Lecture 22

Important Examples

Polynomial Rings: Fix a commutative ring R with identity.

- Let x be an indeterminate.
- A formal sum of the form $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ with $n \in \mathbb{N}$ and $a_i \in R$ is called a polynomial in x with coefficients in R. If $a_n \neq 0$, we say the polynomial has degree n.
- $a_n x^n$ is called leading term – a_n is called leading coefficient.
- If $a_n = 1$, the polynomial is called monic.

- Polynomials of the form a_0 are called constant.

$$R[x] := \{ \text{polynomials in } x \text{ with coefficients in } R \}$$

$p(x) + q(x)$ is given by addition componentwise

$p(x)\,q(x)$ is given by the distributive laws and $(ax^i)(bx^j) := abx^{i+j}$ $\quad a,b \in R$ & $i,j \in \mathbb{N}$

In $(a_0 + a_1x + a_2x^2 + \cdots)(b_0 + b_1x + b_2x^2 + \cdots)$ the coefficient of x^k is $\sum_{i=0}^{k} a_i b_{k-i}$.

$0_{R[x]} = 0_R$ and $1_{R[x]} = 1_R$

$R[x]$ is called the ring of polynomials in x with coefficients in R.

! $R[x]$ is a commutative ring with identity and R is a subring of $R[x]$.

Ex: $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$, $\mathbb{F}_p[x]$ p prime, $\mathbb{Z}/n[x]$

Proposition 6: If S is a subring of R, then $S[x]$ is a subring of $R[x]$.

Proof: Exercise.

Proposition 7: Let R be an integral domain. Let $p(x), q(x) \in R[x]$ be nonzero polynomials. Then

(1) $R[x]$ is an integral domain.

(2) $\deg(p(x)q(x)) = \deg p(x) + \deg q(x)$.

(3) $(R[x])^\times = R^\times$.

Proof:

(1) WTS: $R[x]$ has no zero divisors ($p(x) \neq 0$ & $q(x) \neq 0 \Rightarrow p(x)q(x) \neq 0$)

Suppose $p(x)$ and $q(x)$ have leading terms $a_m x^m$ and $b_n x^n$, respectively. Then $p(x)q(x)$ has leading term $a_m b_n x^{m+n}$. Since R is an ID, then $a_m b_n \neq 0$. Thus, $p(x)q(x) \neq 0$.

(2) From (1).

(3) ($\subseteq$) Suppose $p(x)$ is a unit, say $p(x)q(x) = 1$ in $R[x]$. Then, $\deg p(x) + \deg p(x) = 0$. Since $\deg p(x), \deg q(x) \in \mathbb{N}$, then both $p(x)$ and $q(x)$ are constant polynomials. Thus, $p(x)$ is a unit in R.

($\supseteq$) ✓

Matrix Rings: Fix an arbitrary ring and $n \in \mathbb{Z}^+$.

$$M_n(R) := \left\{ (a_{ij}) \text{ an } n \times n \text{ matrix} \;\middle|\; a_{ij} \in R \text{ for } 1 \leq i,j \leq n \right\}$$

$(a_{ij}) + (b_{ij}) := (a_{ij} + b_{ij})$.

$(a_{ij})(b_{ij}) := (c_{ij})$ where $c_{ij} = \sum_{k=0}^{n} a_{ik} b_{kj}$.

$0_{M_n(R)} = (0)$ the zero matrix.

If R has an identity, then $1_{M_n(R)} = I_n$ the identity matrix.

$M_n(R)$ is called the matrix ring of degree n over R.

- An element $(a_{ij}) \in M_n(R)$ is called a scalar matrix if $a_{ii} = a$ for some $a \in R$ and $1 \leq i \leq n$, and $a_{ij} = 0$ for $i \neq j$, $1 \leq i,j \leq n$.

$$(a_{ij}) = \begin{pmatrix} a & & & \\ & a & & \\ & & \ddots & \\ & & & a \\ & & & & a \end{pmatrix} \quad \text{with } a \in R.$$

- If R has an identity, $GL(n,R) := (M_n(R))^\times$ is called the general linear group of degree n over R.

! $n \geq 2$, $M_n(R)$ is a noncommutative ring (regardless of R's commutativity).

$n \geq 2$, $M_n(R)$ has zero divisors for any ring R.

The set $S := \{$ scalar matrices in $M_n(R)\}$ is a subring of $M_n(R)$.

Prove these!

Ex: $M_n(2\mathbb{Z})$, $M_n(\mathbb{Q})$, $M_n(\mathbb{F}_p)$ p prime, $M_n(\mathbb{H})$, $M_n(\mathbb{Z}/m)$, $M_n\left(M_m(\mathbb{R})\right)$.

Proposition 8: If S is a subring of R, then $M_n(S)$ is a subring of $M_n(R)$.

Proof: Exercise.

Ring Homomorphisms and Isomorphisms

Def: Let R and S be rings. A well-defined map $\varphi: R \longrightarrow S$ is called a ring homomorphism if

(i) $\varphi(a+b) = \varphi(a) + \varphi(b)$ for all $a, b \in R$.

(ii) $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in R$.

Def: Let $\varphi : R \longrightarrow S$ be a ring homomorphism.

(1) φ is called a monomorphism if φ is injective. $\hookrightarrow$

(2) φ is called an epimorphism if φ is surjective. $\twoheadrightarrow$

(3) φ is called an isomorphism if φ is bijective. $\xrightarrow{\cong}$

(4) The kernel of φ is $\operatorname{Ker}\varphi := \{ r \in R \mid \varphi(r) = 0 \}$.

(5) The image of φ is $\operatorname{Im}\varphi := \{ \varphi(r) \mid r \in R \}$.

Proposition 9: Let $\varphi : R \longrightarrow S$ be a ring homomorphism.

(1) $\operatorname{Ker}\varphi$ is a subring of R.

(2) $\operatorname{Im}\varphi$ is a subring of R.

Proof: Exercise.

Examples:

1) $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}/n$ given by $\varphi(a) = [a]$ is a ring epimorphism.

$\operatorname{Ker}\varphi = n\mathbb{Z}$ $\quad$ $\operatorname{Im}\varphi = \mathbb{Z}/n$ $\quad$ $\varphi^{-1}([a]) = \{a + nl \mid l \in \mathbb{Z}\}$

for all $[a] \in \mathbb{Z}/n$

2) Let $n \in \mathbb{Z}$, then $\varphi_n : \mathbb{Z} \longrightarrow \mathbb{Z}$ given by $\varphi_n(x) = nx$ is NOT a ring homomorphism.

$$\varphi_n(x+y) = n(x+y) = nx + ny = \varphi_n(x) + \varphi_n(y)$$

BUT $\quad \varphi_n(xy) = n(xy) \neq (nx)(ny) = \varphi_n(x)\,\varphi_n(y)$

3) Evaluation homomorphism

$e : R[x] \longrightarrow R$ given by $e(p(x)) = p(0_R)$ is a ring homomorphism.

$\ker e = \{$ polynomials with constant term $0\}$ $\qquad$ $\operatorname{Im} e = R$

$e^{-1}(a) = \{$ polynomials with constant term $a\}$ for all $a \in R$

- $e : \mathbb{F}_7[x] \longrightarrow \mathbb{F}_7$

  $e\left([2] + [5]x^4 - x^8\right) = [2] \in \mathbb{F}_7$

- $e : \mathbb{Z}[x] \longrightarrow \mathbb{Z}$

  $e\left(7x^5 - 3x\right) = 0 \in \mathbb{Z}$

4) Let $f: \mathbb{Z} \longrightarrow \mathbb{Z}$ be a ring isomorphism, then $f = id_{\mathbb{Z}}$.

Let $n \in \mathbb{Z}^+$, then

$$f(n) = f(\underbrace{1+1+\cdots+1}_{n\text{-times}}) = \underbrace{f(1)+f(1)+\cdots+f(1)}_{n\text{-times}} = n f(1)$$

$$f(-n) = -f(n) = -n f(1).$$

This means $f(n) = n f(1)$ for all $n \in \mathbb{Z}$.

Since f is a ring homomorphism, $nm f(1) = f(nm) = f(n) f(m) = n f(1)\, m f(1)$.

$$\Rightarrow nm f(1) = nm f(1)^2 \Rightarrow f(1) = f(1)^2 \Rightarrow f(1) = 0 \text{ or } f(1) = 1$$

It follows that $f(1) = 1$ because f is an iso. Hence, $f(n) = n \ \forall n \in \mathbb{Z}$.