GTLA Lecture 28.08.2020

Let $\mathbb{F}$ be a field. Let $n \in \mathbb{Z}_{>0}$

Number systems

integers	$\mathbb{Z}$
polynomials with coefficients in $\mathbb{F}$	$\mathbb{F}[x]$
$n \times n$ matrices with entries in $\mathbb{F}$	$M_n(\mathbb{F})$

Define addition and mult in $\mathbb{Z}$

. . . .

Define addition and mult in $\mathbb{F}[x]$.

. . .

If $a(x) = a_0 + a_1 x + \cdots + a_k x^k$

and $b(x) = b_0 + b_1 x + \cdots + b_\ell x^\ell$

then $a(x)b(x) = c(x)$ where

$c(x) = c_0 + c_1 x + \cdots + c_{k+\ell} x^{k+\ell}$

with $c_j = a_0 b_j + a_1 b_{j-1} + \cdots + a_j b_0$.

Define addition and mult. in $M_n(\mathbb{F})$.

Theorem $\mathbb{Z}$ is a commutative ring.

Theorem $\mathbb{F}[x]$ is a commutative ring.

Theorem $M_n(\mathbb{F})$ is a noncommutative ring.

Multiples

$$m\mathbb{Z} = \{\ldots, -3m, -2m, -m, 0, m, 2m, 3m, \ldots\}$$

Since $m\mathbb{Z} = (-m)\mathbb{Z}$ then we can index multiples in $\mathbb{Z}$ by

$$m \in \mathbb{Z}_{\geq 0}.$$

Let $m(x) \in \mathbb{F}[x]$. The multiples of $m(x)$ are

$$m(x)\mathbb{F}[x] = \{m(x)k(x) \mid k(x) \in \mathbb{F}[x]\}.$$

Proposition Multiples in $\mathbb{F}[x]$ are indexed by monic polynomials

$$m(x) = x^k + c_{k-1}x^{k-1} + \cdots + c_1 x + c_0.$$

__Theorem__ Euclidean Algorithm for $\mathbb{F}[x]$.

Let $d = \deg(m(x))$

Let $a(x) \in \mathbb{F}[x]$ and $m(x)$ a monic polynomial. Then there exist unique $q(x) \in \mathbb{F}[x]$ and $r(x) \in \mathbb{F}[x]$ such that

$$a(x) = q(x)m(x) + r(x)$$

with $\deg(r(x)) < d$.

a sense of ordering!

Let $p(x), q(x) \in \mathbb{F}[x]$.

The __gcd__ of $p(x)$ and $q(x)$ is the monic polynomial $\ell(x)$ such that

$$\ell(x)\mathbb{F}[x] = p(x)\mathbb{F}[x] + q(x)\mathbb{F}[x].$$

The __lcm__ of $p(x)$ and $q(x)$ is the monic polynomial $m(x)$ such that

$$m(x)\mathbb{F}[x] = p(x)\mathbb{F}[x] \cap q(x)\mathbb{F}[x].$$

The polynomials $p(x)$ and $q(x)$ are <u>relatively prime</u> if

$$\gcd(p(x), q(x)) = 1.$$

If $p(x)$ and $q(x)$ are relatively prime then

$$\gcd(p(x), q(x)) = 1$$

and so there exist $r(x), s(x) \in F[x]$ such that

$$1 = p(x)r(x) + q(x)s(x).$$

<u>Example</u> $p(x) = (x-5)^3$

$q(x) = (x-3)^7.$

$$\left(m_{J_3(5)}(x) = (x-5)^3 \qquad J_3(5) = \begin{pmatrix} 5 & 1 & 0 \\ 0 & 5 & 1 \\ 0 & 0 & 5 \end{pmatrix} \right)$$

Find $r(x)$ and $s(x)$ so that

$$1 = p(x)r(x) + q(x)s(x).$$

~~By inspection,~~ Clearly,

$$r(x) = \frac{-14}{256}x^6 + \frac{231}{256}x^5 - \frac{1605}{256}x^4 + \frac{5999}{256}x^3$$

$$-\frac{12648}{256}x^2 + \frac{14307}{256}x - \frac{6777}{256},$$

and

$$s(x) = \frac{14}{256}x^2 - \frac{147}{256}x + \frac{387}{256}.$$

To get $a = mq + r$;

$\quad$ let $q = \max(m\mathbb{Z} \cap \mathbb{Z}_{\le a})$

$\quad\quad r = a - mq$.

Let A and M be rings (so they each have addition and multiplication.

A <u>ring homomorphism from A to M</u> is a function

$$f : A \to M \text{ such that}$$

(a) If $a_1, a_2 \in A$ then
$$f(a_1 + a_2) = f(a_1) + f(a_2)$$

(b) If $a_1, a_2 \in A$ then
$$f(a_1 a_2) = f(a_1) f(a_2)$$

(c) $f(1) = 1$.

<u>Example</u> Let $\mathbb{F}$ be a field and $n \geq 0$ and $A \in M_n(\mathbb{F})$.
The <u>evaluation homomorphism</u> is

$$ev_A : \mathbb{F}[x] \longrightarrow M_n(\mathbb{F}),$$

$$a_0 + a_1 x + \cdots + a_k x^k \longmapsto a_0 + a_1 A + \cdots + a_k A^k.$$

<u>Proposition</u> ev_A is a ring homomorphism.

$$ev_A(p(x)q(x)) = ev_A(p(x)) \cdot ev_A(q(x))$$

and $ev_A(p(x)+q(x)) = ev_A(p(x)) + ev_A(q(x))$.

Many authors write

$$p(A) = ev_A(p(x)).$$

Let

$$\ker(ev_A) = \{p(x) \in \mathbb{F}[x] \mid ev_A(p(x)) = 0\}$$

<u>Proposition</u> Let $m_A(x)$ be the min. poly of A. Then $\boxed{\ker(ev_A) = \underline{m_A}(x)\mathbb{F}[x]}$

"$m_A(x)$ is the smallest polynomial such that $m_A(A) = 0$".

Our example $p(x) = (x-5)^3$

$$q(x) = (x-3)^7$$

We found $r(x)$ and $s(x)$ such that

$$p(x)r(x) + q(x)s(x) = 1.$$

$$A = \left(\begin{array}{ccc|ccccccc} 5 & 1 & 0 & & & & & & & \\ 0 & 5 & 1 & & & & 0 & & & \\ 0 & 0 & 5 & & & & & & & \\ \hline & & & 3 & 1 & & & & & \\ & & & & 3 & 1 & & & 0 & \\ & & & & & 3 & 1 & & & \\ & 0 & & & & & 3 & 1 & & \\ & & & & 0 & & & 3 & 1 & \\ & & & & & & & & 3 & 1 \\ & & & & & & & & & 3 \end{array}\right)$$

Then $m_A(x) = p(x)q(x) = (x-5)^3(x-3)^7$.

Then

$$ev_A(q(x)s(x)) = \overset{q(A)s(A)}{\cancel{p(A)r(A)}}$$

$$= \left(\begin{array}{ccc|ccc} 1 & & 0 & & & \\ 0 & 1 & & & 0 & \\ & & 1 & & & \\ \hline & & & 0 & & \\ & 0 & & & \ddots & 0 \\ & & & 0 & & 0 \end{array}\right)$$

$$ev_A(q(x)s(x)) = q(A)s(A)$$

$$= \left(\begin{array}{c|c} \begin{matrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{matrix} & 0 \\ \hline 0 & \begin{matrix} 1 & & 0 \\ & 1 & \\ & & \ddots & \\ 0 & & & 1 \end{matrix} \end{array}\right)$$

BLOWS MY MIND.

This is the block decomposition theorem