Linear Algebra II

Felix Chen

Contents

§0.1 Primary cyclic decomposition and Jordan canonical forms

Theorem 0.1

For $T \in L(V)$, T irreducible $\iff$ T is primary and cyclic.

Proof. If T is irreducible, then both the primary and cyclic decomposition have only one term, i.e. T is primary and cyclic.

Conversely, if $V = V_1 \oplus V_2$ is a nontrivial decomposition. Since T is cyclic and primary, assume $f_T = p_T = p^r$, where p is a irreducible polynomial.

Suppose $f_{T_1} = p^s, f_{T_2} = p^t$, then $s + t = r$, $s, t < r$. Since $p_{T_1} \mid p^s, p_{T_2} \mid p^t$,

$$p_T = \operatorname{lcm}(p_{T_1}, p_{T_2}) \mid p^{\max\{s,t\}},$$

contradiction! □

Theorem 0.2 (Primary cyclic decomposition)

Let $T \in L(V)$.

- There exists a decomposition $V = \bigoplus_{i=1}^{s} V_i$, each V_i is T-invariant, T_{V_i} primary and cyclic. Let $q_i = p_{T_{V_i}}$.
- $q_1, \dots, q_s$ are uniquely determined by T (ignoring the permutation). They are called the **elementary divisors** of T.

Proof. Existence follows immediately from the previous theorem.

Uniqueness: Let $V = \bigoplus_{i=1}^{t} W_i$ s.t. T_{W_i} is primary and cyclic. Let $\{u_1, \dots, u_k\}$ be the set of all the monic prime factors of the minimal polynomials of $T_{W_1}, \dots, T_{W_t}$.

We can group W_i's by u_i, and each group can be placed in a row in descending order wrt the degree of $p_{T_{W_i}}$.

Let Z_j be the direct sum of the j-th column, note that Z_j is a cyclic decomposition of T.

Now since the cyclic decomposition and primary decomposition are unique, $p_{T_{W_i}}$'s must be unique as well. □

Remark 0.3 — The elementary factors depend on the base field.

Since the invariant subspaces of primary subspace are primary, and invariant subspaces of cyclic subspace are cyclic, we can apply both decomposition (in any order) to get the primary cyclic decomposition of any operators.

For a primary cyclic map T, if we choose the base field to be *algebraically closed* (e.g. $\mathbb{C}$), we can write $f_T = p_T = (x-c)^n$. Let $N = T - c\,\mathrm{id}_V$, then $f_T = p_T = x^n$, from rational canonical form we know that N is similar to $\begin{pmatrix} 0 & 0 \\ I_{n-1} & 0 \end{pmatrix}$. Hence T is similar to

$$J_n(c) := \begin{pmatrix} c & & & & \\ 1 & c & & & \\ & 1 & \ddots & & \\ & & \ddots & c & \\ & & & 1 & c \end{pmatrix},$$

such matrix is called a **Jordan block**. Jordan matrices are the blocked diagonal matrices with each block being a Jordan block.

Theorem 0.4 (Jordan canonical forms)

If f_T can be decompose to product of polynomials of degree 1, then

- $\exists \mathcal{B}$ s.t. $[T]_{\mathcal{B}}$ is a Jordan matrix, this is called the **Jordan canonical form** of T.
- The canonical form is unique under permutations of each Jordan blocks.

Proof. This follows immediately from the primary cyclic decomposition of T. □

Let's look at the subspaces V_i. We know that T_{V_i} is primary and cyclic, thus $f_i = p_i = (x-c_i)^{r_i}$. Let $N_i = T_{V_i} - \mathrm{id}_{V_i}$, $f_{N_i} = p_{N_i} = x^{r_i}$. Let $\mathcal{B}_i = \{\alpha_i, N_i\alpha_i, \ldots, N_i^{r_i-1}\alpha_i\}$, then $[N_i]_{\mathcal{B}_i} = C_{x^{r_i}} = J_{r_i}(0)$.

We can compute the Jordan canonical forms by computing the invariant factors first, and apply the primary decomposition to each factor to get the elementary divisors.

Example 0.5

Let $A = \begin{pmatrix} 2 & & \\ a & 2 & \\ b & c & -1 \end{pmatrix} \in \mathbb{C}^{3\times 3}$.

First note that $f_A = (x-2)^2(x+1)$, then $p_A = (x-2)^2(x+1)$ or $(x-2)(x+1)$.

- If $p_A = (x-2)^2(x+1)$, then $p_1 = (x-2)^2(x+1)$, $q_{11} = (x-2)^2, q_{12} = (x+1)$.

  Hence $A \sim \begin{pmatrix} 2 & & \\ 1 & 2 & \\ & & -1 \end{pmatrix}$.
- $p_A = (x-2)(x-1)$, then $p_1 = (x-2)(x+1)$, $p_2 = (x-2)$. The elementary divisors are $x-2, x-2$ and $x+1$.

  Hence $A \sim \begin{pmatrix} 2 & & \\ & 2 & \\ & & -1 \end{pmatrix}$.

Since $p_A = (x-2)(x+1) \iff (A-2I)(A+I) = 0$, i.e. $3a = ac = 0 \iff a = 0$.

Remark 0.6 — For generic matrix A, the Jordan canonical form can be derived from the *Smith canonical form* of $xI_n - A$.

The diagonal of Jordan canonical forms are the eigen values of T with *algebraic multiplicy*, and f_T, p_T can be easily written down from it. The number of Jordan blocks with eigenvalue c is equal to $\dim\ker(T - c\,\mathrm{id})$, i.e. the *geometric multiplicy* of c.

Example 0.7

We'll compute the Jordan canonical form of $J_n(0)^2$. Since its characteristic polynomial is x^n, and $\dim\ker J_n(0)^2 = 2$, so it has two Jordan block with eigenvalue 0.

But note that $(J_n(0)^2)^m = 0$ iff $m \geq \frac{n}{2}$, thus the minimal polynomial is x^m, the sizes of the Jordan blocks are $\left\lfloor \frac{n}{2} \right\rfloor, \left\lceil \frac{n}{2} \right\rceil$.

Proposition 0.8

Let $n = \dim V$, TFAE:

(1) T is nilpotent;

(2) p_T is a power of x ;

(3) $f_T = x^n$;

(4) $T^n = 0$.

Proof. Trivial. □

The nilpotent matrices and diagonalizable matrices are somehow "independent": If A is both nilpotent and diagonalizable, then $A = 0$.

In light of this idea, we present the following theorem:

Theorem 0.9 (Jordan decomposition)

Let $T \in L(V)$, $n = \dim V$, and F is algebraically closed. There exists unique $D, N \in L(V)$ s.t. $T = D + N$, where D diagonalizable and N nilpotent, and $DN = ND$.

Moreover there exists $f, g \in F[x]$ s.t. $D = f(T), N = g(T)$.

Proof. For $A \in F^{n\times n}$, $\exists P \in \mathrm{GL}_n(F)$ s.t. $P^{-1}AP = J$, where J is a Jordan matrix.

It's clear that we can find $J_1 + J_2 = J$ with J_1 diagonal, J_2 nilpotent (just exactly as what you think), and we can check $J_1 J_2 = J_2 J_1$.

Hence $A = PJ_1P^{-1} + PJ_2P^{-1}$ has the desired properties. But now it's hard to prove the uniqueness, so we'll use another approach.

Let $p_T = \prod_{i=1}^{k}(x - c_i)^{r_i}$, and the elementary divisors $q_i = (x - c_i)^{r_i}$. Let $V_i = \ker(q_i(T))$, so $V = \bigoplus_{i=1}^{k} V_i$ is the primary decomposition of T.

> **Claim.** $\exists f \in F[x]$ s.t. $f \equiv c_i (\mathrm{mod} q_i)$, $i = 1, 2, \ldots, k$.

(This follows from Chinese Remainder Theorem)

Observe that $f(T)\big|_{V_i} = c_i \,\mathrm{id}_{V_i}$ in this case, thus $f(T)$ is diagonalizable. Since $(T - f(T))\big|_{V_i}$ is nilpotent, so $N = T - f(T)$ is nilpotent. This proves the existence part and the polynomial part.

Now it's easy to prove the uniqueness: If $T = D + N = D' + N'$, since D, N are polynomials of T, D and D' is commutative, hence can be simutaneously diagonalized.

Note that $D - D' = N - N'$ is both diagonalizable and nilpotent, thus it must be 0. (N, N' is commutative, so $(N + N')^{m+m'} = 0$, here $N^m = N'^{m'} = 0$) □

Since this theorem requires the field to be algebraically closed, if T is in a smaller field, we wonder whether D and N is in that field.

Let $A \in \mathbb{R}^{n\times n}$, and $A = D + N$ be its Jordan decomposition. We'll prove that $D, N \in \mathbb{R}^{n\times n}$. By taking conjugates,

$$A = D + N \implies A = \overline{D} + \overline{N}.$$

It's clear that $\overline{D} + \overline{N}$ is also a Jordan decomposition of A, so we must have $D = \overline{D}$, which means $D \in \mathbb{R}^{n\times n}$.

In fact when $\mathbb{R}$ is replaced by any perfect field F, this property still holds. To prove this we need to introduce the semisimple maps.

§0.2 Semisimple transformations

As we've already seen, the "diagonalizable" property depends on the base fields, thus next we'll generalize the concepts of "diagonalizable".

Definition 0.10. Let $T \in L(V)$,

- We say T is **simple**(or irreducible) if V has no nontrivial T-invariant subspaces.
- We say T is **semisimple**(or totally reducible) if each T-invariant subspace $W \subset V$ there exists T-invariant subspace Z, s.t. $V = W \oplus Z$.

Obviously simple maps are always semisimple.

Proposition 0.11

Let T be a simple linear operator, then $\forall \alpha \in V \backslash \{0\}$, α is a cyclic vector of T.

Lemma 0.12

Let $T \in L(V)$.

- If T is semisimple, $V' \subset V$ is T-invariant, then $T_{V'}$ is semisimple.
- If $V = \bigoplus_{i=1}^{k} V_i$ s.t. T_{V_i} semisimple, then T is semisimple as well.

Proof. Suppose $W \subset V'$ is a T-invariant subspace. Since T is semisimple, $\exists Z \subset V$ s.t. $V = W \oplus Z$, and Z is T-invariant.

Let $Z' = Z \cap V'$, we claim that $V' = Z' \oplus W$.

Clearly $W \cap Z' = \{0\}$ and $W + Z' \subset V'$. For all $v \in V'$, $\exists w \in W, z \in Z$ s.t. $v = w + z$, since $v, w \in V'$, $z = v - w \in V'$ as well, which means $z \in Z'$.

For the second part, (We can assmue $k = 2$, but here we won't use it).

Let $W \subset V$ be a T-invariant subspace. Since T_{V_i} is semisimple, $\exists Z_i \subset V_i$ s.t.

$$V_i = \left(\left(W + \sum_{j=1}^{i-1} V_j \right) \cap V_i \right) \oplus Z_i.$$

Let $Z = \bigoplus_{i=1}^{k} Z_i$, we claim that $Z \oplus W = V$. If $w \in W \cap Z$, then $w = z_1 + \cdots + z_k$,

$$z_k = w - z_1 - \cdots - z_{k-1} \in Z_k \cap (W + V_1 + \cdots + V_{k-1}) = \{0\}.$$

Thus $z_k = 0$, similarly $z_{k-1} = \cdots = z_1 = 0 = w$.

Note that $W + \sum_{i=1}^{j} V_i \subset W \oplus \sum_{i=1}^{j} Z_i$ for all $j = 1, \ldots, k$, so $V = W \oplus Z$. □

Corollary 0.13

Let $T \in L(V)$, T is semisimple $\iff$ there exists a T-invariant decomposition $V = \bigoplus_{i=1}^{k} V_i$ s.t. each T_{V_i} is simple.

Theorem 0.14

Let $T \in L(V)$.

- T simple $\iff$ f_T is a prime polynomial;
- T semisimple $\iff$ p_T has no multiple factors.

Proof. T simple $\implies$ T cyclic $\implies$ $f_T = p_T$, so we only need to prove p_T is a prime.

Otherwise $p_T = gh$,

$$0 = p_T(T) = g(T)h(T),$$

So either $g(T)$ or $h(T)$ is not inversible. Thus $\ker(g(T)) \neq \{0\} \implies \ker(g(T)) = V \implies g(T) = 0$, contradiction!

If T is not simple, $\exists W \subset V$, W is T-invariant nontrivial subspace, so $f_T = f_{T_W} \cdot f_{T_{V/W}}$ is not a prime.

T semisimple $\implies \exists V_i$, $V = \bigoplus_{i=1}^k V_i$, such that T_{V_i} is simple $\implies p_{T_{V_i}}$ is prime.

$$p_T = \operatorname{lcm}(p_{T_{V_1}}, \dots, p_{T_{V_k}})$$

has no multiple factors.

Conversely if p_T has no multiple factors, consider the primary cyclic decomposition of T :

$$V = \bigoplus_i W_i, \quad f_{T_{W_i}} \text{ primary.}$$

Since p has no multiple factors, $f_{T_{W_i}} = p_{T_{W_i}}$ is prime polynomial.

Hence T_{W_i} simple $\implies T$ semisimple. □

Corollary 0.15

When F is an algebraically closed field:

- T simple $\iff \dim V = 1$.
- T semisimple $\iff$ T is diagonalizable.

This corollary means that "semisimple" is indeed the equivalent description of "diagonalizable" in the algebraic closure.

Note that whether p_T has multiple factors or not does not change under *perfect* field extensions. So "semisimple" is a more general property (it stays the same under more transformations).

Recall that:

Definition 0.16 (Perfect fields)**.** If for all prime polynomials $p \in F[x]$, p has no multiple roots in $\overline{F}$, we say F is a **perfect field**.

Finite fields, fields with charcter 0 and algebraically closed fields are always perfect fields.

We can check that when F is perfect, $f \in F[x]$ has no multiple factors iff f has no multiple factors in $\overline{F}[x]$.

Now we can generalize the Jordan decomposition:

Theorem 0.17 (Jordan decomposition)

Let $T \in L(V)$, $n = \dim V$, and F is perfect. There exists unique $S, N \in L(V)$ s.t. $T = S + N$, where S semisimple and N nilpotent, and $SN = NS$.

Moreover there exists $f, g \in F[x]$ s.t. $S = f(T), N = g(T)$.

To prove this generalized version, we need the following observation:

Proposition 0.18

Let F be a perfect field, $A \in F^{n\times n}$ is semisimple iff A is diagonalizable in $\overline{F}^{n\times n}$.

Proof. A semisimple $\iff p_A$ has no multiple factors in $F[x]$
$\iff p_A$ has no multiple roots in $\overline{F}[x]$
$\iff p_A$ is the product of different monic polynomials of degree 1
$\iff A$ is diagonalizable in $\overline{F}^{n\times n}$. □

Proposition 0.19

Let F be a perfect field, $a \in \overline{F}$. Then $a \notin F \iff$ exists an automorphism σ s.t. $\sigma\big|_F = \mathrm{id}_F$, i.e. $\sigma \in \mathrm{Gal}(\overline{F}/F)$ but $\sigma(a) \neq a$.

Remark 0.20 — This proof is beyond the scope of this class, but the idea is similar to the conjugate operation on $\mathbb{C}/\mathbb{R}$.

Now we prove the Jordan decomposition:

Proof. Let $A = S + N$ is the Jordan decomposition on $\overline{F}^{n\times n}$. Then by applying σ on this equation,

$$A = \sigma(S) + \sigma(N)$$

holds for all $\sigma \in \mathrm{Gal}(\overline{F}/F)$. Since $\sigma(S)$ is also diagonalizable, $\sigma(N)$ is nilpotent, as σ is an automorphism. So by the uniqueness of Jordan decomposition, $\sigma(S) = S, \sigma(N) = N$.

This implies $S, N \in F^{n\times n}$. □

§0.3 Bonus section

Starting from Galois groups mentioned above, let

$$\mathrm{Aut}(E/F) := \{\sigma \in \mathrm{Aut}(E) \mid \sigma|_F = \mathrm{id}_F\}$$

be the automorphism group of field extension E/F.

Example 0.21

Let $F = \mathbb{Q}$, $E = \mathbb{Q}(\sqrt{2})$, then $\sigma : a + b\sqrt{2} \mapsto a - b\sqrt{2}$ is in $\mathrm{Aut}(E/F)$.

If $E = \mathbb{Q}(\sqrt[3]{2})$, if $\sigma \in \mathrm{Aut}(E/F)$, then $\sigma(\sqrt[3]{2})$ is a root of $x^3 - 2 \implies \sigma = \mathrm{id}$. Thus E/F is not a *Galois extension.*

When E/F is a Galois extension, we write $\mathrm{Gal}(E/F) = \mathrm{Aut}(E/F)$.

In the history, this concept is used to solve polynomial equations.

Let $f \in \mathbb{Q}[x]$, let $x_1, \ldots, x_n$ be all roots of f. Consider $E = \mathbb{Q}(x_1, \ldots, x_n)$, and define $\mathrm{Gal}(f) = \mathrm{Gal}(E/\mathbb{Q})$. Back in the times of Galois, the concept of field haven't been developed yet, so what he did is to consider the bijections between the roots of f.

Galois discovered that f has radical solutions if and only if the group $\mathrm{Gal}(f)$ has a property, and he named it "solvable". Since all the subgroups of S_4 are solvable, thus if $\deg f \leq 4$, f always has radical solutions, but $A_5 < S_5$ is not solvable, so polynomials of degree greater than 4 may not have radical solutions.

One of the ultimate goal of modern algebra is to comprehend the group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

A tool developed for this goal is *group representation.* A representation of a group G is a homomorphism $\varphi : G \to \mathrm{GL}(V)$. Since $\mathrm{GL}(V)$ is something people knows very well, so when the elements of an abstract group G is viewed as linear maps, it's easier to discover more properties of G.

When $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, the representation is called a *Galois representation*. Even one dimensional Galois representations are very nontrivial.