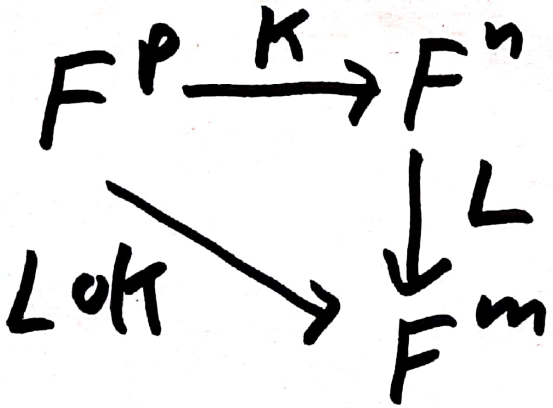
Since for each choice of $m, n \geq 1$ there is a different map, $\mathcal{L}$ should carry the labels $\mathcal{L}_n^m : F_n^m \to \mathrm{Lin}(F^n, F^m)$. We also have $\mathcal{L}_p^n : F_p^n \to \mathrm{Lin}(F^p, F^n)$ and $\mathcal{L}_p^m : F_p^m \to \mathrm{Lin}(F^p, F^m)$. Composition gives

$$\circ : \mathrm{Lin}(F^p, F^n) \times \mathrm{Lin}(F^n, F^m) \to \mathrm{Lin}(F^p, F^m)$$

by

$$(K, L) \longmapsto L \circ K$$



Matrix multiplication is the map

$\cdot : F_n^m \times F_p^n \longrightarrow F_p^m$ by

$(A, B) \longmapsto AB$

and the related diagram

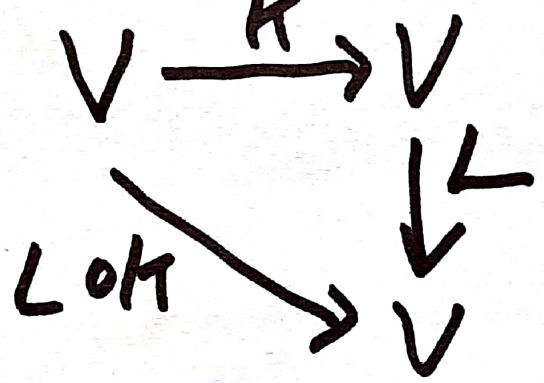
$$\begin{array}{ccc} F^p & \xrightarrow{L_B} & F^n \\ & \searrow^{L_{AB}=L_A \circ L_B} & \downarrow L_A \\ & & F^m \end{array}$$

which gives all linear maps as $A \in F_n^m$ varies, $B \in F_p^n$ varies.

Get:

$$\begin{array}{ccc} F_n^m \times F_p^n & \xrightarrow{\cdot} & F_p^m \\ (A, B) & \longmapsto & AB \\ \downarrow \mathcal{L}_n^m \times \mathcal{L}_p^n & & \downarrow \mathcal{L}_p^m \\ \mathrm{Lin}(F^n, F^m) \times \mathrm{Lin}(F^p, F^n) & \longrightarrow & \mathrm{Lin}(F^p, F^m) \\ (L_A, L_B) & & L_{AB} = L_A \circ L_B \end{array}$$

Let's look closer at the special case $U = Lin(V,V) = End(V) = \{L : V \to V \mid L \text{ lin.}\}$ (endomorphisms of V). Under composition $\circ$ U is closed,



and it is not hard to prove this theorem:

Th: $(End(V), +, \circ, O_V^V, I_V)$ is a ring.

Def. A vector space which also has a product, $*$, giving a ring structure under $+$ and $*$ is called an algebra over the field.

EX: $(F_n^n, +, \cdot, O_n^n, I_n)$ is an algebra over F.

Def. Let $F[t] = \left\{ \sum_{i=0}^{m} a_i t^i \;\middle|\; 0 \le m \in \mathbb{Z}, a_i \in F \right\}$ [6]
be the set of all polynomials in variable t with coefficients in field F. With $+$ and the usual scalar mult. $F[t]$ is a vector space over F. With $+$ and mult. of polynomials

$$\left(\sum_{i=0}^{m} a_i t^i\right)\left(\sum_{j=0}^{n} b_j t^j\right) = \sum_{i=0}^{m}\sum_{j=0}^{n} a_i b_j t^{i+j}$$

$$= \sum_{k=0}^{m+n} \left(\sum_{i=0}^{m} a_i b_{k-i}\right) t^k$$

$F[t]$ is a ring, so $F[t]$ is an algebra over F.

Note: The product is commutative in $F[t]$.

We used the familiar exponent notation t^i for $i \geq 0$ without explanation, meaning "repeated multiplication i times". We can be more rigorous by making this formal inductive definition.

Def: Let $(R, +, \cdot, 0, 1)$ be any ring with mult. identity element 1. For $0 \leq n \in \mathbb{Z}$ and any $x \in R$, define x^n recursively by $x^0 = 1$, $x^{n+1} = x^n \cdot x$ for $0 \leq n \in \mathbb{Z}$. Then

$x^1 = x^{0+1} = x^0 \cdot x = 1 \cdot x = x$

$x^2 = x^{1+1} = x^1 \cdot x = x \cdot x$

$x^3 = x^{2+1} = x^2 \cdot x = (x \cdot x) \cdot x$, etc.

Th (Laws of exponents) In ring R we have
(1) $X^m \cdot X^n = X^{m+n}$ $\forall\, 0 \le m,n \in \mathbb{Z}$,
(2) $(X^m)^n = X^{(mn)}$ "
(3) If $X \cdot Y = Y \cdot X$ then $(X \cdot Y)^n = X^n \cdot Y^n$ $\forall\, 0 \le n \in \mathbb{Z}$.

pf. These can be proved by induction on one of the exponents.

In $End(V)$ we now have defined L^m for $L: V \to V$, $0 \le m \in \mathbb{Z}$, and in F_n^n we have defined A^m for any $A \in F_n^n$, $0 \le m \in \mathbb{Z}$.

Def. For $f(t) \in F[t]$, $0 \ne \sum_{i=0}^{m} a_i t^i$ let $f(L) = \sum_{i=0}^{m} a_i L^i \in End(V)$ and $f(A) = \sum_{i=0}^{m} a_i A^i \in F_n^n$.

In these formulas we understand $L^0 = I_V$ and $A^0 = I_n$. It will be convenient to interpret these as "evaluation" of the poly $f(t)$ at $t = L \in End(V)$ or at $t = A \in F_n^n$, but they are actually ring (algebra) homomorphisms:

$Eval_L : F[t] \to End(V)$ and

$Eval_A : F[t] \to F_n^n$ if we include in the definition how to evaluate the zero polynomial $0 = 0t^0 + 0t^1 + \cdots + 0t^m$ (all coefficients $0 \in F$) by letting $0[L] = 0_V^V$ and $0[A] = 0_n^n$. Get $\forall f(t), g(t) \in F[t]$, $\forall A \in F_n^n$, $\forall L \in End(V)$, $\forall \alpha \in F$,

$(f+g)(L) = f(L) + g(L)$, $(f \cdot g)(L) = f(L) \circ g(L)$, $(\alpha f)(L) = \alpha \cdot f(L)$

$(f+g)(A) = f(A)+g(A)$, $(fg)(A) = f(A)\cdot g(A)$, $(\alpha f)(A) = \alpha \cdot f(A)$

that is, $Eval_L$ and $Eval_A$ respect the ring and vectorspace (algebra) structures.

In basic algebra, often try to "solve" poly. equations like $f(t)=0$, find all $t \in F$ s.t. this is true. If $f(t) = \sum_{i=0}^{m} a_i t^i$ and $a_m \neq 0$ we say $\deg(f) = m$. Degree is not defined for the zero poly. Note: $\deg(fg) = \deg(f)+\deg(g)$, $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$, $\deg(\alpha f) = \deg(f)$ for $0 \neq \alpha \in F$.

Call $f(t)$ "monic" when $a_m = 1$ and $\deg(f) = m$. (top nonzero coefficient is 1).

Important fact about $F[t]$:

Th: (Euclidean Algorithm) For any $a(t), b(t) \in F[t]$ with $b(t)$ not the zero poly, $\exists\, q(t), r(t) \in F[t]$ such that $a(t) = q(t)b(t) + r(t)$ and either $r(t) = 0$ or $\deg(r) < \deg(b)$.

Pf. Long division works in $F[t]$. Divide $b(t)$ into $a(t)$, get quotient $q(t)$ and remainder $r(t)$ with stated properties. □

When "solving" a poly. equation $f(t) = 0$ in F, look for "roots", $\alpha \in F$, such that $f(\alpha) = 0$.

Th: $f(\alpha) = 0$ for $\alpha \in F$ iff $f(t) = q(t) \cdot (t - \alpha)$ for some $q(t) \in F[t]$.

pf: ($\Rightarrow$) Apply Euc. Algo. with $a(t) = f(t)$ and $b(t) = t - \alpha$. Get $\exists\, q(t), r(t) \in F[t]$ s.t. $f(t) = q(t)\cdot(t-\alpha) + r(t)$ with $r(t) = 0$ or $\deg(r) < 1$

If $\deg(r) < 1$ then $r(t) = r_0$ must be a <u>constant</u>

so $0 = f(\alpha) = q(\alpha)\cdot(\alpha - \alpha) + r_0 = r_0$ gives contradiction to $r(t)$ not the zero poly. Thus $r(t) = 0$ and $f(t) = q(t)\cdot(t-\alpha)$.

($\Leftarrow$) If $f(t) = q(t)\cdot(t-\alpha)$ then clearly $f(\alpha) = 0$. □

<u>Cor</u>: If $f(t) \in F[t]$ has distinct roots $\alpha_1, \ldots, \alpha_r \in F$ then $\exists\, q(t) \in F[t]$ s.t. $f(t) = q(t)\cdot(t-\alpha_1)\cdots(t-\alpha_r)$

so $r \leq \deg(f)$. Any root of $q(t)$ is a root of $f(t)$, so we can factor out all $(t-\alpha_i)$ from $q(t)$,

and find some $h(t) \in F[t]$ with no roots in F s.t. $f(t) = h(t) \cdot \prod_{i=1}^{r} (t-\alpha_i)^{k_i}$ for some $1 \le k_i \in \mathbb{Z}$ with $\deg(f) = \deg(h) + k_1 + k_2 + \cdots + k_r$.

Def. Say $0 \neq f(t) \in F[t]$ is **irreducible** when $f(t) = g(t) \cdot h(t)$ implies either $\deg(g) = 0$ or $\deg(h) = 0$, that is, $g(t) =$ constant or $h(t) =$ const.

Since $\deg(f) = \deg(g) + \deg(h)$, $f(t)$ irred. means cannot factor $f(t) = g(t)h(t)$ with $\deg(g) < \deg(f)$ and $\deg(h) < \deg(f)$.

Th: Any $f(t) \in F[t]$, not constant poly, factors into a product of irreducible polys to powers

$$f(t) = (f_1(t))^{k_1} \cdots (f_r(t))^{k_r} \text{ for } f_i(t) \text{ irred.}$$

Ex: For $F=\mathbb{C}$, the only irred. polys. are linear, degree $=1$. (Fundamental Th. of Algebra)
For $F=\mathbb{R}$, the only irred. polys are either linear, $f(t)=at+b$, or quadratic, $f(t)=at^2+bt+c$, where $b^2-4ac<0$.
For $F=\mathbb{Q}$, there are lots of interesting higher degree irred. polys. (Study more algebra!)

Suppose $f(t)=(t-\alpha_1)\cdots(t-\alpha_m)$, so $\alpha_1,\ldots,\alpha_m \in F$ are all the roots of $f(t)$ in F.
What does $f(A)=O_n^n$ mean?

$$f(A)=(A-\alpha_1 I_n)\cdot(A-\alpha_2 I_n)\cdots(A-\alpha_m I_n)=O_n^n$$

A product of matrices may be O_n^n even when <u>none</u> of the matrices is O_n^n.

Ex. $A=\begin{bmatrix}1&0\\0&2\end{bmatrix}$, $f(t)=(t-1)(t-2)$

$$f(A)=\left(\begin{bmatrix}1&0\\0&2\end{bmatrix}-1\begin{bmatrix}1&0\\0&1\end{bmatrix}\right)\left(\begin{bmatrix}1&0\\0&2\end{bmatrix}-2\begin{bmatrix}1&0\\0&1\end{bmatrix}\right)$$

$$=\begin{bmatrix}0&0\\0&1\end{bmatrix}\begin{bmatrix}-1&0\\0&0\end{bmatrix}=\begin{bmatrix}0&0\\0&0\end{bmatrix}=O_2^2.$$

Ex. $A=\begin{bmatrix}1&1\\1&1\end{bmatrix}$, $f(t)=t(t-2)$

$$f(A)=A(A-2I_2)=\begin{bmatrix}1&1\\1&1\end{bmatrix}\begin{bmatrix}-1&1\\1&-1\end{bmatrix}=\begin{bmatrix}0&0\\0&0\end{bmatrix}$$

Questions: ① Given $A\in F_n^n$, find all polys. $f(t)$ such that $f(A)=O_n^n$, "satisfied" by A

② Is there an easy-to-find poly. satisfied by A?

③ Is there a poly of minimal degree " " "?

Hint: For the two examples above, look at

$$\det\left(\begin{bmatrix}t&0\\0&t\end{bmatrix}-A\right)=\det(tI_2-A)$$ using 2×2 det formula.