The second assessment is to be uploaded onto QMplus on 04/04

with deadline

15/04

11 am

as before.

Hand your work in at Maths office.

Last Monday

$(R, +, \times)$ a ring

Theorem 25 $R[x]$ is a ring.

If R is a ring with identity, so is $R[x]$

$\exists\, 1 \in R$

s.t.

$1 \cdot a = a \cdot 1$

$= a$

$\forall a \in R$

If R is commutative, so is $R[x]$

$\forall a, b$

$ab = ba$

Rk I should have mentioned

that $\underset{\shortparallel}{0}$ does not have

$$\cdots 0_R X^n + 0_R X^{n-1} + \cdots + 0_R$$

a well-defined notion of degree.

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

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

holds only if R is

"a ring with no zero divisors"

(integral domain)

For this reason, we will only consider $F[x]$

the identity element w.r.t. $\times$

$=$ the set of polynomial with coeffts in a field $(F, +, \times)$

Prop 27

$F[x]^{\times}$

$\cdots 0x^n + \cdots + 0 \cdot x + 1_F$

$\shortparallel$

1

$\shortparallel$

$g \cdot f$

$\shortparallel$

the subset of units in $F[x]$

$\shortparallel$

$\{ f \in F[x] \mid \exists g \text{ s.t. } f \cdot g = 1 \}$

Theorem 28 (Division algorithm for $F[x]$)

$f, g \in F[x]$, $g \neq 0$. Then there exist $q, r \in F[x]$

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

where r is either 0

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

Pf Please look at the typed-up notes.

Def $f, g \in F[x]$.

We say that g divides f

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

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

Rk

- f divides f

$$f = 1 \cdot f$$

the 1-polynomial

- If $c \in F^\times = F - \{0\}$

cf divides f because $f = (cf)(c^{-1}f)$

$\shortparallel$

$$\parallel$$

$$c \cdot c_n(f) x^n + c \cdot c_{n-1}(f) x^{n-1} + \cdots + c \cdot c_1(f) x$$

$$+ c \cdot c_0(f)$$

if $f = c_n(f) x^n + \cdots + c_1(f) x + c_0(f)$

- If g divides f,

then cg also divides f.

$c \in F^\times = F - \{0\}$.

If g divides f, then, $\exists q$ s.t.

$f = g \cdot q$

$\exists\ f = (cg)(c^{-1}g)$

"c^{-1}" makes sense because $c \in F - \{0\}$ and has multiplicate inverse.

Rk

These are all because the units of $F[x]$ are $F^\times = F - \{0\}$.

Examples

- no polynomial divides x^2+1 in $\mathbb{Q}[x]$.

Not true!

In fact x^2+1

$$c(x^2+1) \quad \forall\, c \in \mathbb{Q}-\{0\}$$

c (because

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

all divide x^2+1.

What I meant was that

no polynomial of degree 1 in $\mathbb{Q}[x]$

Indeed, if there were,

then

$$x^2+1 = (x+a)(x+b)$$

$a, b \in \mathbb{Q}$.

$$= x^2 + (a+b)x + ab$$

$a+b=0 \quad \cdots (*)$

$ab = 1 \quad \cdots (**)$

$(*) \Rightarrow b = -a$

Plugging this into $(**)$,

$$a \cdot (-a) = 1$$

$$\Rightarrow \; -a^2 = 1.$$

However $\quad -a^2 \leq 0$

This is a contradiction!

Therefore, x^2+1 is NOT a product of degree 1 polynomials in $\mathbb{Q}[x]$

- x^2+1 is in fact a product of degree 1 polynomials in $\mathbb{C}[x]$

Indeed,

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

$\mathbb{C}[x] \quad \mathbb{C}[x].$

- $x^2 + 1$ is also divisible

$\mathbb{F}_2[x].$

$\mathbb{Z}_2$

$x^2 + [1] \in \mathbb{F}_2[x].$

$\mathbb{F}_2 = \{[0], [1]\}.$

additive identity

multiplicative identity

$$(X + [1])(X - [1])$$

$$= X^2 + [1]X - [1]X - [1]^2$$

$$= X^2 - [1]$$

because

$$= X^2 + [1] \qquad [-1]_2 = [1]_2$$

$$\quad = -[1]_2$$

Cor 29

Let F be a field

$\alpha \in F$

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

s.t. $f = (X-\alpha)q + r$

Pf $g = (X-\alpha)$

$\deg(r) < \deg(x-\alpha) = 1$

$\Rightarrow \deg(r) = 0$

$\Rightarrow$ r is a non-zero element in F. $\square$

Cor 30 F : a field

$\alpha \in F$

Then the remainder of $f \in F[x]$

when divided by $x-\alpha$ is $f(\alpha)$

In particular,

$$f(\alpha)=0 \iff x-\alpha \text{ divides } f(x).$$

Pf: See the notes.

$\{[0],[1],\cdots,[6]\} = \mathbb{Z}_7 = \mathbb{F}_7$

Examples

Consider $f(x) = x^2+3 \in \mathbb{F}_7[x]$.

$$= x^2+[3]_7$$

Claim: $X - [2]_7$ divides $X^2 + 3$ in $\mathbb{F}_7[X]$.

By Corollary 30, all we need to check is $f([2]_7) = [0]$.

Indeed, $f([2]) = [2]^2 + [3]$

$= [2 \cdot 2] + [3]$

$= [4] + [3] = [7]$

$= [0]$.

Similarly,

$x + [2]$ also divides

$x^2 + 3$

in $\mathbb{F}_7[x]$.

Need to check

$$f(-[2]) = [0].$$

$$\shortparallel$$

$$[-2]$$

- No degree 1 polynomial divides x^2+2 in $\mathbb{F}_5[x]$.