26/11/19

Similarly, any $n \times n$ matrix has a minimal polynomial.

**Prop 19.1** Let $T: V \to V$ linear map, $V$ vector space over $F$.

1) $T$ has a unique minimal poly $m_T(x) \in F[x]$.

2) For $p(x) \in F[x]$,

$$p(T) = 0 \iff m_T(x) \text{ divides } p(x).$$

Pf Sheet 8, Q1.

**Prop 19.2** $T: V \to V$ linear map.

1) $m_T(x)$ divides ~~that~~ the characteristic poly of $T$.

2) If $\lambda$ is an evalue of $T$, then $\lambda$ is a root of $m_T(x)$.

Pf 1) Cayley-Ham + 19.1(2).

2) Let

$$T(v) = \lambda v. \quad (v \neq 0)$$

Then

$$0 = m_T(T)(v) = m_T(\lambda)v.$$

Hence $m_T(\lambda) = 0$. //

Eg. 1) Min. poly of $I$ is $x-1$.

2) Min poly of $J = J_n(\lambda)$:

Well, char. poly of $J$ is $(x-\lambda)^n$.

We also know

$$(J-\lambda I)^{n-1} \neq 0.$$

Therefore min poly. is $(x-\lambda)^n$.

3) If A $n \times n$ over $\mathbb{C}$, with distinct evalues $\lambda_1, \ldots, \lambda_k$ the min poly

$$m_A(x) = \prod_{i=1}^{k} (x-\lambda_i)^{r_i}$$

where $r_i$ is the size of largest $\lambda_i$-block in the JCF of A.

(Sheet 8, Q2).

## 20. Direct sums

**Defn** Let $V$ be a vector space, with subspaces $V_1, \ldots, V_k$. We write

$$V = V_1 \oplus V_2 \oplus \ldots \oplus V_k$$

if, for every $v \in V$, there are unique vectors $v_i \in V_i$ s.t.

$$v = v_1 + v_2 + \ldots + v_k.$$

If  holds, we say $V$ is the <u>direct sum</u> of the subspaces $V_1, \dots, V_K$.

<u>Eg.</u> $\mathbb{R}^2 = Sp(1,0) \oplus Sp(0,1)$

<u>Prop 20.1</u> The following are equivalent:

1) $V = V_1 \oplus V_2$

2) $V_1 \cap V_2 = \{0\}$ and
$\dim V = \dim V_1 + \dim V_2$

<u>Pf.</u> Sheet 8, Q6. //.

<u>Prop 20.2</u> Following are equivalent:

1) $V = V_1 \oplus \dots \oplus V_k$

2) $\dim V = \sum_{i=1}^{k} \dim V_i$,

and if $B_i$ is a basis of $V_i$ then

$$B = B_1 \cup \dots \cup B_k$$

is a basis of $V$.

Pf <u>(1) ⇒ (2)</u> Assume

$$V = V_1 \oplus \dots \oplus V_k .$$

Let $B_i$ be a basis of $V_i$ for each $i$, and

$$B = B_1 \cup \dots \cup B_k .$$

<u>Claim</u> $B$ is a basis of $V$.

<u>Pf</u> a) <u>$B$ spans $V$</u>: clear, since $V = V_1 + \dots + V_k$.

b) <u>$B$ lin. indep</u>

Suppose

$$(🐰) \quad \sum_{b \in B_1} \alpha_b b + \dots + \sum_{c \in B_k} \gamma_c c = 0$$

(where coeffs $\alpha_b, \dots, \gamma_c \in F$).

~~[illegible]~~ Now

$$0 = 0 + \dots + 0$$

is the <u>unique</u> expression for $0$ as a sum in $V_1 + \dots + V_k$. Hence each term in LHS of (🐰) is $0$, and hence all coeffs $\alpha_b, \dots, \gamma_c$ are $0$. Hence $B$ is a basis of $V$.

(2) $\Rightarrow$ (1) Assume (2):

$B = B_1 \cup \dots \cup B_k$ is a basis of $V$. Clearly then

$$V = V_1 + \dots + V_k.$$

Suppose $v \in V$ has expressions

$$v = v_1 + \dots + v_k = v_1' + \dots + v_k'$$

($v_i, v_i' \in V_i$). Then

$$0 = (v_1 - v_1') + \dots + (v_k - v_k').$$

If any $v_i - v_i'$ is not $0$, this will give a linear relation on the vectors in $B$ ⨳.

Hence $v_i = v_i'$ $\forall i$, and so

$$V = V_1 \oplus \dots \oplus V_k. \checkmark$$

Eg. $V = \mathbb{R}^4$. Let

$V_1 = Sp(1100, 0110) = Sp(v_1, v$

$V_2 = Sp(2121) = Sp(v_3)$

$V_3 = Sp(0011) = Sp(v_4)$

Qn Is $\mathbb{R}^4 = V_1 \oplus V_2 \oplus V_3$?

Ans ~~A~~ By 20.2(2), need to check whether

$$v_1, v_2, v_3, v_4$$

is a basis of $\mathbb{R}^4$.

Well,

$$\begin{pmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{pmatrix} \longrightarrow \begin{pmatrix} & & * & \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

So <u>not</u> a basis.

## Direct sums and linear maps

<u>Prop 20.3</u> Let

$$V = V_1 \oplus \ldots \oplus V_k$$

~~wh~~ with basis $\mathcal{B} = \mathcal{B}_1 \cup \ldots \cup \mathcal{B}_k$ ($\mathcal{B}_i$ basis of $V_i$). Let $T : V \to V$ be a linear map, and suppose each $V_i$ is $T$-invariant. Let $T_{V_i}$ be the restriction of $T$ to $V_i$, and

$$A_i = [T_{V_i}]_{\mathcal{B}_i}.$$

Then

$$[T]_{\mathcal{B}} = A_1 \oplus \ldots \oplus A_k$$

$$= \begin{pmatrix} A_1 & & & O \\ & A_2 & & \\ O & & \ddots & \\ & & & A_k \end{pmatrix},$$

block-diagonal matrix.

Pf. As $V_1$ is $T$-invariant, $T(V_1) \leq V_1$, and this implies top left block of $[T]_B$ is $[T_{V_1}]_{B_1}$, and so on. //.

Prop 20.4 Let $T : V \to V$ with $V$ over $\mathbb{C}$, with char poly

$$p(x) = \prod_{i=1}^{k} (x - \lambda_i)^{a_i}$$

where $\lambda_1, \ldots, \lambda_k$ are the distinct evalues of $T$. Define for $1 \leq i \leq k$

$$V_i = \ker (T - \lambda_i I)^{a_i}.$$

Then

$$V = V_1 \oplus \ldots \oplus V_k.$$

Defn The subspaces ~~$V_i$~~

$$V_i = \ker (T - \lambda_i I)^{a_i}$$

are the generalized eigenspaces of $T$.

Pf. Sheet 8, Q8.

Eg $V = \mathbb{C}^3$, $T: V \to V$ given by

$$T(v) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix} v$$

Char poly: $x^2(x-1)$.

Generalised espaces

$$V_1 = \ker(T - I) = Sp(e_1 + e_3)$$

$$V_2 = \ker T^2 = Sp(e_2, e_3).$$

Then $B = B_1 \cup B_2 = \{e_1 + e_3, e_2, e_3\}$

is a basis of $V$, so $V = V_1 \oplus V_2$

and

$$[T]_B = \left(\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & 0 & 0 \\ 0 & 1 & 0 \end{array}\right) = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}.$$

28/11/19

Let $T: V \to V$ have char. poly

$$p(x) = \prod_1^k (x-\lambda_i)^{a_i}$$

and

$$V_i = \ker (T-\lambda_i I)^{a_i}$$

so that

$$V = V_1 \oplus \dots \oplus V_k$$

as in Prop 20.4.

Let $B = B_1 \cup \dots \cup B_k$ basis of $V$, ~~which~~ are $B_i$ basis of $V_i$.

## Prop 20.5

1) Each $V_i$ is $T$-invariant.

2) If $A_i = [T_{V_i}]_{B_i}$ then

$$[T]_B = A_1 \oplus \dots \oplus A_k$$

3) The only evalue of $A_i$ is $\lambda_i$.

Pf. 1) $v \in V_i \Rightarrow (T-\lambda_i I)^{a_i}(v) = 0$

$$\Rightarrow T(T-\lambda_i I)^{a_i}(v) = 0$$

$$\Rightarrow (T-\lambda_i I)^{a_i} T(v) = 0$$

$$\Rightarrow T(v) \in V_i$$

(2) follows from 20.7

(3) As $V_i = \ker(T-\lambda_i I)^{a_i}$,

$$(T_{V_i} - \lambda_i I)^{a_i} = 0$$

(the zero linear map $V_i \to V_i$).

Hence the only evalue of $T_{V_i}$ is $\lambda_i$. //.

Final remark By 20.5, to prove the JCF Thm. 18.3(1), it's enough to prove it for the matrices $A_i$, i.e. for matrices having a single evalue.

## 21. The JCF theorem for matrices with a single evalue.

Let $\dim V = n$, $T: V \to V$ and suppose $T$ has only one evalue $\lambda$. Then char. poly. is $(x-\lambda)^n$, so by C-H

$$(T - \lambda I)^n = 0$$

Define $S = T - \lambda I$.

Then $S^n = O$ and the only evalue of $S$ is $0$.

JCF thm 18.3(1) for $S$:

**Theorem 21.1** Let $\dim V = n$, and $S : V \to V$ linear map s.t. $S^n = O$. Then $\exists$ basis $B$ such that

$$[S]_B = J_{n_1}(0) \oplus \dots \oplus J_{n_k}(0).$$

**Cor. 21.2** Then for

$$T = S + \lambda I$$

~~then~~ we have

$$[T]_B = J_{n_1}(\lambda) \oplus \dots \oplus J_{n_k}(\lambda)$$

(which is the JCF thm 18.3(1) for $T$).

## Pf of Thm 21.1

Want to find basis $\mathcal{B}$ s.t.

$$[S]_{\mathcal{B}} = \begin{array}{c} v_{n_1} \cdots\cdots v_1 \\ \begin{pmatrix} 0 & 1 & & \\ & 0 & 1 & \\ & & \ddots & 1 \\ & & & 0 \end{pmatrix} \end{array} \oplus \cdots\cdots$$

$$J_{n_1}(0)$$

So want basis ordered $v_{n_1}, \ldots, v_1, \ldots$ s.t.

$$S(v_1) = v_2,\ S(v_2) = v_3, \ldots, S(v_{n_1}) = 0.$$

So basis $\mathcal{B}$ should start

$$v_1,\ S(v_1),\ S^2(v_2), \ldots, S^{n_1-1}(v_1)$$

(actually the reverse of this)

where $S^{n_1}(v_1) = 0$.

So we are looking for a basis of $V$ of the form

$$v_1, S(v_1), \ldots, S^{n_1-1}(v_1),$$

$$\vdots$$

$$v_k, S(v_k), \ldots, S^{n_k-1}(v_k)$$

where $S^{n_1}(v_1) = 0, \ldots, S^{n_k}(v_k) = 0$

(Jordan basis).

We prove such a basis exists by induction on $n = \dim V$.

Clear for $n = 1$.

Assume true for vector spaces of dim $< n$.

Let

$$\operatorname{Im}(S) = S(V) \leq V.$$

As $0$ is an evalue, $\ker(S) \neq 0$, so $S(V) \subsetneqq V$, ie.

$$\dim S(V) < n.$$

Let

$$W = S(V).$$

Then $W$ is $S$-invariant, as

$$S(W) = S(S(V)) \leq S(V) = W.$$

Apply induction to the restriction

$$S_W : W \to W.$$

So there is a Jordan basis (as in $\textcircled{$\approx$}$) of $W = S(V)$:

$$\underline{u_1, S(u_1), \ldots, S^{m_1 - 1}(u_1),} \qquad \boxed{\Xi}$$

$$\vdots$$

$$\underline{u_r, S(u_r), \ldots, S^{m_r - 1}(u_r)}$$

where $S^{m_i}(u_i) = 0 \ \forall i$ and

$$\sum_{i=1}^{r} m_i = \dim W.$$

Now we add vectors to this:

1) As each $u_i \in W = S(V)$, $\exists v_i \in V$ s.t. $u_i = S(v_i)$.

Add $v_i$ to the list ▤.

2) Note $\ker(S)$ contains the lin. indep vectors

$$S^{m_1-1}(u_1), \ldots, S^{m_r-1}(u_r)$$

Extend this to a basis of $\ker(S)$ by adding further vectors $w_1, \ldots, w_s$.

Note

$$\dim(\ker(S)) = r+s.$$

Adding the $v_i$'s and $w_i$'s to the list ▤, now have a new list of vectors

⊛

$$v_1, \underset{\overset{\downarrow}{u_1}}{S(v_1)}, \underset{\overset{\downarrow}{S(u_1)}}{S^2(v_1)}, \ldots, S^{m_1}(v_1),$$

$$\vdots$$

$$v_r, S(v_r), \ldots\ldots S^{m_r}(v_r),$$

$$w_1, \ldots, w_s$$

<u>Claim</u> The list ⊛ is a Jordan basis of $V$ (of form $\textcircled{\approx}$).

Pf. <u>Lin indep</u> Suppose $\exists$ linear relation

$$\alpha_1 v_1 + \dots + \alpha_{m_1+1} S^{m_1}(v_1)$$

$$+ \dots + \gamma_1 v_r + \dots + \gamma_{m_r+1} S^{m_r}(v_r) \qquad (\bigstar)$$

$$+ \delta_1 w_1 + \dots + \delta_s w_s = 0.$$

Apply $S$, noting $S^{m_i+1}(v_i) = 0 \ \forall i$: get

$$\alpha_1 S(v_1) + \dots + \alpha_{m_1} S^{m_1}(v_1)$$

$$+ \dots + \gamma_1 S(v_r) + \dots + \gamma_{m_r} S^{m_r}(v_r) = 0$$

(note $S(w_i) = 0 \ \forall i$).

This is a linear relation on the basis $\boxed{\equiv}$ of $S(V)$

Hence

$$\alpha_1 = \dots = \alpha_{m_1} = \dots = \gamma_1 = \dots = \gamma_{m_r}$$
$$= 0.$$

Now eqn $(\bigstar)$ is

$$\alpha_{m_1+1} S^{m_1}(v_1) + \dots + \gamma_{m_r+1} S^{m_r}(v_r)$$
$$+ \sum_1^s \delta_i w_i = 0.$$

This is a linear relation ~~on~~ a a basis of $\ker(S)$, so all coeffs are $0$:

$$\alpha_{m_1+1} = \dots = \gamma_{m_r+1} = \delta_i = 0 \ \forall i.$$

This proves linear independence of .

<u>Basis</u> No. of vectors in list  is

$$(m_1+1)+\ldots+(m_r+1)+s$$
$$=\sum_1^r m_i + r + s$$
$$= \dim W + \dim(\operatorname{Ker} S)$$
$$= \dim(\operatorname{Im} S) + \dim(\operatorname{Ker} S)$$
$$= \dim V = n.$$

Hence  is a basis

Finally, if $\mathcal{B}$ is the basis  (with each ~~from~~ sequence in the first r rows ~~rev~~ reversed), then

$$[S]_{\mathcal{B}} = J_{m_1+1}(0) \oplus \ldots \oplus J_{m_r+1}(0) \oplus \underbrace{J_1(0) \oplus \ldots \oplus J_1(0)}_{s},$$

a JCF.

This completes the proof of JCF Thm 18.3(1) by induction. //

29/11/19

**Defn** Let $T: V \to V$ linear map. A basis $B$ of $V$ such that $[T]_B$ is a JCF, is called a *Jordan basis* of $V$.

Eg. Find a Jordan basis for $S: \mathbb{C}^4 \to \mathbb{C}^4$ defined by

$$S(v) = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} v$$

**Ans** Note only evalue of $S$ is $0$, char. poly $x^4$. Strategy from the inductive pf of 21.1:

**Step 1** Let

$$W = S(V) = Sp(e_1, e_2+e_3).$$

**Step 2** Compute Jordan basis of $S_W : W \to W$:

$$u_1, \; S(u_1)$$

where $u_1 = e_2+e_3$.

**Step 3** Add further vectors

1) Add $v_1$ s.t. $u_1 = S(v_1)$;

take $v_1 = e_4$.

2) Extend $S(u_1)$ $(= 2e_1)$

to a basis of $\ker S$:

add $w_1 = e_2 - e_3$

By the pf of 21.1, here is a Jordan basis of $V = \mathbb{C}^4$:

$$\underset{\overset{\longleftrightarrow}{\text{reverse}}}{v_1, S(v_1), S^2(v_1)}, w_1$$

So basis is

$$\mathcal{B} = 2e_1, e_2+e_3, e_4, e_2-e_3$$

and

$$[S]_{\mathcal{B}} = J_3(0) \oplus J_1(0).$$

# PART C : Rings

## 22. Recap

Study rings $R = (R, +, \times)$, commutative with additive identity 0, multiplicative identity 1.

Egs. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_n$

$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$

($d \in \mathbb{Z}$ non-square)

(eg. $d = -1$, Gaussian integers $\mathbb{Z}[i]$).

Polynomial rings $F[x]$

($F$ a field)

Units : $u \in R$ is a unit if $\exists v \in R$ s.t. $uv = 1$.

Units form a group $U(R)$ under mult.

Eg. $U(\mathbb{Z}) = \{\pm 1\}$.

Integral Domain (ID)

These satisfy extra axiom

$$ab = 0 \implies a = 0 \text{ or } b = 0.$$

Eg, All above egs are ID's except for $\mathbb{Z}_n$ for $n = rs$, non-prime: since then

$$[r][s] = [0].$$

**Irreducibles** Say $a \in R$ is irreducible if

1) $a \neq 0$
2) $a \notin U(R)$
3) $a = bc \quad (b, c \in R)$

$$\Longrightarrow b \text{ or } c \text{ is a unit.}$$

Eg. In $\mathbb{Z}$, irreducibles are the primes

In $F[x]$, they are the irreducible polys.

## Euclidean Domain (ED)

An ID $R$ is an ED if $\exists$ function $\delta : R \setminus 0 \longrightarrow \mathbb{Z}_{\geq 0}$ s.t.

- $\delta(ab) \geq \delta(a) \quad \forall a, b \in R \setminus 0$
- for any $a, b \in R$ with $b \neq 0$, $\exists\, q, r \in R$ s.t.

$$a = qb + r$$

where either $r = 0$ or $\delta(r) < \delta(b)$.

Eg. 1) $R = \mathbb{Z}, \quad \delta(a) = |a|$

2) $R = F[x], \quad \delta(f(x)) = \deg(f)$

3) $R = \mathbb{Z}[i], \quad \delta(a+ib) = a^2 + b^2$

4) $R = \mathbb{Z}[\sqrt{-2}]$, $\delta(a+b\sqrt{-2})$
$= a^2+2b^2$.

(In fact for most values of $d$, $\mathbb{Z}[\sqrt{d}]$ is not an ED.)

## Unique Factorization Domain (UFD)

Say $R$ is a UFD if for any $a \in R$ with $a \neq 0$ and $a \notin U(R)$, the following hold:

1) $\exists$ factorization
$$a = b_1 \dots b_r$$
where each $b_i$ is irreducible

2) the $b_i$'s are unique, apart from mult. by units.

**Thm** Every ED is a UFD.

---

23.

## Homomorphisms and ideals

**Defn** Let $R$, $R'$ be rings.

Say $\phi : R \to R'$ is a homomorphism if

1) $\phi(a+b) = \phi(a)+\phi(b)$ $\forall a, b \in$

2) $\phi(ab) = \phi(a)\,\phi(b)$ $\forall a, b \in$

If $\phi$ is bijective, it is an isomorphism.

**Eg.** 1) Zero homom: $\phi(x) = 0 \ \forall x \in R$

2) $\phi : \mathbb{Z} \to \mathbb{Z}_n$ defined by

$$\phi(x) = [x] \quad \forall x \in \mathbb{Z}.$$

3) $\phi : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{2}]$,

$$\phi(a+b\sqrt{2}) = a - b\sqrt{2} \quad \forall a,b \in \mathbb{Z}.$$

Ex $\phi$ is an isomorphism.

4) $\phi : F[x] \to F$ :

$$\phi(p(x)) = p(0) \quad \forall p(x) \in F[x]$$

(eg. $\phi(x^2-3x+7) = 7$). is a homom.

**Defn** We say $I \subseteq R$ is an ideal if

1) $(I,+)$ is a subgroup of $(R,+)$

2) $i \in I, r \in R \Rightarrow ir \in I$

(concisely: $IR \subseteq I$).

Property (2) is much stronger than closure under × (subring)

**Example** Let $a \in R$ and define

$$I = \{ar : r \in R\}$$
$$= aR$$

**Claim** $aR$ is an ideal of $R$.

**Pf** 1) $0 = a0 \in aR$

$$ar_1 + ar_2 = a(r_1 + r_2) \in aR$$
$$-ar = a(-r) \in aR$$

Hence $(aR, +)$ a subgp of $(R, +)$

2) $(ar)s = a(rs) \in aR$. //

**Defn** We call the ideal

$$aR$$

the **principal ideal** generated by $a$.

Some texts denote $aR$ by $(a)$.

**Eg.** $R = \mathbb{Z}$, $a = 2$.

Principal ideal $2\mathbb{Z} = \{\text{even nos.}\}$.