Lec10A Ring Homomorphisms

February 4, 2021 10:37 AM

Assignment # 2 due Monday @ 11pm.
Office hours Friday 9–11am Monday 9–11am.

Chapter 5 Homomorphisms and Chinese Remainder Algorithm.

5.3 Ring Morphisms

Let R and S be two rings with identities 1_R and 1_S.
A function $\phi : R \to S$ is called a ring morphism (or homomorphism) if $\forall a, b \in R$

(i) $\phi(a +_R b) = \phi(a) +_S \phi(b)$
(ii) $\phi(a \cdot_R b) = \phi(a) \cdot_S \phi(b)$ and
(iii) $\phi(1_R) = 1_S$

Lemma. Let $a \in R$. Then

(iv) $\phi(0_R) = 0_S$
(v) $\phi(-a) = -\phi(a)$
(vi) a is a unit $\Rightarrow \phi(a)$ is a unit

Proof (iv) $\phi(0) = \phi(0+0) \overset{(i)}{=} \phi(0) + \phi(0)$.
$-\phi(0) \quad = \quad -\phi(0)$
$\Rightarrow 0 = \phi(0)$.

(v) $0 = \phi(0) = \phi(a + (-a)) \overset{(i)}{=} \phi(a) + \phi(-a)$.
So $\phi(-a) = -\phi(a)$.

① The modular homomorphism $\phi_n : \mathbb{Z} \to \mathbb{Z}_n$ $n > 1$
where $\phi_n(a) = a \bmod n$.

Example $\phi_7(4 \cdot 9) = \phi_7(36) = 36 \bmod 7 = 1$.
(ii) $\phi_7(4) \cdot \phi_7(9) = 4 \cdot 2 = 1$.

$\mathbb{Z}$ $\quad \mathbb{Z}_7 \quad \mathbb{Z}_7$

② The evaluation homomorphism $\phi_{x=a} : R[x] \to R$
where R is a ring, $a \in R$ and
$\phi_{x=a}(f) = f(a)$. $\qquad \phi(a \cdot b) = \phi(a) \cdot \phi(b)$.

$(x+1)\cdot(2x+3) = 2x^2+5x+3$

$\phi_{x=a}(f) = f(a)$. $\qquad \phi(a\cdot b) = \phi(a)\cdot\phi(b)$.

Example. $\quad f = \underline{(x+1)\circ(2x+3)} = 2x^2+5x+3$

$$\phi_{x=2} \qquad 3 \cdot 7 \quad = \quad 8+10+3=21$$

Proof that $\phi_n : \mathbb{Z} \to \mathbb{Z}_n$ is a ring morphism.

(i) $\phi_n(a +_{\mathbb{Z}} b) = (a +_{\mathbb{Z}} b) \bmod n$

$= ((q_a \cdot n + r_a) + (q_b \cdot n + r_b)) \bmod n$

$= r_a + r_b \bmod n$

$= (a \bmod n) +_{\mathbb{Z}_n} (b \bmod n)$

$= \phi_n(a) +_{\mathbb{Z}_n} \phi_n(b)$

(ii) $\phi_n(a \cdot_{\mathbb{Z}} b) = a\cdot b \bmod n$

$= (q_a \cdot n + r_a)(q_b \cdot n + r_b)$

$= \vdots$

$\longrightarrow = \phi_n(a) \cdot \phi_n(b)$.

(iii) $\phi_n(1_{\mathbb{Z}}) = 1 \bmod \underline{n}$. $\quad (n>1)$.

$= 1_{\mathbb{Z}_n}$

Theorem Let $\phi : R \to S$ be a ring morphism.
Let $\Theta : R[x] \to S[x]$ where $\Theta(\sum \underset{R[x]}{a_i} x^i) = \sum \underset{S[x]}{\phi(a_i)} x^i$
Then Θ is a ring morphism.

Proof. (i). Let $a, b \in R[x]$. $\quad n=$ max of the degrees.

$\Theta(a+b) = \Theta(\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i)$

$= \Theta(\sum (a_i+b_i) x^i$

$= \sum \phi(a_i+b_i) x^i \underset{(i)}{=} \underline{\sum (\phi(a_i)+\phi(b_i)) x^i}$

$= \underline{\sum \phi(a_i) x^i} + \sum \phi(b_i) x^i$

$= \Theta(a) + \Theta(b)$.

$$= \sum \varphi(a_i)x^i + \sum \varphi(b_i)x^i$$
$$= \theta(a) + \theta(b).$$

This extends in the obvious way to $\theta : R[x_1,\dots,x_n] \Rightarrow S[x_1,\dots,x_n]$.

Example. $f = \underline{17}xy^2 + \underline{12}y^3 - \underline{5} \in \mathbb{Z}[y][x]$

$$\phi_7(f) = 3xy^2 + 5y^3 + 2 \in \underbrace{\mathbb{Z}_7[y]}[x].$$

$$\phi_{y=2}(\phi_7(f)) = 3 \cdot x \cdot 4 + 5 \cdot 8 + 2 \in \underline{\mathbb{Z}_7}[x]$$
$$= 5x + 0.$$

$$\phi_{y=2}(f) = 4 \cdot \underline{17} \cdot x + \underbrace{96 - 5}_{=91} \in \mathbb{Z}[x]$$
$$\phi_7(\phi_{y=2}(f)) = 5 \cdot x + 0$$

In general in a polynomial ring $\underline{\phi_n}$ and $\underline{\phi_{y=a}}$ commute.

Application Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ where $a,b,c,d \in R$. $R = \mathbb{Z}[x,y]$.

Is $\det(A) = 0$?

Compute $a \cdot d - b \cdot c$ in R. !!

Suppose $\phi : R \to S$ as a ring morphism.

apply ϕ first then compute det.

$$\phi(\det(A)) = \phi(ad - bc) = \phi(ad) - \phi(bc)$$
$$\underset{(ii)}{=} \phi(a)\cdot\phi(d) - \phi(b)\cdot\phi(c) = \det\left(\begin{bmatrix} \phi(a) & \phi(b) \\ \phi(c) & \phi(d) \end{bmatrix}\right)$$

If $\det(A) = 0_R$ then $\phi(\det(A)) = \phi(0) = 0_S$

Therefore $\phi(\det(A)) \neq 0_S \Rightarrow \det(A) \neq 0_R$

If $\det(A) \neq 0$ then $\phi(\det(A))$ may be 0.

Example. $R = \mathbb{Z}[u,v]$ Is $\det(A) = 0$?

$$A = \begin{bmatrix} u & v & 1-uv \\ v & u & v \\ 1-uv & v & u \end{bmatrix} \quad (\phi_{u=0} \circ \phi_{v=0})(A) = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

(thinking of a bigger A) $\qquad$ $\det = 0.$

$$(\phi_{u=1} \circ \phi_{v=1})(A) = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix} \quad \det = 1 \cdot 0 - 1 \cdot (1-0) = -1.$$

$\Rightarrow \det(A) \neq 0.$ (a proof).

$u=0$, $v=0$

$$\det(A) = (1 + u - uv)(u^2 v + u^2 - u - 2v^2). \in \mathbb{Z}[u,v]$$

$u=1, v=2$

If $\det(A) \neq 0$ but $(\phi_{u=\alpha} \circ \phi_{v=\beta})(\det(A)) = 0.$

then $u=\alpha, v=\beta$ is a root of $\det(A) \in \mathbb{Z}[u,v]$.

What's the probability of picking a root of a polynomial?

Lemma (Schwarz – Zippel 1978)

Let D be an integral domain (e.g. $\mathbb{Z}$) and $S \subset D$.

Suppose $f \in D[x_1, \dots, x_n]$ and $f \neq 0$. If $\alpha_1, \alpha_2, \dots, \alpha_n$ are chosen at random from S then

$$\mathrm{Prob}(f(\alpha_1, \alpha_2, \dots, \alpha_n) = 0) \leq \frac{\deg(f)}{|S|} = \frac{5}{10^6}$$

α is a root of f

$S = [0, 10^6]$