Homomorphisms

Polynomial rings

Fix a comm. ring R w/ 1 (e.g. $R = \mathbb{Z}, \mathbb{R}, \mathbb{Q}$, etc.)

Let X an indeterminate

Defn: A polynomial in X with coefficients in R is a formal, finite sum

$$a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0, \quad a_i \in R, \ i = 0, \dots, n$$

Note: If $a_n \neq 0$ and $a_m = 0$ $\forall m > n$.

then we say the degree of the polynomial is n.

If $a_k = 1$, we often omit it from the notation

e.g. $X^2 + 2$ — 1 is missing.

If $a_n = 1$, we say the polynomial is monic

Defn: The set of polynomials in X w/ coefficients in R is denoted

$$R[X] := \{ \text{polynomials } a_n X^n + \dots + a_0 \mid a_i \in R \}$$

If the degree of $p \in R[x]$ is zero, we say p is a constant polynomial

Obs: $R \hookrightarrow R[x]$

$a \longmapsto a$

Claim: $R[X]$ is a ring.

Pf: $(a_n X^n + a_{n-1} X^{n-1} + \_\_ + a_1 X + a_0) +$

$(b_n X^n + b_{n-1} X^{n-1} + \_\_ + b_1 X + b_0)$

$= (a_n + b_n) X^n + (a_{n-1} + b_{n-1}) X^{n-1} + \_\_ + (a_1 + b_1) X + (a_0 + b_0)$

$(a_n X^n + a_{n-1} X^{n-1} + \_\_\_ + a_1 X + a_0) \cdot$

$(b_m X^m + b_{m-1} X^{m-1} + \_\_ + b_1 X + b_0)$

$= (a_0 \cdot b_0) + (a_1 \cdot b_0 + a_0 \cdot b_1) X + (a_2 \cdot b_0 + a_0 \cdot b_2 + a_1 \cdot b_1) X^2$

$+ \ldots + \left(\sum_{k=0}^{\ell} a_k \cdot b_{\ell - k} \right) X^{\ell} + \_ + (a_n \cdot b_m) X^{n+m}$

$\square$

Example: $\mathbb{Z}[x]$, $\mathbb{Q}[X]$, $(\mathbb{Z}/3\mathbb{Z})[X]$

we may write, e.g.

$$X + 2, \quad x^3 + 2x^2 + 1 \in (\mathbb{Z}/3\mathbb{Z})[x]$$

(omitting the bars over the coefficients)

Factoring polynomials depends on the coefficient ring.

e.g. $x^2 - 2 \in \mathbb{Z}[X]$

$$x^2 - 2 = \underbrace{(x + \sqrt{2})} \cdot \underbrace{(x - \sqrt{2})} \in \mathbb{R}[x]$$

These are not in $\mathbb{Z}[x]$

$x^2+1 \in \mathbb{Z}[x]$, $x^2+1 \in \mathbb{R}[x]$

This polynomial doesn't factor in either ring, but it does factor in $\mathbb{C}[x]$

$$x^2+1 = (x+i)(x-i)$$

It also factors in $(\mathbb{Z}/2\mathbb{Z})[x]$

$$x^2+1 = (x+1)(x+1) \mod 2$$

Because $x^2+2x+1 \equiv x^2+1 \mod 2$

<u>Prop</u>: Let R be an integral domain

$$p(x),\ q(x) \in R[x]$$

① $\text{degree}\,(p(x)\cdot q(x)) = \text{degree}\ p(x) + \text{degree}\ q(x)$

② $R[x]^\times = R^\times$

③ $R[x]$ is an integral domain.

<u>Pf</u>: ① This is mostly: The leading term is

$$(a_n \cdot b_m)\, x^{n+m}$$

Since R is an integral domain and $a_n, b_m \neq 0$

Then $a_n \cdot b_m \neq 0$ (This also proves ③)

② Suppose $p(x) \in R[x]^\times$, say $p(x)\cdot q(x) = 1$.

Then $\deg(p\cdot q) = \deg(1) = 0$

$\Rightarrow \deg(p) = \deg(q) = 0 \Rightarrow p \in R$ $\square$

Example: $\left(\mathbb{Z}/4\mathbb{Z}\right)[x]$

Consider $2x^2+1,\ 2x^5+3x$

$$(2x^2+1)\cdot(2x^5+3x) = (2\cdot 2)x^7 + \text{lower terms}$$
$$= 0\cdot x^7 + \text{lower terms}$$
$$\Longrightarrow \deg\left((2x^2+1)\cdot(2x^5+3x)\right) < \deg(2x^2+1) + \deg(2x^5+3x)$$

Ring homomorphisms

Defn: Let R, S be rings.

A ring homomorphism is a map

$$f: R \longrightarrow S$$

s.t. (1) $f(a +_R b) = f(a) +_S f(b)$ (Group homomorphism)

(2) $f(a \cdot_R b) = f(a) \cdot_S f(b)$

If f is a bijective ring homomorphism, we say it is a ring isomorphism

We say, in this case R is isomorphic to S as rings and write $R \cong S$

Defn: The kernel of a ring homomorphism

$$f : R \to S$$

is the subset

$$\operatorname{Ker} f := f^{-1}(0_S) \subset R$$

Prop: Let R, S be rings

$f : R \to S$ a homom.

① $\operatorname{Im} f \subset S$ is a subring

② $\operatorname{Ker} f \subset R$ is a subring

Moreover, if $r \in R$, $a \in \operatorname{Ker} f$

then $r \cdot a \in \operatorname{Ker} f$

Pf: ① $f(0_R) = 0_S$ (in particular, $\operatorname{Im} f \neq \emptyset$)

$$\ulcorner f(0_R) = f(0_R + 0_R) = f(0_R) + f(0_R)$$

$$\Rightarrow \quad 0_S = f(0_R) \quad \lrcorner$$

Suppose now $f(a), f(b) \in \operatorname{Im} f$.

$$f(a) \cdot f(b) = f(a \cdot b) \in \operatorname{Im} f$$

To see $f(a) - f(b) \in \operatorname{Im} f$.

it suffices to see that $-f(b) = f(-b)$

$$\ulcorner\ f(0_R) = f(b + (-b)) = f(b) + f(-b)$$

$$f(0_R) = 0$$

$$\Longrightarrow f(-b) = -f(b) \quad \lrcorner$$

(2) Since $f(0_R) = 0_S \Longrightarrow 0_R \in \operatorname{Ker} f$

Suppose $a, b \in \operatorname{Ker} f$.

$$f(a-b) = f(a) - f(b) = 0 - 0 = 0$$

$$\Longrightarrow a-b \in \operatorname{Ker} f$$

$$f(a \cdot b) = f(a) \cdot f(b) = 0 \cdot 0 = 0$$

$$\Longrightarrow a \cdot b \in \operatorname{Ker} f.$$

Now suppose $r \in R$.

$$f(r \cdot a) = f(r) \cdot f(a) = f(r) \cdot 0 = 0$$

$\square$

Example:

① $f: \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z}$

$a \longmapsto a \mod 2$

Check: even + even = even even · even = even

$\bar{0} + \bar{0} = \bar{0}$ $\bar{0} \cdot \bar{0} = 0$

even + odd = odd. even · odd = even

$\bar{0} + \bar{1} = \bar{1}$ $\bar{0} \cdot \bar{1} = \bar{0}$

odd + odd = even odd · odd = odd

$\bar{1} + \bar{1} = \bar{0}$ $\bar{1} \cdot \bar{1} = \bar{1}$

$\operatorname{Ker} f = \{\text{evens}\} = 2\mathbb{Z}$

Obs: $f^{-1}(\bar{1}) = \{\text{odds}\} = 1 + 2\mathbb{Z} = \{1 + 2n \mid n \in \mathbb{Z}\}$
$= 1 + \operatorname{Ker} f$

② Non-example

$f_n: \mathbb{Z} \longrightarrow \mathbb{Z}$

$a \longmapsto n \cdot a$

$f_n(a+b) = n \cdot (a+b) = n \cdot a + n \cdot b = f_n(a) + f_n(b)$

BUT

$f_n(a \cdot b) = n \cdot (a \cdot b)$

$f_n(a) \cdot f_n(b) = (n \cdot a) \cdot (n \cdot b) = n^2 \cdot (a \cdot b)$

So f_n is a ring homomorphism iff $n^2 = n$ (i.e. $n = 0, 1$)

So $f_2, f_3, \ldots$ are NOT ring homomorphisms.

<u>Obs</u>: f_0 is the constant map zero

f_1 is the identity

③ $\phi: \mathbb{R}[x] \longrightarrow \mathbb{R}$

$$p(x) \longmapsto \underbrace{p(0)}$$

i.e. the constant term in $p(x)$

Easy to check:

$$\phi(p \cdot q) = (p \cdot q)(0) = p(0) \cdot q(0) = \phi(p) \cdot \phi(q)$$

$$\phi(p+q) = (p+q)(0) = p(0) + q(0) = \phi(p) + \phi(q).$$

$$\operatorname{Ker} \phi = \{ p \in \mathbb{R}[x] \mid p(0) = 0 \}$$

$$= \{ p \in \mathbb{R}[x] \mid p(x) = x \cdot p'(x) \text{ for some } p' \in \mathbb{R}[x] \}$$

<u>Q</u>: What about,

$$\phi_1 : \mathbb{R}[x] \longrightarrow \mathbb{R} \quad ?$$

$$p(x) \longmapsto p(1)$$