arbitrary integral domain. Then we have studied the concept of prime fields.

10.6 KEYWORDS

3. *Prime:* Let D be an integral domain with unity element 1. A non-zero non-unit element a∈D, having only trivial divisors, is called a prime or irreducible element of D

4. *Prime field:* A field is said to be prime if it has no subfield other than itself**.**

10.7 QUESTIONS FOR REVIEW

1. Let F be a field. Explain why Q(F) is isomorphic to F. Why can't we just say that Q(F) = F?
2. Find the quotient field of $Z_2[x]$.
3. Prove that if D_1 and D_2 are isomorphic integral domains, then Q $(D_1) \cong Q(D_2)$.
4. Find the quotient field of $Z[\sqrt{3}i]$.

5. Let R be a set that satisfies all properties of a commutative ring, with the exception of the existence of an identity element 1. Show that if R has no nonzero divisors of zero, then it has a quotient field (which must necessarily contain an identity element).

10.8 SUGGESTED READINGS AND REFERENCES

11. Thomas W Judson (2013). *Abstract Algebra: Theory and Applications*. Orthogonal Publishing.
12. Paul B. Garrett (2007). *Abstract Algebra*. Chapman and Hall/CRC.
13. Vijay K Khanna (2017).*A Course in Abstract Algebra Fifth Edition*. Vikas Publishing House
14. LALJI PRASAD (2016). *Modern Abstract Algebra*. Paramount Publication
15. Stephen Lovett (2016). *Abstract Algebra: Structures and Applications*. Chapman and Hall/CRC.

10.9 ANSWERS TO CHECK YOUR PROGRESS

9. (a) (answer for Check your Progress-1 Q.1)
10. (a) (answer for Check your Progress-1 Q.2)
11. (c) (answer for Check your Progress-2 Q.3)
12. (b) (answer for Check your Progress-2 Q.4)
13. (b) (answer for Check your Progress-3 Q.5)
14. (d) (answer for Check your Progress-3 Q.6)

UNIT – 11: EUCLIDEAN DOMAIN

STRUCTURE

11.0 OBJECTIVES

After studying this unit, you should be able to:

- Understand the concept of Euclidean domain

11.1 INTRODUCTION

In this unit, we will discuss Euclidean rings or Euclidean domains. We will also discuss the various properties of Euclidean domain.

11.2 EUCLIDEAN DOMAIN

Maximal Ideal

Definition: An ideal $S \neq R$ in a ring R is said to be a maximal ideal of R if whenever U is an ideal of R such that $S \subseteq U \subseteq R$, then either $R = U$ or $S = U$.

. . . .

In other words an ideal S of a ring R is said to be maximal ideal if there exists no ideal properly contained in R which itself properly contains S i.e., if it is impossible to find an ideal which lies between S and the full ring R

. . . .

.. . .

Prime Ideal

Definition: Let R be a ring and S an ideal in R. Then S is said to be a prime ideal of R if a b ∈ S ,

a, b ∈ R implies that either a or b is in S

Maximal ideal

Definition : An ideal M in an arbitrary ring R is called a maximal ideal if M ≠ R and the only ideals containing M are M and R .

Principal ideal

Definition: An ideal S of a ring R is said to be a principal ideal if there exists an element a in S such that any ideal T of R containing a also contains S i . e . , S = (a) .

. . . .

Principal Ideal Ring/Principal Ideal Domain

Definition: A commutative ring R without zero divisors and with unity element is a principal ideal ring if every ideal Sin R is a principal ideal i.e, if every ideal Sin R is of the form S = (a) for some a ∈ S.

. . . .

Relatively Prime Elements

Definition : Let D be an integral domain with unity element 1 . Two elements a , b ∈ D are said to be relatively prime if their greatest common divisor is a unit of D .

But any associate of a greatest common divisor is a greatest common divisor. Also the unity element is an associate of any unit. Therefore if a, b are relatively prime we may assume that a greatest common divisor of a and b is 1 i . e . , (a , b) = 1 .

. . . .

Definition : Let I and J be ideals of R. (1) Define the sum of I and J by I + J ={ a + b | a ∈ I , b ∈ J } . (2) Define the product of I and J , denoted

by I . J, to be the set of all finite sums of elements of the form a . b with a ∈ I and b ∈ J .

. . . .

. . . .

The sets of integers and of polynomials (for any field of coefficients) have :

(a) Addition that associates and commutes .

(b) An additive identity element 0 and additive inverses of everything .

(c) Multiplication that associates , commutes and distributes with addition .

(d) A multiplicative identity element 1 .

(e) A cancellation rule: if $a \neq 0$ and $a b = a c$, then $b = c$.

(f) Division with remainders.

Any set D with addition and multiplication rules that has all the properties (a)-(e) above is called an integral domain. A field is one kind of integral domain, and the integers and polynomials are another. Condition (f) will be part of the definition of a Euclidean domain.

. . ..

. . . .

Euclidean Rings or Euclidean Domains

Definition : Let R be an integral domain i . e . , let R be a commutative ring without zero divisors . Then R is said to be a Euclidean ring if to every non-zero element $a \in R$ we can assign a non-negative integer $d(a)$ such that:

(i) For all $a , b \in R$, both non-zero, $d(ab) \geq d(a)$.

(i i) For any $a , b \in R$ and $b \neq 0$, there exist $q , r \in R$ such that $a = q b + r$

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

. . . .

. . ..

Another form

Definition : An integral domain R is called Euclidean if there is a function $d : R - \{0\} \rightarrow N$ with the following two properties: (1) $d(a) \leq d(ab)$ for all nonzero a and b in R , (2) for all a and b in R with $b \neq 0$ we can find q and r in R such that $a = b q + r$, $r = 0$ or $d(r) < d(b)$.

The second part of the above definition is known as division algorithm. Also we do not assign a value to d (0) . Thus d (a) will remain undefined when a = 0 . Also d (a) will be called d -value of a and d (a) must be some non - negative integer for every non - zero element a ∈ R

The main reason that the d - inequality is not included in the definition of a Euclidean domain is that it is irrelevant to prove the two main theorems about Euclidean domains : that every Euclidean domain is a PID1 and that the Euclidean algorithm in a Euclidean domain terminates after finitely many steps and produces a greatest common divisor . There can be greatest common divisors in rings that are not Euclidean (such as in Z [X , Y]) , but it may be hard in those rings to compute greatest common divisors by a method that avoids factorization . When a ring is Euclidean , the Euclidean algorithm in the ring lets us compute greatest common divisors without having to factor , which makes this method practical .

Why is the d - inequality nearly always mentioned in the literature if it's actually not needed ? Well , it is not needed for the two specific results cited in the previous paragraph , but it is convenient to use the d-inequality if we want to prove factorization into irreducibles in a Euclidean domain without proving the result more generally in a PID . There is factorization into irreducibles in every PID , which subsumes the same result for Euclidean domains since Euclidean domains are PIDs , but the proof of the existence of irreducible factorizations in a PID is less concrete than a proof available in Euclidean domains.

. . . .

Noetherian ring.

Definition : A commutative ring where every ideal is finitely generated is called a Noetherian ring.

These rings are named after Emmy Noether, who was one of the pioneers of abstract algebra in the first half of the 20th century . Their importance, as a class of rings, stems from the stability of the Noetherian property under many basic constructions. If R is a Noetherian ring, so is every quotient ring R/I (which may not be an integral domain even if R is), every polynomial ring R[X] (and thus R[X1,...,Xn] by induction on n,

viewing this as R[X1,...,Xn−1][Xn]), and every formal power series ring R[[X]] (and thus R[[X1,...,Xn]]). The PID property behaves quite badly, e.g., if R is a PID other than a field then R[X] is not a PID. For instance, R[X,Y] = R[Y][X] is never a PID for an integral domain R. But if R is Noetherian then R[X,Y] is Noetherian. Briefly, the property "ideals are finitely generated" of Noetherian rings is more robust than the property "ideals are singly generated" of PIDs.

Using this terminology, Corollary 4.6 says in every Noetherian integral domain each element other than 0 or a unit has an irreducible factorization. It is worth comparing the proof of this general result to the special proof we gave in the case of Euclidean domains, where the proof of irreducible factorizations is tied up with features of the Euclidean function on the ring.

In the context of unique factorization domains, it is the uniqueness of the factorization that lies deeper than the existence. We are not discussing uniqueness here, which most definitely does not hold in most Noetherian integral domains. That is, the existence of irreducible factorizations (for all nonzero nonunits) is not a very strong constraint, to the extent that most integral domains you meet in day-to-day practice in mathematics are Noetherian so their elements automatically have some factorization into irreducible elements. But there usually is not going to be a unique factorization into irreducible elements.

. . . . . .

. . . .

Lemma: Every principal ideal domain is Noetherian .

Proof : Let R be a principal ideal domain, and let $I0 \subseteq I1 \subseteq ...$ be a chain of ideals in R. The union $\cup n \in N In$ is also an ideal in R, hence is principal, hence $\cup n \in N In = (i)$ for some $i \in I$. So $i \in In$ for some n. So $In = In+1 = In+2 = \cdots = I$. So the chain of ideals stabilizes.

. .. .

. . . .

Example: Divide 1000 by 501 with remainders : As natural numbers : 1000 = 501 (1) + 499 with a (large) remainder of 499 . As integers : 1000 = 501 (2) + (− 2) with a (much smaller) remainder of −2 .

Another Example : Divide 900 by 200 with remainders :

As natural numbers : 900 = 200 (4) + 100 . As integers , we could take that or equally well : 900 = 200 (5) + (− 100)

In general, when | r |= 1 / 2 | b | , there are two possibilities for r . . .

. . . .

. . . .

Example : . The most familiar examples of Euclidean domains are Z, with norm given by the absolute value , and k [x] for k a field , with norm given by the degree of a polynomial .

Example: The ring of integers is a Euclidean ring.

Solution: Let (I, +, .) be the ring of integers where

I = {...,-3,-2, -1, 0, 1, 2, 3,..}

Let the d function on the non-zero elements of I be defined as d (a) =|a| for all $0 \neq a \in I$

Now if $0 \neq a \in I$, then a is a non-negative integer. Thus we have assigned a non-negative integer to every non-zero element $a \in I$

[d (-5)]=|-5|= 5, d(-1)=|-1|=1 etc.]

Further if a, b ∈ I and are both non zero, then

| ab |=|a|.|b|

$|ab| \geq |a|$

$d (a b) \geq d (a)$

Finally we know that if $a \in I$ and $0 \neq b \in I$, then there exist two integers q and r such that

$a = q b + r$ where $0 \leq r < |b|$

where either r=0 or $1 \leq r <| b|$

where either r=0 or d(r) < d(b).

It should be noted that d(b)=1band if r is a positive integer then r = |r|=d(r).

Therefore the ring of integers is a Euclidean ring.

Example: The ring of polynomials over a field is a Euclidean ring.

Example: Every field is a Euclidean ring.

Solution: Let F be any field. Let the d function on the non-zero elements of F be defined as

d (a) = 0 for all $0 \neq a \in F$

Thus we have assigned the integer zero to every non-zero element in F.

If a and b are two non-zero elements in F then ab is also a non-zero element in F. We have therefore

$d(ab)=0=d(a)$.

Thus we have $d(ab) \geq d(a)$.

Finally if $a \in F$ and $0 \neq b \in F$, then we can write

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

$a=qb+r$ where $q=ab^{-1}$ and $r = 0$.

Hence every field is a Euclidean ring.

. . . . . .

. . . .

Example : Let $R = Z [i]$ be the ring of Gaussian integers . Define a function $d : R - \{ 0 \} \rightarrow N \cup \{0\}$, by sending $a + bi$ to its norm, which is by definition $a2 + b2$. Then the ring of Gaussian integers is a Euclidean domain .

Proof : Note first that if z is a complex number, then the absolute value of z, defined as the square root of the product of z with its complex conjugate $\bar{z}$, is closely related to the norm of z. In fact if z is a Gaussian integer $x + iy$, then $|z|2 = z\bar{z} = x\ 2 + y\ 2 = d(z)$. On the other hand, suppose we use polar coordinates, rather than Cartesian coordinates, to represent a complex number, $z = re^{i\theta}$. Then $r = |z|$. For any pair z1 and z2 of complex numbers, we have $|z1z2| = |z1||z2|$. Indeed this is clear, if we use polar coordinates. Now suppose that both z1 and z2 are Gaussian integers. If we square both sides of the equation above,

we get $d (z1\ z2) = d (z1) d (z2)$.

As the absolute value of a Gaussian integer is always at least one, (1) follows easily. To prove (2), it helps to think about this problem geometrically. First note that one may think of the Gaussian integers as being all points in the plane with integer coordinates. Fix a Gaussian integer α. To obtain all multiples of $\alpha = re^{i\theta}$, that is, the principal ideal (α), it suffices to take this lattice, rotate it through an angle of θ and stretch it by an amount r. With this picture, it is clear that given any other Gaussian integer β, there is a multiple of α, call it $q\alpha$, such that the square of the distance between β and $q\alpha$ is at most $r2/2$. Indeed let $\gamma = \beta/\alpha$. Pick a Gaussian integer q such that the square of the distance between γ and q

is at most 1/2. Then the distance between $\beta = \gamma\alpha$ and $q\alpha$ is at most r2/2. Thus we may write $\beta = q\alpha + r$, (different r of course) such that $d(r) < d(\alpha)$.

. . . .

. . . .

Example. 1. Z is a Euclidean Domain with norm $N(a) = |a|$.

2. If F is a field, then the polynomial ring F [x] is a Euclidean Domain with norm $N(p(x)) = \deg(p(x))$. The proof is very similar to that for Z.

3. $R = Z[i] := \{ a + bi \mid a, b \in Z \}$ is a Euclidean Domain.

Example : The units of $Z[\sqrt{2}]$ are built from integral solutions to $x^2 - 2y^2 = \pm 1$. For instance, one solution is x = 1 and y = 1 , giving the unit $1 + \sqrt{2}$. Its powers are also units (units are closed under multiplication) , so $Z[\sqrt{2}]$ has infinitely many units .

Example : Units in $Z[\sqrt{3}]$ come from integral solutions to $x^2 - 3y^2 = \pm 1$. However, there are no solutions to $x^2 - 3y^2 = -1$ since the equation has no solutions modulo 3: $x^2 \equiv -1 \mod 3$ has no solution. Thus the units of $Z[\sqrt{3}]$ only correspond to solutions to $x^2 - 3y^2 = 1$. One nontrivial solution (that is , other than ± 1) is x = 2 and y = 1 , which yields the unit $2 + \sqrt{3}$. Its powers give infinitely many more units .

Example : The units of $Z[\sqrt{-2}]$ come from integral solutions to $x^2 + 2y^2 = 1$. The right side is at least 2 once $y \neq 0$, so the only integral solutions are $x = \pm 1$ and y = 0, corresponding to the units ± 1. In contrast to the previous two examples , where there are infinitely many units, $Z[\sqrt{-2}]$ has only two units . The following theorem about Euclidean domains is the key to proving certain (imaginary) quadratic rings are not Euclidean. Notice the proof does not require the Euclidean function on the ring to satisfy the d-inequality.

Lemma : Let (R , d) be a Euclidean domain that is not a field, so there is a non-unit $a \in R$ with least d-value among all non-units. Then the quotient ring R/(a) is represented by 0 and units.

Proof : Pick x ∈ R . By division with remainder in R we can write x = a q + r where r = 0 or d (r) < d (a) . If r ≠ 0, then the inequality d (r) < d (a) forces r to be a unit. Since x ≡ r mod a , we conclude that R /(a) is represented by 0 and by units. ———————————

Example : When R = Z we can use a = 2. Then Z / 2Z is represented by 0 and 1 . When R = Z[i] we can use a = 1 + i. Then Z [i] / (1 + i) is represented by 0 and 1 as well as by 0 and i . These examples show some units could be congruent modulo a, but at least every element of the ring is congruent modulo a to 0 or some (perhaps more than one) unit .

We have shown that if R is a Euclidean domain that is not a field , there are elements of R (namely nonunits with least d-value) modulo which everything is congruent to 0 or to a unit from R. A domain that's not a field and which has no element modulo which everything is congruent to 0 or to a unit from R therefore can't be a Euclidean domain.

. . . . . .

Remark : In a domain R, an element a for which the ring R/(a) is represented by 0 and units in R is called a universal side divisor in the literature. This terminology seems strange. What's a side divisor? Remember the property, but forget the label (and don't use it, because nobody will know what you're talking about).

11.3 PROPERTIES OF EUCLIDEAN DOMAIN

Theorem 1 : . In a Euclidean domain, every ideal is principal .

Proof : Suppose R is a Euclidean domain and I ◄ R. Then EITHER I = { 0 } = (0) OR we can take a ≠ 0 in I with d (a) least ; then for any b ∈ I , we can write b = q a + r with r = 0 or d (r) < d (a) ; but r = q – b a ∈ I and so by minimality of d (a) , r = 0; thus a|b and I = (a) . . .

Example : The ring Z [x] is an example of an integral domain that is not a principal ideal domain. Here is a proof : I claim that the ideal (p , x) , for any prime number p ∈ Z , is not principal . Suppose on the contrary

that (p , x) is principal , i . e . , (p , x) = (f) for some f ∈ Z [x] . Since the degree of p is zero (since it is a constant polynomial) , the degree of f must be zero as well . So f must be a constant polynomial . But (p , x) = (f) , so x = f g for some g ∈ Z . So g = ±x and f = ± 1 . So either f = 1 or f = − 1 , and either way , (f) = Z [x] , not (p , x) . So (p , x) is not principal .

Consequently Z [x] cannot be a Euclidean domain . So , while you can do long division in the integers and in k [x] , you cannot do long division " simultaneously , " i .e. , if you try to do long division to divide an integer polynomial by an integer polynomial , at some point you may have to make a non-canonical (e . g . " Do I divide by 3 as many times as possible , or do I divide by x as many times as possible ? ") choice about how to choose a quotient q and remainder r when writing an element a as a = q b + r , given b. So while you can frequently carry out a successful long division in Z [x] , you aren't carrying out an algorithm that a computer could be programmed to do: you are, at some point, making a non-canonical choice. Another good example of a commutative ring that is not a principal ideal domain is k [x , y] for any field k (see the exercise below) , or indeed , R [x , y] for any commutative ring R . Indeed , k [x1 , x2 , .. . ,x n] is not a principal ideal domain , hence also not a Euclidean domain , unless n = 1. Again, you cannot carry out the familiar long division algorithm with polynomials in more than one variable (you can frequently carry out the long division , but you have to make some non - canonical choices in doing so) .

Theorem 2 : Every Euclidean domain is a PID. In particular every Euclidean domain is a UFD.

Proof : Let I be an ideal in a Euclidean domain. We want to show that I is principal . If I = { 0 } then I = (0) . Pick a an element of I , such that d (a) is minimal . I claim that I = (a) . Suppose that b ∈ I . We may write b = a q + r . If r = b – a q ∈ I . If r = 0 then d (r) < d (a) , which contradicts our choice of a . Otherwise r = 0 and b ∈ (a) so that I = (a) is principal .

Theorem 3 : Every Euclidean ring is a principal ideal ring.

Proof : Let R be a Euclidean ring . Let S be an arbitrary ideal of R . If S is the null ideal, then S = (0) i . e . , the ideal of R generated by 0. Therefore S is a principal ideal. So let us suppose that S is not a null ideal . Then there exist elements in S not equal to zero . Let b be a non-zero element in S such that d (b) is minimum i . e . , there exists no element c in S such that d (c) < d (b) .

We shall show that S = (b) i . e . , S is nothing but the ideal generated by b

Let a be any element of S Then by definition of Euclidean ring there exist elements q and r in R such that

a = q b + r where either r = 0 or d (r) < d (b) .

Now q ∈ R, b ∈ S , q b ∈ S because S is an ideal.

Further a ∈ S , q b ∈ S

q b = r ∈ S .

Thus r ∈ S and we have either r = 0 or d (r) < d (b) .

If r ≠ 0 , then d (r) < d (b) which contradicts our assumption that no element in S has d-value smaller than d (b) . Therefore we must have r = 0 .

Then a = q b .

Thus every element a in S is a multiple of the generating element b. Thus a ∈ S → a ∈ (b). Therefore S ⊆ (b) .

Again if x b is an element of (b) , then x ∈ R .

Now x ∈ R , b ∈ S → x b ∈ S . Therefore (b) ⊆ S.

Hence S = (b)

Thus every ideal Sin R is a principal ideal . Therefore R is a principal ideal ring .

Theorem 4 : Every Euclidean ring possesses unity element .

Proof : Let R be a Euclidean ring . Obviously R is an ideal of R .

Therefore there exists an element $u_0 \in R$ such that R = (u_0) i . e . , there exists an element $u_0 \in R$ such that every element in R is a multiple of u_0 .

Since, in particular , $u_0 \in R$ therefore there exists an element c ∈ R such that $u_0 = u_0 c$. We shall show that c is the required unity element. Let now a be any element of R.

Since a ∈ R , therefore there exists some x ∈ R such that $a = u_0 x$.

Now $a c = (u_0 x) c = (u_0 c) x = u_0 x = a$

Thus we have a c = a = c a for all a in R .

Hence c is the unity element .

Theorem 5 : Let R be a Euclidean ring and a and b be any two elements in R , not both of which are zero . Then a and b have a greatest common divisor d which can be expressed in the form

$d = \lambda a + u b$ for some $\lambda , u \in R$

Proof : Consider the set $S = \{ s a + t b : s , t \in R \}$

We claim that S is an ideal of R . The proof is as follows :

Let $x = s_1 a + t_1 b$, and $y = s_2 a + t_2 b$ be any two elements of S .

Then $s_1 , t_1 , s_2 , t_2 \in R$. We have

$x - y = (s_1 – s_2) a + (t_1 – t_2) b \in S$

since $s_1 – s_2$ and $t_1 – t_2$ are both elements of R

Thus S is a subgroup of R with respect to addition.

Also if u be any element of R, then

$x u = u x = u (s_1 a + t_1 b) = (u s_1) a + (u t_1) b \in S$

Therefore S is an ideal of R . Now every ideal in R is a principal ideal .

Therefore there exists an element d in S such that every element in S is a multiple of d .

Since as, therefore from (1), we see that there exists elements , λ , u in R such that $d = \lambda a + u b$.

Now R is a ring with unity element 1.

Putting s = 1 , t = 0 in (1) , we see that $a \in S$ Also putting s = 0 , 1 = 1 in (1), we see that $b \in S$

Now a , b are elements of S Therefore they are both multiples of d

Hence d |a and d |b.

Now suppose c |a and c | b.

Then c| λ a and c |u b . Therefore c is also a divisor of d

Thus d is a greatest common divisor of a and b.

Theorem 6 : Let a, b and c be any elements of a Euclidean ring R . Let (a , b) = 1 i . e . , let the greatest common divisor of a and b be 1 . If a | bc , then a | c .

Proof : If the greatest common divisor of a and b is 1, then by theorem 5 there exists elements λ and u in R such that

$1 = \lambda a + u b$.

Multiplying both members of (1) by c , we get

$c = \lambda a c + u b c$.

But a |b c , so there exists an element q in R such that $b c = q a$

Substituting this value of bc, we get

$c = \lambda a c + u q a = (\lambda c + u q) a$,

which shows that a is a divisor of c. Hence the theorem

Theorem 7 : If p is a prime element in the Euclidean ring R and p | a b where a , b ∈ R then p divides at least one of a or b

Proof : If p divides a , we are nothing to prove . So suppose that p does not divide a . Since p is prime and p does not divide a , therefore p and a are relatively prime i . e . , the greatest common divisor of p and a is 1 . Hence by theorem 4 , we get that p|b .

Theorem 8 : If p divides p', then p is associated top'.

Proof : If p divides p' , they both have positive degree , since they are primes, and so deg(p) = deg (p') by definition of a prime . But then p' = p q , and it follows as usual, taking degrees, that q is a unit.

Examples : (a) In Z , the primes p and −p are associated .

(b) In F [x] , primes f (x) and k f (x) (for any constant k) are associated

The Fundamental Theorem of Arithmetic Revisited:

In a Euclidean domain, every element of positive degree factors as a product of finitely many primes. Moreover, if : p1· · · pn = a = p' 1· · · p' m are two factorizations of a , then each of the p's is associated to one of the p' and vice versa (so there are the same number of p's as p' 's)

Proof : The fact that factorizations exist is the well-ordered axiom. We've seen this! The second part needs a proof, though. If p 1 · · · p n = p' 1· · · p' m , then in particular , p1 divides p' 1 (p'2· · · p' m) , so either p1 divides p' 1 or else p1 divides p' 2· · · p' m. If p1 divides p' 1 , then p1 and p' 1 are associated.

Otherwise p1 divides p' 2(p' 3· · · p' m) , and continuing in this fashion, eventually p 1 is associated to one of the p's . Similarly, every pi is

associated to one of the p' j's, and reversing the argument, every p' j is associated to one of the pi's.

Check Your Progress-1

1 . If R is a Euclidean ring and a , b are in R . If $b \neq 0$ is not a unit in R then

A . $d (a) < d (a , b)$

B . $d (a) > d (a , b)$

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

D . None of the above

2. An integral domain D is of characteristic zero if.

A . $m a = 0 , a \neq 0 \rightarrow m = 0$

B . $m a = 0 , a \neq 0 \rightarrow m \neq 0$

C . $m a = 0 , a \neq 0 \rightarrow m = a$

D . $m a = 0 , a \neq 0 \rightarrow m \neq a$

11.4 LET US SUM UP

In this unit, we have discussed Euclidean rings or Euclidean domains. We have also discussed the various properties of Euclidean domain.

11.5 KEYWORDS

5. ***Homomorphism:*** Homomorphism is derived from two Greek words 'homos', meaning 'link', and 'morphe', meaning 'form'.
6. ***Prime ideal:*** Let R be a ring and S an ideal in R. Then S is said to be a prime ideal of R if $ab \in S$, $a, b \in R$ implies that either a or b is in S
7. ***Maximal Ideal :*** An ideal $S \neq R$ in a ring R is said to be a maximal ideal of R if whenever U is an ideal of R such that $S \subseteq U \subseteq R$, then either R = U or S = U .

8. ***Principal ideal :*** An ideal S of a ring R is said to be a principal ideal if there exists an element a in S such that any ideal T of R containing a also contains S i . e . , S = (a) .

11.6 QUESTIONS FOR REVIEW

1. Prove that a Euclidean ring is necessarily a principal ideal ring with unity. Give two examples of such a ring.
2. Prove that I[√2], the set of real number a+b√2where a, b are integers is a Euclidean ring.
3. The ring of Gaussian integers is a Euclidean ring.
4. The ring of polynomials over a field is a Euclidean ring.

11.7 SUGGESTED READINGS AND REFERENCES

16. Thomas W Judson (2013). *Abstract Algebra: Theory and Applications*. Orthogonal Publishing.
17. Paul B. Garrett (2007). *Abstract Algebra*. Chapman and Hall/CRC.
18. Vijay K Khanna (2017).*A Course in Abstract Algebra Fifth Edition*. Vikas Publishing House
19. LALJI PRASAD (2016). *Modern Abstract Algebra*. Paramount Publication
20. Stephen Lovett (2016). *Abstract Algebra: Structures and Applications*. Chapman and Hall/CRC

11.8 ANSWERS TO CHECK YOUR PROGRESS

15. (a) (answer for Check your Progress-1 Q.1)
16. (a) (answer for Check your Progress-1 Q.2)

UNIT – 12: UNIQUE FACTORIZATION DOMAIN

STRUCTURE

12.0 OBJECTIVES

After studying this unit, you should be able to:

- Explain the concept of Unique Factorization Domain
- Describe polynomial ring over UFD

12.1 INTRODUCTION

In this unit, we will discuss the concept of Unique Factorization Domain. We will discuss various properties of Unique Factorization Domain.

12.2 UNIQUE FACTORIZATION DOMAIN

Prime Elements

Definition : Let D be an integral domain with unity element 1 . A non-zero non-unit element $a \in D$, having only trivial divisors , is called a prime or irreducible element of D . An element $0\ b \in D$ having proper divisors is called a reducible or composite element of D .

From this definition it is obvious that if p is a prime element of D and if $p = x\ y$, where $x , y \in D$, then one of x or y must be a unit in D .

Also $0 \neq b \in D$ is a composite element of D if and only if we can find two elements $x, y \in D$ such that $b = x\,y$ and none of x and y is a unit in D.

. . . .
. . . .

Greatest Common Divisor

Definition: Let R be a commutative ring. If $a, b \in R$ then $0 \neq d \in R$ is said to be a greatest common divisor of a and b if

(i) $d \mid a$ and $d \mid b$.

(ii) Whenever $c \mid a$ and $c \mid b$ then $c \mid d$ . .

.. . .
. . . .

Unique Factorization Domain

Definition: An integral domain R, with unity element 1 is a unique factorization domain if

(a) any non-zero element in R is either a unit or can be written as the product of a finite number of irreducible (prime) elements of R.

(b) the decomposition in part (a) is unique up to the order and associates of the irreducible elements .

. . ..
. . ..

Definition : A polynomial $f \in R[x]$ is primitive if $a|f$ for some $a \in R$ only if a is a unit.

In general commutative rings we have defined the greatest common divisors of elements. But the difficulty is that in an arbitrary commutative ring these might not exist . However , in unique factorization domain their existence is assured. Further we know that in an integral domain with unity in case a greatest common divisor of some

elements exist , it is unique apart from the distinction between associates .

. . . .
. . . .

Notice also that every irreducible element in a UFD is prime. In fact if a|bc, i.e. bc = ak then by decomposing we have b1⋯bkc1⋯cr = ad1⋯dl which implies that a is an associate of some bi or some ci and thas a/b or a/c. Because every prime is irreducible this means that in a UFD every element is a product of primes.

. . . .
. . . .

Theorem 1 : Let D be a domain, if every element is a product of primes then this decomposition is automatically unique up to a unit, i.e. it is a UFD

Proof. Assume a1⋯ak = b1⋯bs. Proceed by induction on k. If k = 1, then a1 = ub1 because a1 is irreducible. Assume k > 2, then a1/bi for some i, say i = 1. By cancellation property we have then a2⋯ak = l1 ·b2 ..·bs and we are dome by induction. ——————————

We know thatZis a UFD. Another important example is the F[x] where F is a field. We will now show that every PID is a UFD. In what follows we will assume that D is a PID.

. . . .
. . . .

Theorem 2 : Every principal ideal domain is a unique factorization domain .

Proof : Let R be a principal ideal domain . Suppose that there exists an nonzero , non - unit element y’ ∈ R such that y0 cannot be written a product of irreducible elements in R. Then y0 cannot itself be irreducible, so y0 = x1 y1 for some non - units x1 , y1 ∈ R , and at least one of the two elements x1 or y1 cannot be written as a product of irreducible

elements; without loss of generality we can assume that that element is y1. Now we apply the same logic to y1, factoring y1 as y1 = x2 y2 for some non-units x2 , y2 ∈ R , with y2 not a product of irreducible elements ; and so on: y0 = x1 y1 = x1 x2 y2 = x1 x2 x3 y3 = . . . yielding an ascending chain of ideals in R : (y0) ⊆ (y1) ⊆ (y2) ⊆ . . . . By Lemma, there exists some n ∈ N such that (y n) = (y n + 1) = (yn+2) = ⊆ , so xn , xn+1 , xn+2 , . . . are all units in R , a contradiction . So every nonzero , non unit element y0 ∈ R can be written uniquely as a product of irreducible elements . For the second half of the proof , that if y0 admits two factorizations y0 = p1 . . . pm = q1 . . . qn , then m = n and the factorizations differ only by rearranging factors and multiplying by units.

. . . .

Here are some more examples of non-UFDs:

• Let Z [√−5] be the ring whose underlying abelian group is Z×Z ,with multiplication

(a , b) (c ,d) = (a c – 5 b d , a d + b c) . Then Z [√−5] is not a UFD .

• Let C∞(R) be the ring of smooth functions f : R → R, with addition given by letting (f + g) (x) = f (x) + g (x) , and with multiplication given by letting (f g) (x) = f (x) g (x) . Then C∞(R) is not a UFD .

. . . .

Theorem 3 : Let R be a unique factorization domain and a and b be any two elements in R , not both of which are zero . Then a and b have a greatest common divisor (a , b) in R . Moreover , if a and b are relatively prime (i . e . , (a , b) is a unit in R) , then a | b c imples a | c .

Proof : Suppose a and b are any two elements, not both of which are zero , of a unique factorization domain R . If one of a and b , say , b is 0 , then obviously a is the greatest common divisor of a and b . If any of a and b , say a , is a unit in R , then obviously a is the greatest common divisor of

a and b . So let us suppose that neither a = 0 nor b = 0 and none of these is a unit in R . Then each of a and b can be uniquely expressed as the product of a finite number of irreducible elements of R . Let

$a = p_1^{m_1} p_2^{m_2} \ldots .$

and $b = p_1^{n_1} p_2^{n_2} \ldots ..$

where we have arranged the expressions in such a way that the same irreducible factors, appear in both . Note that we can definitely do so because the integer 0 can be used as power in any case , if necessary . The elements p's are all different primes and m, n, are all integers > 0 .

Let g_i = minimum (m_i, n_i), where i = 1 , 2 . . , r

Then obviously $p_1^{g_1} p_2^{g_2} \ldots$

is the greatest common divisor of a and b

This proves the existence of greatest common divisor.

Now suppose that a and b are relatively prime 1.e., the grea

test common divisor of a and b is a unit in R. Also suppose that a | b c .

If a is a unit in R , then obviously a is a divisor of c . So let a be not a unit in R . Then a can be uniquely expressed as the product of a finite number of prime elements of R . Let

$a = q_1^{m_1} q_2^{m_2} \ldots ..$

where q's are prime elements of R .

We have a | b c implies b c = k a for some k in R

Since each element of R can be uniquely expressed as the product of a finite number of prime elements of R , therefore each of the prime elements q must occur as a factor of either b or c . But none of q can be a factor of b because otherwise a and b will not remain relatively prime. Therefore each of q must be a factor of c . Hence a is a divisor of c => a | c .

. . . .
. . . .

Theorem 4 : If a is a prime element of unique factorization domain R and b, c are any elements of R , then a | b c → a | b or a | c .

Proof : If a | b , then obviously the theorem is proved . So let a be not a divisor of b . Since a is a prime element of R and a is not a divisor of b , therefore we claim that a and b are relatively prime. Since a is a prime element of R, therefore the only divisors of a are the associates of a or the units of R . Now an associate of a cannot be a divisor of b otherwise a itself will be a divisor of b while we have assumed that a is not a divisor of b . Thus the units of R are the only divisors of a which also divide b . Therefore the greatest common divisor of a and b is a unit of R.

Since a and b are relatively prime , therefore by theorem 1, we have a | b c → a | c

This completes the proof of the theorem.

. . . .
. . . .

12.3 POLYNOMIAL RINGS OVER UFD

Polynomial rings over unique factorization domains.
Let R be a unique factorization domain. Since R is an integral domain with unity, therefore R [x] is also an integral domain with unity . Also any unit , (inversible element) in R [x] must already be a unit in R . Thus the only units in R [x] are the units of R .

. . . .
. . . .

A polynomial p (x) in R [x] is irreducible over R i . e . , irreducible as an element of R [x] if whenever p (x) = (x) b (x) with a (x) , b (x) E [x] , then one of a (x) or b (x) is a unit in R [x] i e . , a unit in R . For example Z , if I is the ring of integers , then I is a unique factorization domain . The polynomial 2x+4 e I [x] is a reducible

element of I (x) . We have 2x* + 4 = 2 (x + 2) . Neither 2 nor x + 2 is a unit in I [x] . On the other hand the polynomial x + 1 e I [x] is an irreducible element of I [x] .

. . . .
. . . .

Content of a polynomial

Definition: Let f(x)=ag+a1x+apx2+..+anx be a polynomial over a unique factorization domain R. Then the content of (x) denoted by c), is defined as the greatest common divisor of the coefficients a, a,, an of f (x) . Obviously the content of f(x) is unique within units of R. Thus if c and c are two contents of f (x) , then we must have c=uc, where u is some unit in R.

. . . .
. . . .

Primitive polynomial

Definition: Let R be a unique factorization domain. Then a polynomtal f (x) = a, + a,x+.+ anx E R [x] is said to be primitive if the greatest common divisor of its coefficients a, ar,., an is a unit in R. Thus a polynomial S (x) is primitive if its content is 1 (that is a unit in R). If f(x)-x"+a, x1.+an-1 x+a, is a monic polynomial over R, then obviously f(x) is primitive.

If I is the ring of integers, then 3x3-5x2-+7 is a primitive member of I [x] while 2x2 - 4x+8 is not a primitive member of I [x] .

. . . .
. . . .

Every irreducible polynomial of positive degree belonging to R [x] is necessarily primitive. But an irreducible polynomial of zero degree may not be primitive. For example 3 E I [x] is irreducible but it is not primitive. Further a primitive polynomial may not be irreducible. For example x°+5x+6El[x] is primitive and it is not irreducible. We have x2 +5x+6=(x+2) (x+3).

. . . .
. . . .

Theorem 5 : Let D be a UFD and let I = (a1 , . . . , ak) be a finitely generated ideal. Then there is a minimal principal ideal (d (I)) containing I.

Proof : Let d be the product of the common primes in the decomposition of the ai' s . Assume that I ⊂ (d 0) , then d0 / ai for i = 1 , . . . , k and thus by definition d0 / d, i . e . (d) ⊂ (d0).

. . . .

Definition : A finitely generated ideal I = (a1 , . . . , ak) ⊂ D is called primitive if (d (I)) = D. A polynomial f ∈ D [x] is called primitive if I = (a1 , . . . , ak) is primitive .

Moreover the content of a polynomial f ∈ D [x] is c (f) ∈ D where c (d) = d (I) ,for I = (a1 , . . . , ak)

Notice that every polynomial f (x) can be then written as f (x) = c (f) g (x) where g (x) is primitive .

. . . .

Recall that:

Lemma : . Let R be a ring and let P ⊂ R be a prime ideal . Let I , J be ideals such that I J ⊂ P Then I ⊂ P or J ⊂ P .

Proof : Assume I not contained in P, then there is an element a ∈ I and a is not contained in P. But a J ⊂ P and because P is prime this implies J ⊂ P. ———————————

. . . .

Corollary : (GAUSS LEMMA) Let D be a UFD. The product of two primitive elements is primitive .

Proof : . Assume I = (a1 , . . . , ak) , J = (b1 , . . . , bs) primitive . We have to prove that I J is primitive . If not there is a proper principle ideal containing it , I J ⊂ (d) . Let d = Πpi, then I J ⊂ (d) ⊂ (pi) and by Lemma ⊂ (pi) or J ⊂ (pi) which is impossible because they are primitive.

. . . .

. . . . **Theorem 6 :** If D is a UFD then D[x] is a UFD.

Proof : Because D[x] is a domain we just have to show that every element is a product of primes and then the statement will follow by Lemma . Let K be the field of fractions of D. Let f(x) ∈ D [x] ⊂ K [x] . Recall that K [x] is a PID and therefore by Theorem a UFD . Then we can decompose f (x) = F1 (x)···Fk (x) where Fi (x) are primes in K [x] . After "clearing the denominator" we can write: d f (x) = g1 (x)· · · gk (x) = c (g 1) · · · c (g k)Πfi(x) in D [x] , where the fi are primitive polynomials. We will show that fi are prime in D[x] from which the statement will follow.

Consider the map of rings:

φ : D [x] / (f i) → K [x] / [(F i) = (fi)] . It is an injective map. In fact let h (x) ∈ D [x] so that h (x) ∈ (Fi) in K [x]. Then h (x) = Fi (x) G (x) after clearing the denominators we have A h (x) = gi (x) H (x) = c (fi) c (H) fi (x) g (x) .

Let A = Πpj , then pj cannot divide fi (x) g (x) since it is primitive . Then pj / c (fi) c (H) and thus by cancellation we obtain : h (x) = B fi (x) g (x) which implies that h (x) ∈ (fi) . The map φ being injective implies that D [x] / (fi) is a subring of a domain : K [x] / [(F i) and thus a domain . It follows that (fi) is prime for all i .

Now consider again d f (x) = c (g1) · · · c (gk) Πfi (x) . Every prime pi dividing d cannot divide Π fi (x) since they are primitive and therefore have to divide c (g1) · · · c (gk) . By cancellation we obtain f (x) = C Π fi (x) . Let C = Π qj be the prime decomposition , it follows then that f (x) = Π qj Π fi (x) , a prime decomposition .

. . . .

. . . .

Another proof

Theorem 7 : . If R is a UFD , then R [x] is a UFD .

Proof : First , we notice that if a ∈ R is prime in R , then a is prime in R [x] (as a degree 0 polynomial) . For if a = b c in R [x] , then deg b = deg c = 0 , hence both b and c are in R , hence one is a unit .

. . . .

Theorem 3: If R is a unique factorization domain, then the product of two primitive polynomials in R[x] is again a primitive polynomial in R[x]

Proof: Let $f(x) = a_0x^0 + a_1x^1 + a_2x^2 + \cdots$ and $g(x) = b_0x^0 + b_1x^1 + b_2x^2 + \cdots$ be two primitive polynomials in R[x]

Let $h(x) = c_0x^0 + c_1x^1 + c_2x^2 + \cdots$

Suppose f(x) is not primitive. Then all the coefficients of h(x) must be divisible by some prime element p of R. Since f(x) is primitive, therefore the prime element p must not divide some coefficient of f(x) Let a, be the first coefficient of f(x) which p does not divide. Similarly let b, be the first coefficient of g (x) which p does not divide. In f(x) g(x), the coefficient of x^{i+j} is c^{i+j}.

Now by our choice of a, p is a divisor of each of the elements of a

Similarly, by our choice of b,p is a divisor of each of the elements of b

Also by assumption p| ci+j.

Hence from (1), we get p|aibj

→p|ai or p|bj

But this is nonsense because according to our assumption p is not a divisor of a and also p is not a divisor of bj.

Hence h(x) must be primitive

This proves the theorem

. . . .

Theorem 8: If R is a unique factorization domain and if f(x), g(x) are in R [x], then c(fg)=c(f) c(g) (upto units)

Proof: The polynomial f(x) in R[x] can be written as f(x)= a f_1(x), where a=c(f) and f_1 (x) is primitive. Similarly the polynomial g(x) can be written as g(x)=bg1(x), where b=c(g) and

g1(x) is primitive. Then

f(x) g(x)=a b f1(x) g1(x).

Since f1(x) and g1(x) are both primitive, therefore f1(x) g1(x)

is also primitive. [Refer theorem 3]

Therefore, we see that the content of f(x) g(x) is either ab or some associate of ab. Thus the content of f(x) g(x) is ab (upto units). Therefore C(fg)=ab=c(f) c(g)

This proves the theorem

. . . .

. . . .

Theorem 9 : Let R be an integral domain. Then the following are equivalent

(a) For every non-zero element a∈R which is not a unit factors as

a = b1 . . . bn

where each bi is irreducible.

(b) R does not contain an infinite increasing chain of principle ideals

(a1) < (a2) < (a3) <· · ·

Proof : Suppose R contains an infinite increasing sequence (a1) < (a2) < (a3) <· · · Then (an) < (1) for all n because (an) < (an+1) ⊆ (1) . Since (an−1) < (an) , an is a proper divisor of an−1 . Say an−1 = an bn where an bn are not units. This provides a non-terminating sequence of factorizations a1 = a2 b2 = a3 b3 b2 = a4 b4 b3 b2 . . . . Conversely such a factorization gives us an increasing chain of ideals.

. . . .

. . . .

Theorem 10 : (Gauss) Let R be a unique factorization domain. Then the polynomial ring in one variable R [x] is a unique factorization domain .

. . . .

. . . .

Remark: The proof factors f (x) ∈ R [x] in the larger ring k [x] where k is the field of fractions of R (see below) , and rearranges constants to get coefficients into R rather than k . Uniqueness of the factorization follows from uniqueness of factorization in R and uniqueness of factorization in k [x] .

. . . .

. . . .

Corollary : A polynomial ring k [x1 , . . . , xn] in a finite number of variables x1 , . . . , xn over a field k is a unique factorization domain . (Proof by induction .)

. . . .

Corollary: A polynomial ring Z [x1 , . . . , xn] in a finite number of variables x1 , . . . , xn over the integers Z is a unique factorization domain . (Proof by induction .)

. . . .

Before proving the theorem itself, we must verify that unique factorization recovers some naive ideas about divisibility. Recall that for r , s ∈ R not both 0 , an element g ∈ R dividing both r and s such that any divisor d of both r and s also divides g, is a greatest common divisor of r and s, denoted g = gcd (r , s) .

. . . .

Theorem 11 : Let R be a unique factorization domain. For r , s in R not both 0 there exists gcd (r , s) unique up to an element of R×. Factor both r and s into irreducibles r = u· p^{e1} 1 . . . p^{em} m , s = v· p^{f1} 1 . . . p^{fn} m where u and v are units and the pi are mutually non-associate irreducibles (allow the exponents to be 0 , to use a common set of irreducibles to express both r and s) . Then the greatest common divisor has exponents which are the minima of those of r and s

gcd (r , s) = pmin (e1 , f1) 1 ...pmin(em , fm) m

Proof: Let g = pmin (e1 , f1) 1 ...pmin (em , fm) m First, g does divide both r and s . On the other hand , let d be any divisor of both r and s . Enlarge the collection of inequivalent irreducibles pi if necessary such that d can be expressed as d = w·ph1 1 ...phm m with unit w and non-negative integer exponents. From d|r there is D ∈ R such that dD = r. Let D = W ·pH1 1 ...pHm m Then wW ·ph1+H1 1 ...phm+Hm m = d·D = r =

u·pe1 1 ...pem m Unique factorization and non-associateness of the pi implies that the exponents are the same: for all i

hi + Hi = ei Thus, hi ≤ ei. The same argument applies with r replaced by s, so hi ≤ fi, and hi ≤min(ei,fi). Thus, d|g. For uniqueness, note that any other greatest common divisor h would have g|h, but also h|r and h|s. Using the unique (up to units) factorizations, the exponents of the irreducibles in g and h must be the same, so g and h must differ only by a unit.

. . . .

Theorem 12 : In the field of fractions k of a unique factorization domain R (extended) greatest common divisors exist.

Proof: We reduce this to the case that everything is inside R. Given elements xi = ai/bi in k with ai and bi all in R, take 06= r ∈ R such that rxi ∈ R for all i. Let G be the greatest common divisor of the rxi, and put g = G/r. We claim this g is the greatest common divisor of the xi. On one hand, from G|rxi it follows that g|xi. On the other hand, if d|xi then rd|rxi, so rd divides G = rg and d|g.

.**Check Your Progress-1**

1. Every finite integral domain is.

    a. of finite characteristic

    b. of not finite characteristic

    c. not a field

    d. None of the above

2. In a UFD if a|c, b|c and (a,b)=1 then

    a. a|b

    b. ab|c

    c. a=b

    d. None of the above

12.4 LET US SUM UP

In this unit, we have discussed the concept of Unique Factorization Domain. We have discussed various properties of Unique Factorization Domain.

12.5 KEYWORDS

UFD: An integral domain R, with unity element 1 is a unique factorization domain if

(a) any non-zero element in R is either a unit or can be written as the product of a finite number of irreducible (prime) elements of R.

(b) the decomposition in part (a) is unique up to the order and associates of the irreducible elements.

12.6 QUESTIONS FOR REVIEW

1. Let R be a UFD. Then show that every prime element in R generates a prime ideal.
2. Let Z[√−5 denote the set of complex numbers of the form a+b√−5 where a and b are integers (and √−5 denotes the complex number √5i. Show that Z[√−5] is not a UFD
3. Z is a UFD.
4. The integral domain R = Z+xQ[x] does not satisfy the ascending chain condition for principal ideals, so it is not a UFD. However, irreducibles in Rare prime

12.7 SUGGESTED READINGS AND REFERENCES

21. Thomas W Judson (2013). *Abstract Algebra: Theory and Applications*. Orthogonal Publishing.
22. Paul B. Garrett (2007). *Abstract Algebra*. Chapman and Hall/CRC.
23. Vijay K Khanna (2017).*A Course in Abstract Algebra Fifth Edition*. Vikas Publishing House
24. LALJI PRASAD (2016). *Modern Abstract Algebra*. Paramount Publication

25. Stephen Lovett (2016). *Abstract Algebra: Structures and Applications*. Chapman and Hall/CRC

12.8 ANSWERS TO CHECK YOUR PROGRESS

17. (a) (answer for Check your Progress-1 Q.1)

18. (b) (answer for Check your Progress-1 Q.2)

UNIT – 13: PRINCIPAL IDEAL DOMAIN

STRUCTURE

13.0 OBJECTIVES

After studying this unit, you should be able to:

- Explain the concept of Principal Ideal Domain
- Describe properties of PID

13.1 INTRODUCTION

In this unit, we will introduce the concept of principal ideal domain. We will discuss various properties of principal ideal domain.

13.2 PRINCIPAL IDEAL DOMAIN

Prime Elements

Definition : Let D be an integral domain with unity element 1 . A non-zero non-unit element $a \in D$, having only trivial divisors , is called a prime or irreducible element of D . An element $0\ b \in D$ having proper divisors is called a reducible or composite element of D .

From this definition it is obvious that if p is a prime element of D and if $p = x\ y$, where $x , y \in D$, then one of x or y must be a unit in D .

Also $0 \neq b \in D$ is a composite element of D if and only if we can find two elements $x, y \in D$ such that $b = x\,y$ and none of x and y is a unit in D.

. . . .

. . . .

Principal ideal

Definition: An ideal S of a ring R is said to be a principal ideal if there exists an element a in S such that any ideal T of R containing a also contains S i.e., S = (a).

Thus an ideal generated by a single element of itself is called a principal ideal.

. . . .

. . . .

Principal Ideal Ring/Principal Ideal Domain

Definition: A commutative ring R without zero divisors and with unity element is a principal ideal ring if every ideal Sin R is a principal ideal i.e, if every ideal Sin R is of the form S = (a) for some $a \in S$.

. . . .

. . . .

Example : Z is a PID .

NOTE : Showing that Z is a PID means showing that if I is an ideal of Z , then there is some integer n for which I consists of all the integer multiples of n .

Proof : Suppose that $I \subseteq Z$ is an ideal . If I = { 0 } then I is the principal ideal generated by 0 and I is principal. If $I \neq \{ 0 \}$ then I contains both positive and negative elements. Let m be the least positive element of I. We will show that $I = < m >$. Certainly $< m > \subseteq I$ as I must contain all integer mulitples of m. On the other hand suppose $a \in I$. Then we can write $a = mq + r$ where $q \in Z$ and $0 \leq r < m$. Then $r = a - qm$. Since $a \in I$ and $-qm \in I$, this means $r \in I$. It follows that r = 0 , otherwise we have a contradiction to the choice of m. Thus a = qm and $a \in < m >$. We conclude $I = < m >$.

. . . . . .

. . . . . .

Example : The ring Z [x] is an example of an integral domain that is not a principal ideal domain.

proof: I claim that the ideal (p , x) , for any prime number p ∈ Z , is not principal . Suppose on the contrary that (p , x) is principal, i. e. , (p , x) = (f) for some f ∈ Z [x] . Since the degree of p is zero (since it is a constant polynomial) , the degree of f must be zero as well . So f must be a constant polynomial . But (p , x) = (f) , so x = f g for some g ∈ Z. So g = ± x and f = ± 1 . So either f = 1 or f = −1, and either way, (f) = Z [x] , not (p , x) . So (p , x) is not principal.

Consequently Z [x] cannot be a Euclidean domain. So, while you can do long division in the integers and in k [x] , you cannot do long division "simultaneously," i.e., if you try to do long division to divide an integer polynomial by an integer polynomial, at some point you may have to make a non-canonical (e.g. "Do I divide by 3 as many times as possible, or do I divide by x as many times as possible?") choice about how to choose a quotient q and remainder r when writing an element a as a = qb+r, given b. So while you can frequently carry out a successful long division in Z [x] , you aren't carrying out an algorithm that a computer could be programmed to do: you are, at some point, making a non-canonical choice.

Another good example of a commutative ring that is not a principal ideal domain is k [x , y] for any field k (see the exercise below), or indeed, R[x, y] for any commutative ring R. Indeed, k[x1, x2, . . . , xn] is not a principal ideal domain, hence also not a Euclidean domain, unless n = 1. Again, you cannot carry out the familiar long division algorithm with polynomials in more than one variable (you can frequently carry out the long division, but you have to make some non-canonical choices in doing so)..

. . . . . .

. . . . . .

13.3 PROPERTIES OF PID

Theorem 1: The ring of integers is a principal ideal ring.

Proof: Let (I, +, .) be the ring of integers. Obviously I is a commutative ring with unity and without zero divisors. Therefore I will be a principal ideal ring if every ideal in I is a principal ideal

Let S be any ideal of the ring of integers. If S is the null ideal, then S=(0) so that S is a principal ideal.

So let us suppose that S ≠(0)

Now S contains at least one non-zero integer, say a. Since S is a subgroup of R under addition, therefore a ∈ S → -a ∈ S.

This shows that S contains at least one positive integer because if 0 ≠ a, then one of a and -a must be positive.

Let S be the set of all positive integers in S. Since S is not empty, therefore by the well ordering principle S must possess a least positive integer. Let s be the least element. We will now show that S is the principal ideal generated by s i.e., S=(s).

Suppose now that n is any integer in S. Then by division algorithm, there exist integers q and r such that n=qs+r with 0 ≤ r < s

Now, s ∈ S, q ∈ I

Therefore, qs ∈ S

and

n ∈ S, qs ∈ S → n – qs ∈ S

→r ∈ S

But 0 ≤ r < s and s is the least positive integer such that s ∈ S. Hence r must be 0.

Therefore, n = qs

Thus n ∈ S → n=qs for some q ∈ I.

Hence S is a principal ideal of I generated by s.

Since S was an arbitrary ideal in the ring of integers, therefor the ring of integers is a principal ideal ring.

. . . .

. . . .

Theorem 2: Every field is a principal ideal ring.

Proof: A field has no proper ideals.

The only ideals of a field are (i) the null ideal which is a principal ideal generated by 0 and (ii) the field itself which is also a principal ideal generated by 1. Thus a field is always a principal ideal ring.

. . . . . .

Theorem 3: If F is a field then the ring of polynomials F[x] is a PID.

Proof. Let $I \in R$. If $I = \{0\}$ then $I = (0)$. Otherwise let $0 \neq p(x)$ be a polynomial such that $p(x) \in I$ and deg $p(x) \leq$ deg $q(x)$ for all $q(x) \in I - \{0\}$. Check that $I = (p(x))$.

Note: Z[x] is not a PID. E.g. the ideal (2,x) is not a principal ideal of Z[x] .

Another Proof

Let F be a field . Then the polynomial ring F[x] is a PID .

NOTE : Recall that F [x] has one important property in common with Z , namely a division algorithm . This is the key to showing that F [x] is a PID .

Proof : Let $I \subseteq F[x]$ be an ideal. If $I = \{0\}$ then $I = <0>$ and I is principal. If $I \neq \{0\}$, let f (x) be a polynomial of minimal degree m in I . Then $<f(x)> \subseteq I$ since every polynomial multiple off (x) is in I . We will show that $I = <f(x)>$. To see this suppose $g(x) \in I$. Then $g(x) = f(x)q(x) + r(x)$ where $q(x), r(x) \in F[x]$ and $r(x) = 0$ or deg (r (x)) < m . Now $r(x) = g(x) - f(x)q(x)$ and so $r(x) \in I$. It follows that $r(x) = 0$ otherwise r (x) is a polynomial in I of degree strictly less than m , contrary to the choice of f (x) . Thus $g(x) = f(x)q(x)$, $g(x) \in <f(x)>$ and $I = <f(x)>$.

. . . . . .

Theorem 4: If R is a Euclidean domain then R is a PID.

Proof: Let $I \subseteq R$, $I \neq \{0\}$. Choose $a \in I$ such that $a \neq 0$ and that $N(a) \leq N(b)$ for all $b \in I - \{0\}$. Check that $(a) = I$.

Note: It is not true that every PID is a Euclidean domain. Take e.g. $\alpha = 1/2 + \sqrt{19}/2\, i$ and let $Z[\alpha] = \{a + b\alpha \mid a,b \in Z\}$. Then $Z[\alpha]$ is a PID, but it is not a Euclidean domain.

Another Proof

Let R be a Euclidean domain . Then R is a principal ideal domain .

Proof : Choose a Euclidean norm δ on R . Let $I \subseteq R$ be an ideal, and choose an element $i \in R$ with minimal norm, i . e . , $\delta (i) \leq \delta (i ')$ for all $i ' \in I$. I claim that $I = (i)$. Clearly $(i) \subseteq I$, since $i \in I$ and I is an ideal . Conversely , if $j \in I$, then $\delta (j) \geq \delta (i)$, and there exists some q , r such that $j = iq + r$ and either $r = 0$ or $\delta (r) < \delta (i)$. We solve for r to get $r = j – i q$, and since j and iq are both in I, so is r. So $\delta (r) < \delta (i)$ is impossible , since i was assumed to have minimal norm among the elements of I. So r = 0. So j = iq. So $j \in (i)$. So $I \subseteq (i)$. Hence every ideal in R is principal .

. . . . . .

Theorem 5: Let R be a PID. Then a nonzero ideal I of R is prime if and only if it is maximal.

Proof: We already know that a maximal ideal is necessarily prime. So let P be a non-zero prime ideal of R. Assume that M is another ideal with $P \subset M$. Since R is a PID, we can write P = (p) and M = (m). Then $(p) \subseteq (m)$, which means that $mr = p$ for some $r \in R$. Thus either m or r is in P. By assumption, m does not belong to P, so that $r \in P$. Then $r = sp$ for some $s \in R$. Substituting, that means $msp = p$, so that $ms = 1$ and m is a unit. Thus M = R. So any ideal bigger than P is all of R and P is maximal .

. . . . . .

PIDs that aren’t Euclidean

Suppose that you have an integral domain R, and you want to know if it is a principal ideal domain. One way of checking this is to see if there is an obvious choice of Euclidean norm on it; for Z and k[x] and a handful of other rings (like Z[i]) there is a function $R\backslash\{0\} \rightarrow N$ which you have

been calling a “norm” for years, so it’s very natural to check that this norm in fact satisfies the axioms for a Euclidean norm, making the domain R Euclidean and hence a principal ideal domain.

However, there are other ways of checking whether a domain is a principal ideal domain (for example: the famous ideal class group of a Dedekind domain is a group which is trivial if and only if the Dedekind domain is a PID, but we will not get to ideal class groups this semester; these are covered in topics classes in number theory, algebraic geometry, and algebraic K-theory). It is also true that not every principal ideal domain is a Euclidean domain, so a domain may be a PID even in cases where it is totally impossible to produce a Euclidean norm on the domain.

Suppose you have an integral domain that you suspect is not Euclidean. If you can show that the integral domain is not a PID, then it cannot be Euclidean; but not every PID is Euclidean. It is usually cumbersome to show that a given principal ideal domain fails to be Euclidean. The best way to try to do this is to show that Euclidean domains have additional properties which not all principal ideal domains have.

. . . .

Theorem 6 : Every principal ideal domain is a unique factorization domain .

Proof : Let R be a principal ideal domain . Suppose that there exists an nonzero , non - unit element y’ ∈ R such that y0 cannot be written a product of irreducible elements in R. Then y0 cannot itself be irreducible, so y0 = x1 y1 for some non - units x1 , y1 ∈ R , and at least one of the two elements x1 or y1 cannot be written as a product of irreducible elements; without loss of generality we can assume that that element is y1. Now we apply the same logic to y1, factoring y1 as y1 = x2 y2 for some non-units x2 , y2 ∈ R , with y2 not a product of irreducible elements ; and so on: y0 = x1 y1 = x1 x2 y2 = x1 x2 x3 y3 = . . . yielding an ascending chain of ideals in R : (y0) ⊆ (y1) ⊆ (y2) ⊆ . . . . By Lemma, there exists some n ∈ N such that (y n) = (y n + 1) = (yn+2) = ⊆ , so xn , xn+1 , xn+2 , . . . are all units in R , a contradiction . So every

nonzero , non-unit element $y_0 \in R$ can be written uniquely as a product of irreducible elements . For the second half of the proof , that if y_0 admits two factorizations $y_0 = p_1 \ldots p_m = q_1 \ldots q_n$, then $m = n$ and the factorizations differ only by rearranging factors and multiplying by units.

. . . .

Theorem 7 : . Let R be a PID . Then R satisfies the prime divisor property , i . e . , any non-unit irreducible $\pi \in R$ is prime . Consquently , R has unique factorization , i . e . , if α is any nonzero nonunit in R , then it can be written uniquely (up to reordering and units) in the form $\alpha = \pi_1\pi_2 \cdots \pi_k$ where π_i are primes of R.

Proof. The second statement follows formally from the first (I have said many times now that the prime divisor property and unique factorization are equivalent—if you want to review the argument, look back at the cases of Z or Z [i]) . Thus it suffices to show any non-unit irreducible $\pi \in R$ is prime . Let π be a non-unit irreducible . Recall π is prime means $\pi \mid \alpha\beta \Rightarrow \pi \mid \alpha$ or $\pi \mid \beta$. So suppose $\pi \mid \alpha\beta$ for some $\alpha, \beta \in R$. The idea is to look at the “gcd” $(\pi, \alpha) = (\pi) + (\alpha)$ of π and α . Note that $(\pi, \alpha) = (\gamma)$ for some $\gamma \in R$ since R is a PID . We know $(\gamma) = (\pi, \alpha) \mid (\pi)$ and $(\gamma) = (\pi, \alpha) \mid (\alpha)$ by the definition of divides for ideals . This means, $\pi = m\gamma$ and $\alpha = n\gamma$ for some $m, n \in R$. Since π is irreducible , either m or γ is a unit and the other is an associate of π . If γ is an associate of π, this means $\pi \mid \alpha = n\gamma$, so the prime divisor property holds. Thus we may assume γ is a unit. This means $1 \in (\gamma) = (\pi, \alpha)$, i . e . , $1 = r\pi + s\alpha$ for some $r, s \in R$. Thus $\beta = r\pi\beta + s\alpha\beta$, but π divides both terms on the right , so therefore $\pi|\beta$. Hence the prime divisor property holds.

. . . .

Lemma : . Let R be a subring of C. The principal ideals (α) of R are in 1-1 correspondence with the set of associate classes of R.

Notes

Now the issue with unique factorization in $Z[\sqrt{-3}]$ was the following: $4 = 2 \cdot 2 = (1 + \sqrt{-3}) \cdot (1 - \sqrt{-3})$ but 2, $1 + \sqrt{-3}$ and $1 - \sqrt{-3}$ are all irreducible in $Z[\sqrt{-3}]$. In the language of ideals, we can write this as $(4) = (2)(2) = (1 + \sqrt{-3})(1 - \sqrt{-3})$. (Note in the former equation $(1 + \sqrt{-3})$ is just the number $1 + \sqrt{-3}$ in parentheses, but in the latter equation it means the ideal generated by $1 + \sqrt{-3}$. Hopefully there will be no confusion about this notation, as the meaning should be clear from context.) The resolution of this nonunique factorization using ideals is the following: the ideals (2), $(1 + \sqrt{-3})$ and $(1 - \sqrt{-3})$ are not irreducible! Indeed, (2) and $(1 + \sqrt{-3})$ have a "common factor" $(2, 1 + \sqrt{-3}) = (2) + (1 + \sqrt{-3})$ = n 2m + (1 + p −3)n : m, n ∈ R o . In fact, since $2\sqrt{-3} = 2(-1) + (1 + \sqrt{-3})\,2$ and $(1 + \sqrt{-3})\sqrt{-3}) = -3+\sqrt{-3} = 2(-2) + (1+\sqrt{-3})\cdot 1$ are both of the form $2m + (1 + \sqrt{-3})n$ for m, n ∈ Z, we have $(2, 1 + \sqrt{-3}) = 2m + (1 + \sqrt{-3})n : m, n \in Z$. (You can just check this set is closed under addition and multiplication by elements in R.) Now this ideal contains both (2) and $(1 + \sqrt{-3})$, so it divides them. It is easy to see 1 does not belong to $(2, 1 + \sqrt{-3})$, hence $(2, 1 + \sqrt{-3}) \neq (1) = R$; in other words , $(2, 1 + \sqrt{-3})$ is a nontrivial divisor of R . Note the non-proper ideal R of R , always divides (contains) every ideal trivially , just like the number 1 divides any integer—in fact R is the principal ideal generated by 1 , so in the correspondence described above , it is the principal ideal corresponding to 1 and its associates , i . e . , the principal ideal corresponding to the units. Thus any proper ideal which divides another ideal may be thought of as a nontrivial divisor .

. . . .

Example : Check that the ideal $(2, 1 + \sqrt{-3})$ in $Z[\sqrt{-3}]$ is not principal. (Use contradiction.)

Hence $(2, 1 + \sqrt{-3})$ corresponds to some "ideal number" in $Z[\sqrt{-3}]$, which should basically be the element $\zeta 3$ that is not in the ring. In fact, if we pass to the ring $Z[\zeta 3]$, we see that the ideal $(2, 1 + \sqrt{-3}) = (\zeta 3) = (1) = Z[\zeta 3]$ is principal. Indeed, all ideals of $Z[\zeta 3]$ are principal, just like for Z, because we have unique factorization. We will go over

this formally later. Actually, this example is of Z[$\sqrt{-3}$] does not illustrate the power of ideals because it is not a Dedekind domain. (A Dedekind domain must be integrally closed, meaning it should contain all the integers in its quotient field.) If it were a Dedekind domain, we would have unique factorization into prime ideals, e.g., there would be prime ideals p, q in Z[$\sqrt{-3}$] such that (2) = pq, (1 + $\sqrt{-3}$) = p 2 and (1 − $\sqrt{-3}$) = q 2 . This would resolve the factorization (4) = (2)(2) = (pq)(pq) = p 2 q 2 = (1 + $\sqrt{-3}$) (1 − $\sqrt{-3}$), however there is only one prime ideal dividing (2), namely (2, 1 + $\sqrt{-3}$) = (2 , 1 − $\sqrt{-3}$). Hence, to really make use of ideals, we need to pass to the integral closure Z [ζ3] of Z [$\sqrt{-3}$] which already has unique factorization, so one does not really gain anything by using ideals. While, this example does not illustrate the full power of ideals, there is some interesting geometry going on. See the pictures in of Stillwell. To see the full power of ideals, we will need to move to another field F where the full ring of integers OF does not have unique factorization.

. . . .

Theorem 8 : Let R be a PID. Then a nonzero ideal I of R is prime if and only if it is maximal.

Proof. We already know that a maximal ideal is necessarily prime. So let P be a non-zero prime ideal of R. Assume that M is another ideal with P ⊂ M. Since R is a PID, we can write P = (p) and M = (m) . Then (p) ⊆ (m) , which means that mr = p for some r ∈ R. Thus either m or r is in P. By assumption, m /∈ P, so that r ∈ P. Then r = sp for some s ∈ R. Substituting, that means msp = p , so that ms = 1 and m is a unit. Thus M = R. So any ideal bigger than P is all of R and P is maximal.

. . . .

Example : . R = Z [(1+$\sqrt{-19}$) / 2] is a PID that is not Euclidean. R is a PID; for proof, see an algebraic number theory course. Here is a sketch that R is not Euclidean. Let a ∈ R be nonzero and not a unit, with |a| minimal. Then look at R/(a). If b ∈ R, b = aq + r with |r| < |a|. Then r is 0

or a unit. So every element of R/(a) is represented by 0 or a unit. The only units of Rare ±1, so R/(a) has ≤ 3 elements. If a ≠ ±1, 0, then R/(a) has ≥ 4 elements (actually $|a|^2$).

. . . . . .

Theorem 9 : . Let R be a PID, and let d ∈ R \ { 0 } . Then the following are equivalent: (1) R.d = <d> is a prime ideal. (2) d is irreducible in R. (3) R.d is a maximal ideal in R.

Proof. 1) implies 2): If d = a.b then as d ∈ R.d is prime we must have a ∈ R.d or b ∈ R.d. By symmetry we may assume a ∈ R.d (and hence, since R.d is a proper ideal and R.a ⊆ R.d we see that a is not a unit). But then there is some r ∈ R with a = r . d , and so d = a . b = (r . b) . d and hence (1 – r . b) . d = 0 and so since R is an integral domain and d , 0 we must have r.b = 1, that is b ∈ R × .

2) implies 3): Suppose that d is irreducible, and that R.d ⊆ I ✁ R. Since R is a PID, we must have I = R.a for some a ∈ R, and R.d ⊆ R.a shows that d = a.b for some b ∈ R. But then as d is irreducible we must have one of a orb a unit. But if a is a unit, then R.a = R, while if b is a unit d and a are associates and so generate the same ideal, that is R.d = I. It follows R.d is a maximal ideal as claimed.

3) implies 1): We have already seen that in any ring a maximal ideal must be prime.

. . . . . .

Remark : Note that the implication “1) implies 2)” holds in any integral domain, while “3) implies 1)” holds in any commutative ring. In a general ring d ∈ R irreducible is equivalent to the ideal R.d being maximal amongst principal ideals in R.

It is also worth pointing out that the Lemma reduces the problem classifying prime and maximal ideals in a PID R to the problem of finding irreducible elements in R. When R is say C[t], this is easy: by the

fundamental theorem of algebra a monic polynomial $p \in C[t]$ is irreducible if and only if $p = t - \lambda$ for some $\lambda \in C$. On the other hand if R = Q[t] then it is in general very difficult to decide if a polynomial $p \in Q[t]$ is irreducible. For the ring R = Z[i] it is possible to give a fairly complete description of the irreducibles .

. . . .

Noetherian ring.

Definition : A commutative ring where every ideal is finitely generated is called a Noetherian ring.

These rings are named after Emmy Noether, who was one of the pioneers of abstract algebra in the first half of the 20th century . Their importance, as a class of rings, stems from the stability of the Noetherian property under many basic constructions. If R is a Noetherian ring, so is every quotient ring R/I (which may not be an integral domain even if R is), every polynomial ring R[X] (and thus $R[X_1,...,X_n]$ by induction on n, viewing this as $R[X_1,...,X_{n-1}][X_n]$), and every formal power series ring R[[X]] (and thus $R[[X_1,...,X_n]]$). The PID property behaves quite badly, e.g., if R is a PID other than a field then R[X] is not a PID. For instance, R[X,Y] = R[Y][X] is never a PID for an integral domain R. But if R is Noetherian then R[X,Y] is Noetherian. Briefly, the property "ideals are finitely generated" of Noetherian rings is more robust than the property "ideals are singly generated" of PIDs.

Using this terminology, Corollary 4.6 says in every Noetherian integral domain each element other than 0 or a unit has an irreducible factorization. It is worth comparing the proof of this general result to the special proof we gave in the case of Euclidean domains, where the proof of irreducible factorizations is tied up with features of the Euclidean function on the ring.

In the context of unique factorization domains, it is the uniqueness of the factorization that lies deeper than the existence. We are not discussing uniqueness here, which most definitely does not hold in most Noetherian integral domains. That is, the existence of irreducible factorizations (for all nonzero nonunits) is not a very strong constraint, to the extent that

most integral domains you meet in day-to-day practice in mathematics are Noetherian so their elements automatically have some factorization into irreducible elements. But there usually is not going to be a unique factorization into irreducible elements.

. . . . . .

Theorem 10 : Every principal ideal domain is Noetherian.

Proof. Let R be a principal ideal domain, and let $I0 \subseteq I1 \subseteq \ldots$ be a chain of ideals in R. The union $\cup$ In is also an ideal in R, hence is principal, hence $\cup$ In = (i) for some $i \in I$. So $i \in In$ for some n. So In = In+1 = In+2 = $\cdots$ = I. So the chain of ideals stabilizes.

. . . . . .

Check Your Progress-1

1. If R is a commutative ring with unit element then

   a. every maximal ideal is a prime ideal

   b. every prime ideal is maximal ideal

   c. every ideal is a prime ideal

   d. every ideal is a maximal ideal

2. If F is a field then its only ideal are A: F itself; B: (0) .

   a. A and B are true

   b. A is true, b is false

   c. A is false, B is true

   d. Both false

13.4 LET US SUM UP

In this unit, we have introduced the concept of principal ideal domain. We have discussed various properties of principal ideal domain.

13.5 KEYWORDS

9. ***Principal ideal:*** An ideal S of a ring R is said to be a principal ideal if there exists an element a in S such that any ideal T of R containing a also contains S i.e., S = (a).
10. ***Principal Ideal ring:*** A commutative ring R without zero divisors and with unity element is a principal ideal ring if every ideal Sin R is a principal ideal i.e, if every ideal Sin R is of the form S = (a) for some a ∈ S.

13.6 QUESTIONS FOR REVIEW

1. Show that Z[x] is not a PID.
2. Show that Z is a PID
3. Show that the ring of Gaussian integers is a PID.

13.7 SUGGESTED READINGS AND REFERENCES

26. Thomas W Judson (2013). *Abstract Algebra: Theory and Applications*. Orthogonal Publishing.
27. Paul B. Garrett (2007). *Abstract Algebra*. Chapman and Hall/CRC.
28. Vijay K Khanna (2017).*A Course in Abstract Algebra Fifth Edition*. Vikas Publishing House
29. LALJI PRASAD (2016). *Modern Abstract Algebra*. Paramount Publication
30. Stephen Lovett (2016). *Abstract Algebra: Structures and Applications*. Chapman and Hall/CRC

13.8 ANSWERS TO CHECK YOUR PROGRESS

19. (a) (answer for Check your Progress-1 Q.1)
20. (a) (answer for Check your Progress-1 Q.2)

UNIT – 14: RING OF POLYNOMIALS

STRUCTURE

14.0 OBJECTIVES

After studying this unit, you should be able to:

- Explain the concept of rings of polynomials
- Describe different type of rings pf polynomial

14.1 INTRODUCTION

In this unit, we will discuss rings of polynomials. We will discuss various properties of rings of polynomials and study different types of rings of polynomials.

14.2 RINGS OF POLYNOMIALS

Polynomial Rings

Definition: Let R be an arbitrary ring and let x, called an indeterminate, be any symbol not an element of R. By a polynomial in x over R is meant an expression of the form

$f(x) = a_0 x^0 + a_1 x^1 + a_2 x^2 + \ldots$, where a's are elements of R and only a finite number of them are not equal to 0, the zero element of R.

. . . .

. . . .

Set of all polynomials over a ring.

Definition: Let R be an arbitrary ring and x an indeterminate. The set of all polynomials f(x),

$f(x) = \sum a_n x^n = a_0 x^0 + a_1 x^1 + a_2 x^2 + \ldots$

where the a's are elements of the ring R and only a finite number of them are not equal to zero, is called R [x] .

We shall make a ring out of R [x] . Then R [x] will be called the ring of all polynomials over the ring R .

. . . .

. . . .

Zero Polynomial

Definition: The polynomial $f(x) = a_0 x^0 + a_1 x^1 + a_2 x^2 +$ ... in which all the coefficients are equal to 0 is called the zero polynomial over the ring R .

. . . .

. . . .

Degree of a Polynomial

Definition: Let $f(x) = a_0 x^0 + a_1 x^1 + a_2 x^2 +$ ... be a polynomial over an arbitrary ring R. We say that n is the degree of the polynomial f (x) if and only if $a_n \neq 0$ and $a_m=0$ for all m>n .

We shall write deg f (x) to denote the degree of f (x) . Thus the degree of f (x) is the largest non-negative integer i for which the ith coefficient of f (x) is not 0 . If in the polynomial (x) , a

(i . e . , the coefficient of x) is not 0 and all the other coefficients are 0, then according to our definition, the degree of f (x) will be zero.. Also according to our definition, if there is no non-zero coefficient in f (x) , then its degree will remain undefined. Thus we do not define the degree of the zero polynomial. Also it is obvious that every non-zero polynomial will possess a unique degree.

Note. If $f(x) = a_0 x^0 + a_1 x^1 + a_2 x^2 +$ ... is a polynomial of degree n i.e., if $a_n \neq 0$ and $a_m=0$ for all m>n, then it is convenient to write $f(x) = a_0 x^0 + a_1 x^1 + a_2 x^2 + \ldots + a_n x^n$. It will remain

understood that all the terms in f (x) which follow the term $a_n x^n$ have zero coefficients. Also we shall call $a_n x^n$ as the leading term and an as the leading coefficient of the polynomial. The term $a_0 x^0$ is called the constant term. For example f (x) – 2 x0 + 3x - 4x + 5 x3 – 8 x4 is a polynomial of degree 4 over the ring of integers. Here -8 is the coefficient and 2 is the zero th coefficient. The coefficients of all terms which contain powers of x greater than 4 will be regarded as zero. Similarly g (x) = 3 x is a polynomial of degree zero over the ring of integers. In this polynomial the coefficients of x, x, x,...are all equal to zero. The zero polynomial over an arbitrary ring R will be represented by 0.

. . . .
. . . .

Set of constant polynomials over a ring.

Definition: Let R be an arbitrary ring and R [x] the set of all polynomials over R. Let R' denote the set of all polynomials over R whose coefficients are all zero except for the constant term, which may be either zero or non-zero. That is R ' = { $a x^0 : a \in$ R }

Then R' will be called as the set of constant polynomial in R [x] .

Definition of an irreducible polynomial over a field: Let F be a field and f (x) be a non-zero and non-unit polynomial in F [x] i . e . , f (x) be a polynomial of positive degree. Then f (x) is said to be irreducible over F (or prime) if it has no proper divisors in F [x] ; f (x) is reducible over F if it has a proper divisor in F [x] .

. . . .
. . . .

14.3 DIFFERENT TYPE OF POLYNOMIAL RINGS

Degree of the sum and the product of two polynomials

Theorem 1: Let f (x) and g (x) be two non-zero polynomials over an arbitrary ring R Then

(i) deg [f (x) + g (x)] < Max [deg f (x) , deg g (x)] ; if f (x) + g (x) ≠ 0 .

(ii) deg [f (x) g (x)] < deg f (x) + deg g (x) if f (x) g (x) ≠ 0 .

. . . . . .

. . . . . .

Ring of Polynomials

Theorem 2: The set of all polynomials over an arbitrary ring R is a ring with respect to addition and multiplication of polynomials .

Proof : Let f (x) , g (x) ∈ R [x] . Then f (x) + g (x) and f (x) g (x) are also polynomials over R. Therefore R [x] is closed with respect to addition and multiplication of polynomials.

Now let $f(x) = a_0x^0 + a_1x^1 + a_2x^2 + \ldots$, $g(x) = b_0x^0 + b_1x^1 + b_2x^2 + \ldots$,

$h(x) = c_0x^0 + c_1x^1 + c_2x^2 +$ ... be any arbitrary elements of R [x] .

Commutativity of addition: We have

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

Associativity of addition: We have

[f (x) + g (x)] + h (x) = f (x) + [g (x) + h (x)] .

Existence of additive identity: Let 0 (x) be the zero polynomial over R.

Then f (x) + 0 (x) = f (x)

Therefore , the zero polynomial 0 (x) is the additive identity.

Existence of additive inverse: Let – f (x) be the polynomial over R

Then – f (x) + f (x) = 0 (x) = the additive identity.

Therefore, each member of R [x] possesses additive inverse.

Associativity of Multiplication: We have

[f (x) g (x)] h (x) = f (x) [g(x) h (x)] since corresponding coefficients in these two polynomials are equal.

Distributivity of multiplication with respect to addition: We have

f (x) [g (x) + h (x)] = f (x) g (x) + f(x) h (x) .

Similarly we can prove the right distributive law.

Hence R [x] is a ring. This is called the ring of all polynomials over R.

. . . . . .

. . . . . .

Polynomials over an integral domain

Theorem 3: If is an integral domain, then the polynomial ring D [x] is also an integral domain.

Proof: Let D be a commutative ring without zero divisors and with unity element 1

D [x] is also a ring.

To prove that D [x] is an integral domain, we should prove that

(i) D [x] is commutative, (ii) is without zero divisors and (iii) possesses the unity element.

Now, D [x] is commutative

As f (x) g (x) = g (x) f (x).

If 1 is the unity element of D, then the constant polynomial is the unity element of D [x]. We have f (x) . 1 = f (x)

Therefore, the polynomial 1 is the unity element of D [x)

D [x] is without zero divisors.

Let f (x) , g (x) be two non-zero elements of D [x] .

Then f (x) g (x) cannot be a zero polynomial i e., the zero element of D [x] . The reason is that at least one coefficient of f (x) g (x) is not equal to 0

Therefore, D is without zero divisors

Hence D [x] is an integral domain.

. . . .

Polynomials over a field

Theorem 4: If F is a field, then the set F [x] of all polynomials over F is an integral domain.

Proof: Every field is an integral domain. So give the same

proof as we have given in Theorem 3 and then in Theorem 4.

We shall call the set F [x] as the polynomial domain over the field F

. . . .

Theorem 5: The polynomial domain F[x] over a field F is not a field.

Proof: In order to show that F[x] is not a field, we should show that there exists a non-zero element of F[x] which has no multiplicative inverse. Let f(x) be any element of F[x] such that
deg f(x) is greater than zero. The inverse of f(x) cannot be the zero polynomial because the product of f(x) and the zero polynomial will be equal to the zero polynomial and not equal to the unity element of F[x]
Suppose now g(x) is any non-zero polynomial. Then F being a field, we have
deg [f (x) g (x)) = deg. f (x) + deg g (x) > 0 because deg f (x) > 0 and deg g (x) > 0
The degree of the unity element of F [x] is 0. Hence f (x) g (x) cannot be equal to the unity element of F [x] . Thus f (x) does not possess multiplicative inverse.
F [x] is not a field.

. . . . . .

Theorem 6 : Let K be a field and let f (x) be a polynomial in K [x] . Then we can write f (x) = g(x) h (x) where g (x) is a linear polynomial if and only if f (x) has a root in K.
Proof. First note that a linear polynomial always has a root in K. Indeed any linear polynomial is of the form ax + b, where a = 0. Then it is easy to see that α = −a b is a root of ax + b. On the other hand, the kernel of the evaluation map is an ideal, so that if g (x) has a root α, then in fact so does f (x) = g (x) h (x) . Thus if we can write f (x) = g (x) h (x) , where g (x) is linear, then it follows that f(x) must have a root. Now suppose that f(x) has a root at α. Consider the linear polynomial g(x) = x − α. Then the kernel of evα is equal to (x − α). As f is in the kernel, f(x) = g (x) h (x) , for some h (x) ∈ R [x]

. . . . . .

Theorem 7 : Let K be a field and let f (x) be a polynomial of degree two or three. Then f (x) is irreducible if and only if it has no roots in K.

Proof. If f (x) has a root in K, then f (x) = g (x) h (x) , where g (x) has degree one, by (theorem 6). As the degree of f is at least two, it

follows that h (x) has degree at least one. Thus f (x) is not irreducible. Now suppose that f(x) is not irreducible. Then f (x) = g (x) h (x) , where neither g nor h is a unit. Thus both g and h have degree at least one. As the sum of the degrees of g and h is at most three, the degree of f, it follows that one of g and h has degree one.

. . . .

Definition : Let p be a prime. F_p denotes the unique field with p elements.

Of course, F_p is isomorphic to Z_p. However, as we will see later, it is useful to replace Z by F.

Example : . First consider the polynomial x2 + 1. Over the real numbers this is irreducible. Indeed, if we replace x by any real number a, then a2 is non-negative and so a2 + 1 cannot equal zero.

On the other hand ±i is a root of x2+1, as i 2+1 = 0. Thus x2+1 is reducible over the complex numbers. Indeed x2+1 = (x + i) (x – i) . Thus an irreducible polynomial might well become reducible over a larger field.

Consider the polynomial x2 + x + 1. We consider this over various fields. As observed in (theorem 7) this is reducible iff it has a root in the given field.

Suppose we work over the field F5. We need to check if the five elements of F_5 are roots or not. We have $1^2 + 1 + 1 = 3$, $2^2 + 2 + 1 = 2$, $3^2 + 3 + 13$, $4^2 + 4 = 1$ Thus x2 + x + 1 is irreducible over F5. Now consider what happens over the field with three elements F3. Then 1 is a root of this polynomial. As neither 0 nor 2 are roots, we must have x2 + x + 1 = (x – 1) ^{2} = (x + 2)2 , which is easy to check.

Now let us determine all irreducible polynomials of degree at most four over F_2. Any linear polynomial is irreducible. There are two such x and x + 1. A general quadratic has the form f(x) = x2 + ax + b. b = 0, else x divides f(x). Thus b = 1. If a = 0, then f(x) = x2 + 1, which has 1 as a zero. Thus f(x) = x2 + x + 1 is the only irreducible quadratic.

Now suppose that we have an irreducible cubic f(x) = x3 + a x + b x + 1 . This is irreducible iff f(1) $\neq$ 0, which is the same as to say that there are an odd number of terms. Thus the irreducible cubics are f(x) = x3 + x2 + 1 and x3 + x + 1.

Finally suppose that f(x) is a quartic polynomial. The general irreducible is of the form x4 + ax3 + bx2 + cx + 1. f(1) = 0 is the same as to say that either two of a, b and c is equal to zero or they are all equal to one. Suppose that f(x) = g(x)h(x).

If f(x) does not have a root, then both g and h must have degree two. If either g or h were reducible, then again f would have a linear factor, and therefore a root. Thus the only possibilty is that both g and h are the unique irreducible quadratic polynomials. In this case f(x) = (x2 + x + 1)2 = x4 + x2 + 1.

Thus x4 + x3 + x2 + x + 1, x4 + x3 + 1, and x4 + x + 1 are the three irreducible quartics.

Obviously it would be nice to have some more general methods of proving that a given polynomial is irreducible. The first is rather beautiful and due to Gauss. The basic idea is a follows. Suppose we are given a polynomial with integer coefficients. Then it is natural to also consider this polynomial over the rationals. Note that it is much easier to prove that this polynomial is irreducible over the integers than it is to prove that it is irreducible over the rationals. For example it is clear that x2 − 2 is irreducible over √ the integers. In fact it is irreducible over the rationals as well, that is, 2 is not a rational number.

. . . .

Theorem 8 : A nonzero nonconstant polynomial f (x) ∈ F [x] is irreducible if and only if f (x) = g (x) h (x) implies that either g or h is a constant.

Proof. Suppose f (x) is irreducible and f (x) = g (x) h (x) . Then one of g (x) , h (x) is a unit. But we showed earlier that the units in F [x] are the constant polynomials. Suppose that f (x) is a nonzero nonconstant polynomial, and f (x) = g (x) h (x) implies that either g or h is a constant. Since f is nonconstant, it's not a unit. Note that if f (x)

= g (x) = h (x) , then g, h ≠ 0, since f ≠ . Therefore, the condition that f(x) = g (x) h (x) implies that either g or h is a constant means that f (x) = g (x) h (x) implies that either g (x) or h (x) is a unit — again, since the nonzero constant polynomials are the units in F [x]. This is what it means for f to be irreducible.

. . . .

Example. Show that $x^2 + 1$ is irreducible in R [x] but not in C [x] .

$x^2 + 1$ has no real roots, so by the Root Theorem it has no linear factors. Hence, it's irreducibile in R [x] . However, $x^2 + 1 = (x + i)(x - i)$ in C [x]

. . . .

Corollary : Let F be a field. A polynomial of degree 2 or 3 in F[x] is irreducible if and only if it has no roots in F.

Proof. Suppose f ∈ F [x] has degree 2 or 3. If f is not irreducible, then f (x) = g (x) h (x) , where neither g nor h is constant. Now deg g ≥ 1 and deg h ≥ 1 , and deg g + deg h = deg f = 2 or 3. This is only possible if at least one of g or h has degree 1. This means that at least one of g or h is a linear factor ax + b, and must therefore have a root in F. Since f (x) = g (x) h (x) , it follows that f has a root in F as well. Conversely, if f has a root c in F, then x − c is a factor of f by the Root Theorem. Since f has degree 2 or 3, x − c is a proper factor, and f is not irreducible.

. . . .

Remark. The result is false for polynomials of degree 4 or higher. For example, $(x^2 + 1)^2$ has no roots in R, but it is not irreducible over R . .

. . . .

Theorem 9 : . Let R be an integral domain. Then the units in R [x] are precisely the units in R.

Proof. One direction is clear. A unit in R is a unit in R [x] . Now suppose that f (x) is a unit in R[x] . Given a polynomial g, denote by d (g) the degree of g (x). Now f (x) g (x) = 1. In particular neither f (x) nor g (x) is zero. Thus 0 = d (1) = d (f g) = d (f) + d (g) .

Thus both of f and g must have degree zero. It follows that f (x) = f0 and that f0 is a unit in R[x].

. . . .

Definition : 1 Let F be a filed and F[X] be the polynomial ring. Let f1, . . . , fr ∈ F[X] be polynomials, not all zero. An element d ∈ F[X] is said to be a Greatest common divisor (gcd) if

1. d | fi ∀ i = 1, . . . , r,

2. If there is an elment d’ ∈ F [X] such that d’ |fi ∀ i = 1, . . . , r then d’ |d.

. . . .

Theorem 10 : Let F be a filed and F[X] be the polynomial ring. Let f1, . . . , fr ∈ F [X] be polynomials, not all zero. Suppose d1 and d2 are two GCDs of f1, . . . , fr. Then d1 = ud2 for some unit u ∈ F. Further, if we assume that both d1, d2 are monic then d1 = d2. That means, monic GCD of f1, . . . , fr ∈ F[X] is UNIQUE.

Proof : By property (2) of the definition, d1 = ud2 and d2 = vd1 for some u, v ∈ F[X]. Hence d1 = uvd1. Since d1 6= 0, we have uv = 1i, so u is an unit. Now, if d1, d2 are monic then comparing the coefficients of the top degree terms in the equation d1 = ud2 it follows that u = 1 and hence d1 = d2. This completes the proof.

Remarks. (1) Note that Z has only two unit, 1 and -1. When you computed GCD of integers, definition assumes that the GCD is positive. That is why GCD of integers is unique

. . . . . .

Theorem 11 : Let F be a filed and F [X] be the polynomial ring . Let I be a non zero ideal of F[X] . Then I = F [X] d for some d ∈ F [X] . In fact, for any non-zero d ∈ I with deg (d) least , we have I = F [X] d .

Proof. Let k = min { deg (f) : f ∈ I, f ≠ 0}. Pick d ∈ I such that d ≠ 0 and deg (d) = k. Now claim I = F [X] d . Clearly, I ⊇ F [X] d . Now , let f ∈ I . By division f = q d + r with r = 0 or deg (r) < k . Note r = f – q d ∈ I. We prove r = 0. If r ≠ 0, then deg (r) < k would contradicts the minimality of k. So, r = 0 and f = q d ∈ F [X] d . This completes the proof.

. . . . . .

Definition : Let F[X] be a the polynomial ring over a field F.

1. An element f ∈ F[X] is said to be a an reducible over F if f = gh for some non-unit g, h ∈ F[X] (equivalently, deg(g) > 0 and deg(h) > 0.)

2. f ∈ F[X] is said to be irredubible over F if it is not reducible.

3. A non-scalar irreducible element f ∈ F[X] over F is called a prime in F[X].

. . . . . .

Theorem 12 : Let R = F [X] be the polynomial ring over a field F. Let p ∈ R be a prime element and f, g ∈ R. Then p | f g ⇒ either p | f or p | g

Proof. Assume p | f g and p does not divide f. We will prove that p | g. We have f g = p w for some w ∈ R. Also R f + R p = R. Therefore, 1 = x f + y p for some x, y ∈ R. Hence g = xfg + yp = xwp + yp. This completes the proof.

Corollary : Let R = F[X] be the polynomial ring over a field F. Let p ∈ R be a prime element and f1, f2, . . . , fr ∈ R. Then p | f1f2 · · · fr =⇒ p | fi for some i = 1, . . . , r.

Proof. Use induction and the above thoerem.

. . . .

Theorem 13 : (Unique factorization in polynomial rings). Let f be a non constant polynomial in F[x], i.e. f is neither 0 nor a unit. Then there exist irreducible polynomials p1, . . . , pk, not necessarily distinct, such that f = p1 · · · pk. In other words, f can be factored into a product of irreducible polynomials (where, in case f is itself irreducible, we let k = 1 and view f as a one element "product"). Moreover, the factorization is unique up to multiplying by units, in the sense that, if q1, . . . , ql are irreducible polynomials such that f = p1 · · · pk = q1 · · · ql , then k =l , and, possibly after reordering the qi, for every i, 1 ≤ i ≤ k, there exists a ci ∈ F* such that qi = ci pi.

Proof : The theorem contains both an existence and a uniqueness statement. To prove existence, we argue by complete induction on the degree deg f of f. If deg f = 1, then f is irreducible and we can just take k = 1 and p1 = f. Now suppose that existence has been shown for all polynomials of degree less than n, where n > 1, and let f be a polynomial of degree n. If f is irreducible, then as in the case n = 1 we take k = 1 and p1 = f. Otherwise f = gh, where both g and h are nonconstant polynomials of degrees less than n. By the inductive hypothesis, both g and h factor into products of irreducible polynomials. Hence the same is the true of the product gh = f. Thus every polynomial of degree n can be factored into a product of irreducible polynomials, completing the inductive step and hence the proof of existence. To prove the uniqueness part, suppose that f = p1 · · · pk = q1 · · · ql where the pi and qj are irreducible. The proof is by induction on the number k of factors in the first product. If k = 1, then f = p1 and p1 divides the product q1 · · · ql . By Corollary , there exists an i such that p1 qi . After relabeling the qi , we can assume that i = 1. Since q1 is irreducible and p1 is not a unit, there exists a c ∈ F* such that q1 = cp1. We claim that l = 1 and hence that q1 = f = p1. To see this, suppose that l ≥ 2. Then p1 = cp1q2 · · · ql . Since p1 ≠ 0, we can cancel it to obtain 1 = cq2 · · · ql . Thus qi is a unit for i ≥ 2, contradicting the fact that qi is irreducible. This proves

uniqueness when $k = 1$. For the inductive step, suppose that uniqueness has been proved for all polynomials which are a product of $k - 1$ irreducible polynomials, and let $f = p_1 \cdots p_k = q_1 \cdots q_l$ where the p_i and q_j are irreducible as above. before, p_1 $q_1 \cdots q_l$ hence, there exists an i such that p_1 q_i . After relabeling the q_i , we can assume that $i = 1$ and that there exists a $c_1 \in F*$ such that $q_1 = c_1p_1$. Thus $p_1 \cdots p_k = c_1p_1q_2 \cdots q_l$, and so canceling we obtain $p_2 \cdots p_k = (c_1q_2) \cdot \cdots \cdot q_l$. Then, since the product on the left hand side involves $k-1$ factors, by induction $k-1$ = `-1 and hence $k = l$. Moreover there exist $c_i \in F^*$ such that $q_i = c_i p_i$ if $i > 2$, and $c_1q_2 = c_2p_2$. After renaming c -1 1 c_2 by c_2, we see that $q_i = c_i p_i$ for all $i \geq 1$. This completes the inductive step and hence the proof of uniqueness.

. . . .

Check Your Progress-1

1. If polynomials f(x) and g(x) are primitive polynomials then.

    a. f.g is primitive

    b. f+g is primitive

    c. f-g is primitive

    d. f/g is primitive

2. If R is a integral domain then R[x] is.

    a. integral domain

    b. not integral domain

    c. field

    d. commutative domain ring

14.4 LET US SUM UP

In this unit, we have discussed rings of polynomials. We have discussed various properties of rings of polynomials and studied different types of rings of polynomials.

.

14.5 KEYWORDS

1. ***Polynomial ring:*** Let R be an arbitrary ring and let x, called an indeterminate, be any symbol not an element of R. By a polynomial in x over R is meant an expression of the form $f(x) = a_0x^0 + a_1x^1 + a_2x^2 + \cdots$, where a's are elements of R and only a finite number of them are not equal to 0, the zero element of R.

14.6 QUESTIONS FOR REVIEW

1. Show that the polynomial ring I[x] over the ring of integers is not a principal ideal ring.
2. Show that if a ring R has no zero divisors, then the ring R[x] has also no zero divisors.
3. The polynomial $x^2 + 1$ is irreducible in Z[x].

14.7 SUGGESTED READINGS AND REFERENCES

31. Thomas W Judson (2013). *Abstract Algebra: Theory and Applications*. Orthogonal Publishing.
32. Paul B. Garrett (2007). *Abstract Algebra*. Chapman and Hall/CRC.
33. Vijay K Khanna (2017).*A Course in Abstract Algebra Fifth Edition*. Vikas Publishing House
34. LALJI PRASAD (2016). *Modern Abstract Algebra*. Paramount Publication
35. Stephen Lovett (2016). *Abstract Algebra: Structures and Applications*. Chapman and Hall/CRC

14.8 ANSWERS TO CHECK YOUR PROGRESS

21. (d) (answer for Check your Progress-1 Q.1)
22. (a) (answer for Check your Progress-1 Q.2)