27/11/17

Defn Let $S: V \to V$ with $S^n = 0$. A basis B of V as in Thm 18.8 is called a Jordan basis of V.

[More generally, for any $T: V \to V$, a Jordan basis of V is a basis B s.t.

$$[T]_B = \text{JCF matrix}].$$

Eg. Define $S: \mathbb{C}^4 \to \mathbb{C}^4$ by

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

Find a Jordan basis of $\mathbb{C}^4 = V$

Ans Use the idea of pf of 18.8.

Step 1 Let

$$W = S(V)$$
$$= \text{col-sp}(A)$$
$$= \text{sp}(e_1, e_2 + e_3).$$

Step 2 Find a Jordan basis:

$u_1, S(u_1)$

$= e_2+e_3, 2e_1$

Step 3 Add vectors to this:

1) find v_1 s.t. $u_1 = S(v_1)$:
take $v_1 = e_4$

2) extend $S(u_1)$ to a basis of $\ker(S)$: add $w_1 = e_2 - e_3$.

By the proof of 18.8, Jordan basis of $V = \mathbb{C}^4$ is

$B = e_4, e_2+e_3, 2e_1, e_2-e_3$.

Check

$[S]_B = J_3(0) \oplus J_1(0)$.

Minimal polynomial

Defn Let V be vector space over F, and $T: V \to V$.
A poly. $m(x) \in F[x]$ is a minimal poly for T if

1) $m(T) = 0$
2) leading coeff of $m(x)$ is 1 (this says $m(x)$ is monic)
3) $\deg(m)$ is as small as possible

Note Such a poly exists, by Cayley-Hamilton.

Prop 18.10 A linear map $T: V \to V$ has a unique min. poly.

Pf. Space $m_1(x)$ and $m_2(x)$ are different min. polys. They must have the same degree, so

$$m_1(x) = x^r + \cdots$$
$$m_2(x) = x^r + \cdots$$

Then $\deg(m_1 - m_2) < r$, and $(m_1 - m_2)(T) = 0$. ⊗

Write

$$m_T(x)$$

for the min. poly of $T: V \to V$.

Similarly an $n \times n$ matrix has a unique min poly $m_A(x)$.

Basic property of $m_T(x)$:

Prop 18.11 Let $T: V \to V$ and let $p(x) \in F[x]$. Then

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

Pf ($\Longleftarrow$) $p(x) = m_T(x)\, q(x)$

$$\Longrightarrow p(T) = m_T(T)\, q(T)$$
$$= 0$$

($\Longrightarrow$) Space $p(T) = 0$. Write

$$p(x) = q(x)\, m_T(x) + r(x)$$

where $\deg(r) < \deg(m_T)$.

Then

$$0 = p(T) = q(T)\, m_T(T) + r(T)$$
$$= r(T).$$

As $\deg(r) < \deg(m_T)$, this implies $r = 0$, so m_T divides p. //

Prop 18.12

(1) $m_T(x)$ divides the char. poly. of T.

(2) Every evalue of T is a root of $m_T(x)$.

Pf (1) Let $p(x)$ be the char. poly of T. By Cayley-Hamilton, $p(T) = 0$. Hence m_T divides p by 18.11.

(2) Let λ be an evalue of T, and v an evector, so

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

Then

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

As $v \neq 0$, this implies $m_T(\lambda) = 0$. //

Eg. 1) Min. pdy of I is

$$x - 1.$$

2) Min. pdy of

$$J = J_n(\lambda) = \begin{pmatrix} \lambda & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda \end{pmatrix}.$$

Well, char pdy is $(x-\lambda)^n$, (so min pdy divides this by 18.12).

Also

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

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

Hence

$$m_J(x) = (x-\lambda)^n$$

(Here $m_J(x)$ = char. pdy of J.)

To compute min. poly:

Suppose A is $n \times n$ over $\mathbb{C}$, with distinct evalues $\lambda_1, \ldots, \lambda_r$.

Then

$$m_A(x) = (x-\lambda_1)^{a_1} \cdots (x-\lambda_r)^{a_r}$$

where a_i is the size of the largest λ_i-block in the JCF of A.

(Sheet 8 qn).

Completion of proof of JCF Th 18.3 (1)

(A) Direct sums

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

We say

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

if every vector $v \in V$ can be expressed as

$$v = v_1 + v_2 + \cdots + v_k$$

for <u>unique</u> vectors $v_i \in V_i$.

We say V is the direct sum of the subspaces $V_1, \dots, V_k$.

Eg $\mathbb{R}^2 = \mathrm{Sp}(1,0) \oplus \mathrm{Sp}(0,1)$.

Prop 18.13 The following are equivalent:

1) $V = V_1 \oplus V_2$

2) $\dim V = \dim V_1 + \dim V_2$

and $V_1 \cap V_2 = \{0\}$.

Pf. Sheet 8, q4.

Prop 18.14 The following are equivalent:

1) $V = V_1 \oplus V_2 \oplus \dots \oplus V_k$

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

and if B_i is a basis of V_i, $(1 \le i \le k)$, then

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

is a basis of V.

28/11/17

Proof (1) $\Rightarrow$ (2)

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

Let B_i be a basis of V_i, and

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

Claim B is a basis of V.

Pf. Span: This is clear, since

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

Lin. indep. Suppose

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

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

$0 = 0 + \dots + 0$ is the unique expression for zero vector 0 as a sum of vectors in $V_1, \dots, V_k$.

Hence each term in LHS of (🐰) is 0, i.e.

$$\sum_{b \in B_1} \alpha_b b = 0, \text{ etc.}$$

As each B_i is a basis of V_i, hence is linearly indep, this means all coeffs $\alpha_b, \dots, \gamma_c$ in (🐰) are 0.

Hence Claim is proved,
so (2) holds.

(2) $\Rightarrow$ (1) Assume (2): let B_i be a basis of V_i, and then $B = B_1 \cup \dots \cup B_k$ is a basis of V.

Clearly this implies

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

Suppose for uniqueness, suppose

$$\begin{aligned} v &= v_1 + \dots + v_k \\ &= v_1' + \dots + v_k' \end{aligned}$$

where $v_i, v_i' \in V_i$.

Then

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

If any $(v_i - v_i')$ is nonzero, this will give a linear relation on the vectors in B with some nonzero coeffs.

As B is a basis, this is not possible. Hence

$$v_i = v_i' \quad \forall i.$$

So any $v \in V$ is a unique sum $v_1 + \dots + v_k$, i.e.

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

Prop 18.14 makes it easy to recognise direct sums:

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

$V_1 = \mathrm{Sp}\left((1,1,0,0), (0,-1,1,0)\right)$

$V_2 = \mathrm{Sp}\left(2,1,2,1\right)$

$V_3 = \mathrm{Sp}\left(0,0,1,1\right)$

Is $V = V_1 \oplus V_2 \oplus V_3$?

Ans Need to see whether

$$B = \{(1,1,0,0), (0,-1,1,0), (2,1,2,1), (0,0,1,1)\}$$

is a basis of $V = \mathbb{R}^4$. NO !

Link with linear maps:

Prop 18.15 Suppose

$$V = V_1 \oplus \cdots \oplus V_k$$

with basis $B = B_1 \cup \cdots \cup B_k$,

(B_i basis of V_i).

Suppose $T: V \to V$ is a linear map such that each V_i is T-invariant.

Let $T_i = T_{V_i}$, restriction of T to V_i, and

$$A_i = [T_i]_{B_i}.$$

Then

$$[T]_B = A_1 \oplus \cdots \oplus A_k,$$

block-diagonal matrix.

Pf Since $T(V_1) \subseteq V_1$, the top left block of $[T]_B$ is $[T_1]_{B_1} = A_1$. Similarly, the next diagonal block is $[T_2]_{B_2} = A_2$, and so on. //

(B) Reduction of JCF proof to case of 1 evalue

This is

Thm 18.16 Let $T: V \to V$ have 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

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

Then

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_k.$$

Deduction of JCF thm 18.3(1)

Let $T: V \to V$. Then

$$V = V_1 \oplus \cdots \oplus V_k$$

as in 18.16.

Claim 1 Each V_i is T-invariant.

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

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

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

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

Hence $T(V_i) \subseteq V_i$.

Claim 2 Each restriction $T_i = T_{V_i}$ has only one evalue, namely λ_i.

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

$$(T_i - \lambda_i I)^{a_i} = O_{V_i}$$

So λ_i is the only evalue of T_i.

Final Step

By 18.9 (JCF thm in case of one evalue)

there is a Jordan basis B_i of V_i (i.e. basis s.t. $[T_i]_{B_i} = J_i$, a JCF matrix $J_{n_1}(\lambda_i) \oplus \dots \oplus J_{n_r}(\lambda_i)$).

By 18.14 and 18.15, $B = B_1 \cup \dots \cup B_k$ is a basis of V, and

$$[T]_B = J_1 \oplus \dots \oplus J_k,$$

which is a JCF matrix.

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

Proof of Thm 18.16

Recall (MIP2): F field, $F[x]$ is the set of polys. in x over F. Any two polys $f(x), g(x)$ of degree ≥ 1 have a hcf $(f(x), g(x)) = d(x)$ (poly. of highest degree dividing f & g). Also $\exists$ polys. $s(x), t(x)$ such that

$$d = sf + tg$$

If hcf$(f,g) = 1$, say f, g are coprime.

Prop 18.17 Let V be over F, and $T: V \to V$ linear map.

Suppose $f(x), g(x) \in F[x]$ are coprime and

$$f(T)\, g(T) = 0.$$

Then

$$V = \ker f(T) \oplus \ker g(T).$$

Pf. By  , $\exists$ polys. $s, t \in F[x]$ s.t.

$$1 = sf + tg.$$

So

$$s(T) f(T) + t(T) g(T) = 1_V,$$

the identity map.

Let $v \in V$. Then

$$\begin{aligned} v &= s(T)f(T)(v) + t(T)g(T)(v) \\ &= v_1 + v_2 \end{aligned}$$

Then $v_1 \in \ker g(T)$, since

$$\begin{aligned} g(T)(v_1) &= g(T)\, s(T)\, f(T)(v) \\ &= s(T) f(T) g(T)(v) \\ &= 0 \end{aligned}$$

Similarly $v_2 \in \ker f(T)$. Hence

$$\underline{V = \ker f(T) + \ker g(T)}$$

Also

$v \in \ker f(T) \cap \ker g(T)$

$\Rightarrow v = s(T) f(T)(v) + t(T) g(T)(v)$

$= 0.$

So $\ker f(T) \cap \ker g(T) = 0.$

Hence result by 18.13. //.

Proof of Thm 18.16

$T: V \to V$ has char poly

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

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

We aim to prove

$$V = V_1 \oplus \cdots \oplus V_k$$

by induction on k.

Case $k = 1$: Here

$$p(x) = (x - \lambda)^a$$

(where $a = \dim V$)

and $\ker (T-\lambda I)^a = V$

by Cayley-Hamilton.

Now assume $k > 1$. Let

$$f(x) = (x-\lambda_1)^{a_1}, \quad g(x) = \prod_{i=2}^{k} (x-\lambda_i)^{a_i}.$$

Then $\text{hcf}(f,g) = 1$ and

$$f(T)\,g(T) = p(T) = 0.$$

Hence by 18.17,

$$V = \ker f(T) \oplus \ker g(T).$$
$$= V_1 \oplus \ker g(T).$$

By inductive hypothesis applied to the restriction of T to $\ker(g(T))$,

$$\ker g(T) = V_2 \oplus \cdots \oplus V_k.$$

Hence

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_k,$$

completing pf of 18.16 by induction. //

PART C : Ring Theory

19. Recap.

We study rings $R = (R, +, \times)$

that are commutative with 1, i.e.

1) $(R, +)$ abelian gp.

2) $(R, \times)$ assoc., commutative with identity 1

3) distributive.

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

$F[x]$, F field.

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

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

Units $u \in R$ unit if $\exists v \in R$

s.t. $uv = 1$.

Units form unit group (under $\times$),

written $U(R)$

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

$U(F[x]) = F^*$

More unit gps: Sheet 8.

Integral Domains (ID):

Extra axiom:

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

Eg All above, except $\mathbb{Z}_n$ (n not prime)

Irreducible elts

Say $a \in R$ is <u>irreducible</u>

if $a \neq 0$, $a \notin U(R)$ and

$$a = bc \quad (b, c, \in R)$$

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

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

In $F[x]$, have irreducible poly's.

Euclidean Domains (ED)

An ID R is an ED if

$\exists\, \delta : R \setminus 0 \longrightarrow \mathbb{Z}_{\geq 0}$ s.t.

1) $\delta(ab) \geq \delta(a) \quad \forall a, b \in R \setminus 0$

2) if $a, b \in R$, $b \neq 0$

Then $\exists\, q, r \in R$ s.t.

$$\underline{a = qb + r}$$

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

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

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

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

4) $R = \mathbb{Z}[\sqrt{-2}]$,

& $\delta(a + b\sqrt{-2}) = a^2 + 2b^2$

(check 8, qn).

Unique Factorization Domain (UFD)

Def: An ID R is a UFD if for any $a \in R$, $a \neq 0$, unit

1) $a = b_1 \cdots b_r$, b_i irreducible elts

2) the irreducibles b_i are unique apart from mult. by units.

Thm 19.1 Every ED is a UFD.

20. Homomorphisms & ideals

R, R' commutative with 1.

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

1) $\phi(a+b) = \phi(a) + \phi(b)$

2) $\phi(ab) = \phi(a)\phi(b)$

$\forall a, b \in R$.

If ϕ is a bijection, it is an isomorphism.

Note $\phi(0) = 0'$

But $\phi(1)$ might not be $1'$.

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

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

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

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

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

Check ϕ is an isomorphism.

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

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

Ideals

Defn $I \subseteq R$ is an ideal if

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

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

(concisely, $IR \subseteq I$).

Note: (2) is much stronger than closure of I under $\times$.

Eg. 1) $R = \mathbb{Z}$

I = set of even nos.

2) $R = \mathbb{Z}$, $n \in \mathbb{Z}$

$I = \{nx : x \in \mathbb{Z}\}$

all multiples of n

3) Any R, let $a \in R$ and

$$I = \{ar : r \in R\}$$
$$= (a).$$

Then I is an ideal of R, called the <u>principal ideal</u> generated by a.