Day 22 July 8, 2024

Polynomials rings

Throughout, R is a commutative ring with unity.

Def. A polynomial over R with indeterminate x is an expression of the form

$$p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n,$$

where each coefficient a_i, $0 \le i \le n$, is an elt of R and $a_n \neq 0$.
We call a_n the leading coefficient and say that $p(x)$ is monic if $a_n = 1$.
If $p(x) \neq 0$, then the degree of $p(x)$ is $\deg p(x) := n$.
We also define $\deg 0 := -\infty$.
The set of all polynomials over R with indeterminate x is denote $R[x]$.

The set $R[x]$ inherits binary operations from R via the usual addition & multiplication of polynomials.

Ex. $p(x) = 6 + 3x^3$ & $q(x) = 4 + 8x^2 + 4x^4 \in \mathbb{Z}_{12}[x]$

$$p(x) + q(x) = 10 + 8x^2 + 3x^3 + 4x^4$$
$$p(x)q(x) = 24 + 48x^2 + 24x^4 + 12x^3 + 24x^5 + 12x^7 = 0$$

So $\mathbb{Z}_{12}[x]$ is not an integral domain!

Prop. Let R be a commutative ring with unity. Then $R[x]$ is a commutative ring with unity.

(Proof.) Exercise.

① Additive inverse of a polynomial is obtained by replacing each coeff. w/ its add. inverse.

② Check that polynomial multiplication plays nicely. ☒

Prop. Let R be an I.D. Then $R[x]$ is an I.D. and

$$\deg(p(x)q(x)) = \deg p(x) + \deg q(x),$$

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

(Proof.) Write

$$p(x) = a_0 + a_1x + \cdots + a_nx^n \text{ \& } q(x) = b_0 + b_1x + \cdots + b_mx^m,$$

with $a_n \neq 0$ & $b_m \neq 0$. Then

$$\deg p(x) = n \quad \text{and} \quad \deg q(x) = m$$

and $a_nb_m \neq 0$, since R is an I.D. The leading term $a_nb_mx^{n+m}$ of $p(x)q(x)$ is nonzero, so $p(x)q(x) \neq 0$ and $\deg p(x)q(x) = n+m = \deg p(x) + \deg q(x)$. ☒

Def. Let R be a commutative ring with unity. Then the ring $R[x,y] := (R[x])[y]$ is called the ring of polynomials in two indeterminates over R. In fact,

$$R[x_1, \ldots, x_n] := (R[x_1, \ldots, x_{n-1}])[x_n]$$

is the ring of polynomials in n indeterminates over R, $n \geq 2$.

Prop. Let R be a commutative ring with unity and fix $\alpha \in R$. Then the map $\phi_\alpha : R[x] \to R$ defined by

$$\phi_\alpha(p(x)) := p(\alpha) := a_0 + a_1\alpha + \cdots + a_n\alpha^n,$$

where $p(x) = a_0 + a_1 x + \cdots + a_n x^n$, is a homomorphism.

(Proof.) Exercise. $\boxtimes$

We call ϕ_α the evaluation homomorphism at α.

The division algorithm

Thm. Let F be a field and let $f(x), g(x) \in F[x]$, with $g(x) \neq 0$. Then there exist unique polynomials $q(x), r(x) \in F[x]$ such that

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

where $\deg r(x) < \deg g(x)$.

(Proof.)

Existence.

If $f(x) = 0$, take $q(x) = 0$ & $r(x) = 0$.

$\$$ $f(x) \neq 0$ and let $n := \deg f(x)$

$m := \deg g(x)$.

If $m > n$, take $q(x) = 0$ & $r(x) = f(x)$.

$\$$ $m \leq n$. We'll use induction on n.

Write

$f(x) = a_0 + a_1 x + \cdots + a_n x^n$ & $g(x) = b_0 + b_1 x + \cdots + b_m x^m$

and define

$$h(x) := f(x) - \frac{a_n}{b_m} x^{n-m} g(x).$$

need F to be a field

Note that $\deg h(x) < n$.
By our inductive hypothesis, $\exists\ q_h(x), r(x) \in F[x]$ s.t.

$$h(x) = g(x)\, q_h(x) + r(x)$$

and $\deg r(x) < \deg g(x)$. Now let

$$q(x) = q_h(x) + \frac{a_n}{b_m} x^{n-m}$$

and notice that $f(x) = g(x)\, q(x) + r(x)$.

Uniqueness. § we have

$$g(x)\, q_0(x) + r_0(x) = f(x) = g(x)\, q_1(x) + r_1(x),$$

with $\deg r_0(x), \deg r_1(x) < \deg g(x)$.
Then

$$r_1(x) - r_0(x) = g(x)\, q_0(x) - g(x)\, q_1(x) = g(x)\,(q_0(x) - q_1(x)).$$

$$\deg\big(g(x)(q_0(x) - q_1(x))\big) = \deg(r_1(x) - r_0(x))$$

$$\deg\big(g(x)(q_0(x) - q_1(x))\big) = \deg g(x) + \deg(q_0(x) - q_1(x))$$

$$\deg(r_1(x) - r_0(x)) \le \max\{\deg r_1(x), \deg r_0(x)\} < \deg g(x)$$

So $\deg(q_0(x) - q_1(x)) < 0 \Rightarrow q_0(x) - q_1(x) = 0$

So $r_1(x) - r_0(x) = 0$.

Def. Let R be a commutative ring with unity and fix $\alpha \in R$ and $p(x) \in R[x]$. Then α is a zero or root of $p(x)$ if $p(x) \in \operatorname{Ker} \phi_\alpha$.

Cor. Let F be a field. Then $\alpha \in F$ is a root of $p(x) \in F[x]$ iff the polynomial $x - \alpha$ is a factor of $p(x)$ in $F[x]$.

(Proof.)

If $x-\alpha$ is a factor of $p(x)$, write

$$p(x) = (x-\alpha)q(x).$$

Then

$$\begin{aligned}\phi_\alpha(p(x)) &= \phi_\alpha((x-\alpha)q(x)) \\ &= \phi_\alpha(x-\alpha)\cdot\phi_\alpha(q(x)) \\ &= (\alpha-\alpha)\cdot q(\alpha) = 0\cdot q(\alpha) = 0,\end{aligned}$$

so $p(x) \in \operatorname{Ker} \phi_\alpha$.

If $p(x) \in \operatorname{Ker}\phi_\alpha$, write $p(x) = (x-\alpha)q(x) + r(x)$, with $\deg r(x) < \deg(x-\alpha) = 1$.

Then

$$\begin{aligned}0 = \phi_\alpha(p(x)) &= \phi_\alpha((x-\alpha)q(x) + r(x)) \\ &= \phi_\alpha(x-\alpha)\cdot\phi_\alpha(q(x)) + \phi_\alpha(r(x)) \\ &= 0\cdot q(\alpha) + r(\alpha) \to r(\alpha) = 0.\end{aligned}$$

If $\deg r(x) < 1$, then either $r(x) = 0$

or $r(x) = a$ for some $a \in R$ w/ $a \neq 0$.

Since $r(\alpha) = 0$, $r(x) = 0$. Then $p(x) = (x-\alpha)q(x)$. ∎