28.07.2020
GTLA Lecture 1

Number systems

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

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

Define multiplication in $\mathbb{F}[x]$ by

$$a(x)b(x) = c_0 + c_1 x + \cdots + c_{k+l} x^{k+l}$$

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

$a(x) = a_0 + a_1 x + \cdots + a_k x^k$ and
$b(x) = b_0 + b_1 x + \cdots + b_l x^l$.

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

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

Since $m\mathbb{Z} = (-m)\mathbb{Z}$ multiples in $\mathbb{Z}$ are indexed by $m \in \mathbb{Z}_{\geq 0}$.

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

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

<u>Theorem</u> Euclidean Algorithm for $\mathbb{F}[x]$.

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

$$a(x) = q(x)m(x) + r(x) \text{ and } \deg(r(x)) \in \{0, 1, \ldots, d-1\}.$$

Let $a(x), b(x) \in \mathbb{F}[x]$. The <u>gcd</u> of $a(x)$ and $b(x)$ is the monic polynomial $l(x)$ such that

$$l(x)\mathbb{F}[x] = a(x)\mathbb{F}[x] + b(x)\mathbb{F}[x].$$

The <u>lcm</u> of $a(x)$ and $b(x)$ is the monic polynomial $m(x)$ such that

$$m(x)\mathbb{F}[x] = a(x)\mathbb{F}[x] \cap b(x)\mathbb{F}[x].$$

The polynomials $a(x)$ and $b(x)$ are <u>relatively prime</u> if

$$\gcd(a(x), b(x)) = 1.$$

<u>Example</u> Let $a(x) = (x-5)^3$ and $b(x) = (x-3)^7$ in $\mathbb{C}[x]$. Then

$$\gcd(a(x), b(x)) = 1$$

and so there exist polynomials $r(x)$ and $s(x)$ such that

$$1 = a(x)\, r(x) + b(x)\, s(x).$$

By inspection,

$$r(x) = \frac{-14}{256}x^6 + \frac{231}{256}x^5 - \frac{1605}{256}x^4 + \frac{5990}{256}x^3 - \frac{12648}{256}x^2 + \frac{14307}{256}x - \frac{6773}{256}$$

and

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

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

A <u>ring homomorphism</u> <u>from A to M</u> is a function $f : A \to M$ 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 ~~$a \in \mathbb{Z}_{70}$~~ and $A \in M_n(\mathbb{F})$.

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

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

<u>Proposition</u> ev_A is a ring homomorphism from $\mathbb{F}[x] \to M_n(\mathbb{F})$.

Proposition
Let $m_A(x)$ be the minimal polynomial of A. Let

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

Then

$$\ker(ev_A) = m_A(x)\mathbb{F}[x].$$

Theorem (Cayley-Hamilton) Let $n \in \mathbb{Z}_{>0}$ and let $A \in M_n(\mathbb{F})$. Then

$$\det(x - A) \in \ker(ev_A).$$

Theorem Let $n \in \mathbb{Z}_{>0}$ and $A \in M_n(\mathbb{F})$.
Let $m_A(x)$ be the minimal polynomial of A.
Assume $m_A(x) = p(x)q(x)$ with $\gcd(p(x), q(x)) = 1$.
Write

$$1 = p(x)r(x) + q(x)s(x) \text{ and let}$$

$P_U = ev_A(p(x)r(x))$ and $P_W = ev_A(q(x)s(x))$.
Define $V = \mathbb{F}^n$, $U = P_U \cdot \mathbb{F}^n$, $W = P_W \cdot \mathbb{F}^n$.
Then

$$V = U \oplus W.$$

The same thing said a different way.

Let

$$A = J_3(5) \oplus J_7(3) = \left(\begin{array}{c|c} \begin{matrix} 5 & 1 & 0 \\ 0 & 5 & 1 \\ 0 & 0 & 5 \end{matrix} & 0 \\ \hline 0 & \begin{matrix} 3 & 1 & & & & & \\ & 3 & 1 & & & 0 & \\ & & 3 & 1 & & & \\ & & & 3 & 1 & & \\ & & & & 3 & 1 & \\ & 0 & & & & 3 & 1 \\ & & & & & & 3 \end{matrix} \end{array}\right)$$

Then

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

and

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

Note

$$m_{J_3(5)}(x) = (x-5)^3 = p(x)$$

$$m_{J_7(3)}(x) = (x-3)^7 = q(x)$$

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