# Week 8

Last Friday, we started the new section about polynomials.

<u>Def</u> $(R, +, \times)$ a ring.

$R[X]$ the set of polynomials in one variable $X$

$$f = f(X) = c_d X^d + c_{d-1} X^{d-1} + \dots + c_1 X + c$$

where $c_i$'s are elements of $R$.

$\deg(f)$ = the largest $n$ for which the coeffient $c_n$ of $X$ is non-zero.

$$f(X) = \sum_{n=0} c_n(f) X^n$$

$$c_n(f) = 0 \quad \forall n > \deg(f)$$

$$c_{\deg(f)}(f) \neq 0 \quad \text{at} \quad n = \deg(f)$$

Theorem 25

$R[X]$ is a ring

w.r.t addition

$$f+g = \sum_{n=0}^{\max(\deg(f), \deg(g))} (c_n(f) + c_n(g)) X^n$$

$$fg = \sum_{n=0}^{\deg(f)+\deg(g)} c_n(fg) X^n$$

where $$\underset{=}{c_n}(fg) = \sum_{r=0}^{n} c_r(f) c_{n-r}(g)$$

$$c_0(fg) = c_0(f) c_0(g)$$

$$c_1(fg) = \sum_{r=0}^{1} c_r(f) c_{n-r}(g)$$

$$= c_0(f) c_1(g) + c_1(f) c_0(g)$$

$$C_2(fg) = C_0(f)C_2(g) + C_1(f)C_1(g)$$
$$+ C_2(f)C_0(g)$$

$\vdots$

If $R$ is a ring with identity,

then so is $R[x]$.

If $R$ is commutative, then so is

$R[x]$.

To check that

$(R \neq 0)$

Let $f, g \in R[x]$.

(GOAL $f+g \in R[x]$)

For any $n \geq 0$, we know that

$$c_n(f) \in R$$

$$c_n(g) \in R$$

Then by $(R+0)$ for $(R, +, \times)$,

$$c_n(f) + c_n(g) \in R$$

Therefore $$\sum_n \left(c_n(f) + c_n(g)\right) x^n \in R[x].$$

(R+1) I need to show

if $f, g, h \in R[x]$.

then $f+(g+h) = (f+g)+h$

For any $n \geq 0$,

we know

$$c_n(f) + \left( c_n(g) + c_n(h) \right)$$

$$= \left( c_n(f) + c_n(g) \right) + c_n(h)$$

by (R+1) for $(R, +, \times)$.

Therefore,

$$\underline{\left( \sum_n c_n(f) X^n \right)} + \left( \underbrace{\sum_n c_n(g) X^n}_{\sum_n (c_n(g) + c_n(h)) X^n} + \sum_n c_n(h) X^n \right)$$

$$= \underbrace{\left( \sum_n c_n(f) X^n + \sum_n c_n(g) X^n \right)}_{\sum_n (c_n(f) + c_n(g)) X^n} + \sum_n c_n(h) X^n$$

(R+2) asks for the identity element w.r.t. $(R[X], +)$

In fact,

$$\underline{\text{"}0\text{"}} = \cdots \underline{0_R} \cdot X^n + 0_R \cdot X^{n-1} + \cdots + 0_R \cdot X + 0_R$$

$0_R$ on the RHS are
the identity element w.r.t.
$(R,+)$

would do, i.e.

$\forall f \in R[x]$.

$$f+0 = 0+f = f.$$

$$f+0 = \sum_n \left(c_n(f) + c_n(0)\right) x^n$$

$$= \sum_n \left(c_n(f) + 0_R\right) x^n$$

(R+2)

for $(R,+,\times)$

$$= \sum_n c_n(f)\, x^n = f$$

Similarly

$$0 + f = \sum_n (c_n(0) + c_n(f))x^n$$

$$= \sum_n (0 + c_n(f))x^n$$

$$= \sum_n c_n(f)x^n$$

Combining those two,

$$f + 0 = 0 + f = f.$$

(R+3) asks for the inverse of $f$ w.r.t. "+".

Given $f = \sum_n c_n(f) x^n$,

the inverse is

$$g = \sum_n (-c_n(f)) x^n.$$

I need to check that

$$f + g = g + f = 0$$

In fact $f+g$

$$= \sum c_n(f) x^n + \sum (-c_n(f)) x^n$$

$$= \sum_n (c_n(f) + (-c_n(f))) x^n$$

$$= \sum_n 0_R X^n = 0$$
$p$

(R+3) for $(R, +, \times)$

Similarly for $g + f = 0$

(R+4) asks for $f + g = g + f$.

This follows from

$$C_n(f) + C_n(g) = C_n(g) + C_n(f)$$

given by (R+4) for $(R, +, \times)$,

$(R\times 0)$, $(R\times 1)$, $(R\times +)$ $(R+\times)$

are left as exercises!

**Prop 26** If $R$ is a ring with identity, then $R[x]$ is **not** a division ring.

**Pf** Look at the notes for the proof.

**Rk** Given $f, g \in R[x]$,

$$\deg(fg) \leq \deg(f) + \deg(g)$$

$$fg = c_0(f)\,c_0(g)$$

$$+$$

$$(c_0(f)\,c_1(g) + c_1(f)\,c_0(g))\,X^1$$

$$+$$

$$\vdots$$

$$+$$

$$c_{\deg(f)} \cdot c_{\deg(g)}\,X^{\deg(f)+\deg(g)}$$

when

$$f = \sum c_n(f)\,X^n$$

$$g = \sum c_n(g)\,X^n$$

$$* \deg(fg) = \deg(f) + \deg(g)$$

only if $C_{\deg(f)} \cdot C_{\deg(g)} \neq 0$

in $R$.

$R = \mathbb{Z}_6$

$f = [2]X + [1]$ of degree 1

$g = [3]X + [2]$ of degree 1.

$$fg = ([2]X + [1])([3]X + [2])$$

$$= [2][3]X^2 + [2][2]X$$

$$+ [1][3]X + [1][2]$$

$$= [6]x^2 + ([4]+[3])x + [2]$$

$$= [0]x^2 + [1]x + [2].$$

The degree of $fg$ is just $1$,

i.e. $\deg(fg) < \deg(f) + \deg(g)$.

This happens because even if $a, b \in R$ are both non-zero, its product $ab$ might be $0_R$

## Non-examinable remark

A commutative ring $(R, +, \times)$

which satisfies the property:

if $\forall a, b \in R$

& $a \neq 0_R$, $b \neq 0_R$

then $ab \neq 0_R$

is called an integral domain.

Example $\mathbb{Z}$, any field.

If $R$ is an integral domain

$$\deg(fg) = \deg(f) + \deg(g)$$

always holds.

It is for this reason we will

focus on $F[x]$

the ring of polynomials in $X$

with coefficients in a field $F$.

Prop 27 Let $(F, +, \times)$ be a field.

The units $F[x]^\times$ of $F[x]$

are $F^\times = F - \{0\}$

Hint If $f$ is a unit in $F[x]$,

then $\exists$ $g \in F[x]$

s.t.

$$fg = gf = 1_F$$

the identity element

cf $(F-\{0\}, \times)$

where $1_F = 0X^n + 0X^{n-1} + \cdots + 0 \cdot X + 1_F$

<u>Pf</u> Let $f$ be a unit in $F[x]$.

By definition, $\exists\, g \in F[x]$

s.t. $fg = gf = 1$.

$$\deg(fg) = \deg(1) = 0$$

$\shortparallel \Leftarrow$ by the remark above.

$\deg(f) + \deg(g)$

$$\Rightarrow \quad \deg(f) = \deg(g) = 0$$

i.e. $f = c$ for some

$c \in F \setminus \{0\}$

by Prop 16.

More precisely

if $f = c = 0$, then

$$f \cdot g = 0 \neq 1$$

in $F$. Hence $c \neq 0$

$\square$

# Theorem 28

Division algorithm in $F[x]$.

Recall from Week 1,

given $a \in \mathbb{Z}$

& $b \in$ $b > 0$,

we saw that there exist

$q, r \in \mathbb{Z}$

$0 \le r < b$

s.t. $a = bq + r$

Let $F$ be a field

& $f, g \in F[x]$

$\neq$

$0$

Then there exist $q, r \in F[x]$

s.t. $f = g \cdot q + r$

where either $r = 0$

or $\deg(r) < \deg(g)$

$(r \neq 0)$ (analogue of $r < b$)

above.

Example

① $f = x^4 + 2x^3 + x^2 - 4$

$g = x^3 - 1$ in $\mathbb{Q}[x]$.

what are $q$ & $r$?

$q = x + 2$

$r = x^2 + x - 2$

② $f = x^2 + x - 2 = (x+1)(x-2)$

$g = 3x - 3$ in $\mathbb{Q}[x]$.

what are $q$ & $r$?

$$x + 2 \in q$$

$$x^3 - 1 \overline{\smash{)}\, x^4 + 2x^3 + x^2 - 4}$$

$$x^4 - x$$

$$2x^3 + x^2 + x - 4$$

$$2x^3 - 2$$

$$x^2 + x - 2$$

$r$

$$\deg(r) = 2$$

$$< \deg(g) = \deg(x^3 - 1)$$

$$= 3.$$

$$\frac{1}{3}x + \frac{2}{3} \leftarrow q$$

$$3x - 3 \,\overline{)\, x^2 + x - 2}$$

$$x^2 - x$$

$$2x - 2$$

$$2x - 2$$

$$r \nearrow 0$$

If you remembered that the division algorithm for $\mathbb{Z}$ was the key ingredient for

Euclid's algorithm for $\mathbb{Z}$,

it's possible to imagine that Theorem 28

can be used to do Euclid's algorithm

for $F[x]$

<u>Def</u> $f, g \in F[x]$

We say that $g$ divides $f$

(or $g$ is a factor of $f$)

if $\exists\, q \in F[x]$

s.t. $f = g \cdot q$

$(= q \cdot g)$

<u>Rk</u> $x^2+1$ in $\mathbb{Q}[x]$

There is no polynomial that divides this poly.

If $f$ was a polynomial dividing

$x^2+1$,

then $f = ax+b$

& $\exists\ g = cx+d$ s.t.

$(ax+b)(cx+d)$

$\shortparallel$

$x^2+1$.

Just check that there are no

$a, b, c, d \in \mathbb{Q}$

that satisfy

On the other hand,

$$x^2+1 \quad \text{in} \quad \mathbb{C}[x]$$

has two factors.

$$x^2+1=(x+\sqrt{-1})(x-\sqrt{-1})$$

so there are polynomials of degree 1 that divide $x^2+1$.

Division of polynomials depend on the coefficient field.

Rk In this example,

$$\frac{1}{2}\left(x+\sqrt{-1}\right)$$

$$10^{100}\left(x+\sqrt{-1}\right)$$

$$\vdots$$

all divide $x^2+1$.

because

$$\frac{1}{2}\left(x+\sqrt{-1}\right)\cdot 2\left(x-\sqrt{-1}\right)$$

$$\frac{1}{2}x+\frac{\sqrt{-1}}{2} \qquad \mathbb{C} \qquad\qquad 2x-2\sqrt{-1} \qquad \mathbb{C}$$

For that matter, for any

$$c \in \mathbb{C} - \{0\},$$

$$c(x + \sqrt{-1}) \text{ divides } x^2 + 1$$

because

$$c(x + \sqrt{-1}) \cdot \frac{1}{c}(x - \sqrt{-1})$$

$$= x^2 + 1.$$

The units $F[x]^\times = F^\times$

come into the picture

more prominently

than before