1 Canonical Forms

1.1 Review

1.1.1 Strategy to Find the Intersection of Two Subspaces

Suppose $W_1 = \operatorname{span}\{x_1, \ldots, x_k\}$ and $W_2 = \operatorname{span} y_1, \ldots, y_l$.

We want to find all the solutions of

$$\sum_{i=1}^{k} \lambda_i x_i = \sum_{j=1}^{l} \mu_j y_j.$$

These form a homogeneous system of equations, and we know how to solve it!

1.1.2 Strategy for Finding Jordan Canonical Basis

Fix an eigenvalue λ and find the dot diagram for $T|_{K_\lambda}$.

1. First find $(T - \lambda I)^3 v_1 \in \ker(T - \lambda I) \cap (\operatorname{im}(T - \lambda I)^3)$.
2. Solve for v_1, thus obtaining the first cycle.
3. Extend to a basis $(T-\lambda I)^3 v_1$, $(T-\lambda I)^2$, $(T-\lambda I)^2 v_3, \cdots \in \ker(T-\lambda I) \cap \operatorname{im}(T-\lambda I)^2$
4. Repeat the procedure for $v_2, v_3, \ldots$

2 Canonical Forms

Theorem 2.1

Let $A, B \in M_{n\times n}(\mathbb{F})$ be such that their characteristic polynomial split.

Then A, B are similar if and only if they have the same JCF (up to the reordering of blocks).

Remark 2.2. This is a useful method to test the similarity of matrices.

Proof.

First note the following observations:

1. A is similar to its Jordan Canonical form, because $[L_A]_\beta = J_A$ for some basis β.
2. If J_1 and J_2 are matrices in JCF, then they are similar to each other.
3. If J_1, J_2 are matrices in JCF corresponding to the same linear transfromation, then they are similar to each other (the basis can be reordered).

Let $\sim: M_{n\times n}(\mathbb{F}) \times M_{n\times n}(\mathbb{F}) \to M_{n\times n}(\mathbb{F})$ denote the relation

By the first observation, A is similar to J_A and B is similar to J_B.

If A, B are similar, then $A \sim B$, but $A \sim J_A$ and $B \sim J_B$, and hence $J_A \sim J_B$.

Suppose, on the other hand, that $J_A \sim J_B$ are the same up to reordering of blocks, and thus J_A and J_B are similar to each other by the second observation. $\square$

3 Review of Polynomials

Let $\mathbb{F}$ be a field.

Let $\mathbb{F}[x]$ denote the polynomials over $\mathbb{F}$.

We define a polynomial as a formal exrpession $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, where $a_i \in \mathbb{F}$ and $n \geq 0$.

Two polynomials are equal to each other if and only if all coefficients of the terms with the same power are equal.

A polynomial $f(x)$ can be evaluated at any element $c \in \mathbb{F}$ so that $f(c) = \sum_{i=1}^{n} a_i c^i \in \mathbb{F}$.

Polynomials are not the same as polynomial-functions, because the polynomials may be equal while the correspnodingq polynomial-functions are not.

For example, $f(x) = x^3 - x$ over $\mathbb{F} = \mathbb{Z}_2$ gives the zero function.

Definition 3.1. If $a_n \neq 0$, the degree of a polynomial is defined as $\deg f = n$.

e.g. $\deg f = 0$ if and only if $f(x) = a_0 \neq 0$.

Convention: $\deg 0 = -\infty$

The following properties hold:

- $\deg(fg) = \deg(f) + \deg(g)$
- $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$

Definition 3.2. If the leading coefficient a_n is such that $a_n = 1$, $f(x)$ is said to be *monic*.

3.1 Division Algorithm

If $f(x)$, $g(x) \in \mathcal{P}(\mathbb{F})$ and $g(x) \neq 0$, then there exist $q(x)$ and $r(x) \in \mathcal{P}(\mathbb{F})$ such that $f(x) = q(x)g(x) + r(x$ such that $\deg(r) < \deg(g)$.

These q, r can be found by long division.

Lemma 3.3

If $a \in \mathbb{F}$ and $f(a) = 0$, then $(x-a)|f(x)$.

Proof.

We use the Factor Theorem.

Note that $f(x) = f(x)(x-a) + r(a)$, where $\deg(r) \leq 0$, so r is constant.

We evaluate it at a: $f(a) = 0 + r(a)$, and hence $r(a) = 0.$, which means that $r(x) = 0$. $\square$

Lemma 3.4

If $a_1, \ldots, a_s \in \mathbb{F}$ are distinct zeroes of $f(x)$, then $\prod_{i=1}^{s}(x - a_i)|f(x)$.

Thus, $\deg f \geq s$, so $f(x)$ can have at most $\deg f$ zeroes.

Definition 3.5. We say that $f \in \mathbb{F}[x]$ is irreducible if $\deg f > 0$ and it cannot be written as a product of two polynomials of lesser positive degree.

e.g. $x - a$ is irreducible for all $a \in \mathbb{F}$. $x^2 + 1$ is irreducible over $\mathbb{R}$.

More generally, a quadratic or cubic polynomial is irreducible if and only if there is no zero in $\mathbb{F}$.

For the polynomial of degree greater than or equal to 4.

e.g. $(x^p - p) \in \mathbb{F}[\mathbb{Q}]$ is irreducible for all p prime.

Example 3.6

Over $\mathbb{Z}_2$, we know by plugging in 0 and 1 that $x^3 + x + 1$ is irreducible.

However, since over $\mathbb{Z}_2$ we have $(a + b)^2 = a^2 + b^2$, then $x^4 + x^2 + 1 = (x^2 + x + 1)^2$.

Definition 3.7. Two nonzero polynomials are relatively prime if there is no polynomial of positive degree dividing both of them.

Example 3.8

Over $\mathbb{Z}_2$, we know that $x^3 + x + 1$ and $x^4 + x^2 + 1$ are relatively prime, because $x^3 + x + 1$ is irreducible, and thus the only factor of positive degree is $x^3 + x + 1$. However, $(x^3 + x + 1) | x^4 + x^2 + 1$, since the quotient would be linear (but $x^4 + x^2 + 1$ has no zeroes).

Remark 3.9. In this way we see that distinct monic irreducible polynomials are relatively prime.

Theorem 3.10

If $f(x)$, $g(x)$ are relative prime, three exists $u(x)$ and $v(x) \in \mathbb{F}[x]$ such that $f(x)u(x) + g(x)v(x) = 1$.

Lemma 3.11

Suppose that f and g are polynomials that are relatively prime and $f | gh$. Then $f | h$.

Proof.

We know that $1 = fu + gv$, and therefore $h = fuh + ghv$, which means that $f | h$. □

Theorem 3.12

If $\phi(x)$ is irreducible and $\phi(x) | f(x)g(x)$, then $\phi(x) | f(x)$ or $\phi(x) | g(x)$.

Theorem 3.13 (Unique Factorisation)

If $f(x) \neq 0$, we can write $f(x) = c \prod_{i=1}^{n_s} \phi_s(x)^{n_s}$, where $c \in \mathbb{F} \setminus \{0\}$ and $\phi_i(x)$ are distinct monic irreducible polynomials with $n_i \geq 1$.

The factorisation is unique up to the ordering of the factors.

Example 3.14

Factor into irreducible polynomials over $\mathbb{F} = \mathbb{Z}_3$ $x^4 + x^2 + 1 = x^4 - 2x^2 + 1 = (x^2 - 1)^2$.

Remark 3.15. If $f(x) \neq 0$ and $f(x) = c\prod_{i=1}^{n_s} \phi_s(x)^{n_s}$, then the possible factors of $f(x)$ are $d\prod_{i=1}^{k_s}$ for $0 \leq k_i \leq n_i$ and $d \in \mathbb{F} \setminus \{0\}$.

4 Minimal Polynomials

Let V be a finite dimensional vector space over $\mathbb{F}$.

Suppose that $T \in \mathrm{End}(V)$ has a characteristic polynomial $f(t)$ with $\deg(f) = \dim$.

Recall that by Cayley-Hamilton Theorem we have that $f(T) = 0$.

Note that, however, f might not be monic, so we can rescale it in such a way that there exists a monic polynomial g of degree $\dim V$ such that $g(T) = 0$.

Definition 4.1. A minimal polynomial of T is a monic polynomial of the least degree such that $p(T) = 0$.

Remark 4.2. Note that $1 \leq \deg(p) \leq \dim V$.

By Cayley-Hamilton Theorem, a minimal polynomial exists.

e.g. Ifdim $V = n$ and $T = I$, then $t - 1$ is a minimal polynomial of T.

Example 4.3

For $V = \mathbb{F}^2$, $A \in M_{2\times 2}(\mathbb{F})$ such that $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$, then the characteristic polynomial is a minimal polynomial, because $A - \lambda I \neq 0$ for all $c \in \mathbb{F}$.