Last updated: Nov 15, 2024

Abstract Algebra Notes Week 11   Wed, Nov 13 2024

Sec 17.1 Polynomial rings

Def (Sec 17.1) Let R be a commutative ring with unity. A <u>polynomial over R with indeterminate x</u> is an expression of the form

$$f(x) = a_0 + a_1 x + a_2 x^2 + \dots + \underbrace{a_n}_{\text{leading coefficient}} x^{n}$$

degree of f, $\deg f(x)$

where $\underbrace{a_0, a_1, \dots, a_n}_{\text{coefficients of } f} \in R$ and $a_n \neq 0$.

Let $R[x]$ denote the set of all polynomials w/ coefficients in R.

Define the sum of two polynomials

$$p(x) = a_0 + a_1 x + \dots + a_n x^n$$

$$q(x) = b_0 + b_1 x + \dots + b_m x^m$$

to be

$$p(x) + q(x) = c_0 + c_1 x + \dots + c_k x^k$$

where $c_i = a_i + b_i$ for each i. (Note: some coefficients may be 0)

Define the product of $p(x)$ and $q(x)$ to be

$$p(x)\, q(x) = c_0 + c_1 x + c_2 x^2 + \dots + c_{m+n} x^{m+n}$$

where $c_i = a_0 b_i + a_1 b_{i-1} + a_2 b_{i-2} + \dots + a_{i-1} b_1 + a_i b_0$

for each i. (Note: some coefficients may be 0)

Thm (Thm 17.3) If R is a commutative ring with unity, then $R[x]$ is a commutative ring with unity.

Prop (Prop 17.4) If R is an integral domain, then

① $\deg p(x) + \deg q(x) = \deg(p(x)\, q(x))$

② $R[x]$ is an integral domain

Thm (Division algorithm) (Thm 17.6)

Let F be a field, and let $f(x)$, $g(x)$ be polynomials in $F[x]$. If $g(x)$ is nonzero, there exist unique polynomials $q(x)$, $r(x) \in F[x]$ such that

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

where either $\deg r(x) < \deg g(x)$ or $r(x)$ is the zero polynomial.

Ex $\quad f(x) = x^3 - x^2 + 2x - 3$, $\quad g(x) = x - 2 \in \mathbb{Q}[x]$

$$\begin{array}{r|l}
 & x^2 + x + 4 \\ \hline
x - 2 & x^3 - x^2 + 2x - 3 \\
 & x^3 - 2x^2 \qquad - \\ \hline
 & \quad\ x^2 + 2x - 3 \\
 & \qquad \vdots \\ \hline
 & \qquad\quad 5
\end{array}$$

So $\quad f(x) = g(x) \underbrace{(x^2 + x + 4)}_{q(x)} + \underbrace{5}_{r(x)}$

Def $\quad \alpha \in F$ is a <u>root</u> or <u>zero</u> of a polynomial $p(x)$ if $p(\alpha) = 0$.

Corollary of the division algorithm (Corollary 17.8)

Let F be a field. An elt $\alpha \in F$ is a root of $p(x) \in F[x]$ iff $(x - \alpha)$ is a factor of $p(x)$ in $F[x]$

Proof $\quad$ Exercise

$\boxed{\text{Sec } 16.3}$

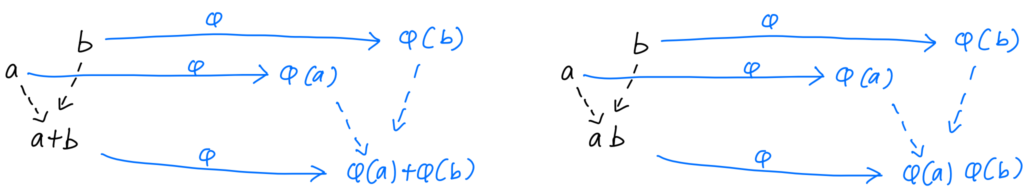
Part I: Ring homomorphisms

(Just as a group homomorphism preserves the group operation, a ring homomorphism preserves the two ring operations)

Def A <u>ring homomorphism</u> from a ring R to a ring S is a map $\varphi : \overset{\text{domain}}{R} \longrightarrow \overset{\text{codomain}}{S}$ satisfying

$$\underbrace{\varphi(a +_R b) = \varphi(a) +_S \varphi(b)}_{\varphi \text{ preserves addition}} \quad \text{AND} \quad \underbrace{\varphi(a \cdot_R b) = \varphi(a) \cdot_S \varphi(b)}_{\varphi \text{ preserves multiplication}} \quad \text{for all } a, b \in R$$

Illustration:



Def The <u>kernel</u> of $\varphi : R \to S$ is the set

$$\ker \varphi = \{ x \in R : \varphi(x) = 0_S \}$$

Def If a ring homomorphism is injective and surjective, it is called an <u>isomorphism</u>.

Ex Given $n \in \mathbb{Z}_{>0}$, the map $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}_n$

defined by $a \longmapsto a \pmod{n}$

is a ring homomorphism.

Check that $\varphi(a+b) = \varphi(a) + \varphi(b)$

$\varphi(ab) = \varphi(a)\,\varphi(b)$

See Textbook Ex 16.20

$\ker \varphi = \{ nk : k \in \mathbb{Z} \} = n\mathbb{Z}$

It is a surjective map.

Ex The map $\varphi : \mathbb{C} \longrightarrow \mathbb{C}$

$\varphi(a+bi) = a - bi$

Prove that $\varphi(x+y) = \varphi(x) + \varphi(y)$ for all $x, y \in \mathbb{C}$ (See week 12 practice)

Prove that $\varphi(xy) = \varphi(x)\,\varphi(y)$ for all $x, y \in \mathbb{C}$:

$$\varphi\big((a+bi)(c+di)\big) = \varphi\big((ac-bd) + (ad+bc)i\big)$$

$$= ac - bd - (ad+bc)i$$

$$= (a-bi)\,(c-di)$$

$$= \varphi(a+bi)\,\varphi(c+di)$$

Prove that φ is injective:

Let $\varphi(a+bi) = \varphi(c+di)$

$a - bi = c - di$

Then $a = c$ and $b = d$, so $a+bi = c+di$.

Prove that φ is surjective (See week 12 practice)

<u>Ex</u> Let $\mathbb{R}[x]$ denote the ring of all polynomials with real coefficients.

* Consider the map $\varphi : \mathbb{R}[x] \longrightarrow \mathbb{R}$

$$p(x) \mapsto p(5)$$

that is, if $p(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$

then $\varphi(p(x)) = a_0 + a_1 5 + a_2 5^2 + \dots + a_n 5^n$

Then φ preserves addition and multiplication.

This map is called the <u>evaluation homomorphism</u> at 5.

<u>Note</u> $\ker \varphi = \{ p(x) \in \mathbb{R}[x] : \underbrace{\varphi(p(x))}_{p(5)} = 0 \}$

$= \{ p(x) \in \mathbb{R}[x] : 5$ is a zero / root of $p(x) \}$

$p(x) \in \ker \varphi$ iff 5 is a root of $p(x)$

* In general, given $\alpha \in \mathbb{R}$,

the map $\varphi_\alpha : \mathbb{R}[x] \longrightarrow \mathbb{R}$

$$p(x) \mapsto p(\alpha)$$

is called <u>the evaluation homomorphism at α</u>.

<u>Note:</u> $p(x) \in \ker \varphi_\alpha$ iff α is a root of $p(x)$

<u>Recall</u> Since $\mathbb{R}$ is a field, an elt $\alpha \in \mathbb{R}$ is a root of $p(x) \in \mathbb{R}[x]$ iff $(x-\alpha)$ is a factor of $p(x)$ in $\mathbb{R}[x]$.

<u>Prop</u> (Some properties of ring homomorphism) (Prop 16.22)

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

1. If R is a commutative ring, $\varphi(R)$ is a commutative ring

Compare with fact from group theory (Sec 11):

"If $f: G \to H$ is a group homomorphism and G is abelian, then $f(G)$ is also abelian"

2. $\varphi(0_R) = 0_S$

Compare with Prop 11.4 (1): "If $f: G \to H$ is a group homomorphism, then $f(e_G) = e_H$"

3. We cannot say the same about the multiplicative identity (unity) since not all rings have them.

If R and S have unities 1_R and 1_S (respectively) and if φ is surjective, then $\varphi(1_R) = 1_S$.

4. If R is a field, then either $\varphi(R)$ is the zero ring or $\varphi(R)$ is a field.

<u>Proof of 2</u>

$$\varphi(0_R) \overset{\text{def of } 0_R}{=} \varphi(0_R + 0_R) \overset{\text{def of homomorphism}}{=} \varphi(0_R) + \varphi(0_R)$$

and

$$\varphi(0_R) = 0_S + \varphi(0_R)$$

So $0_S + \varphi(0_R) = \varphi(0_R) + \varphi(0_R)$.

By cancellation (since $(S,+)$ is a group), we have $\varphi(0_R) = 0_S$

5. HW: If $\ker \varphi = \{0\}$, then φ is injective

Part II: Ideals

(Normal subgroups play a special role in group theory — they allow us to construct quotient groups.
In ring theory, the special subrings are called "ideals" and they will allow us to construct "quotient rings")

Notation: If A is a subset of a ring R and $r \in R$,

$$rA \overset{\text{def}}{=} \{ra : a \in A\} \quad \text{and} \quad Ar \overset{\text{def}}{=} \{ar : a \in A\}$$

<u>Def</u> Let R be a ring.
A <u>(two-sided) ideal</u> of R is a subring I of R such that $\underbrace{rI \subset I \quad \text{and} \quad Ir \subset I}$ for all $r \in R$,

i.e. for all $r \in R$ and $a \in I$, both ra and ar are in I.

Think: An ideal "absorbs" elements from R

<u>Ex</u> For every ring, the subrings $\{0\}$ and R are both ideals of R.

<u>Fact</u> Suppose R is a ring with unity 1.
If I is an ideal in R and $1 \in I$, then $I = R$

<u>Proof</u>
- $I \subset R$ because I is a subring of R.
- To show $R \subset I$, let $r \in R$.
  Then $r = r1 \in I$ since I is an ideal and $1 \in I$. □

Ideal test

A subset I is an ideal of R if:

* I is an additive subgroup of R
* If $a \in I$ and $r \in R$ then both $\underbrace{ar \text{ and } ra \text{ are in } I}_{\text{"the absorbing property of } I\text{"}}$.

Note We can take this to be the definition of ideal.

Fact Let R be a commutative ring with unity, and $a \in R$. Then the set

$$\langle a \rangle \overset{\text{def}}{=} \{ar : r \in R\}$$

is an ideal of R.

Proof Show that $\langle a \rangle$ is an additive subgroup of R HW (See Example 16.24)

Show that $s\langle a \rangle \subseteq \langle a \rangle$ for all $s \in R$:

Let $s \in R$ and $y \in \langle a \rangle$. Then $y = ar$ for some $r \in R$.

We have $sy = s(ar) = a(sr) \in \langle a \rangle$.

Since R is commutative

Thus $\langle a \rangle$ satisfies the definition of an ideal $\square$

Def Let R be a commutative ring with unity.

An ideal of the form $\langle a \rangle = \{ar : r \in R\}$ for some $a \in R$ is called a principal ideal.

Say that $\langle a \rangle$ is the principal ideal generated by a.

Ex Given $n \in \mathbb{Z}_{>0}$, the set $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\} = \{\ldots, -2n, -n, 0, n, 2n, \ldots\}$

(Ex 16.26) is an ideal of $\mathbb{Z}$.

By def, $n\mathbb{Z}$ is the principal ideal of $\mathbb{Z}$ generated by n (it can also be generated by $-n$)

Ex Let $\mathbb{Z}[x]$ denote the ring of polynomials w/ integer coefficients.

Then $\mathbb{Z}[x]$ is a commutative ring w/ unity

① $I = \langle x \rangle$

$= \{$ integer polynomials of the form $a_1 x + a_2 x^2 + \dots + a_n x^n \}$

$= \{$ integer polynomials with no constant term $\}$

is the principal ideal generated by x

② $I = \langle x^2+1 \rangle$,

the principal ideal generated by x^2+1,

is the set of integer polynomials that are multiples of (x^2+1),

$$I = \{ f(x)(x^2+1) : f(x) \in \mathbb{R}[x] \}$$

③ Let $I = \{ f(x) \in \mathbb{Z}[x] : f(0) \text{ is an even integer} \}$

Fact: I is not a principal ideal

Proof

Suppose $I = \langle p(x) \rangle \overset{\text{def}}{=} \{ f(x)\, p(x) : f(x) \in \mathbb{Z}[x] \}$
for some polynomial $p(x)$ in $\mathbb{Z}[x]$.

The constant polynomial 2 is in I,
so $2 = f(x)\, p(x)$ for some $f(x) \in \mathbb{Z}[x]$

So $p(x)$ must be $1, -1, 2$, or -2.

Since $p(x) \in I$, $p(0)$ is even, so $p(x) \neq 1$ and $p(x) \neq -1$.

So $p(x) = 2$ or -2.

The polynomial x is also in I,

so $x = h(x)\,2$ or $x = h(x)(-2)$ for some $h(x) \in \mathbb{Z}[x]$.

Since the coefficients of $h(x)$ are integers,

this is impossible.

So I is not principal $\square$

Exercise:

Prove that $I = \langle x, 2\rangle \overset{\text{def}}{=} \{ f(x)\,2 + g(x)\,x : f(x), g(x) \in \mathbb{Z}[x] \}$

Prop (Prop 16.27) The kernel of a ring homomorphism $\varphi : R \to S$ is an ideal of R.

Proof We know from group theory that

$\ker\varphi$ is an additive subgroup of R.

Let $r \in R$, $a \in \ker\varphi$.

Show that $ar \in \ker\varphi$:

$\varphi(ar) = \varphi(a)\varphi(r) = 0\,\varphi(r) = 0$

Show that $ra \in \ker\varphi$:

$\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)\,0 = 0$. $\square$

Ex Let $R = \mathrm{Mat}_2(\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{Z} \right\}$ and

let I be the subset of R consisting of matrices

with even entries.

HW: You have shown in HW/quiz that I is a subring.

Now show that I is an ideal.

— the end —