Primary and Cyclic Decomposition Theorems, Part I

Vojta Tůma

MFF UK, KAM/IUUK

April 14, 2013 / Spring School of Algebra

Table of Contents

Intro

Our setting: V is a vector space, T is a linear operator.

We want to decompose T, in order to understand it.

What is a good decomposition of a an operator?

Good decomposition – an example

Operator T is *diagonalisable* if there exist a basis such that T is represented by a diagonal matrix.

Good decomposition – an example

Operator T is *diagonalisable* if there exist a basis such that T is represented by a diagonal matrix.

- We can then easily compute rank, determinant, range, kernel ...
- We can readily identify some "natural" subspaces on which T is well-behaved – the characteristic spaces.
- However, not every T is diagonalisable.

Table of Contents

Characteristic polynomial

Characteristic polynomial of the operator T is the polynomial $\det(A - xI)$, where A is a matrix that represents T.

Characteristic polynomial

Characteristic polynomial of the operator T is the polynomial $\det(A - xI)$, where A is a matrix that represents T.

Root c of the characteristic polynomial is called *characteristic value*, and its corresponding space — the kernel of the mapping $A - cI$ — is called *characteristic space*.

Characteristic polynomial

Characteristic polynomial of the operator T is the polynomial $\det(A - xI)$, where A is a matrix that represents T.

Root c of the characteristic polynomial is called *characteristic value*, and its corresponding space — the kernel of the mapping $A - cI$ — is called *characteristic space*.

Characteristic spaces are *independent* and *invariant* – which is pretty cool.

Characteristic polynomial – example

Example

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \qquad p = x^2 + 1$$

$$\begin{bmatrix} 3 & 1 & -1 \\ 2 & 2 & -1 \\ 2 & 2 & 0 \end{bmatrix} \qquad p = (x-1)(x-2)^2$$

Minimal polynomial

A polynomial p is called *annihilating* if $p(T) = 0$.

Annihilating polynomials form an ideal, and there is a unique monic generator – *minimal polynomial* M of T.

Minimal polynomial

A polynomial p is called *annihilating* if $p(T) = 0$.

Annihilating polynomials form an ideal, and there is a unique monic generator – *minimal polynomial* M of T.

Minimal polynomial always exists, and divides the characteristic polynomial (the Cayley-Hamilton theorem).

Minimal polynomial

A polynomial p is called *annihilating* if $p(T) = 0$.

Annihilating polynomials form an ideal, and there is a unique monic generator – *minimal polynomial* M of T.

Minimal polynomial always exists, and divides the characteristic polynomial (the Cayley-Hamilton theorem).

Operator T is diagonalisable iff M is a product of distinct monomials.
Operator T is triangulable iff M is a product of monomials (i.e., we are in a algebraically closed field).

Minimal polynomial – example

Example

$$\begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} \qquad \text{here } A^3 = 4A, \quad \text{thus } (x^3 - 4x)(A) = 0$$

$$\Rightarrow M_A \in \{x(x+2), x(x-2), (x+2)(x-2), x(x+2)(x-2)\}$$

Table of Contents

Independent subspaces

Subspaces $W_1, \ldots, W_k$ are *independent* if whenever we have $\alpha_i \in W_i$ such that $\sum \alpha_i = 0$, then $\alpha_i = 0$.

Independent subspaces

Subspaces $W_1, \dots, W_k$ are *independent* if whenever we have $\alpha_i \in W_i$ such that $\sum \alpha_i = 0$, then $\alpha_i = 0$.

For independent subspaces the space W spanned by all W_i is called *direct sum* of the subspaces W_i and is denoted by $\bigoplus W_i$.
Example: characteristic spaces, skew-symmetric matrices.

Projections

A *projection* is a mapping E such that $E^2 = E$.

Projections

A *projection* is a mapping E such that $E^2 = E$.

Some properties:

- $a \in \mathrm{Rng}(E) \iff Ea = a$,
- $V = \mathrm{Rng}(E) \oplus \ker(E)$,
- E is diagonalisable.

Projections and direct sums

Whenever we have direct sum decomposition into W_i, we also have mappings E_i such that

- $Ea = \sum E_i a$ (that is, $I = \sum E_i$),
- $E_i^2 = E_i$,
- $E_i E_j = 0$.

Projections and direct sums

Whenever we have direct sum decomposition into W_i, we also have mappings E_i such that

- $Ea = \sum E_i a$ (that is, $I = \sum E_i$),
- $E_i^2 = E_i$,
- $E_i E_j = 0$.

But, the converse also holds! Whenever we have such mappings E_i, the subspaces $\mathrm{Rng}(E_i)$ form a direct sum decomposition.

Proof.

Projections and direct sums

Whenever we have direct sum decomposition into W_i, we also have mappings E_i such that

- $Ea = \sum E_i a$ (that is, $I = \sum E_i$),
- $E_i^2 = E_i$,
- $E_i E_j = 0$.

But, the converse also holds! Whenever we have such mappings E_i, the subspaces $\mathrm{Rng}(E_i)$ form a direct sum decomposition.

Proof.

From $I = \sum E_i$ we have that $\mathrm{Rng}(E_i)$ spans V.

Projections and direct sums

Whenever we have direct sum decomposition into W_i, we also have mappings E_i such that

- $Ea = \sum E_i a$ (that is, $I = \sum E_i$),
- $E_i^2 = E_i$,
- $E_i E_j = 0$.

But, the converse also holds! Whenever we have such mappings E_i, the subspaces $\mathrm{Rng}(E_i)$ form a direct sum decomposition.

Proof.

From $I = \sum E_i$ we have that $\mathrm{Rng}(E_i)$ spans V. Let $a = \sum a_i$, assume $a_i = E_i b_i$. Then

$$E_j a = \sum_i E_j a_i = \sum_i E_j E_i b_i = E_j b_j = a_j.$$

$\square$

Projections and operators

We want a decomposition into W_i's such that they are invariant under T – so that $Ta = \sum T_i E_i a$,
and that the restrictions of T are in some elementary form.

Projections and operators

We want a decomposition into W_i's such that they are invariant under T – so that $Ta = \sum T_i E_i a$,
and that the restrictions of T are in some elementary form.

Proposition

A necessary and sufficient condition for W_i's to be invariant under T is that $E_i T = T E_i$ (for every i).

Proof.

Projections and operators

We want a decomposition into W_i's such that they are invariant under T – so that $Ta = \sum T_i E_i a$,
and that the restrictions of T are in some elementary form.

Proposition

A necessary and sufficient condition for W_i's to be invariant under T is that $E_i T = TE_i$ (for every i).

Proof.

Let T commute, $a \in W_i$. Then
$Ta = TE_i a = E_i Ta \Rightarrow Ta \in \mathrm{Rng}(E_i)$.

Projections and operators

We want a decomposition into W_i's such that they are invariant under T – so that $Ta = \sum T_i E_i a$,
and that the restrictions of T are in some elementary form.

Proposition

A necessary and sufficient condition for W_i's to be invariant under T is that $E_i T = TE_i$ (for every i).

Proof.

Let T commute, $a \in W_i$. Then
$Ta = TE_i a = E_i Ta \Rightarrow Ta \in \mathrm{Rng}(E_i)$.
Let W_i be invariant. Take $a = \sum E_i a$, $Ta = \sum TE_i a$,
$TE_i a = E_i b_i$.

Projections and operators

We want a decomposition into W_i's such that they are invariant under T – so that $Ta = \sum T_i E_i a$,
and that the restrictions of T are in some elementary form.

Proposition

A necessary and sufficient condition for W_i's to be invariant under T is that $E_i T = TE_i$ (for every i).

Proof.

Let T commute, $a \in W_i$. Then
$Ta = TE_i a = E_i Ta \Rightarrow Ta \in \mathrm{Rng}(E_i)$.
Let W_i be invariant. Take $a = \sum E_i a$, $Ta = \sum TE_i a$,
$TE_i a = E_i b_i$. Then $E_j TE_i a = E_j E_i b_i$, thus
$E_j Ta = E_j b_j = TE_j a$. $\square$

Primary decomposition – example

Example

$$\begin{bmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 2 \end{bmatrix},$$

its characteristic and minimal polynomial are $(x-2)(x^2+1)$, thus it is not diagonalisable.

Primary decomposition – example

Example

$$\begin{bmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 2 \end{bmatrix},$$

its characteristic and minimal polynomial are $(x-2)(x^2+1)$, thus it is not diagonalisable.
But! $\mathrm{Ker}((T^2+I))$ and $\mathrm{Ker}((T-2I))$ together span V, hooray!

Primary decomposition theorem

Theorem

Let $p = \prod_i p_i^{r_i}$ *be the minimal polynomial of* T, *where* p_i *are distinct irreducible monic polynomials; and let* $W_i = \mathrm{Ker}(p_i^{r_i}(T))$. *Then*

- $\bigoplus_i W_i$ *is a direct sum decomposition of* V,
- W_i*'s are invariant under* T,
- *the minimal polynomial for restriction of* T *on* W_i *is* $p_i^{r_i}$.

Primary decomposition theorem

Theorem

Let $p = \prod_i p_i^{r_i}$ be the minimal polynomial of T, where p_i are distinct irreducible monic polynomials; and let $W_i = \mathrm{Ker}(p_i^{r_i}(T))$. Then

- *$\bigoplus_i W_i$ is a direct sum decomposition of V,*
- *W_i's are invariant under T,*
- *the minimal polynomial for restriction of T on W_i is $p_i^{r_i}$.*

Proof idea: we shall reach the W_i's by constructing projections – by finding polynomials h_i such that $h_i(T)$ is I on W_i and 0 on $W_{j \neq i}$.

Primary decomposition theorem – proof

Proof.

Let $f_i = p/p_i^{r_i} = \prod_{j \neq i} p_j^{r_j}$. Thus there are g_i's such that $\sum_i f_i g_i = 1$.

Primary decomposition theorem – proof

Proof.

Let $f_i = p/p_i^{r_i} = \prod_{j \neq i} p_j^{r_j}$. Thus there are g_i's such that $\sum_i f_i g_i = 1$.

We set $E_i = h_i = f_i g_i$. As p divides $f_i f_j$, we have $E_i E_j = 0$. From primality we have $\sum E_i = I$, and thus the E_i's are projections and give rise to a direct sum decomposition.

Primary decomposition theorem – proof

Proof.

Let $f_i = p/p_i^{r_i} = \prod_{j \neq i} p_j^{r_j}$. Thus there are g_i's such that $\sum_i f_i g_i = 1$.

We set $E_i = h_i = f_i g_i$. As p divides $f_i f_j$, we have $E_i E_j = 0$. From primality we have $\sum E_i = I$, and thus the E_i's are projections and give rise to a direct sum decomposition.

Take $a \in \mathrm{Rng}(E_i)$, then
$p_i^{r_i}(T)a = p_i^{r_i}(T)E_i a = p_i^{r_i}(T)f_i(T)g_i(T)a = 0$.

Primary decomposition theorem – proof

Proof.

Let $f_i = p/p_i^{r_i} = \prod_{j \neq i} p_j^{r_j}$. Thus there are g_i's such that $\sum_i f_i g_i = 1$.

We set $E_i = h_i = f_i g_i$. As p divides $f_i f_j$, we have $E_i E_j = 0$. From primality we have $\sum E_i = I$, and thus the E_i's are projections and give rise to a direct sum decomposition.

Take $a \in \mathrm{Rng}(E_i)$, then $p_i^{r_i}(T)a = p_i^{r_i}(T)E_i a = p_i^{r_i}(T) f_i(T) g_i(T) a = 0$.

Take $a \in W_i$, then $p_i^{r_i}$ divides $f_j g_j$, thus $E_j a = 0$ and $E_i a = a$.

Primary decomposition theorem – proof

Proof.

Let $f_i = p/p_i^{r_i} = \prod_{j \neq i} p_j^{r_j}$. Thus there are g_i's such that $\sum_i f_i g_i = 1$.

We set $E_i = h_i = f_i g_i$. As p divides $f_i f_j$, we have $E_i E_j = 0$. From primality we have $\sum E_i = I$, and thus the E_i's are projections and give rise to a direct sum decomposition.

Take $a \in \mathrm{Rng}(E_i)$, then $p_i^{r_i}(T)a = p_i^{r_i}(T)E_i a = p_i^{r_i}(T) f_i(T) g_i(T) a = 0$.

Take $a \in W_i$, then $p_i^{r_i}$ divides $f_j g_j$, thus $E_j a = 0$ and $E_i a = a$.

Let g be such that $g(T_i) = 0$. Then $g(T) f_i(T) = 0$, thus $p_i^{r_i} f_i$ divides $g f_i$. $\square$

Table of Contents

Cyclic subspaces and annihilators

Let v be a finite-dimensional vector in V, by $Z(v) = Z(v, T)$ ve denote the *cyclic subspace* generated by v – it is the smallest T-invariant subspace containing v, that is,

$$Z(v) = \operatorname{span}\{v, Tv, T^2v, \ldots\} = \{f(T)v \colon f(X) \in \mathbf{F}[X]\}.$$

Again, the minimal polynomial $f_v(X)$ such that $f_v(T)v = 0$ is called the *T-annihilator* of v.

Olin's lemmata

1. $Z(v) = \{f(T)v\colon \deg f(X) < \deg f_v(X)\}$ and $\{v, Tv, \dots, T^{\deg f_v(X)-1}\}$ is a basis of $Z(v)$. The minimal polynomial of restriction of T to $Z(v)$ is $f_v(T)$.

Olin's lemmata

1. $Z(v) = \{f(T)v\colon \deg f(X) < \deg f_v(X)\}$ and $\{v, Tv, \dots, T^{\deg f_v(X)-1}\}$ is a basis of $Z(v)$. The minimal polynomial of restriction of T to $Z(v)$ is $f_v(T)$.
2. Let $p(X)$ be an irreducible factor of $f_v(X)$ of degree d. The set $\{v, Tv, \dots, T^{d-1}v\}$ is linearly independent, and $Z(v) = \operatorname{span}\{v, Tv, \dots, T^{d-1}v\} \oplus Z(p(T)v)$.

Olin's lemmata

1. $Z(v) = \{f(T)v \colon \deg f(X) < \deg f_v(X)\}$ and $\{v, Tv, \ldots, T^{\deg f_v(X)-1}\}$ is a basis of $Z(v)$. The minimal polynomial of restriction of T to $Z(v)$ is $f_v(T)$.
2. Let $p(X)$ be an irreducible factor of $f_v(X)$ of degree d. The set $\{v, Tv, \ldots, T^{d-1}v\}$ is linearly independent, and $Z(v) = \operatorname{span}\{v, Tv, \ldots, T^{d-1}v\} \oplus Z(p(T)v)$.
3. If $f_v(X)$ and $f_u(X)$ are relatively prime, $Z(u+v) = Z(v) \oplus Z(u)$ and $f_{u+v}(X) = f_u(X)f_v(X)$.

Olin's lemmata – proof

Proof.

Take $w \in Z(u) \cap Z(v)$, then for some $h(X)$ and $g(X)$ we have $w = h(T)v = g(T)u$, thus $f_v(T)w = f_v(T)h(T)v = 0$ and similarly $f_u(T)w = 0$.

Olin's lemmata – proof

Proof.

Take $w \in Z(u) \cap Z(v)$, then for some $h(X)$ and $g(X)$ we have $w = h(T)v = g(T)u$, thus $f_v(T)w = f_v(T)h(T)v = 0$ and similarly $f_u(T)w = 0$. Therefore, $f_w(X)$ divides both $f_v(X)$ and $f_w(X) \Rightarrow Z(v) + Z(u) = Z(v) \oplus Z(u)$.

Olin's lemmata – proof

Proof.

Take $w \in Z(u) \cap Z(v)$, then for some $h(X)$ and $g(X)$ we have $w = h(T)v = g(T)u$, thus $f_v(T)w = f_v(T)h(T)v = 0$ and similarly $f_u(T)w = 0$. Therefore, $f_w(X)$ divides both $f_v(X)$ and $f_w(X) \Rightarrow Z(v) + Z(u) = Z(v) \oplus Z(u)$.

Since $v + u \in Z(v) \oplus Z(u)$, we have $Z(v + u) \subseteq Z(v) \oplus Z(u)$.

Olin's lemmata – proof

Proof.

Take $w \in Z(u) \cap Z(v)$, then for some $h(X)$ and $g(X)$ we have $w = h(T)v = g(T)u$, thus $f_v(T)w = f_v(T)h(T)v = 0$ and similarly $f_u(T)w = 0$. Therefore, $f_w(X)$ divides both $f_v(X)$ and $f_w(X) \Rightarrow Z(v) + Z(u) = Z(v) \oplus Z(u)$.

Since $v + u \in Z(v) \oplus Z(u)$, we have $Z(v + u) \subseteq Z(v) \oplus Z(u)$.

There are $a(X)$ and $b(X)$ so that $1 = a(X)f_v(X) + b(X)f_u(X)$.

Olin's lemmata – proof

Proof.

Take $w \in Z(u) \cap Z(v)$, then for some $h(X)$ and $g(X)$ we have $w = h(T)v = g(T)u$, thus $f_v(T)w = f_v(T)h(T)v = 0$ and similarly $f_u(T)w = 0$. Therefore, $f_w(X)$ divides both $f_v(X)$ and $f_w(X) \Rightarrow Z(v) + Z(u) = Z(v) \oplus Z(u)$.

Since $v + u \in Z(v) \oplus Z(u)$, we have $Z(v+u) \subseteq Z(v) \oplus Z(u)$.

There are $a(X)$ and $b(X)$ so that $1 = a(X)f_v(X) + b(X)f_u(X)$. Then,

$$v = a(T)f_v(T)v + b(T)f_u(T)v = b(T)f_u(T)(u+v).$$

$\square$