BHARATHIDASAN UNIVERSITY

Tiruchirappalli- 620024

Tamil Nadu, India

Programme	:	M. Sc. Mathematics
Course Title	:	ALGEBRA - I
Course Code	:	24S2M05CC

UNIT - V

RING HOMOMORPHISMS AND POLYNOMIAL RINGS

Dr. C. Durairajan

Professor

Department of Mathematics

Ring Homomorphisms

- A ring homomorphism $\phi : R \to S$ is a mapping from rings R to S that preserves the two ring operations, namely
  1. $\phi(a+b) = \phi(a) + \phi(b)$ and
  2. $\phi(ab) = \phi(a)\phi(b)$

  for all $a, b \in R$.

Example

1. For any rings R and $R^{‘}$, there is always at least one homomorphism: $\phi : R \longrightarrow R^{‘}$ defined by $\phi(r) = 0$ for all $r \in R$, where 0 is the additve identity of $R^{‘}$. We call it the trivial homomorphism or zero-homomorphism.
2. Let $r \in \mathbb{Z}$ and let $\phi_r : \mathbb{Z} \longrightarrow \mathbb{Z}$ be defined by $\phi_r(n) = rn$ for all $n \in \mathbb{Z}$. Then ϕ is not a ring homomorphism $\phi_r(mn) = rmn$ but $\phi_r(m)\phi_r(n) = rmrn$.

Examples

- The functions $\phi : \mathbb{R}[x] \to \mathbb{R}$ defined by $\phi(f(x)) = f(1)$ and $\phi : \mathbb{C} \to \mathbb{C}$ defined by $\phi(a + bi) = a - bi$ are ring homomorphisms.
- Let R be a ring and let I be an ideal. Then $\phi : R \to \frac{R}{I}$ defined by $\phi(r) = r + I$ for all $r \in R$ is a ring homomorphism.
- Let $\phi : R \longrightarrow R`$ be a ring homomorphism. Then
  1. $\phi(0) = 0$.
  2. $\phi(r^{-1}) = \phi(r)^{-1}$ for all $r \in R$.
  3. If S is a subring of R, then $\phi(S)$ is a subring of $R`$.
  4. $Ker(\phi)$ is an ideal in R.

Isomorphisms

- A ring homomorphism with one-to-one and onto is called an isomorphism.

  Note that in the above ring homomorphism $\phi : \mathbb{C} \to \mathbb{C}$ defined by $\phi(a + bi) = a - bi$ is an isomorphism.

Theorem

Let $\phi : R \longrightarrow R^{‘}$ be a ring isomorphism.

1. ϕ^{-1} is an isomorphism
2. $r \in R$ is a unit(zero-divisor) iff $\phi(r)$ is a unit(zero-divisor),
3. R is commutative if and only if $R^{‘}$ is commutative,
4. R is an integral domain if and only if S is an integral domain and
5. R is a field if and only if S is a field.

- If R is a ring, the ring of polynomials in x with coefficients in R is denoted $R[x]$. It consists of all formal sums

$$\sum_{n=0}^{\infty} a_i x^i.$$

Here $a_i = 0$ for all but finitely many values of i. That is,

$R[x] = \{a_n x^n + \cdots + a_1 x + a_0 \mid a_i \in R, n$ is a nonnegative integer $\}$.

$R[x]$ is called a **polynomial ring over** R.

Continue ...

- Let $\sum_{i=0}^{\infty} a_i x^i, \sum_{i=0}^{\infty} a_i x^i \in R[x]$, then
$$\sum_{i=0}^{\infty} a_i x^i + \sum_{i=0}^{\infty} b_i x^i = \sum_{i=0}^{\infty} (a_i + b_i) x^i$$
and
$$\left(\sum_{i=0}^{\infty} a_i x^i\right)\left(\sum_{i=0}^{\infty} a_i x^i\right) = \sum_{i=0}^{\infty} c_i x^i \text{ where } c_k = \sum_{i+j=k} a_i b_j.$$
- Let $f(x) = a_n x^n + \cdots + a_1 x + a_0$. If $a_n \neq 0$, then **n is called the degree of** $f(x)$ and is denoted by $deg(f(x))$. This is, if n is the largest integer for which an $a_n \neq 0$, we say that $f(x)$ has degree n. If all the coefficients of p(x) are zero, then $p(x)$ **is called the zero polynomial,** and its degree is not defined. Some author defined its degree is 0 because it is a constant polynomial.

Continue ...

- Let R be an integral domain, then $R[x] = \{a_n x^n + \cdots + a_1 x + a_0 \mid a_i \in R, n \text{ is a nonnegative integer } \}$ is an integral domain.
- Let R be a field, then $R[x]$ not a filed. For Example, let us take the set $\mathbb{R}$ of all reals, it is a field but $\mathbb{R}[x]$ is not a field because inverse of x does not exist.
- Let R be a Principal Ideal Domain(PID), then $R[x]$ need not be a PID. For example, $\mathbb{Z}$ is a PID but $\mathbb{Z}[x]$ is not a PID because the ideal generated by $\langle 2, x \rangle$ is not a principal ideal.
- A nonconstant polynomial over a field is said to be an irreducible polynomial if it can not be written as a product of two polynomials of degree greater than 0. For example, $x^2 + 1$ is irreducible over $\mathbb{R}$ but not irreducible over $\mathbb{C}$ because

Continue ...

Let $\mathbb{F}$ be a field, then

1. $deg(f(x)g(x)) = deg(f(x)) + deg(g(x))$ for all $f(x), g(x) \in \mathbb{F}[x]$ are not equal to 0.
2. $deg(f(x)g(x)) \geq deg(f(x))$ for all $f(x), g(x) \in \mathbb{F}[x]$ with $g(x) \neq 0$.
3. **Divison Algorithm**
   For every $f(x), g(x) \in \mathbb{F}$, $g(x) \neq 0$, there exist $q(x), r(x) \in \mathbb{F}[x]$ such that $f(x) = q(x)g(x) + r(x)$ where $r(x) = 0$ or $deg(r(x)) < deg(g(x))$.

30/4/21

D - ID

$a \mid b$ if $\exists\, c \in D \ni b = ac$

a & b associate if $\exists$ unit $u \in D \ni a = ub$ or $b = ua$

$\mathbb{Z}$, ± 1 are units

$2, -2$ associates

$n, -n$ associates

① irreducible elts

non-zero & non-unit (a) = if a cannot be written as a product of two non unit elts

$\mathbb{Z}$, (5) $= ab$

$1, 5$ 1 or 5   5 or 1

$6 = 2 \times 3$ not irreducible

unit

a is irr. if $a = bc \Rightarrow$ either b is unit or c is "

An ideal I of a ring R is said to be a principal ideal if $I = \langle a \rangle$ for some $a \in R$ i.e. I is generated by a single elt.

A ring R is said to be a principal ideal ring if every ideal is a principal ideal.

Eg: $\mathbb{Z}$ is a principal ideal ring

Let I be an ideal of $\mathbb{Z}$

① If $I = \{0\} = \langle 0 \rangle$, $\therefore$ I is principal ideal

② If $I \neq \{0\}$, then choose $n \in I$ such that n is the least +ve integer in I

Claim: $I = \langle n \rangle$

Let $m \in I$.

By division algorithm for m & $n \in \mathbb{Z}$, there exist $q, r \in \mathbb{Z}$ $\ni$ $m = qn + r$ where $r = 0$ or $0 < r < n$

Since $n \in I$ $\Rightarrow qn \in I$

$\Rightarrow m - qn \in I$ since $m \in I$

i.e., $r \in I$

Since $0 \leq r < n$ & n is the least +ve integer in I

$\Rightarrow r = 0$

$\therefore$ $m - qn = 0$ i.e., $m = qn$

$\therefore$ $m \in I = \langle n \rangle$

$\therefore$ Every ideal in $\mathbb{Z}$ is a principal ideal

$\therefore$ $\mathbb{Z}$ is a principal ideal ring

—— x ——

Theorem (Division Algorithm) Let $\mathbb{F}$ be a field, Let $f(x), g(x) \in \mathbb{F}[x]$ with $g(x) \neq 0$, then there exist $q(x), r(x) \in \mathbb{F}[x]$ such that $f(x) = q(x)g(x) + r(x)$ where $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

Proof: ① If $\deg f(x) < \deg g(x)$

$\Rightarrow$ Choose $q(x) = 0$, $r(x) = f(x)$

$\Rightarrow f(x) = 0g(x) + r(x)$

where $r(x) = 0$ or $\deg r(x) = \deg f(x) < \deg g(x)$

i.e., $\deg r(x) < \deg g(x)$

② If $\deg f(x) \geq \deg g(x)$, then we prove by induction on $\deg f(x) = n$.

If $\deg f(x) = 1$, then $f(x) = ax + b$, $a \neq 0$, $a, b \in \mathbb{F}$

$$f(x) = 1(ax+b) + 0$$

$r(x) = 0$ or $\deg r(x) < \deg(ax+b) = 1$

Assume that this is true for $\deg f(x) \leq n-1$.

We have to prove for n.

Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, $a_n \neq 0$ —— (I)

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

By case (2)

$\Rightarrow n \geq m$

$$x^{n-m} g(x) = b_0 x^{n-m} + b_1 x^{n-m+1} + \cdots + b_m x^n, \; b_m \neq 0$$

$$\Rightarrow \frac{a_n}{b_m}\left(x^{n-m} g(x)\right) = \frac{a_n b_0}{b_m} x^{n-m} + \frac{a_n b_1}{b_m} x^{n-m+1} + \cdots + \frac{a_n b_m}{b_m} x^n \quad \text{(II)}$$

① − ② ⇒ $f(x) - \frac{a_n}{b_m} x^{n-m} g(x)$ has deg $\le n-1$

i.e. $f(x) - \frac{a_n}{b_m} x^{n-m} g(x)$ is a polyl in $\mathbb{F}[x]$ of deg $\le n-1$

By induction hypothesis, $f(x) - \frac{a_n}{b_m} x^{n-m} g(x)$, $g(x) \in \mathbb{F}[x]$

⇒ $\exists\, q_1(x), r(x) \in \mathbb{F}[x]$ such that

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

where $r(x) = 0$ or $\deg r(x) < \deg g(x)$

$$\Rightarrow f(x) = \left(\frac{a_n}{b_m} x^{n-m} + q_1(x)\right) g(x) + r(x)$$

Clearly $q(x) = \frac{a_n}{b_m} x^{n-m} + q_1(x) \in \mathbb{F}[x]$

∴ $f(x) = q(x) g(x) + r(x)$ where $r(x) = 0$ or $\deg r(x) < \deg g(x)$

Thus, we proved

$\mathbb{F}[x]$

Ex. Prove that $\mathbb{F}[x]$ is a principal ideal domain

Hint

↓ $\mathbb{Z}$ (PIR)

① I $\qquad I = \{0\} = \langle 0 \rangle$

② I

n − least +ve integer $\qquad I \neq \{0\}$

$f(x)$ − least deg polyl ⇒ ∃ a least deg poly $f(x) \ne 0$

$I = \langle n \rangle = \langle f(x) \rangle$

let $g(x) \in I$

$\Rightarrow g(x) = f(x)\, h(x)$

$g(x), f(x) \in F[x]$ $\quad \exists\, q(x), r(x) \in F[x]$

$g(x) = f(x)\, q(x) + r(x)$

$r(x) \in I$

$= 0$

$\times$

Continue ...

- Every ideal in it is a Principal ideal.
- In fact, the ideal is generated by the least degree polynomial in it. That is, let F be a field and I a nonzero ideal in $F[x]$ with $g(x) \in F[x]$. Then $I = \langle g(x) \rangle \Leftrightarrow g(x)$ is a nonzero Polynomial of minimum degree in I.
- Let F be a field and $p(x) \in F[x]$. Then $< p(x) >$ is a maximal ideal in $F[x] \Leftrightarrow p(x)$ is irreducible over F.
- Let F be a field. Then $p(x)$ is irreducible over F iff $\frac{F[x]}{\langle p(x) \rangle}$ is a field.

Continue ...

- $\frac{\mathbb{Z}_3[x]}{\langle x^2+1\rangle}$ is a field because x^2+1 is irreducible over $\mathbb{Z}_3$.
- The content of a nonzero Polynomial $a_nx^n+\cdots+a_1x+a_0, a_i\in\mathbb{Z}$, is the $gcd(a_n, a_{n-1}, \ldots, a_1, a_0)$.
- A primitive polynomial is an element of $\mathbb{Z}[x]$ with content 1.
- A polynomial with leading coefficient 1 is called a monic polynomial.
- Every monic polynomial over $\mathbb{Z}$ is a primitive polynomial. But the converse need not be true because $3x^{15}-4x+8$ is a primitive polynomial over $\mathbb{Z}$ but not a monic polynomial over $\mathbb{Z}$.
- The product of two primitive polynomials is again a primitive polynomial. This is due to Gauss.

Continue ...

- If a polynomial can be written as a product of two polynomials over $\mathbb{Q}$, then it can be written as a product of two polynomials over $\mathbb{Z}$.

  The above two statements are due to Gauss.
- Let $f(x) \in \mathbb{Z}[x]$. If $f(x)$ is irreducible over $\mathbb{Z}$, then it is irreducible over $\mathbb{Z}$.
- Let p be a prime and suppose that $f(x) \in \mathbb{Z}[x]$ with $degf(x) \geq 1$. Let $\bar{f}(x)$ be the polynomial in $\mathbb{Z}_p[x]$ obtained from $f(x)$ by reducing all the coefficients of $f(x)$ modulo p. If $f(x)$ is irreducible over $\mathbb{Z}_p$ and $\deg \bar{f}(x) = \deg f(x)$, then $f(x)$ is irreducible over $\mathbb{Q}$.

Euclidean domain

Eisenstein's Criterion

Let $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. If there is a prime p such that $p \nmid a_n, p|a_{n-1}, p|a_{n-2}, \cdots, p|a_0$ and $p^2 \nmid a_0$, then $f(x)$ is irreducible over $\mathbb{Q}$.

- Using the Eisenstein's Criterion, we can prove
  1. for any prime p, the pth cyclotomic polynomial $x^{p-1} + x^{p-2} + \cdot + x^2 + x^1 + 1$ is irreducible over $\mathbb{Q}$.
  2. If an integer a is a square free integer, then $x^n - a$ is irreducible over $\mathbb{Q}$.
- An integral domain D is called a **Euclidean domain** if there is a function d from $D \setminus \{0\}$ to the nonnegative integers such that
  1. $d(a) \leq d(ab)$ for all nonzero a, b in D and
  2. if $a, b \in D, b \neq 0$, then there exist elements q and r in D such that $a = bq + r$ where $r = 0$ or $d(r) < d(b)$.

UFD

- In our previous slide, the polynomials over a field satisfy all these conditions. Therefore, it is an Euclidean domain.
- Every Euclidean domain is a principal ideal domain.
- Every Euclidean domain is a unique factorization domain.
- Let D be an integral domin. A nonzero and nonunit element a of D is said to be
  1. **irreducible** if whenever $b, c \in D$ with $a = bc$, then b or c is a unit.
  2. **prime** if $a|bc \Rightarrow a|b$ or $a|c$.
- An integral domain D is said to be a **unique factorization domain(UFD)** if every nonzero and nonunit element in D can be written as a product of irreducible elements in a unique way.

Examples

- If D is a unique factorization domain, then D[x] is a unique factorization domain. but integral domain need not be UFD. For example, the ring $\mathbb{Z}[\sqrt{-5}] = \{a + 1b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ is an integral domain but not a unique factorization domain because

$$46 = 2 \times 23 \text{ and } 46 = (1 + 3\sqrt{-5})(1 - 3\sqrt{-5}).$$

- The elements a, b of D are associates if $a = ub$ where u is a unit of D.
- In a PID, irreducible elements are primes and vice versa.
- $ED \subseteq PD \subseteq UFD \subseteq ID$.
- The ring of Gaussian integers, $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ is a ED.

References

- M. Artin, **Algebra**, Prentice Hall of India, New Delhi, 1994.
- David S. Dummit and Richard M. Foote,**Abstract Algebra**, 2nd Edition, Wiley Student Edition, 2008.
- I. N. Herstein, **Topics in Algebra**, John Wiley, 2nd Edition, 1975.
- Joseph Gallian, **Contemporary Abstract Algebra** , 9th Edition
- C. Lanski, **Concepts in Abstract Algebra**, AMS Indian edition, 2010.
- Serge Lang, **Algebra** - Revised third edition, Springer, Verlag - 2002.
- R. Solomon, **Abstract Algebra**, AMS Indian edition, 2010.
- John B. Fraleigh, **A First course in Abstract Algebra**, Narosa Publishing House, 2003.