46.1.

Modules over PIDs:

AKA linear algebra in more generality.

Recall that an R-module M is free if it has a finite basis: there exist $a_1, \dots, a_n \in M$ s.t., for all $x \in M$, we have $x = r_1 a_1 + \dots + r_n a_n$ for unique $r_1, \dots, r_n$.

Have $M \cong R^n$ as R-modules.

Proposition. Let R be an integral domain, and let M be a rank (dimension) n R-module.

Then any set of $n+1$ vectors is linearly dependent.

Proof 1. Embed R in its quotient field F.

By linear algebra, there is a relation in F. Clear denominators.

Proof 2. Use determinants.

Def. If R is a domain and M is any R-module,

$$\mathrm{Tor}(M) := \{ x \in M : rx = 0 \text{ for some } 0 \neq r \in R \}.$$

This is the torsion submodule (ex: prove it's a submodule) of M.

If $\mathrm{Tor}(M) = 0$, then M is torsion-free.

Def. For any submodule $N \subseteq M$, the <u>annihilator</u> of N is

$$\mathrm{Ann}(N) = \{ r \in R : rn = 0 \text{ for all } n \in N \}.$$

Basic properties: (0) $\mathrm{Ann}(\{x\}) = \mathrm{Ann}(Rx)$.

(1) $\mathrm{Ann}(N) \trianglelefteq R$.

(2) If $N \not\subseteq \mathrm{Tor}(M)$ (if N is "not a torsion submodule") then $\mathrm{Ann}(N) = 0$.

(3) If $N \subseteq L$ then $\mathrm{Ann}(L) \subseteq \mathrm{Ann}(N)$.

(4) If R is a PID, $N \subseteq L$, $\mathrm{Ann}(N) = (a)$, $\mathrm{Ann}(L) = (b)$, then $a \mid b$.

(5) If R is a PID, and $x \in M$, $\mathrm{Ann}(x) \mid \mathrm{Ann}(M)$.

Example. Consider the $\mathbb{Z}$-module $M = \mathbb{Z} \times \mathbb{Z}/6$.

Then: $\mathrm{Tor}(M) \cong \mathbb{Z}/6$.

$\mathrm{Ann}(0 \times \mathbb{Z}/6) = 6\mathbb{Z} \subseteq \mathbb{Z}$.

$\mathrm{Ann}(0 \times 2\mathbb{Z}/6) = 3\mathbb{Z} \subseteq \mathbb{Z}$.

$\mathrm{Ann}(0 \times 3\mathbb{Z}/6) = 2\mathbb{Z} \subseteq \mathbb{Z}$.

Def. If R is an integral domain, the rank of an R-module M is the maximum # of R-linearly independent elements of M.

By proposition,

$\mathrm{rk}(\text{any submodule of } M) \leq \mathrm{rk}(M)$.

46.3. (= 47.1)

Careful! A torsion-free R-module need not be free.

(exercise 12.1.5.)

Example. $R = \mathbb{Z}[x]$, $M = (2, x)$ ideal of R hence an R-module.

Torsion free because R is.

This has rank 1.

Theorem. Let R be a PID, M a free R-module of rank n, $N \subseteq M$ submodule. Then:

(1) N is free of rank m, with $m \leq n$.

(2) There is a basis $y_1, \dots, y_n$ of M s.t. $a_1 y_1, \dots, a_m y_m$ is a basis of N for some $a_1 \dots a_m$ satisfying $a_1 \mid a_2 \mid \cdots \mid a_m$.

Example. $R = \mathbb{Z}$, ~~$N \subseteq M$~~ ~~are~~ ~~$(2\mathbb{Z})^3 \subseteq \mathbb{Z}^3$~~.

let $M = \mathbb{Z}^2$,

$N \subseteq M = \langle (6, 8), (10, 4) \rangle$.

Pop quiz: what is N? Not obvious by looking.

$N \subseteq (2\mathbb{Z})^2$. Is it equal ___?

Anyway, can write bases for M, N simultaneously.

Proof. Assume $N \neq \{0\}$.

Let $\Sigma = \{(a_\varphi) : \varphi \in \mathrm{Hom}_R(M, R)\}$.

what does that mean? If φ is an R-mod hom $M \to R$,

$\varphi(N)$ is an R-submodule of R,

hence an ideal,

hence a principal ideal (a_φ).

Then Σ is nonempty, containing (0).
It contains a maximal elt. because R is Noetherian

consider

$\nu : M \longrightarrow R$ where $\nu(N) = (a_\nu)$ maximal

Write $a_1 = a_\nu$ and let $y \in N \longrightarrow a_1$.

Claim. $a_1 \neq 0$. Use freeness, maximality.
Here is an elt. of $\mathrm{Hom}_R(M, R)$ whose image is not just zero. Have projection homomorphisms

$$\pi_i : \underbrace{r_1 m_1 + r_2 m_2 + \cdots + r_n m_n}_{\text{Here } m_1 \cdots m_n \text{ is any basis}} \longrightarrow r_i$$

Since $N \neq 0$, some element has to have some nonzero coordinate.

Claim. $a_1 \mid \varphi(y)$ for all $\varphi \in \mathrm{Hom}_R(M, R)$.
Let $(d) = (a_1, \varphi(y))$ so that $d = r_1 a_1 + r_2 \varphi(y)$ for $r_1, r_2 \in R$.

Get a homomorphism $M \longrightarrow R$

$$\psi := r_1 \nu + r_2 \varphi.$$

Then $\psi(y) = (r_1 \nu + r_2 \varphi)(y) = r_1 \nu(y) + r_2 \varphi(y)$
$= r_1 a_1 + r_2 \varphi(y) = d$.

So $d \in \psi(N)$ and $(d) \subseteq \psi(N)$.
But $(a_1) \subseteq (d)$, and (a_1) was maximal
so $(a_1) = (d) = \psi(N)$ and since $d \mid \varphi(y)$,
$a \mid \varphi(y)$.

In particular, $a_1 \mid \pi_i(y)$ for all i.

Writing $\pi_i(y) = a_1 b_i$ for some $b_i \in R$ for each i,

$$y_1 := \sum_{i=1}^{n} b_i \underbrace{m_i}_{\text{Basis for } M}$$

with

$$a_1 y_1 = \sum a_1 b_i m_i = \sum \pi_i(y)\, m_i$$
$$= y_1$$

$a_1 = v(y) = v(a_1 y_1) = a_1 v(y_1)$ and $a_1 \neq 0$ in a domain,

$\underline{v(y_1) = 1}$.

Now:

Claim. We can choose y_1 as an element in a basis for M and $a_1 y_1$ as a basis element for N. Namely:

(a) $M = Ry_1 \oplus \operatorname{Ker} v$

(b) $N = Ra_1 y_1 \oplus (N \cap \operatorname{Ker} v)$.

(a): If $M \ni x = \underbrace{v(x) y_1}_{\in Ry_1} + \underbrace{(x - v(x) y_1)}$,

$v(x - v(x) y_1)$
$= v(x) - v(x) v(y_1) = 0$
So $\in \operatorname{Ker}(v)$.

Why is the sum direct?

If $ry_1 \in \operatorname{Ker}(v)$, $0 = v(ry_1) = rv(y_1) = r$.

46.6.

(b): Since a_1 generates $\nu(N)$, $a_1 \mid \nu(x')$ for all $x' \in N$.

Writing $\nu(x') = ba_1$,

$$x' = \nu(x')\,y_1 + (x' - \nu(x')\,y_1)$$
$$= \underbrace{ba_1 y_1}_{\in Ra_1 y_1} + \underbrace{(x' - ba_1 y_1)}$$

in N: x' is by choice $a_1 y_1 = y \in N$.

in $\ker(\nu)$ because
$$\nu(x') - \nu(ba_1 y_1)$$
$$= ba_1 - ba_1 \underbrace{\nu(y_1)}_{=1}.$$

Direct as a special case of (a).

Part (1) of theorem. (N is free of rank $\leq$ rank (M.))
Induct on $m :=$ rank (N).
If $m = 0$, N is a torsion module, hence 0 if also free.
If $m > 0$, $N \cap \ker(\nu)$ has rank $m-1$ by direct sum decompo.
By induction, it's free and we just added one basis elt.

Part (2): Induct on $n :=$ rank (M).

Question: why the hell do DF write $n =$ rank (M), $m =$ rank (N)?

By (1), $\ker(\nu)$ is free; of rank $n-1$ because sum is direct.

By induction, $\ker(\nu)$ has a basis $y_2 \dots y_n$
s.t. $a_2 y_2, \dots, a_m y_m$ is a basis for $N \cap \ker(\nu)$
~~a~~ with $a_2 \dots a_m \in R$ satisfying $a_2 \mid a_3 \mid \dots \mid a_m$.

46.7. $(= 47.5) = 48.1$.

By direct sum magic, y_1 and $a_1 y_1$ complete these to bases. Need $a_1 | a_2$.

$$\text{Define } \varphi : M \longrightarrow R$$
$$y_1 \longrightarrow 1$$
$$y_2 \longrightarrow 1$$
$$\text{other } y_i \longrightarrow 0.$$

Then $a_1 = \varphi(a_1 y_1) \in \varphi(N)$, so $(a_1) \subseteq \varphi(N)$.

But a_1 was chosen maximal, so $(a_1) = \varphi(N)$.

Since $a_2 = \varphi(a_2) \in \varphi(N)$, $a_2 \in (a_1)$ and $a_1 | a_2$. QED.

$\boxed{48.}$ Restate theorem and start here.

Def. An R-module M is cyclic if $M = Rm$ for some $m \in M$.

(Cyclic submodules of R itself: principal ideals)

Then consider $\pi : R \longrightarrow M$
$$r \longrightarrow rm$$

Surjective, so $M \cong R/\mathrm{Ker}(\pi)$ by first iso thm.

If R is a PID, $M \cong R/(a)$ with $(a) = \mathrm{Ann}(M)$.

Thm. (Fund. Theorem for modules / PID's. Existence)

Let M be a f.g. R-module with R a PID. Then:

(1) M is isomorphic to the direct sum of finitely many cyclic modules:
$$M \cong R^r \oplus R/(a_1) \oplus \cdots \oplus R/(a_m)$$
for some integer $r \geq 0$

nonzero $a_1, \dots, a_m \in R$ not units, $a_1 | a_2 | \cdots | a_m$.

47.6. = 48.2

(2) M is torsion free iff free.

(3) In the decomp. above,

$\mathrm{Tor}(M) \cong R/(a_1) \oplus \cdots \oplus R/(a_n)$.

Proof. Start w/ a surjection

$$\pi : R^n \longrightarrow M$$
$$b_i \longrightarrow x_i$$

where: $\{x_1, \ldots, x_n\}$ is a minimal set of generators of M
$\{b_1, \ldots, b_n\}$ is a basis for R^n

Surjective, with $R^n/\mathrm{Ker}\,\pi \cong M$.

Use previous result. Have a basis $y_1 \ldots y_n$ of R^n

with: $a_1y_1 \ldots a_my_m$ a basis for $\mathrm{Ker}\,\pi$, $a_1 | a_2 | \cdots | a_n$.

So,

$$M \cong R^n/\mathrm{Ker}\,\pi = (Ry_1 \oplus \cdots \oplus Ry_n)/(Ra_1y_1 \oplus \cdots \oplus Ra_my_m)$$
$$\cong R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m) \oplus R^{n-m}.$$

To see this, map

$Ry_1 \oplus \cdots \oplus Ry_n \longrightarrow \text{RHS}$

$(\alpha_1 y_1, \ldots, \alpha_n y_n) \longrightarrow (\alpha_1 \pmod{a_1}, \ldots, \alpha_m \pmod{a_m}, \alpha_{m+1}, \ldots, \alpha_n)$.

Gives (1).

(2) is true because all the $R/(a)$ are torsion.

47.7 = 48.3.

Notes:

(1) This is already interesting for $R = \mathbb{Z}$.

(2) We will also prove uniqueness: r is uniquely determined, as are the ideals (a_i).

(3) r is called the free rank or Betti number of M; $a_1 \dots a_m \in R$ are the invariant factors.

(4) You can use CRT to decompose the $R/(a)$ further, into

$$R/(p_1^{a_1}) \oplus \cdots \oplus R/(p_k^{a_k}) \quad \text{for prime elts. } p_i \in R$$

pos integers a_i.

These are the elementary divisors of M.

Both of these decompositions are interesting!

A similar argument gives:

Theorem. (Primary Decomposition) Let —

R PID, M nonzero torsion R-module

Write $a = \mathrm{Ann}(M)$. ($\mathrm{Ann}(M)$ is an ideal, hence principal.)

If $a = u p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ unique factorization,

$N_i = \{x \in M : p_i^{\alpha_i} x = 0\}$

Then N_i is a submodule of M w/ annihilator $p_i^{\alpha_i}$ the submodule of M of all elts. annihilated by a power of p_i, and

$$M = N_1 \oplus \cdots \oplus N_n.$$

Note. Above theorems tell us $a \neq 0$. Otherwise we don't get started!

45.4. A bit more structure theory.

Lemma: If R is a PID, $p \in R$ prime, $F = R/(p)$ a field.

Then:

(1) If $M = R^r$, $M/pM \cong F^r$.

(2) If $M = R/(a)$ with $a \neq 0 \in R$,

$$M/pM \cong \begin{cases} F & \text{if } p \mid a \\ 0 & \text{if } p \nmid a. \end{cases}$$

(3) If $M = R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_k)$

each a_i divisible by p.

Then $M/pM \cong F^k$.

Proof. (2) $\to$ (3) essentially immediate.

(1) $R^r \longrightarrow (R/(p))^r$ natural surjection.

Compute the kernel.

(2) what is $pM = p(R/(a))$?

This is $\dfrac{(p)+(a)}{(a)}$ in $R/(a)$.

$$(p)+(a) = \begin{cases} (p) & \text{if } p \mid a. \\ R & \text{otherwise}. \end{cases} \quad \text{(PID, hence UFD.)}$$

Example. (basic algebraic number theory)

Let $R = \mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z} \quad (i^2 = -1).\}$.

Then R and any quotient is a FG $\mathbb{Z}$-module.

If $p \in \mathbb{Z}$ is prime, what is $\mathbb{Z}[i]/p\mathbb{Z}[i]$?

It's a torsion module.

Use the elem. divisor / primary decomp thm.

As a $\mathbb{Z}$-module, is omorphic to either

$$\mathbb{Z}/p \times \mathbb{Z}/p \quad \text{or} \quad \mathbb{Z}/p^2.$$

Never mind, this is not interesting.

Only the ring structure makes it interesting.

48.5. Theorem (Uniqueness)

Two f.g. R-modules are isomorphic if they have:

(1) the same free rank and list of invariant factors, or

(2) " " " list of elementary divisors.

Proof. Boring, see DF.

Matrix Canonical Forms.

The setup.

F = a field (so $F[x]$ is a PID)

V = fd vector space / F.

$T \in \mathrm{End}(V)$.

Then V is an $F[x]$-module where x acts by T.

V is fg as an F-module, hence as an $F[x]$-module.

Will decompose V as an $F[x]$-module

invariant factor decomp. $\Rightarrow$ get rational canonical form

elementary divisor decomposition $\Rightarrow$ Jordan canonical form.

Point: Choose a basis for V w.r.t. matrix rep'n of T is nice.

48.6. Recall the basic setup.

$\lambda \in F$ is an eigenvalue of T if $Tv = \lambda v$ for some $v \in V$ (an eigenvector)

The associated eigenspace is $\{v \in V : Tv = \lambda v\}$ a subspace of V.

Recall, TFAE:

(1) λ is an eigenvalue of T

(2) $\lambda I - T$ is a singular (not invertible) elt. of $\mathrm{End}(V)$

(3) The characteristic polynomial $\mathrm{char}_T(x) = \det(xI - T)$ satisfies $\mathrm{char}_T(\lambda) = 0$.

Definition. The unique monic polynomial generating $\mathrm{Ann}(V)$ in $F[x]$ is called the minimal polynomial of T, $\mathrm{min}_T(x)$.

Recall: $\mathrm{Ann}(V) = \{f \in F[x] : f(T) = 0\}$ is a principal ideal, has a unique generator up to units, demand monic to make it unique.

Recall the Cayley-Hamilton theorem:

$$\mathrm{min}_T(x) \mid \mathrm{char}_T(x).$$

Equivalently, $\mathrm{char}_T(T) = 0$.

48.7.

By our structure theorem, as $F[x]$-modules

$$V \cong F[x]/(a_1(x)) \oplus F[x]/(a_2(x)) \oplus \cdots \oplus F[x]/(a_m(x))$$

where the invariant factors $a_i(x)$ satisfy

$$a_1(x) \mid a_2(x) \mid \cdots \mid a_m(x).$$

If we insist they be monic, they are unique.

Now, ~~as~~ $\mathrm{Ann}(V) = (a_m(x))$, this is the minimal polynomial.

We always have a nice basis for $F[x]/(a(x))$ as an F-vector space: if $k = \deg(a(x))$, then $1, x, x^2, \ldots, x^{k-1}$.

The linear transformation "multiply by x" has ~~basis~~ matrix

$$\begin{bmatrix} 0 & 0 & \cdots & 0 & -b_0 \\ 1 & & 0 & & -b_1 \\ & \ddots & & & \vdots \\ 0 & & & & \vdots \\ & & & 1 & -b_{k-1} \end{bmatrix}$$

where $a(x) = x^k + b_{k-1}x^{k-1} + b_{k-2}x^{k-2} + \cdots + b_0$.

(Stare at it for awhile.)

This is called the companion matrix of $a(x)$.

48.8 = 49.1

With $V \cong F[x]/(a_1(x)) \oplus \cdots \oplus F[x]/(a_m(x))$,

choose such bases for each of the factors, get a block diagonal matrix

$$\begin{pmatrix} C_{a_1(x)} & & & \\ & C_{a_2(x)} & & \\ & & \ddots & \\ & & & C_{a_m(x)} \end{pmatrix}$$

where each $C_{a_i(x)}$ is a companion matrix of the form above. This is the rational canonical form of T. It is unique because the a_i are.

So, for example:

Theorem. If $S, T \in \mathrm{End}(V)$ then TFAE:

(1) S and T are conjugate

(2) S and T have the same rat'l canonical form

(3) The $F[x]$-modules obtained from V via S and T are isomorphic.

Moreover, in matrix language, any $n \times n$ matrix is conjugate to a unique matrix in rational canonical form. (Over any field.)

Also, doesn't change when you pass to extension fields.

49.2.

Lemma. The determinant of a block diagonal matrix
$$\begin{pmatrix} D_1 & & \\ & \ddots & \\ & & D_n \end{pmatrix} \quad \text{is} \quad \det(D_1)\cdots\det(D_n).$$

(Prove by "pure thought.")

So the characteristic polynomial of the RCF is the product of the companion matrices.

Proposition. Let $a(x) = x^k + b_{k-1}x^{k-1} + \cdots + b_0$ w/ companion matrix
$$\begin{bmatrix} 0 & & & -b_0 \\ 1 & \ddots & & -b_1 \\ & \ddots & 0 & \vdots \\ & & 1 & -b_{k-1} \end{bmatrix} \qquad \det \begin{bmatrix} x & & & +b_0 \\ -1 & \ddots & & \vdots \\ & \ddots & x & \vdots \\ & & -1 & x+b_{k-1} \end{bmatrix}$$

Then its charpoly is just $a(x)$.

Proof 1. If you assume Cayley-Hamilton ($\min_T(x) \mid \mathrm{char}_T(x)$),

* $\min_T(x) = a(x)$ by construction
* $\mathrm{char}_T(x)$ is of the same degree. Done.

Proof 2. If you want to prove CH this way, do an elementary computation.

For example: Add x times last row to next-to-last
x times next-to-last to previous.
etc.

Get $\det \begin{bmatrix} 0 & & & f \\ -1 & \ddots & & * \\ & \ddots & 0 & \vdots \\ & & -1 & x \end{bmatrix}$ with
$$f = b_0 + x(b_1 + x(b_2 + \cdots + x(x + b_{k-1})\cdots)$$
$$= a(x).$$

49.3.

Corollary (of Proof 2)
For a companion matrix, $\min_T(x) = \mathrm{char}_T(x)$.

Now, in rat'l canonical form,

$\min_T(x)$ = the last (largest) invariant factor
$\mathrm{char}_T(x)$ = product of the invariant factors
$a_1(x) \cdots a_m(x)$.

Cor. (Cayley-Hamilton Theorem).
1. $\min_T(x) \mid \mathrm{char}_T(x)$.
2. $\mathrm{char}_T(T) = 0$.

Computations (ugh, see DF).

Example. Determine, up to conjugacy, all $A \in GL_3(\mathbb{Q})$ with $A^6 = I$.

Solution. We will have

$$\min_A(x) \mid x^6 - 1 = (x-1)(x+1)(x^2-x+1)(x^2+x+1).$$

$$\text{So } \min_A(x) = \begin{cases} x-1 \\ x+1 \\ x^2-x+1 \\ x^2+x+1 \\ (x-1)(x+1) \\ (x-1)(x^2-x+1) \\ (x+1)(x^2-x+1) \\ (x-1)(x^2+x+1) \\ (x+1)(x^2+x+1) \end{cases}$$

The irreducible quadratics cannot occur!
Need, e.g. $(x^2-x+1) \cdot \{\text{some divisor of } x^2-x+1\}$
= cubic. NOPE

49.4 = 50.1

$\min_A(x) = x-1$: $A - 1 = 0$. So $A = I$.

$\min_A(x) = x+1$: $A + 1 = 0$, $A = -I$.

$\min_A(x) =$ cubic. This is easy.

e.g. if $\min_A(x) = x^3 - 1$, then A has RCF

$$\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

$\min_A(x) : x^2 - 1$.

Then the smaller inv. factor can be $x-1$ or $x+1$:

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}.$$

Exercise.

(1) Repeat for $GL_3(\mathbb{C})$ (where everything factors)

(2) Determine, up to conjugacy, all the homomorphisms ("representations")

$$\mathrm{Sym}(3) \longrightarrow GL_3(\mathbb{Q})$$
$$\mathrm{Sym}(3) \longrightarrow GL_3(\mathbb{C}).$$

Jordan canonical form.

We factored the $F[x]$-module V as

$$V \cong F[x]/(a_1(x)) \oplus \cdots\cdots \oplus F[x]/(a_m(x))$$

with invariant factors $a_1 | \cdots | a_m$.

49.5 = 50.2

Consider the other factorization

$$V \cong F[x]/(p_1(x)^{e_1}) \oplus \cdots \oplus F[x]/(p_m(x)^{e_m})$$

into irreducibles, and let's assume F is algebraically closed so the p_i are all linear.

(In fact: enough if F contains the eigenvalues of T)

Choose a basis for each subspace $F[x]/p(x)^e$, write down the matrix WRT that basis.

Lump these together to get a basis for V and a block diagonal matrix for T in that basis.

We have $p(x) = x - \lambda$ for some $\lambda \in \mathbb{C}$ and indeed λ will range over the eigenvalues of T.

why? The minimum polynomial on the ith piece V_i is $p_i(x)$ to some power. (Think about rat'l CF)
All the invariant factors divide it.
So Char poly is product of such factors.

For $F[x]/(x-\lambda)^e$, could choose $1, x, x^2, \ldots, x^{e-1}$ as a basis.

But better: Choose $1, x-\lambda, (x-\lambda)^2, \ldots (x-\lambda)^{e-1}$.

49.6 = 50.3

How does multiplication by x act?

$$1 \longrightarrow x = (x-\lambda) + \lambda \cdot 1$$

$$x - \lambda \longrightarrow x^2 - \lambda x = (x-\lambda)^2 + \lambda \cdot (x-\lambda)$$

$$\vdots$$

$$(x-\lambda)^{a-1} \longrightarrow \underbrace{(x-\lambda)^a}_{\text{This is } 0.} + \lambda (x-\lambda)^{a-1}$$

So, w.r.t. this basis, the matrix of T is

$$\begin{bmatrix} \lambda & & & & 0 \\ 1 & \lambda & & & \\ & 1 & \ddots & & \\ & & \ddots & \ddots & \\ 0 & & & 1 & \lambda \end{bmatrix}.$$

It is customary to write the basis backwards to get

$$\begin{bmatrix} \lambda & 1 & & & 0 \\ & \lambda & 1 & & \\ & & \ddots & \ddots & \\ & & & \ddots & 1 \\ 0 & & & & \lambda \end{bmatrix}.$$

We see again, $\mathrm{char}_T(x) = (x-\lambda)^a$ so the one eigenvalue is a.

49.7 ∓ 50.4

This matrix is a Jordan block of size k with eigenvalue λ.

Theorem. (1) Let $T \in \mathrm{End}(V)$, over a field containing the eigenvalues of T. Then, there is a ~~unique~~ basis wrt which T ~~could~~ has a matrix in Jordan canonical form

$$\begin{bmatrix} J_1 & & \\ & \ddots & \\ & & J_m \end{bmatrix}$$

J_i : Jordan blocks of the shape we saw.

(2) The Jordan form is unique up to rearrangement of the J_i.

(Follows from uniqueness of elem divisor decomposition).

The subspace corresponding to each J_i is a generalized eigenspace:

Eigenspace for λ is $\{v \in V : (T-\lambda)v = 0\}$.

Generalized eigenspace is $\{v \in V : (T-\lambda)^k v = 0 \text{ for some } k\}$.

Note however that the J_i's or their eigenvalues are not necessarily distinct.

50.5

<u>Cor.</u> If a matrix A is <u>diagonalizable</u> (conjugate to a diagonal matrix D), then D is the Jordan form.

(2) Two diagonal matrices are similar if and only if their diagonal entries are the same up to a permutation.

In <u>other words</u>: A matrix is diagonalizable iff it has a <u>basis</u> of <u>eigenvectors</u>; up to conjugacy, such matrices are determined by their eigenvalues (w/ multiplicity).

<u>Cor.</u> Given a LT T over a field containing all the eigenvalues. Then T is diagonalizable iff the minimal polynomial has no repeated roots.

<u>Pf.</u> If diagonalizable, then $\min_T(x) = \prod_{\lambda \text{ distinct}} (x-\lambda)$.

[Think about this directly.] So $\longrightarrow$ is true.

$\longleftarrow$: Jordan form it.

$\min_T(x)$ is the LCM of min polys of Jordan blocks.

~~The~~ $\min_T(x)$ if T has matrix $\begin{bmatrix} \lambda & 1 & & \\ & \lambda & \ddots & \\ & & \ddots & 1 \\ & & & \lambda \end{bmatrix}$.

Visibly, $\min_T(x) = (x-\lambda)^k$ (k = size of matrix).

No repeated roots means <u>all the Jordan blocks are 1×1.</u>

So no room for 1's over the diagonal.

50.6.

Example. Describe all $A \in GL_3(\mathbb{C})$ with $A^6 = I$.

Could use RCF. This time, $x^6 - 1 = \prod_{i=0}^{5} (x - \zeta_6^i)$ and there are lots of possibilities.

Use Jordan form instead.

Get: $\begin{bmatrix} * & 0 & 0 \\ 0 & * & 0 \\ 0 & 0 & * \end{bmatrix}$ where the $*$ are any 6th roots of unity (note: reorderings are conjugate)

$\begin{bmatrix} \mu & 1 & 0 \\ 0 & \mu & 0 \\ 0 & 0 & \lambda \end{bmatrix}$ where μ, λ are 6th roots of unity (not nec. distinct)

$\begin{bmatrix} \mu & 1 & 0 \\ 0 & \mu & 1 \\ 0 & 0 & \mu \end{bmatrix}$.

See DF for a variety of examples.

50.7.

Smith normal form. (for exercises).

Let $0 \neq A \in M_{m\times n}(R)$ for a PID R. Then, there are invertible $m\times m$ and $n \times n$ matrices S, T (w/ coeffs in R) s.t.

$$SAT = \begin{bmatrix} q_1 & & & & & \\ & q_2 & & & 0 & \\ & & \ddots & & & \\ & & & q_r & & \\ & 0 & & & 0 & \\ & & & & & \ddots \\ & & & & & & 0 \end{bmatrix}$$

with $q_i \mid q_{i+1}$ for all i.