ADVANCED TOPICS IN ALGEBRA

LECTURE 5

(lecture and problems to solve)

2020/21

DECOMPOSITION OF SPACE INTO CYCLIC SPACES

We shall prove a theorem about decomposition of a space into cyclic spaces, given a linear mapping f of the space into itself. Namely, we shall prove the existence of a basis in which the space is a direct sum of special cyclic spaces. This corresponds to existence of a matrix B (changing the basis) such that $B^{-1}FB$ has a special diagonal blocks form (a *Jordan matrix*), where F is a matrix of f in some basis.

Theorem 28. Let V be a linear space of finite dimension and let $f : V \to V$ be a linear mapping. Then the space V can be decomposed into a direct sum of cyclic spaces

$$V = V_1 \oplus V_2 \oplus \ldots \oplus V_m,$$

$$\phi_{V_{i+1}}(x) | \phi_{V_i}(x),$$

and

$$\phi_{V_1}(x) = \phi_V(x).$$

Proof. We shall prove the theorem by induction with respect to $n = \dim(V)$.

If $n = 1$ the conclusion holds trivially.

Now assume that the theorem is true for all $k < n$. Let $\boldsymbol{v}$ be a vector whose annihilator $\phi_1(x)$ is equal to the annihilator ϕ_V of the whole space V. Let us denote the cyclic space generated by $\boldsymbol{v}$ by V_1.

We have $\dim(V/V_1) < \dim(V)$. We consider now the space V/V_1 and the linear mapping $f^{(V_1)} : V/V_1 \to V/V_1$ given (recall) by the formula:

$$f^{(V_1)}([\boldsymbol{v}]_{V_1}) = [f(\boldsymbol{v})]_{V_1}.$$

By our induction hypothesis the conclusion of the theorem holds for the the space V/V_1 and the linear mapping $f^{(V_1)}$. Let

$$V/V_1 = S_2 \oplus S_3 \oplus ... \oplus S_m,$$

where S_i are cyclic subspaces of V/V_1.

Let $[\boldsymbol{s_i}]_{V_1}$ be a generator of the cyclic space S_i. Let $\phi_i(x)$ be the annihilator of $[\boldsymbol{s_i}]_{V_1}$. We shall show that there exists $\boldsymbol{s'_i} \in [\boldsymbol{s_i}]_{V_1}$ whose annihilator is $\phi_i(x)$. Because $\phi_i(x)$ is the annihilator of $[\boldsymbol{s_i}]_{V_1}$, we have

$$\phi_i(f^{(V_1)}([\boldsymbol{s_i}]_{V_1}) = [\phi(f)(\boldsymbol{s_i})]_{V_1} = [\boldsymbol{0}]_{V_1} = V_1.$$

Hence $\phi(f)(\boldsymbol{s_i}) \in V_1$. As all elements of V_1 (which is a cyclic space w.r.t. f) are of the form $\gamma(f)(\boldsymbol{v})$, where $\gamma(x)$ is some polynomial, we have

$$\phi_i(f)(\boldsymbol{s_i}) = \gamma(f)(\boldsymbol{v}),$$

for some polynomial $\gamma(x)$. By our induction assumption $\phi_i(x)$ divides $\phi(x)$, hence

$$\phi(x) = \delta(x)\phi_i(x).$$

Thus we have

$$\delta(f)\gamma(f)(\boldsymbol{v}) = \delta(f)\phi_i(f)(\boldsymbol{s_i}) = \phi(f)(\boldsymbol{s_i}) = \mathbf{0}.$$

This implies that

$$\delta(x)\phi_i(x) = \phi(x)|\delta(x)\gamma(x),$$

and we obtain

$$\phi_i(x)|\gamma(x).$$

Therefore

$$\gamma(x) = \phi_i(x)\vartheta(x)$$

for some polynomial $\vartheta(x)$. Because $\phi_i(f)(\boldsymbol{s_i}) = \gamma(f)(\boldsymbol{v})$, we have

$$\phi_i(f)(\boldsymbol{s_i} - \vartheta(f)(\boldsymbol{v})) = \mathbf{0}).$$

Set

$$\boldsymbol{s'_i} := \boldsymbol{s_i} - \vartheta(f)(\boldsymbol{v}).$$

Assume that the annihilator $\rho(x)$ of $\boldsymbol{s'_i}$ is of smaller degree than the degree of ϕ_i. Then we would get

$$\rho(f^{(V_1)}([\boldsymbol{s_i}]_{V_1}) = [\rho(f)(\boldsymbol{s'_i}) + \vartheta(f)(\boldsymbol{v})]_{V_1} = [\rho(f)(\boldsymbol{s'_i})]_{V_1} + [\vartheta(f)(\boldsymbol{v})]_{V_1} = [\mathbf{0}]_{V_1},$$

$$\big(\text{here we use } \boldsymbol{v} \in V_1\text{; hence } \vartheta(f)(\boldsymbol{v}) \in V_1 \text{ which implies } [\vartheta(f)(\boldsymbol{v})]_{V_1} = [0]_{V_1}\big)$$

but this condradicts the fact that the annihilator of $[\boldsymbol{s_i}]_{V_1}$ (w.r.t. $f^{(V_1)}$) is ϕ_i. Thus we have proved that the annihilator of $\boldsymbol{s'_i}$ is ϕ_i. Of course, we also have $[\boldsymbol{s'_i}]_{V_1} = [\boldsymbol{s_i}]_{V_1}$ and

$$V/V_i = \Gamma(f^{(V_1)}, [\boldsymbol{s'_i}]_{V_1}).$$

For every vector $\boldsymbol{w}$ of V :

$$[\boldsymbol{w}]_{V_1} = \xi_2(f^{(V_1)})([\boldsymbol{s'_2}]_{V_1}) + \ldots + \xi_m(f^{(V_1)})([\boldsymbol{s'_m}]_{V_1})$$

for some polynomials ξ_i, $2 \leqslant i \leqslant m$ (because $S_2, \ldots, S_m$ are cyclic spaces with generators $[(\boldsymbol{s'_2}]$,...,$[(\boldsymbol{s'_m}]$, respectively). Hence for some $w_1 \in V_1$

$$\boldsymbol{w} = \boldsymbol{w_1} + \xi_2(f)(\boldsymbol{s'_2}) + \ldots + \xi_m(f)(\boldsymbol{s'_m}). \tag{1}$$

Thus we can represent $\boldsymbol{w}$ as a linear combination of vectors from the bases of the spaces V_1, $\Gamma(f, \boldsymbol{s'_2}), \ldots, \Gamma(f, \boldsymbol{s'_m})$. We have

$$\dim(V) = \dim(V_1) + \dim(V/V_1) = \dim(V_1) + \dim(S_2 \oplus \ldots \oplus S_m) =$$
$$\dim(V_1) + \dim(\Gamma(f^{(V_1)}, [\boldsymbol{s'_2}])) + \ldots + +\dim(\Gamma(f^{(V_1)}, [\boldsymbol{s'_m}])) =$$
$$\dim(V_1) + \deg(\phi_2(x)) + \ldots + \deg(\phi_m(x)) =$$
$$\dim(V_1) + \dim(\Gamma(f, \boldsymbol{s'_2})) + \ldots + \dim(\Gamma(f, \boldsymbol{s'_m})).$$

Hence the sum of the bases of the spaces V_1 and $\Gamma(f, \boldsymbol{s'_i})$, $2 \leqslant i \leqslant m$ is a basis of the space V, for otherwise, in view of (1) we would have $\dim(V) > \dim(V_1) + \dim(\Gamma(f, \boldsymbol{s'_2})) + \ldots + \dim(\Gamma(f, \boldsymbol{s'_m}))$. From this we obtain

$$V = V_1 \oplus \Gamma(f, \boldsymbol{s'_2}) \oplus \ldots \oplus \Gamma(f, \boldsymbol{s'_m}).$$

□

From the above theorem we derive as a corollary the following theorem about a decomposition of a linear space into irreducible cyclic factors.

Theorem 29. Let V be a linear space of finite dimension and let $f : V \to V$ be a linear mapping. Then the space V can be decomposed into a direct sum of cyclic spaces

$$V = V_1^{(1)} \oplus \ldots \oplus V_{n_1}^{(1)} \oplus V_1^{(2)} \oplus \ldots \oplus V_{n_2}^{(2)} \oplus \ldots \oplus V_1^{(k)} \oplus \ldots \oplus V_{n_k}^{(k)},$$

where the spaces $V_j^{(i)}$ is are not further reducible and the annihilator of $V_j^{(i)}$ is $\psi_i^{r(i,j)}(x)$, where $\psi_i(x)$ is a prime polynomial and $r(i,j) > 0$.

Proof. Let

$$V = V_1 \oplus V_2 \oplus \ldots \oplus V_m$$

be the decomposition of V into cyclic spaces from Theorem 28.

$$\phi_i(x) = \psi_1^{r(i,1)}(x) \cdot \psi_2^{r(i,2)}(x) \ldots \cdot \psi_k^{r(i,k)}(x).$$

Because $\phi_{i+1}(x) | \phi_i(x)$ we have $r(i,j) \geqslant r(i+1,j)$. Of course, for some i we may have $r(i,j) = 0$. Therefore let n_j be the maximal i such that $r(i,j) > 0$.

By Theorem 23 every space V_i can be expressed as a direct sum of cyclic spaces whose annihilators are $\psi_j^{r(i,j)}$. Regrouping the summands of the direct sums giving the spaces V_i we obtain the conclusion.

□

Theorem 30. Each linear mapping $f : V \to V$ from a finite dimensional linear space V to itself has in some basis a matrix representation

$$F = \begin{bmatrix} B_1 & & & \\ & B_2 & & \\ & & \ldots & \\ & & & B_r \end{bmatrix}. \tag{2}$$

for some r, where all blocks B_i have the form

$$\begin{bmatrix} 0 & & & & -a_0 \\ 1 & 0 & & & -a_1 \\ & 1 & & & -a_2 \\ & & & & \vdots \\ & & & 0 & -a_{p-2} \\ & & & 1 & -a_{p-1} \end{bmatrix}.$$

Proof. Let

$$V = V_1 \oplus \ldots \oplus V_m$$

be the decomposition of V into a direct sum of cyclic spaces from Theorem 28.

Let $x^{p_i} + a_{p_i-1}^{(i)} x^{p_i-1} + \ldots + a_1^{(i)} x + a_0^{(i)}$ be the annihilator of the cyclic space space V_i. Let $\boldsymbol{v_i}$ be a generator of V_i. Then the vectors $\boldsymbol{v_i}$, $f(\boldsymbol{v_i}), \ldots, f^{p_i-1}\boldsymbol{v_i}$ are linearly independent (for otherwise there would be a polynomial of degree smaller than p_i annihilating $\boldsymbol{v_i}$.) Then the matrix of the mapping f on the space V_i in the basis

$$\mathcal{B}_i = \langle \boldsymbol{v_i}, f(\boldsymbol{v_i}), \ldots, f^{p_i-1}\boldsymbol{v_i} \rangle$$

consists of columns that are representations of the images of the vectors from the basis in the same basis:

$$f(v_i) = \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, f(f(v_i)) = f^2 \begin{bmatrix} 0 \\ 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix}, \dots f(f^{p_i-2}(v_i)) = f^{p_i-1} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix}, f(f^{p_i-1}(v_i)) = f^{p_i} = \begin{bmatrix} -a_0^{(i)} \\ -a_1^{(i)} \\ \vdots \\ -a_{p_i-2}^{(i)} \\ -a_{p_i-1}^{(i)} \end{bmatrix}.$$

□

In the proof of the above theorem we used only the fact that a linear space can be represented as a direct sum of cyclic spaces. In the next theorem, which also states the possibility of diagonal-like matrix representation of a linear mapping, we will use the decomposition into a direct sum of irreducible cyclic spaces.

Theorem 31. Let V be a linear space over the field of complex numbers. Each linear mapping $f : V \to V$ from a finite dimensional linear space V to itself has in some basis a matrix representation

$$F = \begin{bmatrix} D_1 & & & \\ & D_2 & & \\ & & \dots & \\ & & & D_r \end{bmatrix}. \tag{3}$$

for some r, where all blocks D_i have the form either

$$D_i = [t]$$

or

$$\begin{bmatrix} t & & & & & \\ 1 & t & & & & \\ & 1 & & & & \\ & & \dots & & & \\ & & & t & & \\ & & & 1 & t & \end{bmatrix}. \quad (Jordan\ \ blocks)$$

Proof. Let

$$V = V_1^{(1)} \oplus \dots \oplus V_{n_1}^{(1)} \oplus V_1^{(2)} \oplus \dots \oplus V_{n_2}^{(2)} \oplus \dots \oplus V_1^{(k)} \oplus \dots \oplus V_{n_m}^{(k)}$$

be the decomposition of V into a direct sum of irreducible cyclic spaces from the conclusion of Theorem 29. Let

$$W = V_j^{(i)}$$

for some i, j.

Because W is cyclic and irredicible its annihilator must be of the form $(x-t)^m$. (note that if there were factors $(x-t_1)^{m_1}, \dots, (x-t_q)^{m_q}$, for pairwise different t_i's, of W's annihilator, then W would be a direct sum of q cyclic spaces). Let $\boldsymbol{w}$ be a generator of W. Consider now the following vectors:

$$\boldsymbol{v_0} = \boldsymbol{w}, \boldsymbol{v_1} = (f - t \cdot \mathrm{id})(\boldsymbol{w}), \boldsymbol{v_2} = (f - t \cdot \mathrm{id})^2(\boldsymbol{w}), \dots, \boldsymbol{v_{m-1}} = (f - t \cdot \mathrm{id})^{m-1}(\boldsymbol{w}).$$

There are m vectors here and to show that they form a basis of W it is enough to show that they are linearly independent. Assume they are not. Then there exist $\alpha_0, \alpha_1, \ldots, \alpha_{m-1}$, not all equalto zetro, such that

$$\alpha_0 \boldsymbol{w} + \alpha_1 (f - t \cdot \mathrm{id})(\boldsymbol{w}) + \ldots + \alpha_{m-1} (f - t \cdot \mathrm{id})^{m-1}(\boldsymbol{w}) = \mathbf{0}.$$

Then the polynomial

$$\phi(x) = \alpha_0 + \alpha_1 (x - t) + \ldots + \alpha_{m-1} (x - t)^{m-1}$$

would annihilate $\boldsymbol{w}$ but $p = \deg(\phi(x)) < m$ and this contradicts our assumption that $(x - t)^m$ is the annihilator of $\boldsymbol{w}$.

We have

$$f(\boldsymbol{v_0}) = f(\boldsymbol{w}) = f(\boldsymbol{w}) - t\boldsymbol{w} + t\boldsymbol{w} = \boldsymbol{v_1} + t\boldsymbol{v_0},$$

$$f(\boldsymbol{v_1}) = f(f(\boldsymbol{w}) - t\boldsymbol{w}) = f(f(\boldsymbol{w}) - t\boldsymbol{w}) - t(f(\boldsymbol{w}) - t\boldsymbol{w}) + t(f(\boldsymbol{w}) - t\boldsymbol{w}) =$$
$$(f - t \cdot \mathrm{id})((f - t \cdot \mathrm{id})(\boldsymbol{w})) + (f(\boldsymbol{w}) - t \cdot \boldsymbol{w}) = \boldsymbol{v_2} + t\boldsymbol{v_1},$$

and, generally, for $i < m - 1$

$$f(\boldsymbol{v_i}) = f((f - t \cdot \mathrm{id})^i(\boldsymbol{w})) = f((f - t \cdot \mathrm{id})^i(\boldsymbol{w})) - t(f - t \cdot \mathrm{id})^i(\boldsymbol{w}) + t(f - t \cdot \mathrm{id})^i(\boldsymbol{w}) =$$
$$(f - t \cdot \mathrm{id})^{i+1}(\boldsymbol{w}) + t(f - t \cdot \mathrm{id})^i(\boldsymbol{w}) = \boldsymbol{v_{i+1}} + t\boldsymbol{v_i},$$

and for $i = m - 1$

$$f(\boldsymbol{v_{m-1}}) = f((f - t \cdot \mathrm{id})^{m-1}(\boldsymbol{w})) =$$
$$f((f - t \cdot \mathrm{id})^{m-1}(\boldsymbol{w})) - t(f - t \cdot \text{m-1d})^{m-1}(\boldsymbol{w}) + t(f - t \cdot \mathrm{id})^i(\boldsymbol{w}) =$$
$$(f - t \cdot \mathrm{id})^m(\boldsymbol{w}) + t(f - t \cdot \mathrm{id})^{m-1}(\boldsymbol{w}) = \mathbf{0} + t\boldsymbol{v_{m-1}}.$$

This gives the form of the columns of the matrix representing f in the basis $\boldsymbol{v_0}, \ldots, \boldsymbol{v_{m-1}}$. These columns are as in the conclusion of the theorem.

□

Problem 1. Let V be a linear space and $f : V \to V$ be a linear mapping. Is it true that for each vector $\boldsymbol{v} \in V$ the space V is a direct sum $\Gamma(f, \boldsymbol{v}) \oplus W$, where W is an f-invariant subspace of V?

Problem 2. Let V be a linear space and $f : V \to V$ be a linear mapping and $\psi(x)$ its characteristic polynomial. Derive from Theorem 29 the theorem that says that $\psi(f)(\boldsymbol{v}) = \mathbf{0}$ for each $\boldsymbol{v} \in V$. In other words: if φ is the annihilator of the space V, then $\varphi(x) | \psi(x)$.

Problem 3. Let $f : \mathbb{R}^2 \to \mathbb{R}^2$ be a rotation by the angle $\pi/2$. Find the annihilator of $\mathbb{R}^2$ for this linear mapping.

Problem 4. Find the mapping $f : \mathbb{R}^{100} \to \mathbb{R}^{100}$ such that the annihilator of $\mathbb{R}^{100}$ is equal to $\phi(x) = x^2 + 1$. Find a matrix representation of f?

Problem 5. Find the mapping $f : \mathbb{C}^{100} \to \mathbb{C}^{100}$ such that the annihilator of $\mathbb{C}^{100}$ is equal to $\phi(x) = x^2 + 1$. Find a matrix representation of f?

Problem 6. Recall the argument that a linear space is cyclic (with respect to some fixed linear mapping) if and only if the degree of its annihilator is equal to its dimension.