ADVANCED TOPICS IN ALGEBRA

LECTURE 2

(lecture and problems to solve)
2020/21

ANNIHILATORS

We begin a cycle of lectures that will lead to a theorem about a matrix representation of a linear mapping in simple diagonal-like form.

Let

$$w(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

be a polynomial whose domain is $\mathcal{K}$ and whose coefficients $a_0, \ldots, a_n$ are in $\mathcal{K}$ (here always $\mathcal{K} = \mathbb{R}$ or $\mathcal{K} = \mathbb{C}$). Let V be a linear space (over a field $\mathcal{K}$) and let $f : V \to V$ be a linear mapping. Let us define a mapping $w(f)$ in the following way:

$$w(f) = a_n \underbrace{f \circ f \circ \cdots \circ f}_{n\,\text{times}} + a_{n-1} \underbrace{f \circ f \circ \cdots \circ f}_{n-1\,\text{times}} + \ldots = a_1 f + a_0 \mathrm{id}.$$

As the composition of linear mappings is a linear mapping and the sum of linear mappings is a linear mapping, the mapping $w(f)$ is again a linear mapping from V to V.

Problem 1. Let a linear mapping $f : \mathbb{R}^2 \to \mathbb{R}^2$ be represented by the matrix

$$F = \begin{bmatrix} 1, & 2 \\ 2, & -1 \end{bmatrix}.$$

Calculate the matrix of the mapping $w(f)$, where $w(x) = 3x^2 + x - 1$. Find $w(f)(\boldsymbol{v})$, where

$$\boldsymbol{v} = \begin{bmatrix} 2 \\ 0 \end{bmatrix}.$$

Problem 2. Prove that if $f : V \to V$ is a linear mapping and

$$w(x) = u(x)v(x)$$

for polynomials $u(x)$, $v(x)$ and $w(x)$ then

$$w(f) = u(f) \circ v(f).$$

Theorem 5. Let V be a linear space (over a field $\mathcal{K}$) of finite dimension $\dim(V) = n \in \mathbb{N}$ and let $f : V \to V$ be a linear mapping. Let $\boldsymbol{v} \in V$. There exists a polynomial $w(x) \neq 0$ of degree n such that $w_f(\boldsymbol{v}) = 0$.

Proof. Consider $n + 1$ vectors

$$\boldsymbol{v} = \mathrm{id}(\boldsymbol{v}),$$

$$f(\boldsymbol{v}),$$

$$f^2(\boldsymbol{v}) = (f \circ f)(\boldsymbol{v}) = f(f(\boldsymbol{v})),$$

$$\vdots,$$

$$f^n(\boldsymbol{v}) = \underbrace{f \circ f \circ \cdots \circ f}_{n \text{ times}}(\boldsymbol{v}) = \underbrace{f(f(\ldots(f}_{n \text{ times}}(\boldsymbol{v})\ldots)).$$

As the dimension of the space V is n, these vectors must be linearly dependent, which means that some linear combination of these vectors where not all coefficients are equal to zero is the zero vector:

$$a_n f^n(\boldsymbol{v}) + a_{n-1} f^{n-1}(\boldsymbol{v}) + \ldots a_1 f(\boldsymbol{v}) + a_0 \boldsymbol{v} = \mathbf{0}.$$

Thus the polynomial

$$w(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots a_1 x + a_0$$

satisfies the conclusion of the theorem.

□

Let V be a linear space (over a field $\mathcal{K}$) of finite dimension $\dim(V) = n \in \mathbb{N}$ and let $f : V \to V$ be a linear mapping. Now, when we already know that for every vector $\boldsymbol{v} \in V$ there exists a polynomial $w(x) \neq 0$ of degree n such that $w(f)(\boldsymbol{v}) = 0$, we can find such a polynomial $\phi(x)$ of minimal degree with the coefficient at the greatest power equal to one. We call this polynomial an *annihilator* of the vector $\boldsymbol{v}$.

Theorem 6. For each $\boldsymbol{v}$ there exists only one annihilator.

Proof. Assume that there are two annihilotors ϕ and ψ of a vector $\boldsymbol{v}$. Consider $\xi(x) = \psi(x) - \phi(x)$. Of course

$$\xi(f)(\boldsymbol{v}) = \psi(f)(\boldsymbol{v}) - \phi(f)(\boldsymbol{v}) = \mathbf{0} - \mathbf{0} = \mathbf{0}.$$

But, as ϕ and ψ have the same coefficient equal to 1 at the greatest power, $\xi(x)$ has a smaller degree than ϕ and ψ and this is a contradiction.

□

The next theorem identifies the class of these polyniomials $w(x)$ for which $w(f)(\boldsymbol{v}) = \mathbf{0}$.

Theorem 7. Let V be a linear space (over a field $\mathcal{K}$) of finite dimension $\dim(V) = n \in \mathbb{N}$ and let $f : V \to V$ be a linear mapping. Let $\boldsymbol{v} \in V$ and let $\phi(x)$ be an annihilator of the vector $\boldsymbol{v}$. Let $w(x)$ be another polynomial. Then $w(f)(\boldsymbol{v}) = \mathbf{0}$ if and only if $\phi(x)|w(x)$.

Proof. Assume that $\phi(x)|w(x)$. Then we have

$$w(x) = u(x)\phi(x)$$

for some polynomial $u(x)$. Then, by the conclusion of Problem 2, we have

$$w(f)(\boldsymbol{v}) = u(f) \circ \phi(f)(\boldsymbol{v}) = u(f)(\phi(f)(\boldsymbol{v})) = u(f)(\mathbf{0}) = \mathbf{0}.$$

Now let us prove the inverse implication and assume that

$$w(f)(\boldsymbol{v}) = \mathbf{0}.$$

Assume also that $w(x)$ is not divisible by $\phi(x)$. Thus

$$w(x) = u(x)\phi(x) + r(x)$$

where $r(x)$ is a polynomial of smaller degree than $\phi(x)$. But then we obtain

$$\mathbf{0} = u(f) \circ \phi(f)(\boldsymbol{v}) + r(f)(\boldsymbol{v}) = u(f)(\phi(f)(\boldsymbol{v})) + r(f)(\boldsymbol{v}) = \mathbf{0} + r(f)(\boldsymbol{v}) = r(f)(\boldsymbol{v}).$$

Thus $r(f)(\boldsymbol{v}) = \mathbf{0}$, but this contradicts our choice of ϕ as a polynomial of the smallest degree such that $\phi(f)(r(f)(\boldsymbol{v})) = 0$. This contradiction completes the proof.

□

Theorem 8. Assume that $\psi(x)$ and $\phi(x)$ are the annihilators of the vectors $\boldsymbol{u}$ and $\boldsymbol{v}$, respectively. Then

$$(\psi \cdot \phi)(f)(\boldsymbol{u} + \boldsymbol{v}) = \mathbf{0}.$$

Proof. We have

$$(\psi \cdot \phi)(f)(\boldsymbol{u} + \boldsymbol{u}) = (\psi \cdot \phi)(f)(\boldsymbol{u}) + (\psi \cdot \phi)(f)(\boldsymbol{u}) =$$
$$(\phi \cdot \psi)(f)(\boldsymbol{u}) + (\psi \cdot \phi)(f)(\boldsymbol{v}) = \phi(f) \circ \psi(f)(\boldsymbol{u}) + \psi(f) \circ \phi(f)(\boldsymbol{v}) =$$
$$\phi(f)(\psi(f)(\boldsymbol{u})) + \psi(f)(\phi(f)(\boldsymbol{v})) = \mathbf{0} + \mathbf{0} = \mathbf{0}.$$

□

Theorem 9. Assume that $\psi(x)$ and $\phi(x)$ are the annihilators of the vectors $\boldsymbol{u}$ and $\boldsymbol{v}$, respectively. Assume also that $\psi(x)$ and $\phi(x)$ are relatively prime polynomials, i.e. they do not have common divisors which are polynomials of positive degree. Then the polynomial $\psi(x) \cdot \phi(x)$ is the annihilator of the vector $\boldsymbol{u} + \boldsymbol{v}$.

Proof. From Theorems 7 and 8 we know that the annihilator $\xi(x)$ of the vector $\boldsymbol{u} + \boldsymbol{v}$ divides the polynomial $\psi(x) \cdot \phi(x)$. Now let us notice that

$$\boldsymbol{v} = (\boldsymbol{u} + \boldsymbol{v}) + (-\boldsymbol{u})$$

and that the annihilator of $-\boldsymbol{u}$ is the same as that of $\boldsymbol{u}$, namely it is equal to $\psi(x)$. Hence, again by the previous theorem, the annihilator of $\boldsymbol{v}$, $\phi(x)$, divides $\xi(x)\dot{\psi}(x)$. Becausde $\phi(x)$ and $\psi(x)$ are relatively prime polynomials, $\phi(x)$ must divide $\xi(x)$. Also, by the analogous argument we show that $\psi(x)$ must divide $\xi(x)$. Thus, again because $\phi(x)$ and $\psi(x)$ are relatively prime polynomials, $\phi(x) \cdot \psi(x)$ divides $\xi(x)$. Thus we have

$$\xi(x) | \phi(x) \cdot \psi(x) \text{ and } \phi(x) \cdot \psi(x) | \xi(x)$$

which implies

$$\xi(x) = \phi(x) \cdot \psi(x).$$

□

Problem 3. Let $V = \mathbb{R}^2$. Let a liner mapping f be given by the matrix

$$F = \begin{bmatrix} 1, 2 \\ -2, 1 \end{bmatrix}.$$

Find the annihilators (with respect to f) of the vectors

$$\boldsymbol{e_1} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \boldsymbol{e_2} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, -\boldsymbol{e_1} = \begin{bmatrix} -1 \\ 0 \end{bmatrix}, \boldsymbol{v} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \boldsymbol{w} = \begin{bmatrix} -1 \\ 1 \end{bmatrix}.$$

Problem 4. Using induction prove the following generalizations of Theorems 8 and 9.

Theorem 10. Let f be a fixed linear mapping of a vector space V into V. If $\phi_1(x), \phi_2(x), \ldots, \phi_m(x)$ are the annihilators (with respect to f) of vectors $\boldsymbol{v_1}, \ldots, \boldsymbol{v_m}$, then the annihilator $\psi(x)$ of their sum $\boldsymbol{w} = \boldsymbol{v_1} + \ldots + \boldsymbol{v_m}$ divides the product ot their annihilators $\phi_1(x) \cdot \phi_2(x) \cdot \ldots \cdot \phi_m(x)$.

Theorem 11. Let f be a fixed linear mapping of a vector space V into V. If the annihilators $\phi_1(x), \phi_2(x), \ldots, \phi_m(x)$ (with respect to f) of vectors $\boldsymbol{v_1}, \ldots, \boldsymbol{v_m}$ are relatively prime, then the annihilator $\psi(x)$ of their sum $\boldsymbol{w} = \boldsymbol{v_1} + \ldots + \boldsymbol{v_m}$ is the product of their annihilators

$$\psi(x) = \phi_1(x) \cdot \phi_2(x) \cdot \ldots \cdot \phi_m(x).$$

Let f be a fixed linear mapping of a vector space V into V. Let $\langle \boldsymbol{e_1}, \ldots, \boldsymbol{e_n} \rangle$ be a basis of V and let $\phi_1(x), \phi_2(x), \ldots, \phi_n(x)$ be the annihilators of the vectors $\boldsymbol{e_1}, \ldots, \boldsymbol{e_n}$, respectively. Let $\phi(x) = \phi_1(x) \cdot \phi_2(x) \cdot \ldots \cdot \phi_n(x)$. By Theorem 7

$$\phi(f)(\boldsymbol{e_i}) = \mathbf{0}$$

for each $1 \leqslant i \leqslant n$. Because $\phi(f)$ is a linear mapping we also have

$$\phi(f)(\boldsymbol{v}) = \mathbf{0}$$

for each $\boldsymbol{v} \in V$.

Hence the family of these polynomials $w(x)$ for which $w(f)(\boldsymbol{v}) = \mathbf{0}$ for every vector $\boldsymbol{v}$ in V is nonempty. Let ϕ_V be a polynomial with this property which is of the smallest possible degree and which has the coefficient at the greatest power equal to one. We call it an *annihilator of the space* V (or the *minimal polynomial of the mapping* f).

Problem 5. Prove the following theorem.

Theorem 12. There exists only one annihilator of the space V, and for every polynomial $w(x)$,

$$w(f)(\boldsymbol{v}) = \mathbf{0}$$

for every $\boldsymbol{v} \in V$ if and only if $\phi_V(x) | w(x)$.

Hint: the method of proof is very similar to that of the proof that there exists only one annihilator of a vector.

Theorem 13. Let f be a fixed linear mapping of a vector space V into V. Let $\langle \boldsymbol{e_1}, \ldots, \boldsymbol{e_n} \rangle$ be a basis of v and let $\phi_1(x), \phi_2(x), \ldots, \phi_n(x)$ be the annihilators of the vectors $\boldsymbol{e_1}, \ldots, \boldsymbol{e_n}$, respectively. Then the annihilator of the space is the least common multiple of the polynomials $\phi_1(x), \phi_2(x), \ldots, \phi_n(x)$.

Proof. Let $w(x)$ be the least common multiple of the polynomials $\phi_1(x), \phi_2(x), \ldots, \phi_n(x)$. Then by Theorem 7 $w(f)(\boldsymbol{e_i}) = \mathbf{0}$ for each vector $\boldsymbol{e_i}$, $1 \leqslant i \leqslant n$. Thus by linearity of $w(f)$ we have $w(f)(\boldsymbol{v}) = \mathbf{0}$ for each vector $\boldsymbol{v} \in V$. Hence, by Theorem 12:

$$\phi_V | w(x).$$

Thus we have

$$w(x) = \phi_V(x)D(x)$$

for some polynomial $D(x)$. If $\deg(D(x)) > 1$, then $\phi_V(x)$ is not the common multiple of the polynomials $\phi_1(x), \phi_2(x), \dots, \phi_n(x)$. . Let us assume that it is not a multiple of, say, some $\phi_i(x)$. But then it is not the annihilator of V. Thus $D(x)$ is a constant, but this constant must be 1, because the coefficients at the greatest power in ϕ_V and $w(x)$ are equal to 1.

□

Let $V_1, V_2 < V$ be linear subspaces of the space V. If $V_1 \cap V_2 = \{\mathbf{0}\}$ then the space $V_1 \oplus V_2$ spanned over the subspaces V_1, V_2 (which consists of all the vectors of the form $v_1 + v_2$, $v_1 \in V_1, v_2 \in V_2$) is called the *direct sum* of the spaces V_1, V_2.

Let f be a fixed linear mapping of a vector space V into V. A linear subspace W of the linear space V is called *invariant* (*with respect to* f) if $f[W] \subseteq W$.

Theorem 14. Let f be a fixed linear mapping of a vector space V into V. The annihilator (with respect to f) of the direct sum of invariant spaces V_1 and V_2 is the least common multiple if their annihilators

Proof. Let $\boldsymbol{e_1}, \boldsymbol{e_2}, \dots, \boldsymbol{e_k}$ be a basis of V_1 and $\boldsymbol{e'_1}, \boldsymbol{e'_2}, \dots, \boldsymbol{e'_m}$ be a basis of V_2. Let $\phi_1(x)$, $\phi_2(x)$ be the annihilators of V_1 and V_2, respectively. By Theorem 13 the annihilator $\xi(x)$ of the space

$$V_1 \oplus V_2 = \operatorname{span}\{\boldsymbol{e_1}, \boldsymbol{e_2}, \dots, \boldsymbol{e_k}, \boldsymbol{e'_1}, \boldsymbol{e'_2}, \dots, \boldsymbol{e'_m}\}$$

is the least common multiple of the annihilators of the vectors of the basis

$$\{\boldsymbol{e_1}, \boldsymbol{e_2}, \dots, \boldsymbol{e_k}, \boldsymbol{e'_1}, \boldsymbol{e'_2}, \dots, \boldsymbol{e'_m}\}.$$

Let $\tau_i(x)$ be the annihilator of $\boldsymbol{e_i}$, $1 \leqslant i \leqslant k$ and $\mu_i(x)$ be the annihilator of $\boldsymbol{e'_j}$, $1 \leqslant j \leqslant m$. Denotnig by $\mathrm{LCM}(\rho(x), \vartheta(x))$ the least common multiple of polynomials $\rho(x), \vartheta(x)$ we have

$$\xi(x) = \mathrm{LCM}(\tau_1(x), \dots, \tau_k(x), \mu_1(x), \dots, \mu_m(x)) =$$
$$\mathrm{LCM}(\mathrm{LCM}(\tau_1(x), \dots, \tau_k(x)), \mathrm{LCM}(\mu_1(x), \dots, \mu_m(x))) = \mathrm{LCM}(\phi_1(x), \phi_2(x)).$$

□

Theorem 15. Let f be a fixed linear mapping of a vector space V into V. There exists a vector $\boldsymbol{v}$ whose annihilator is the same as that of the whole space V.

Proof. Let $\boldsymbol{e_1}, \dots, \boldsymbol{e_n}$ be a basis of v. Let

$$\psi(x) = \phi_1^{k_1}(x)\phi_2^{k_2}(x)\dots\phi_m^{k_m}(x)$$

be a decomposition of the annihilator of the space V into relatively prime non-decomposable factors of positive degree whose coefficients at the greatest power are equal to 1. The polynomial $\psi(x)$ can be represented as

$$\psi(x) = \phi_i^{k_i}(x)M_i(x),$$

(where $M_i(x) = \prod_{j\neq i} \phi_j^{k_j}$.) Consider vectors

$$\boldsymbol{v_{1,i}} := M_1(f)(\boldsymbol{e_i}).$$

At least one of the vectors $\phi_1^{k_1-1}(f)(\boldsymbol{v_{1,i}})$ must be a nonzero one, because otherwise $\phi_1^{k_1-1}(f) \circ M_1(f)$ would map each vector of V into zero and the polynomial $\phi_1^{k_1-1}(x)M_1(x)$ is of a smaller degree than $\psi(x)$. Let it be vector $\boldsymbol{v_{1,i_1}}$. Analogously we find vectors $\boldsymbol{v_{j,i_j}}$, $1 \leqslant j \leqslant m$, such that $\phi_j^{k_j-1}(f)(\boldsymbol{v_{j,i_j}}) \neq \mathbf{0}$ and such that $\phi_j^{k_j}(f)(\boldsymbol{v_{j,i_j}}) = \mathbf{0}$. Note that the annihilator of the vector $\boldsymbol{v_{j,i_j}}$ is equal to $\phi_j^{k_j}(x)$. Thus, by Theorem 10, the annihilator of the vector

$$\boldsymbol{v} = \sum_{j=1}^{m} \boldsymbol{v_{j,i_j}}$$

is equal to the product $\prod_{j=1}^{m} \phi_j^{k_j}(x) = \psi(x)$.

□

Problem 6. Prove that the degree of the annihilator of a space does not exceed the dimension of the space.

Problem 7. Let f be a fixed linear mapping of a vector space V into V. Prove that $w(f)$ maps V into $\mathbf{0}$ if $w(x)$ is the characteristic polynomial of f.