Linear Algebra Cheat Sheet

Daniel Lin

Based on notes by Martin Lieback and *Linear Algebra Done Right*

Contents

1 Basics

Ways to show a set B is a basis of V:

- LI & span$(B) = V$
- LI & has n vectors.
- span$(B) = V$ & has n vectors. (This is very flexible, as you may construct another set of vectors B' with span(B) = span(B'), and then prove that span$(B') = V$)

Ways to show that a matrix $A \in F^{n\times n}$ is invertible:

- $\det(A) \neq 0$
- rank$(A) = n$. i.e. all rows are LI, or all columns are LI.
- All eigenvalues are not 0.
- $\dim \ker A = 0$
- A is full-rank.
- Only solution to $A\boldsymbol{x} = 0$ is $\boldsymbol{x} = 0$.
- $A\boldsymbol{x} = b$ has a unique solution $\forall b \in F^n$.
- If you are given A explicitly or you know what A^{-1} should be, construct an invertible matrix and prove $AA^{-1} = A^{-1}A = I$. (Example: prove that change of base matrix is invertible)
- rref has no all-zero row.

Note if A is invertible, $A(W) = W$ for any A-invariant $W \leq V$.

Properties of rank:

- $rank(A) = rank(A^T)$
- Rank is unchanged by elementary row/column operations.
- rank $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$ = rank(A) + rank(B)

tr is a linear function, and:

$$\mathrm{tr}(A) = \mathrm{tr}(A^T), \mathrm{tr}(AB) = \mathrm{tr}(BA)$$

But in general $\mathrm{tr}(AB) \neq \mathrm{tr}(A)\mathrm{tr}(B)$

Alternative definition for determinant:

$$\det(A) = \sum_{\pi \in S_n} sgn(\pi) a_{1,\pi(1)} ... a_{n,\pi(n)}$$

2 Diagonalisation and Similarity

The following statements are equivalent:
(1) Linear map T is diagonalisable
(2) There is a basis containing Eigenvectors.
(3) $\sum_i g(\lambda_i) = n$ where $n = dim(V)$.
(4) $\forall i, a(\lambda_i) = g(\lambda_i)$
(5) $m(x)$ is a product of DISTINCT linear factors.

For a matrix A, diagonalisable also means $A \sim D$ for some diagonal matrix D.

For any diagonalisable linear map T and invariant subspace W, T_W is also diagonalisable.

Given V is vector space over $\mathbb{C}$, with $\dim V = n \geq 2$.

- If map $T \neq 0$ but $T^k = 0$ for some $k \in \mathbb{Z}$, then T is not diagonalisable.
- If $T^k = I_V$ for some $k \in \mathbb{Z}$, then T is diagonalisable with Eigenvalues being roots of unity of k. (i.e. $\lambda^k = 1$)

For every square matrix A over $\mathbb{C}$, there is a symmetric P s.t. $P^{-1}AP = A^T$. So every square matrix over $\mathbb{C}$ is similar to its transpose. And if A is invertible, there is a matrix B s.t. $B^2 = A$ (B is called square root of A)

Properties shared between similar matrices

- det
- tr
- $c(x), m(x)$
- Eigenvalues and their multiplicities
- rank
- nullity

For any general polynomial(powers of x can be negative) $p(x)$ and similar matrices A, B, $p(A) \sim p(B)$.

JCF and RCF are official ways to determine whether two matrices are similar or not. But these requires a lot of calculations.
For small matrices, directly find a matrix P to prove A, B are similar.
Disprove similarity

- By showing any one of the above listed properties (e.g. rank) differ, Or show any one of the properties differ for $p(A), p(B)$. (e.g. you may show $A^m = 0, B^m \neq 0$, or $A - kI, B - KI$ has different ranks)

- Find JCF/RCF R of A, if $B = p(A)$ for some general polynomial $p(x)$, then $B \sim p(R)$. Check if $R, p(R)$ are similar.

3 Direct Sum

Sum $V + W := \{v + w : v \in V, w \in W\}$, and it has dimension

$$\dim(V + W) = \dim(V) + \dim(W) - \dim(V \cap W)$$

Direct sum $V \oplus W$ is defined as $V + W$ and all vectors can be written in a unique way. The following statements are equivalent for direct sum:
(1) $V = V_1 \oplus V_2 \oplus ... \oplus V_k$
(2) $\dim V = \sum_{i=1}^{k} \dim V_i$ (to ensure $V = V_1 + V_2 + ... + V_k$) and if B_i is a basis for V_i, $B = \cup_{1 \le i \le k} B_i$ is a basis of V. (If $k = 2$, second part simplifies to $V_1 \cap V_2 = \{0\}$.)

Remark. For $k = 2$, we just need $V_1 \cap V_2 = \{0\}$ instead of union of basis being a basis. But this does not work for general case.

4 Rules of block matrix

Concerning many small subspaces, we may write matrices as blocks for convenience. And the elementary row operations are (all multiplications are left-multiplications):
(1) Adding P(a matrix) times of one row to another row

$$\begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix} \to \begin{pmatrix} A_1 & A_2 \\ A_3 + PA_1 & A_4 + PA_2 \end{pmatrix}$$

(2) Exchange two rows.
(3) (Left) Multiply one row with invertible matrix P.

All these operations will not change the rank of matrix. Similarly we can define column operations, but with right multiplication. (As exercise, think of why rank is not changed)

Determinant of triangular matrix

$$\det(\begin{pmatrix} A & C \\ 0 & B \end{pmatrix}) = \det(\begin{pmatrix} A & 0 \\ C & B \end{pmatrix}) = \det(A)\det(B)$$

Transpose

$$\begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix}^T = \begin{pmatrix} A_1^T & A_3^T \\ A_2^T & A_4^T \end{pmatrix}$$

If B has columns $\beta_1, \beta_2, ..., \beta_m$,

$$AB = (A\beta_1, A\beta_2, ..., A\beta_m)$$

If matrix $A = A_1 \oplus A_2 \oplus ... \oplus A_r$,

- $A^{-1} = A_1^{-1} \oplus A_2^{-1} \oplus ... \oplus A_r^{-1}$
- $c_A(x) = \prod_{i=1}^{r} c_{A_i}(x)$
- $m_A(x) = lcm(m_{A_1}(x), ..., m_{A_r}(x))$
- For any scalar λ, $\dim E_\lambda(A) = \sum_{i=1}^{r} \dim E_\lambda(A_i)$
- A is similar to any permutation of the blocks.
- for any polynomial $p(x)$, $p(A) = p(A_1) \oplus ... \oplus p(A_r)$

5 Quotient space, invariant subspace

Dimension of quotient space

$$\dim(V/W) = \dim(V) - \dim(W)$$

and basis of V/W can be found by extending a basis $\{w_1, ..., w_s\}$ for W to a basis of V by adding $\{v_1, ..., v_r\}$. Then $\{W + v_1, ..., W + v_r\}$ is a basis of V/W.

Given an T-invariant subspace W, let $X = [T_W]_{B_W}$ and $Y = [\overline{T}]_{\overline{B}}$ (where $\overline{T} = V/W$, and $\overline{B}$ is one basis of $\overline{T}$). Now if $B = B_W \cup \overline{B}$,

$$[T]_B = \begin{pmatrix} X & Z \\ 0 & Y \end{pmatrix}$$

so

$$c_T(x) = c_{T_W}(x) c_{\overline{T}}(x)$$

Also $m_{T_W}(x) \mid m_T(x), m_{\overline{T}}(x) \mid m_T(x)$.

Given an linear transformation T and polynomial $f(x)$, $\mathrm{Ker}(f(T))$ and $\mathrm{Im}(f(T))$ are both invariant.
If V_i are all T-invariant, then

$$f(T)(V_1 \oplus ... \oplus V_r) = f(T)(V_1) \oplus ... \oplus f(T)(V_r)$$

6 Isomorphism of vector spaces

An isomorphism between vector spaces V, W is as a bijective linear map $T : V \to W$. The bijective condition is equivalent to $Ker(\phi) = 0$ and $dim(V) = dim(W)$. Given a basis B, $T : v \mapsto [v]_B$ is an isomorphism between V and F^n. The following are properties of isomorphism

- Inverse of isomorphism is also an isomorphism
- composition of isomorphism is an isomorphism
- Isomorphism is an equivalence relation on the set of all vector spaces.
- Isomorphism sends linearly independent sets in V to linearly independent sets in W, and send spanning sets in V to spanning sets in W. So isomorphism send basis to basis. (That means isomorphic vector spaces have the same dimension)
- In fact, if two spaces are F-vector spaces with the same dimension n, they must be isomorphic. (As they are both isomorphic to F^n)

7 Triangularisation and Cayley-Hamilton

Product, inverse of upper triangular matrices are all upper triangular. Determinant of upper triangular is product of its diagonal elements.

Process of triangularisation Any matrix with characteristic polynomial that can be decomposed into linear factors can be triangularised.

1. Find one Eigenvector ω_1 for T and let $W_1 = \text{span}(\omega_1)$
2. Find one Eigenvector $W_1 + \omega_2$ for $\overline{T}$ and let $W_2 = \text{span}(\omega_1, \omega_2)$. Remember to change w_2 to standard basis.
3. repeat until you obtain a basis.
4. For the last base vector, you can directly add one of e_i, the canonical base, that is not in the span to complete the basis.

Equivalent condition for transformation T to be triangularisable: exists sequence of T-invariant subspaces $V_1 \subset V_2 \subset \cdots \subset V_n$ s.t. $\dim V_i = i$.

Companion matrix of a monic polynomial $p(x) = x^n + a_{n-1}x^{n-1} + \cdots a_0 \in F[x]$ is defined as

$$C(p) := \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & & \ddots & \cdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}$$

Cayley-Hamilton arguments The arguments used in the proof of this theorem is very useful: if we are studying transformation T, using induction on $\dim V = n$

1. Prove the statement if there is an T-invariant $W \neq \{0\}, V$, then we can study $T_W, \overline{T}$ defined on $W, V/W$ with smaller dimension. (So we can use inductive hypothesis)

2. Assume V has no T-invariant subspaces except $\{0\}, V$, then for any $0 \neq v \in V$,
$$B = \{v, T(v), \cdots, T^{n-1}(v)\}$$
is a basis and $[T]_B = C(c_T(x))$.

8 Polynomials

Degrees

$$\deg(p(x)q(x) = \deg(p(x)) + \deg(q(x)),\ \deg(p+q) = \max\{\deg p, \deg q\}$$

Irreducibility
Irreducibility of a polynomial $p(x)$ with degree d over finite field: for each positive integer $n < d/2$, check if every irreducible polynomial of degree n is not a factor of $p(x)$. (For $d = 2, 3$ check the existence of roots)

Irreducible polynomials over some finite fields

- $\mathbb{F}_2$
  - Degree 1: x, $x + 1$
  - Degree 2: $x^2 + x + 1$
  - Degree 3: $x^3 + x + 1$, $x^3 + x^2 + 1$
  - Degree 4: $x^4 + x^3 + 1$, $x^4 + x + 1$, $x^4 + x^3 + x^2 + x + 1$
  - Degree 5: $x^5 + x^4 + x^3 + x^2 + 1$, $x^5 + x^4 + x^3 + x + 1$, $x^5 + x^4 + x^2 + x + 1$, $x^5 + x^3 + x^2 + x + 1$, $x^5 + x^3 + 1$, $x^5 + x^2 + 1$
- $\mathbb{F}_3$
  - Degree 1: x, $x + 1$, $x - 1$
  - Degree 2: $x^2 + 1$, $x^2 + x - 1$, $x^2 - x - 1$
  - Degree 3: $x^3 - x + 1$, $x^3 - x - 1$, $x^3 + x^2 - 1$, $x^3 - x^2 + 1$, $x^3 + x^2 + x + 1$, $x^3 + x^2 + x - 1$, $x^3 + x^2 - x + 1$, $x^3 - x^2 + x + 1$

Finding gcd WOLG say $\deg f \geq \deg g$, do Euclid division

$$f = qg + r_1, \deg(r_1) < \deg(g)$$

$$g = q_1 r_1 + r_2, \deg(r_2) < \deg(r_1)$$
$$r_1 = q_2 r_2 + r_3, \deg(r_2) < \deg(r_1)$$
$$r_1 = q_2 r_2 + r_3, \deg(r_3) < \deg(r_2)$$
$$\cdots$$
$$r_{n-1} = q_n r_n + r_{n+1}, \deg(r_{n+1}) < \deg(r_n)$$
$$r_n = q_{n+1} r_{n+1}$$

then $d := r_{n+1}$ is $gcd(f, g)$. Reversing this process gives r, s s.t. $d = rf + sg$.

Check irreducibility over $\mathbb{Q}[x]$, use Gauss's lemma
Given monic polynomial $p(x) \in \mathbb{Q}[x]$ with integer coefficients. If $\alpha \in \mathbb{Q}$ is a root of $p(x)$ then $\alpha \in \mathbb{Z}$ and if $p(x)$ reducible over $\mathbb{Q}$, then it has factorisation $p = ab$ where a, b are monic with integer coefficients.

If $p(x) \in F[x]$ is irreducible and $p|g_1 \cdots g_r$ where $g_i \in F[x]$, then $p|g_i$ for some i.

For any polynomial $p(x)$ and linear map T,

$$p(T) = 0 \Leftrightarrow m_T(x) \,|\, p(x)$$

For $C(p(x))$, $m(x) = c(x) = p(x)$.

Process of finding $m_T(x)$
(1) Find $c(x)$
(2) Begin by taking one power of each irreducible factor, gradually increase power, and find the smallest degree sending T to 0.
Note for any $0 \neq v \in V$, if $\{v, T(v), \cdots T^s(v)\}$ is LI, then $\deg(m_T) \geq s + 1$.

Useful property to find $m(x)$
If

$$A = \begin{pmatrix} \lambda & a_1 & & & \\ & \lambda & a_2 & & \\ & & \ddots & & \\ & & & \lambda & a_{n-1} \\ & & & & \lambda \end{pmatrix}$$

then (1) if $\forall i, a_i \neq 0$, $m(A) = (x - \lambda)^n$
(2) if $\exists i, a_i = 0$, $m(A) = (x - \lambda)^k$ (where $k < n$)

If v is Eigenvector of A s.t. $Av = \lambda v$, then v is also Eigenvector of $p(A)$ with Eigenvalue $p(\lambda)$ for any polynomial p.
If A, B are invertible, then $m_{AB}(x) = m_{BA}(x)$.

9 Primary decomposition

$$m(x) = \prod_{i=1}^{k} f_i(x)^{n_i}$$

where $f_i(x)$ are distinct irreducible polynomial and $V_i = \text{Ker}(f_i(T)^{n_i})$. Then we have:

1. $V = V_1 \oplus ... \oplus V_k$ (Primary decomposition)
2. each V_i is T-invariant.
3. $m(x)$ of T_{V_i} is $f_i(x)^{n_i}$

10 Jordan Canonical Form

Properties of a Jordan block $J = J_n(\lambda)$

- $m(x) = c(x) = (x - \lambda)^n$
- λ is the only Eigenvalue with $a(\lambda) = n, g(\lambda) = 1$. And $E_\lambda = Span(e_1)$
- $J - \lambda I$ creates a chain: $e_n \to e_{n-1} \to ... \to e_1 \to 0$
- $J \sim J^T$
  - Hence, for any matrix $A \in M_n(\mathbb{C})$, $A \sim A^T$.
- If $F = \mathbb{C}$ AND $\lambda \neq 0$, then $J_n(\lambda)^2 \sim J_n(\lambda^2)$. More generally, as long as $\lambda, \lambda^2 \neq 0$ in F, this statement holds.

Power of Jordan block

$$J_r(\lambda)^n = \begin{pmatrix} \lambda^n & n\lambda^{n-1} & \binom{n}{2}\lambda^{n-2} & \cdots & \binom{n}{r-1}\lambda^{n-r+1} \\ & \lambda^n & n\lambda^{n-1} & \cdots & \binom{n}{r-2}\lambda^{n-r+2} \\ & & \lambda^n & \cdots & \binom{n}{r-3}\lambda^{n-r+3} \\ & & & \ddots & \\ & & & & \lambda^n \end{pmatrix}$$

Steps of finding a JCF for $n \times n$ **matrix** A

1. Calculate $m(x), c(x)$, and $a(\lambda), g(\lambda)$ for each Eigenvalue.
2. For Eigenvalue λ, $a(\lambda)$ = sum of sizes of λ-blocks, $g(\lambda)$ = number of λ-blocks, highest power in $m(x)$ = size of largest λ-block.

3. If a unique JCF is not yielded, for each Eigenvalue λ, let r = highest power of $x - \lambda$ in $m(x)$, $l = n - a(\lambda)$, a_i = number of blocks with size i $(1 \leq i \leq r)$. Calculate $m_i = rank(A - \lambda I)^i - l$ for $1 \leq i \leq r$. We have:
   - $m_{r-1} = a_r$
   - $m_{r-2} = 2a_r + a_{r-1}$
   - $m_{r-3} = 3a_r + 2a_{r-1} + a_{r-2}$
   - ...
   - $m_1 = (r-1)a_r + ... + 2a_3 + a_2$

After you have computed JCF, you may find Jordan basis.
Steps of finding Jordan basis

1. For each Eigenvalue λ_i, let $S = T_{V_i} - \lambda I$ where V_i is the corresponding subspace in primary decomposition. Find $S(V), ..., S^r(V)$ (make sure $S^{r+1}(V) = 0$, and ideally find a basis of each of them.

2. Beginning with a basis $\{u_1, u_2, ..., u_k\}$ of $S^r(V)$, add vectors $v_1, ..., v_k$ such that $S(v_i) = u_i$. This gives (at least part of) basis of $S^{r-1}(V)$. And then add vectors $w_1, w_2, ..., w_k$ such that $S(w_i) = v_i$ to give $S^{r-2}(V)$. Do this for r times so that you get (at least part of) basis of V.

3. Finally, complete $Ker(S)$ by adding vectors $\omega_1, ..., \omega_s$ to $\{u_1, u_2, ..., u_k\}$ to make a basis of $Ker(S)$. (This is because not every vector in kernel is in $S^r(V)$)

4. If basis is not yet completed, repeat step 2 on ω_1. If still not complete do step 2 to ω_2, ... The basis must be complete after doing step 2 to each vector ω_i.

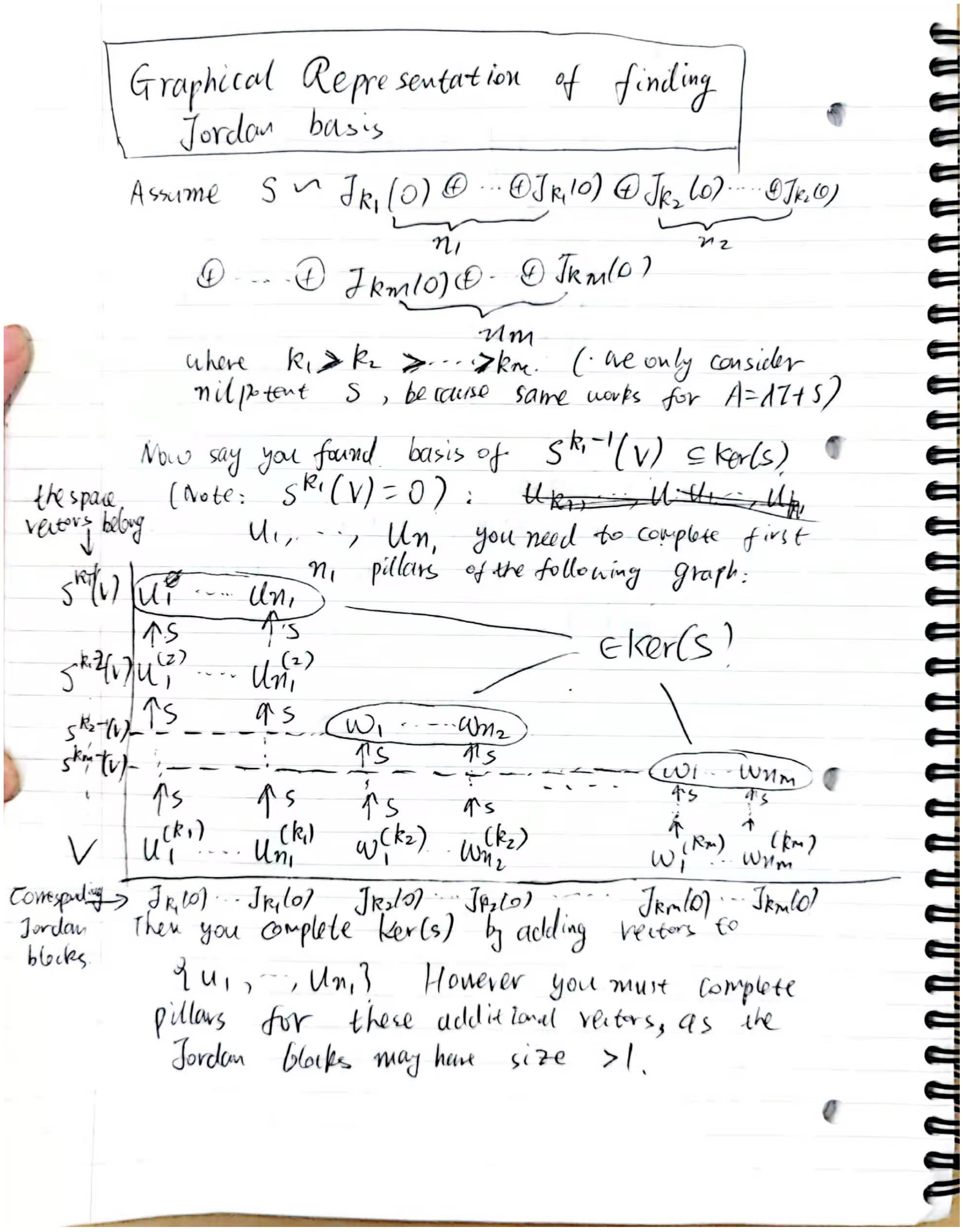

Figure 1: Graphical representation of Jordan basis

11 Rational Canonical Form

The limit of JCF is very obvious, we require Jordan basis to contain set of vectors in the form $u, S(u), S^2(u), ...S^r(u)$ (where $S = T - \lambda I$) and $S^{r+1}(u) = 0$. This is only possible when $c(x)$ is a product of linear factors. Now we loosen the condition, and only require $S^{r+1}(u) \in Span(u, S(u), S^2(u), ...S^r(u))$. $Span(u, S(u), S^2(u), ...S^r(u)) =: Z(u, S)$ is called S-cyclic subspace and the corresponding matrix is exactly of the form $C(p(x))$. This form is possible for any matrix over any field.

Note: $C(f) \oplus C(g) \sim C(fg)$ if f, g are coprime.

Steps of finding RCF for matrix A

1. Find $c_A(x) = \prod_{i=1}^{t} f_i(x)^{m_i}, m_A(x) = \prod_{i=1}^{t} f_i(x)^{s_i}$ where $f_i(x)$ are distinct irreducible factors
2. By primary decomposition, $V = \bigoplus_{i=1}^{t} V_i$ where $V_i = Ker(f_i(A))^{s_i})$, with $dim(V_i) = m_i d_i$ where $d_i = deg(f_i(x))$
3. For each restriction A_{V_i}, let $k_1 = s_i$, write down all possible combinations of $C(f_i(x)^{k_1}) \oplus C(f_i(x)^{k_2}) \oplus ...$ such that $k_1 \geq k_2 \geq ...$ and $d_i \sum_{j=1} k_j = dim(V_i) = m_i d_i$ (i.e. $\sum_{j=1} k_j = m_i$)
4. Use the fact that for each $1 \leq i \leq t$, $rank(f_i^s(A_{V_i})) = rank(f_i^s(A)) - \sum_{j \neq i} dim(V_j)$ for any $1 \leq s < s_i$, find $rank(f_i^s(A_{V_i}))$. And then find n_j = number of blocks with annihilator $f_i(x)^j$ using the following formulas:
   - $rank(f_i^{s_i-1}(A_{V_i})) = d_i n_{s_i}$
   - $rank(f_i^{s_i-2}(A_{V_i})) = 2d_i n_{s_i} + d_i n_{s_i-1}$
   - ...
   - $rank(f_i(A_{V_i})) = (s_i - 1)d_i n_{s_i} + (s_i - 2)d_i n_{s_i-1} + ... + 2d_i n_3 + n_2$
5. Finally, join the cyclic canonical form of each V_i together.

A trivial result: for any linear transformation T and vector v, if $B = \{v, Tv, T^2v, ..., T^{n-1}v\}$ is a basis, then for any polynomial $f(x)$ with $deg(f) \leq n - 1$ we have:

$$f(T)v = 0 \Rightarrow f(T) = 0$$

However, this does not hold for arbitrarily chosen vector v.

12 Inner Product Space and dual space

Some notations

V^* - dual space of V (space of linear functional $V \to F$), $dim(V^*) = dim(V)$

For any subset $X \subseteq V$ (not necessarily subspace), annihilator $X^0 = \{\phi \in V^* :$

$\phi(x) = 0 \, \forall x \in X\}$. If W is subspace, $dim(W^0) = dim(V) - dim(W)$
$\overline{V}$ - a space same as V except for scalar multiplication $\lambda * v := \overline{\lambda} v$.
If $W \subseteq V$(not necessarily subspace), $W^{\perp} = \{u \in V : (u, w) = 0 \, \forall w \in W\}$

Relationships between V and dual space
$\overline{V}$ is isomorphic to V^* by the map $v \to f_v$. ($f_v(w) = (w, v)$) So every linear functional is essentially an inner product.
$W^{\perp} \subseteq \overline{V}$ is isomorphic to $W^0 \subseteq V^*$ by the same map $v \to f_v$. (If we change scalar product in $W^{\perp}$ to $\lambda * v = \overline{\lambda} v$)

$(U + W)^0 = U^0 \cap W^0, (U \cap W)^0 = U^0 + W^0$
$V = W \oplus W^{\perp}$

12.1 Dual Space

Dual basis has interesting properties. If $v_1, ..., v_n$ is basis of V and $f_1, ..., f_n$ is the dual basis of V^*, then

- If $v \in V$, then $v = \sum f_i(v) v_i$
- If $f \in V^*$, then $f = \sum f(v_i) f_i$.
- (Corollary) $v = 0 \Leftrightarrow \forall f \in V^*, f(v) = 0$.
- (Corollary) $f = 0 \Leftrightarrow \forall v \in V^*, f(v) = 0$.

We can see some symmetry here. Consider two vector spaces V, W with dimension n and basis $\{v_i\}$ for V, basis $\{w_j\}$ for W. We define a pairing function $\varphi : V \times W \to F$ by $\varphi(v_i, w_j) = \delta_{i,j}$. So note

$$\{\varphi(v_i, \cdot)\}_{i=1,2,...,n} \subset W^*$$

is exactly dual basis of $\{v_i\}$ in W^*. Similarly $\{\varphi(\cdot, w_j)\}_{j=1,2,...,n}$ is a dual basis of $\{w_j\}$ in V^*. So V can be treated as dual space of W and W can be treated as dual basis of V. The concept of dual is indeed buried under a larger space $(V \times W)$, and the function φ is an example of bilinear form.

Given $f \in V^*$, $V/\ker f \cong F$ as f is vector space homomorphism. So $\dim \ker f = \dim V - 1$.

Finding dual basis

1. If given basis of V: $\{v_1, v_2, ..., v_n\}$, for each i find vector w_i s.t. $\forall j, (v_j, w_i) = \delta_{ij}$. Then f_{w_i} is a dual basis.
2. If given basis of V^*: $\{f_1, f_2, ..., f_n\}$. For each i find v_i s.t. $\forall j, f_j(v_i) = \delta_{ij}$
3. To prove $\{f_1, f_2, ..., f_n\}$ is a basis of V^*, use canonical basis $\{e_1, ..., e_n\}$ of V and construct vectors

$$(f_1(e_1), ..., f_1(e_n)), (f_2(e_1), ..., f_2(e_n)), ..., (f_n(e_1), ..., f_n(e_n))$$

Prove these vectors are LI.

12.2 Inner Product Space

Definition

1. $(\lambda_1 v_1 + \lambda_2 v_2, w) = \lambda_1(v_1, w) + \lambda_2(v_2, w)$
2. $(v, w) = \overline{(w, v)}$
3. $(v, v) > 0$ if $v \neq 0$

From 2 we have $(v, v) \in \mathbb{R}$ and from 1, 2 we have $(v, \lambda_1 w_1 + \lambda_2 w_2) = \overline{\lambda_1}(v, w_1) + \overline{\lambda_2}(v, w_2)$. Third axiom proves a good way to prove $u = v$: show $(u - v, u - v) = 0$

Matrix of inner product:
Given basis $B = \{v_1, v_2, ..., v_n\}$, matrix of inner product $A = (a_{ij}) = ((v_i, v_j))$. Note A is Hermitian ($A^T = \overline{A}$) and positive definite. In fact, every positive definite Hermitian matrix A corresponds to an inner product defined by $(v, w) = [v]_B^T A[\overline{w}]_B$.
If $A = (a_{i,j})_{n\times n}$, then $x^T Ay = \sum_{1\leq i,j\leq n} x_i y_j a_{i,j}$.

Properties of Hermitian matrix

- diagonal elements are all real
- determinant is real
- sum of Hermitian matrices is Hermitian
- inverse of Hermitian is Hermitian
- When two Hermitian matrices commute, their product is Hermitian. (May not hold in general)
- All Eigenvalues are real.
- Positive definite $\Leftrightarrow$ all Eigenvalues are positive

With the definition $\|v\| := \sqrt{(v,v)}$, we have the following equations/inequalities

- Over $\mathbb{R}$,
$$\langle u, v\rangle = \frac{\|u+v\|^2 - \|u-v\|^2}{4}$$
Over $\mathbb{C}$,
$$\langle u, v\rangle = \frac{\|u+v\|^2 - \|u-v\|^2 + \|u+iv\|^2 i - \|u-iv\|^2 i}{4}$$
- Cauchy-Schwartz: $|(u, v)| \leq \|u\|\|v\|$

- Pythagoras: if $(u, v) = 0$, then $\|u + v\|^2 = \|u\|^2 + \|v\|^2$. In fact as long as $\mathrm{Re}((u, v)) = 0$ this holds.
- Trig inequality: $\|u + v\| \leq \|u\| + \|v\|$.
- Trig inequality2: $\|u - v\| \leq \|u - w\| + \|w - v\|$

Orthonormal basis and Gram-Schmidt
Orthogonality $\Rightarrow$ linearly independent.
In any inner product space, we can find an orthonormal basis. And any orthonormal set can be extended to an orthonormal basis.
Gram-Schmidt Process(yielding orthonormal basis from a basis):

1. Find a basis $v_1, ..., v_n$ of V.
2. Let $u_1 = \frac{v_1}{\|v_1\|}$, $w_2 = v_2 - (v_2, u_1)u_1$. Then let $u_2 = \frac{w_2}{\|w_2\|}$, $\{u_1, u_2\}$ is orthonormal.
3. Repeat until you find $\{u_1, ..., u_n\}$. This set is orthonormal basis.

Change of basis matrix between orthonormal basis must be unitary, i.e. $P^T\overline{P} = I$.
Properties of unitary matrices:

- length-preserving ($\forall v, \|Pv\| = \|v\| \Leftrightarrow P$ is unitary)
- form a group under composition
- columns form an orthonormal basis.
- Eigenvalues satisfy $|\lambda| = 1$
- $det = 1$

Fourier coefficient If $u_1, ..., u_n$ is an orthonormal basis and $v = \sum_{i=1}^n \lambda_i u_i$, then $\lambda_i = (v, u_i)$ and $\|v\| = \sum_{i=1}^n |\lambda_i|^2$

Projection and shortest distance Given a subspace W, every $v = w + w'$ where $w \in W, w' \in W^{\perp}$. Orthogonal projection map $\pi_W(v) = w$.

Finding shortest distance from a point v to W:

- Pick a basis of W, use Gram-Schmidt to change it to orthonormal basis.
- Use Fourier coefficient to find component of v in W, which is $\pi_W(v) =: w$.
- distance is $\|v - w\|$, and w is the closest point in W to v.

12.3 Adjoint map and spectral theorem

Adjoint of T: the unique map T^* s.t. $(T(u), v) = (u, T^*(v))$.
Given orthonormal basis E, if $A = [T]_E$, $[T^*]_E = \overline{A}^T$.

Rules of adjoint:

- $(S + T)^* = S^* + T^*$
- $(\lambda T)^* = \overline{\lambda} T^*$
- $(T^*)^* = T$
- $(ST)^* = T^* S^*$
- $Ker(T^*) = Im(T)^\perp$
- $Im(T^*) = Ker(T)^\perp$

Properties of self-adjoint map:

- The matrix w.r.t ORTHONORMAL basis is Hermitian
- Eigenvalues are real
- Eigenvectors of distinct Eigenvalues are orthogonal
- If $W \subseteq V$ is T-invariant, $W^\perp$ is also T-invariant.
- Any restriction is self-adjoint.

Note: the only map with $\forall v, (Tv, v) = 0$ is 0 map. And T is self-adjoint $\Leftrightarrow$ $\forall v, (Tv, v) \in \mathbb{R}$
Though not every map is self-adjoint, but for any map T, T^*T must be self-adjoint (Just like $A^T A$ must be symmetric.)

Steps to diagonalise a self-adjoint map(or a Hermitian matrix):

1. Compute a basis for each Eigenspace
2. Use Gram-Schmidt to find an orthonormal basis for each Eigenspace.
3. Union all basis. Put them as columns of P if you need, P here must be orthogonal/unitary.

Spectral Theorem arguments These arguments can be used for other proofs.

1. Do induction on $n = \dim V$, and first prove the statement for $n = 1$.
2. Find some vector v_1 you need for statement (e.g. Eigenvector), and let $W = Span(v_1)$.
3. Find set W' s.t. $W \oplus W' = V$. W' can be $W^\perp$ in some cases.

4. use induction hypothesis on W'. And then combine it with v_1 to prove the statement.

Positive map The following are equivalent for a linear map T:

- $T = T^*$ and $\forall v, (Tv, v) \geq 0$.
- $T = T^*$ and all Eigenvalues are non-negative.
- T has a positive square root. i.e. $\exists R, s.t.\ R^2 = T$ and R is positive.
- T has a self-adjoint square root.
- $T = R^*R$ for some map R.

Positive map in our course is defined as $T = T^*$ and $\forall v, (Tv, v) > 0$, but general idea still applies.
The following are equivalent for a linear map T:

1. T is isometry ($\forall v, \|Tv\| = \|v\|$)
2. $\forall u, v, (Tu, Tv) = (u, v)$
3. For every orthonormal list $\{v_1, ..., v_k\}$, $\{Tv_1, ..., Tv_k\}$ is also orthonormal.
4. there exists orthonormal basis $e_1, ..., e_n$ s.t. $Te_1, ..., Te_n$ is orthonormal basis.
5. $T^*T = I$
6. $TT^* = I$
7. T^* is isometry
8. T is invertible with $T^{-1} = T^*$

This concept extends to non-degenerate symmetric or skew-symmetric bilinear form.

13 Bilinear Form

This is a generalisation of inner product to arbitrary field F.

All bilinear forms (u, v) can be written as $[u]_B^T A[v]_B$ where basis $B = \{v_1, ..., v_n\}$ and $a_{i,j} = (v_i, v_j)$.
Symmetric bilinear form has symmetric A ($A^T = A$) whereas skew-symmetric bilinear form has skew-symmetric A ($A^T = -A$). And if $char(F) \neq 2$, skew-symmetric bilinear form has $\forall v, (v, v) = 0$.
Bilinear form is symmetric or skew-symmetric iff $(v, w) = 0 \Leftrightarrow (w, v) = 0$

Non-degenerate: $V^\perp = 0$ i.e. $\forall v, (u, v) = 0 \Rightarrow u = 0$. For any non-degenerate bilinear form:

- $v \to f_v$ ($f_v(u) := (v, u)$) is isomorphism between V, V^*.
- $dim(W^\perp) = dim(V) - dim(W)$
- Non-degenerate $\Leftrightarrow$ corresponding matrix A is invertible(full-rank)

Congruent matrices: If P is a change of basis matrix from B_1 to B_2, then $(u, v) = [u]_1^T A[v]_1 = [u]_2^T P^T AP[v]_2 = [u]_2^T B[v]_2$. So A is called congruent to B if exists invertible P s.t. $B = P^T AP$.
Trick to prove/disprove congruence: $\det B = (\det P)^2 \det A$. But may not work in general.

Congruence of non-degenerate skew-symmetric matrix (n must be even): always congruent to

$$J_m = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \oplus ... \oplus \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ (m blocks)}$$

Congruence of non-degenerate symmetric matrix: has orthogonal basis($(v_i, v_j) = 0$ and $(v_i, v_i) \neq 0$) and matrix wrt to that basis is diagonal. Steps to find such basis:

1. find v_1 s.t. $(v_1, v_1) \neq 0$.
2. Compute $Span(v_1)^\perp$ and find $v_2 \in \{v_1\}^\perp$ s.t. $(v_2, v_2) \neq 0$.
3. Compute $Span(v_1, v_2)^\perp$ and find $v_3 \in Span(v_1, v_2)^\perp$ s.t. $(v_3, v_3) \neq 0$.
4. Repeat until getting a basis.

Comparison between inner product space and bilinear form space

Inner Product	Bilinear form
Only defined for $\mathbb{R}, \mathbb{C}$	defined for any field F
not bilinear on $\mathbb{C}$	Inner products on $\mathbb{R}$ are bilinear forms
$(u, v) = u^T A\overline{v}$ for some Hermitian, positive-definite A	$(u, v) = u^T Av$, any A works
If $v \neq 0, (v, v) > 0$	Not necessarily true, field may not have order
You can always define orthogonality	Only make sense for non-degenerate symmetric/skew-symmetric cases
$W^\perp \oplus W$	main problem is $(v, v) = 0$ for some non-zero v. Statement holds if $(v, v) \neq 0 \; \forall v \in W$
Can always find orthonormal basis	not true in general, but orthogonal basis exists for symmetric ones

13.1 Quadratic form

This is a special case of symmetric bilinear form, defined by $Q(v) = (v, v)$. Bilinear form induced by quadratic form: $(x, y) = \frac{1}{2}(Q(x + y) - Q(x) - Q(y))$
Two quadratic forms are equivalent if the corresponding matrices are congruent, or you can directly change variables to prove equivalence.

By the process of diagonalising symmetric bilinear form, we can always find an equivalent quadratic form for $Q(x)$ in the form of:

$$Q'(x) = \sum \alpha_i x_i^2$$

if Q is non-degenerate, clearly $\alpha_i \neq 0$.
As a result

- on $\mathbb{C}$, all non-degenerate quadratic forms are equivalent to $Q_0(x) = \sum x_i^2$
- on $\mathbb{R}$, all non-degenerate quadratic forms are equivalent to $Q_{p,q}(x) = \sum_{i=1}^{p} x_i^2 - \sum_{i=p+1}^{q} x_i^2$ for unique p, q.

However for $\mathbb{Q}$, there are infinite inequivalent non-degenerate quadratic forms on $\mathbb{Q}^n$. These can be given by $Q_d(x) := x_1^2 + \cdots + x_{n-1}^2 + dx_n^2$ where d is a square-free integer. (not divisible by any integer square)