Abstract Algebra Notes Day 11 Tue, Nov 25 2025

Gallian Ch 16 Polynomial rings

(extra)

Def Let R be a commutative ring with unity.
A polynomial over R with indeterminate x 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 If R is a commutative ring with unity,
then $R[x]$ is a commutative ring with unity.

Prop 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

Gallian Ch 14 | Part I: 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 $r \in R$,

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

<u>Def</u> Let R be a ring.

A <u>(two-sided) ideal</u> of R is a subring I of R such that $\underbrace{rI \subset I \text{ and } Ir \subset I}$ 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 $1 \in I$. $\square$

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 $\underbrace{ar \text{ and } ra \text{ are in } I}$.

"the absorbing property of I"

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

Ex

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

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

$$I = \{ \text{integer polynomials of the form } a_1x + a_2x^2 + \dots + a_nx^n \}$$
$$= \{ \text{integer polynomials with no constant term} \}$$

is an ideal of $\mathbb{Z}[x]$.

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

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

(another possible notation is aR)

is an ideal of R.

Proof Show that $\langle a \rangle$ is an additive subgroup of R.

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 <u>principal ideal</u>.

Say that $\langle a \rangle$ is <u>the principal ideal generated by a</u>.

Ex Given $n \in \mathbb{Z}_{>0}$, the set $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\} = \{\ldots, -2n, -n, 0, n, 2n, \ldots\}$ 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 $a_1x + a_2x^2 + \dots + a_nx^n \}$

$= \{$ 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 $I = \{ f(x) \in \mathbb{Z}[x] : f(0)$ 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 $I = \langle x, 2 \rangle \overset{\text{def}}{=} \{ f(x)\, 2 + g(x)\, x : f(x), g(x) \in \mathbb{Z}[x] \}$

(Group activity Day 11 & next HW)

— end of Part I —