Linear Algebra II

Felix Chen

Contents

First we prove a lemma:

Lemma 0.1

Let $\alpha \in V$ with $p_\alpha = p_T$, $\forall L \in V/R\alpha$, exists $\beta \in L$ s.t. $p_\beta = p_L$.
Here $f \cdot L := f(T_{V/R\alpha})L$, so $fL = 0 \iff f(T)\beta \in R\alpha$, $\forall \beta \in L$.

Proof. For all $\beta \in L$, we must have $p_\beta L = 0$, since $L = \beta + R\alpha, T(R\alpha) = R\alpha$.
If $p_L\beta \neq 0$, since $p_L\beta \in R\alpha$, thus $p_L\beta = f\alpha$ for some $f \in R$.
Because $p_L \mid p_\beta \mid p_\alpha = p_T$,

$$\left(\frac{p_\alpha}{p_L}\right) f\alpha = p_\alpha \beta = 0.$$

We have $\frac{p_\alpha}{p_L} f$ is an annihilator of α, hence it's a multiple of p_α, i.e. $p_L \mid f$.
Let $f = p_L h$, $\beta_0 = \beta - h\alpha$, we have $p_L\beta_0 = f\alpha - p_L h\alpha = 0 \implies p_{\beta_0} = p_L$. □

Returning to our original theorem, we'll prove by induction on n.

Take $\alpha_1 \in V$ s.t. $p_{\alpha_1} = p_T$. Consider $V/R\alpha_1$, its dimension is strictly lesser than n. By induction hypo, $\exists L_2, L_3, \ldots, L_r \in V/R\alpha_1$, such that

$$V/R\alpha_1 = \bigoplus_{i=1}^{r} RL_i, \quad p_{L_r} \mid \cdots \mid p_{L_2}.$$

Take $\alpha_i \in L_i$ s.t. $p_{\alpha_i} = p_{L_i}$, we must have $p_{\alpha_r} \mid \cdots \mid p_{\alpha_1} = p_T$.
If there exists $g_i\alpha_i \in R\alpha_i$ s.t. $\sum_{i=1}^{r} g_i\alpha_i = 0$, then

$$\sum_{i=2}^{r} g_i L_i = 0 \implies g_i L_i = 0 \implies g_i\alpha_i = 0.$$

For any $\gamma \in V$, since $\gamma \in \gamma + R\alpha_1$, by induction hypo, $\gamma + R\alpha_1 = \sum_{i=2}^{r} h_i L_i$.
This means $\gamma - \sum_{i=2}^{r} h_i\alpha_i \in R\alpha_1$, this completes the existence part of the theorem.

As for the uniqueness part, note that $p_T = \operatorname{lcm}(p_1, \ldots, p_r) = p_1$ and $f_T = p_1 \cdots p_r$, suppose $q_1, \ldots, q_s$ are also invariant factors of T, we must have $p_1 = q_1 = p_T$ and $\prod p_i = \prod q_i$.
Assume for contradiction that $\exists 2 \leq t \leq \min\{r, s\}$ s.t. $p_t \neq q_t$, but $p_i = q_i$ for all $i < t$.
Multiplying p_t on both sides of $\bigoplus_{i=1}^{r} R\alpha_i = \bigoplus_{i=1}^{s} R\beta_i$ we get:

$$\bigoplus_{i=1}^{t-1} Rp_t\alpha_i = p_t V = \bigoplus_{i=1}^{t-1} Rp_t\beta_i \oplus \bigoplus_{i=t}^{s} Rp_t\beta_i.$$

Now observe that

- For monic polynomial f, g, if $p_\alpha = fg$, then $p_{f\alpha} = g$ as $h(f\alpha) = 0 \iff (fh)\alpha = 0$.

Hence

$$\dim Rp_t\alpha_i = \deg p_{p_t\alpha_i} = \deg \frac{p_i}{p_t} = \deg \frac{q_i}{p_t} = \deg Rp_t\beta_i.$$

This implies $\bigoplus_{i=t}^{s} Rp_t\beta_i = \{0\}$, in particular $p_t\beta_t = 0 \implies p_t \mid q_t$. Similarly $q_t \mid p_t \implies p_t = q_t$, contradiction!

Theorem 0.2

Let G be a finite abelian group, then $\exists g_1, \dots, g_r \in G\backslash\{0\}$, such that $G = \bigoplus_{i=1}^{r} \mathbb{Z}g_i$ and $|\mathbb{Z}g_r| \mid \cdots \mid |\mathbb{Z}g_1|$.

Remark 0.3 — The proof is identical to the proof above.

§0.1 Rational canonical forms

Let $d_i = \deg p_i = \dim R\alpha_i$, $\mathcal{B}_i = \{\alpha_i, \dots, T^{d_i-1}\alpha_i\}$ is a basis of $R\alpha_i$. Then $[T_{R\alpha_i}]_{\mathcal{B}_i}$ is the companian matrix C_{p_i}, hence T can be represented as a blocked diagonal matrix with each block is C_{p_i} for invariant factors p_i. This is called the **rational canonical form** of T.

Definition 0.4. We say $A \in F^{n\times n}$ is **rational** if exists monic $p_1, \dots, p_r \in F[x]$, such that $p_r \mid \cdots \mid p_1$ and $A = \operatorname{diag}(C_{p_1}, \dots, C_{p_r})$.

Theorem 0.5

Let $T \in L(V)$, then T has a unique rational canonical form.

Proof. If $[T]_{\mathcal{B}'} = \operatorname{diag}(C_{q_1}, \dots, C_{q_r})$ is another rational canonical form, let $\mathcal{B}' = (\mathcal{B}'_1, \dots, \mathcal{B}'_r)$.

It's easy to observe that $\operatorname{span} \mathcal{B}'_i = R\beta_i$, where β_i is the first element in $\mathcal{B}_i$, so $V = \bigoplus_{i=1}^{r} R\beta_i$ is a cyclic decomposition of V, by the previous theorem we deduce the canonical form is unique. □

So far we've proved that $A \sim B \iff A, B$ have the same rational canonical form. Note that this canonical form does not require any extra properties of the base field F.

Next we'll see some applications of it. Different from Jordan canonical forms, rational canonical forms focus more on theory than computaion.

Proposition 0.6 (Rational canonical forms don't depend on fields)

Let $A \in F^{n\times n}$ has rational canonical form A', and the invariant factors are $p_1, \dots, p_r \in F[x]$.

If $K \subset F$ is a smaller field s.t. $A \in K^{n\times n}$, then A' is still the rational canonical form of A in K. i.e. $A' \in K^{n\times n}$, and $\exists P \in K^{n\times n}, A' = PAP^{-1}$.

Proof. Let A'' be the rational form of A on K. By the uniqueness of rational canonical forms, we must have $A' = A''$, since they are both the rational form of A on F. □

Proposition 0.7 (Similarity in larger fields implies similarity in smaller fields)
Let A, B be matrices on F, and $A \sim B$ in F. If $A, B \in K^{n\times n}$, where K is a subfield of F, then $A \sim B$ in K as well.

Proof. Let C be the rational canonical form of A, B, since $A, B \in K^{n\times n}$, by the previous proposition, $C \in K^{n\times n}$ and $A \sim C \sim B$ in K. □

Proposition 0.8
$\forall A \in F^{n\times n}$, $A \sim A^t$.

Proof. Firstly when $A = C_f$ for some $f \in F[x]$, A has only one invariant factor f. Note that $f_{A^t} = p_{A^t} = f_A = p_A = f$, so the invariant factor of A^t is also f, by rational canonical forms we're done.

Next for generic matrix A, just take the rational canonical form B. By above we have

$$A \sim B \implies A \sim B \sim B^t \sim A^t.$$

□

Example 0.9 (How to compute the rational canonical forms (in low dimensions))
Let $A = \begin{pmatrix} 5 & -6 & -6 \\ -1 & 4 & 2 \\ 3 & -6 & -4 \end{pmatrix} \in \mathbb{Q}^{3\times 3}$. First observe that $f_A = (x-1)(x-2)^2$.

Since $(x-1)(x-2)$ is the minimal polynomial of A, so the invariant factors are $p_1 = (x-1)(x-2), p_2 = (x-2)$. Hence the rational canonical form of A is

$$\begin{pmatrix} 0 & -2 & 0 \\ 1 & 3 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

Next we'll find vectors α_1, α_2 s.t. $p_{\alpha_i} = p_i$. So $P = (\alpha_1, A\alpha_1, \alpha_2)$ will be the transition matrix.

Proposition 0.10
Let T be a diagonalizable map, $\sigma(T) = \{c_1, \ldots, c_k\}$. Let $V_1, \ldots, V_k$ be the primary decomposition of V,

- Let $\alpha = \sum_{i=1}^{k} \beta_i, \beta_i \in V_i$, then $R\alpha = \text{span}\{\beta_1, \ldots, \beta_k\}$, $p_\alpha = \prod_{\beta_i \neq 0}(x - c_i)$.
- Let $d_i = \dim V_i$, then $p_j = \prod_{d_i \geq j}(x - c_i)$.

Proof. Trivial but need some work to check it. □

§0.2 Primary cyclic decomposition and Jordan canonical forms

Theorem 0.11
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 0.12 (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 0.13 — 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 0.14 (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 $\mathcal{B}_i = \{\alpha_i, N_i\alpha_i, \dots, N_i^{r_i-1}\alpha_i\}$, 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 0.15

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 0.16 — 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 0.17

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 0.18

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 0.19 (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 $J_1J_2 = J_2J_1$.

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 0.20. $\exists f \in F[x]$ 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 $N^m = N'^{m'} = 0$) □