Linear Algebra II

Felix Chen

Contents

§0.1 Cyclic decomposition

In the following contents we'll assmue $R = F[x]$ if it's not specified.

Definition 0.1 (Cyclic maps)**.** Let V be a finite dimensional vector space and $T \in L(V)$. For $\alpha \in V$, $R\alpha = \{f\alpha \mid f \in R\} = \operatorname{span}\{\alpha, T\alpha, \dots\}$ is the smallest T-invariant subspace containing α.

We say T is **cyclic** if $\exists \alpha$ s.t. $V = R\alpha$. In this case α is called a **cyclic vector**.

Here $R\alpha$ is called the cyclic subspace spanned by α.

Remark 0.2 — The word "cyclic" comes from the theory of modules.

Note that $\dim R\alpha = 1 \iff \alpha$ is an eigenvector.

Example 0.3

Let $A = E_{21} \in F^{2\times 2}$. Then A is cyclic because $A\varepsilon_1 = \varepsilon_2$, $A\varepsilon_2 = 0$. This means ε_1 is a cyclic vector of A,

Now there's a natural question: When is T cyclic and how to find its cyclic vectors?

For a given vector α, let $M_\alpha = \{f \in R \mid f\alpha = 0\}$ is an ideal of R.

Note that $M_T \subset M_\alpha$ as $f \in M_T \implies f(T)\alpha = 0$, so M_α is nonempty, it has a generating element p_α, called the **annihilator** of α.

Proposition 0.4

Let $d = \deg p_\alpha$, then $\{\alpha, T\alpha, \dots, T^{d-1}\alpha\}$ is a basis of $R\alpha$. In particular, $\dim R\alpha = \deg p_\alpha$.

Proof. Linear independence:

If $\sum_{i=0}^{d-1} c_i T^i \alpha = 0$, let $g = \sum_{i=0}^{d-1} c_i x^1$.

$$g\alpha = 0 \implies g \in M_\alpha \implies p_\alpha \mid g.$$

But $\deg g \le d-1 < d = \deg p_\alpha \implies g = 0$.

Spanning:

Clearly $T^i\alpha \in R\alpha$. $\forall f \in R$, let $f = qp_\alpha + r$ with $\deg r < \deg p_\alpha$. Hence $f\alpha = r\alpha \in \operatorname{span}\{\alpha, T\alpha, \dots, T^{d-1}\alpha\}$. ☐

Since α is a cyclic vector $\iff \dim R\alpha = \dim V$, and $\deg p_\alpha \le \deg p_T \le \deg f_T = \dim V$, so we care whether these two inequalities can attain the equality.

Proposition 0.5

There exists $\alpha \in V$ s.t. $p_\alpha = p_T$.

Proof. Let $p_T = \prod_{i=1}^k p_i^{r_i}$.

$$W_i = \ker(p_i^{r_i}(T)) \implies V = \bigoplus_{i=1}^k W_i.$$

We claim that $\ker(p_i^{r_i-1}) \subsetneq W_i$ as $p_{T_{W_i}} = p_i^{r_i}$.

Take a vector $\alpha_i \in W_i \backslash \ker(p_i^{r_i-1}(T))$. By definition $p_{\alpha_i} \mid p_i^{r_i}, p_{\alpha_i} \nmid p_i^{r_i-1} \implies p_\alpha = p_i^{r_i}$.

Let $\alpha = \sum_{i=1}^k \alpha_i$. If $f\alpha = 0$, then $f\alpha_i = 0$ for $i = 1, \dots, k$ as $f\alpha_i \in W_i$.

$$f\alpha_i = 0 \implies p_{\alpha_i} \mid f \implies p_T \mid f.$$

This means we must have $p_\alpha = p_T$. □

Now we come to a conclusion:

Corollary 0.6

T is cyclic $\iff \deg p_T = \dim V \iff p_T = f_T$.

In this case, α is a cyclic vector $\iff p_\alpha = p_T$.

Let $n = \dim V$, T be a cyclic map, α be a cyclic vector. By previous proposition, $\{\alpha, T\alpha, \dots, T^{n-1}\alpha\}$ is a basis of V. Denote the basis by $\mathcal{B}$.

Observe that $[T]_\mathcal{B}$ is equal to

$$A = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -c_0 \\ 1 & 0 & 0 & \cdots & 0 & -c_1 \\ 0 & 1 & 0 & \cdots & 0 & -c_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & -c_{n-2} \\ 0 & 0 & 0 & \cdots & 1 & -c_{n-1} \end{pmatrix}$$

where c_i are the coefficients of $p_\alpha = p_T = f_T = \sum_{i=0}^n c_i x^i$. For a monic polynomial f, define C_f to be the matrix as above, called the **companion matrix** of f.

Proposition 0.7

If exists a basis $\mathcal{B}$ s.t. $[T]_\mathcal{B} = C_f$ for some monic polynomial f, then T is cyclic and $p_T = f$.

Proof. Let $\mathcal{B} = \{\alpha_1, \dots, \alpha_n\}$, we have $T^i\alpha_1 = \alpha_{i+1} \implies R\alpha_1 = V$ and $p_{\alpha_1} = f$. □

Remark 0.8 — In fact we can check directly that f is the characteristic polynomial of C_f.

This gives another proof of Cayley-Hamilton theorem:

Proof. For any $\alpha \in V$, consider $T_{R\alpha} \mid f_T$.

$$f_{T_{R\alpha}} = f_{C_{p_\alpha}} = p_\alpha \mid f_T$$

This implies that f_T is an annihilating polynomial of α, which means $f_T(\alpha) = 0, \forall \alpha \in V$, i.e. $f_T(T) = 0$. $\square$

Theorem 0.9 (Cyclic decomposition)

Let $T \in L(V)$, $\dim V = n$. There exists $\alpha_1, \dots, \alpha_r \in V$ s.t. $V = \bigoplus_{i=1}^r R\alpha_i$.

Furthermore, $p_{\alpha_r} \mid \cdots \mid p_{\alpha_1} = p_T$, $f_T = \prod_{i=1}^r p_{\alpha_i}$.

Here p_{α_i}'s are called the **invariant factors** of T. The invariant factors are *totally determined* by T.

First we prove a lemma:

Lemma 0.10

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 $p_L\beta_0 = f\alpha - p_L h\alpha = 0 \implies p_{\beta_0} = p_L$. $\square$

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, $\exists L_2, L_3, \dots, L_r \in V/R\alpha_1$, 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 $p_T = \operatorname{lcm}(p_1, \dots, p_r) = p_1$ and $f_T = p_1 \cdots p_r$, suppose $q_1, \dots, q_s$ 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 0.11

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

Remark 0.12 — The proof is identical to the proof above.

§0.2 Rational canonical forms

Let $d_i = \deg p_i = \dim R\alpha_i$, $\mathcal{B}_i = \{\alpha_i, \ldots, T^{d_i-1}\alpha_i\}$ 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 0.13. We say $A \in F^{n\times n}$ is **rational** if exists monic $p_1, \ldots, p_r \in F[x]$, such that $p_r \mid \cdots \mid p_1$ and $A = \operatorname{diag}(C_{p_1}, \ldots, C_{p_r})$.

Theorem 0.14

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

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

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. $\square$

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 0.15 (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 $p_1, \ldots, p_r \in F[x]$.

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. $\square$

Proposition 0.16 (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. $\square$

Proposition 0.17
$\forall A \in F^{n\times n}$, $A \sim A^t$.

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

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

$\square$

Example 0.18 (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 0.19
Let T be a diagonalizable map, $\sigma(T) = \{c_1, \dots, c_k\}$. Let $V_1, \dots, V_k$ be the primary decomposition of V,

- Let $\alpha = \sum_{i=1}^k \beta_i, \beta_i \in V_i$, then $R\alpha = \operatorname{span}\{\beta_1, \dots, \beta_k\}$, $p_\alpha = \prod_{\beta_i \neq 0}(x - c_i)$.
- 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. $\square$

§0.3 Primary cyclic decomposition and Jordan canonical forms

Theorem 0.20

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 0.21 (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 $q_i = p_{T_{V_i}}$.
- $q_1, \ldots, q_s$ 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 $\{u_1, \ldots, u_k\}$ be the set of all the monic prime factors of the minimal polynomials of $T_{W_1}, \ldots, T_{W_t}$.

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 0.22 — 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 0.23

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.