HAlg Note

1 Basic Knowledge

Lagrange's Theorem: If $H \subseteq G$ is a subgroup, then $|H|$ divides $|G|$. **I**: If G is finite, then $g^{|G|} = e \ \forall g \in G$. **II**: $o(g) \mid |G|$ **III**: If $|G| = p$ prime, G is cyclic.

Complement-wise Operations: $\phi : V_1 \times V_2 \to V_1 \oplus V_2$ by **I**:$(\vec{v}_1, \vec{u}_1) + (\vec{v}_2, \vec{u}_2) := (\vec{v}_1 + \vec{v}_1, \vec{u}_1 + \vec{u}_2)$, $\lambda(\vec{v}, \vec{u}) := (\lambda\vec{v}, \lambda\vec{u})$ (ps:V_1, V_2 通过 ϕ 定义的 map 所形成的 vector space 记作 $V_1 \oplus V_2$)

External Direct Sum: 一个" 代数结构"(Vector Space), 定义为 set 是 $V_1 \oplus \cdots \oplus V_n := V_1 \times \cdots \times V_n$ 且有一组运算法则 component-wise operations

Projections: $pr_i : X_1 \times \cdots \times X_n \to X_i$ by $(x_1, ..., x_n) \mapsto x_i$ **Canonical Injections**: $in_i : X_i \to X_1 \times \cdots \times X_n$ by $x \mapsto (0, ..., 0, x, 0, ..., 0)$

Useful Way of Thinking Matrix: $A_{n\times m}B_{m\times n} = A\begin{pmatrix}\mathbf{b}_{*1} & \mathbf{b}_{*2} & \cdots \mathbf{b}_{*n}\end{pmatrix} = \begin{pmatrix}A\mathbf{b}_{*1} & A\mathbf{b}_{*2} & \cdots A\mathbf{b}_{*n}\end{pmatrix}$ $\quad rank(\mathbf{a}_{*k}\mathbf{b}_{k*}^T) \le 1$

$$A_{n\times m}B_{m\times n} = \begin{pmatrix}\mathbf{a}_{1*}^T \\ \vdots \\ \mathbf{a}_{n*}^T\end{pmatrix} B = \begin{pmatrix}\mathbf{a}_{1*}^T B \\ \vdots \\ \mathbf{a}_{n*}^T B\end{pmatrix} \qquad A_{n\times m} = A_{n\times m} I_m \begin{matrix} = A(\vec{e}_1 & \vec{e}_2 & \cdots & \vec{e}_n) \\ = (A\vec{e}_1 & A\vec{e}_2 & \cdots & A\vec{e}_n) \end{matrix} \qquad A_{n\times m}B_{m\times n} = \begin{pmatrix}\mathbf{a}_{*1} \cdots \mathbf{a}_{*m}\end{pmatrix}\begin{pmatrix}\mathbf{b}_{1*}^T \\ \vdots \\ \mathbf{b}_{m*}^T\end{pmatrix} = \sum_{k=1}^m \mathbf{a}_{*k}\mathbf{b}_{k*}^T$$

$^\oplus$ **Division Ring**: If R is ring and it's multiplicative inverse $\forall a \in R \setminus \{0_R\}$ $\quad$ $^\oplus$ **Characteristic of Field**: F is field, $char(F) = p$ if 可以有 $1/p$ 的操作.

2 Summary

Name	Group $(G, *)$	Ring $(R, +, \cdot)$	Vector Space $(F - V)$	Module $(R - M)$
Def	**Closure**: $g * h \in G$ $\quad \forall g,h,k \in G$ **Associativity**: $(g*h)*k = g*(h*k)$ **Identity**: $\exists e \in G, e*g = g*e = g$ **Inverse**: $\exists g^{-1} \in G, g*g^{-1} = g^{-1}*g = e$	$(R,+)$ is *abelian group* with 0_R $\quad \forall a,b,c \in R$ $(R,\cdot)$ is **monoid** with 1_R (monoid is closure) i.e. **Associativity**: , $(a\cdot b)\cdot c = a\cdot(b\cdot c)$ **Identity**: $1_R \cdot a = a \cdot 1_R = a$ **Distributive**: $a\cdot(b+c) = a\cdot b + a\cdot c$ $(b+c)\cdot a = b\cdot a + c\cdot a$	$(V, \dot{+})$ is *abelian group* $\quad \forall \vec{v}, \vec{w} \in V$ $\exists$ map $F \times V \to V : (\lambda, \vec{v}) \to \lambda\vec{v}$ $\quad \forall \lambda, \mu \in F$ **I**: $\lambda(\vec{v} \dot{+} \vec{w}) = (\lambda\vec{v}) \dot{+} (\lambda\vec{w})$ **II**: $(\lambda+\mu)\vec{v} = (\lambda\vec{v}) \dot{+} (\mu\vec{v})$ **III**: $\lambda(\mu\vec{v}) = (\lambda\mu)\vec{v}$ **IV**: $1_F\vec{v} = \vec{v}$	$(M, \dot{+})$ is *abelian group* $\quad \forall m_1, m_2 \in M$ $\exists$ map $R \times M \to M : (r, m) \to rm$ $\quad \forall r_1, r_2 \in R$ **I**: $r(m_1 \dot{+} m_2) = (\lambda m_1) \dot{+} (\lambda m_2)$ **II**: $(r_1 + r_2)m_1 = (r_1 m_1) \dot{+} (r_1 m_1)$ **III**: $r_1(r_2 m_1) = (r_1 r_2)m_1$ **IV**: $1_R m_1 = m_1$
Prop	**I**: $(gh)^{-1} = h^{-1}g^{-1}$	**I**. $0\cdot a = a \cdot 0 = 0$ $\quad \forall a,b \in R$ **II**. $(-a)\cdot b = a\cdot(-b) = -(a\cdot b)$ **Commutative Ring**: add $\forall a,b \in R, ab = ba$	**I**. $0\vec{v} = 0$ and $\vec{0}\lambda = \vec{0}$ $\quad \forall \vec{v} \in V, \lambda \in F$ **II**. $(-1)\vec{v} = -\vec{v}$ **III**. $\lambda\vec{v} = \vec{0} \Leftrightarrow \lambda = 0$ or $\vec{v} = \vec{0}$ ⋆	**I**. $0_R m = 0_M$; $r0_M = 0_M$ $\quad \forall r \in R, m \in M$ **II**. $(-r)m = r(-m) = -(rm)$
Remark	G, H groups $\Rightarrow G \times H$ also.	For ring R $[1_R = 0_R \Leftrightarrow R = \{0\}]$		
e.g.	Cyclic group; GL_n ; D_n ; $\mathbb{Z}$	$Mat(n,F)$; $R[X]$; $\mathbb{Z}/m\mathbb{Z}$; $\mathbb{Z}$	$\mathbb{R}[x]_{<n}$; $Mat(n,F)$; $Hom(V,W)$	$R = \mathbb{Z}$ Abelian Group; $R = F$ Vector Space
Sub objects	**Subgroup** (H): $\quad \forall h_1, h_2 \in H$ **I**: $H \ne \emptyset$; **II**: $h_1 * h_2 \in H$; **III**: $h_1^{-1} \in H$.	**Subring** (R'): $\quad \forall a, b \in R'$ **I**. $1_R \in R'$ **II**. $a - b \in R'$ **III**. $ab \in R'$	**Subspace** (U): $\quad \forall \vec{v}, \vec{u} \in U, \lambda, \mu \in F$ **I**. $\vec{0} \in U$ **II**. $\vec{u} + \vec{v} \in U$ and $\lambda\vec{u} \in U$ (or: $\lambda\vec{u} + \mu\vec{v} \in U$)	**Submodule** (M'): $\quad \forall m_1, m_2 \in M'$ **I**. $0_M \in M'$ $\quad \forall r_1, r_2 \in R$ **II**. $m_1 - m_2 \in M'$ and $r_1 m_1 \in M'$ (or: $r_1 m_1 - r_2 m_2 \in M'$)
Create	H, K subgroups $\Rightarrow H \cap K$ also.	R, S subring $\Rightarrow R \cap S$ also.	V, W subspaces $\Rightarrow V \cap W, V + W$ also.	M, N submodules $\Rightarrow M \cap N, M + N$ also.
Generate objects	**Generated Group** $\langle T \rangle$: $\langle T \rangle := \{g_1^{a_1} ... g_k^{a_k} \mid k \in \mathbb{N}, g_i \in T, a_i \in \mathbb{N}\}$	**Generated Ideal** $_R\langle T \rangle$: R is *commutative ring* $_R\langle T \rangle := \{\sum_{i=1}^n r_i t_i : n \in \mathbb{N}, r_i \in R, t_i \in T\}$	**Generated subspaces** $\langle T \rangle$: $\langle T \rangle := \{\alpha_1\vec{v}_1 + \cdots + \alpha_n\vec{v}_n : \alpha_i \in F, \vec{v}_i \in T, n \in \mathbb{N}\}$	**Generated submodules** $_R\langle T \rangle$ $\langle T \rangle := \{r_1 t_1 + \cdots + r t_n : r_i \in R, t_i \in T, n \in \mathbb{N}\}$
Special	**Cyclic Group**: $\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$	**Principal Ideal**: $_R\langle a \rangle$ i.e. aR	$\langle \emptyset \rangle := \{\vec{0}\}$	**Cyclic submodule**: If $M =_R \langle t \rangle$
Prop	$\langle T \rangle$ is the smallest the {generated things} containing T. ps: 默认 $^2T \subseteq R$ $\ ^4T \subseteq M$			
Homo	**Homomorphism**: $\phi : G \to H$ $\quad \forall g_1, g_2 \in G$ **I**. $\phi(g_1 * g_2) = \phi(g_1) * \phi(g_2)$	$f : R \to S$ hom: $\quad \forall a, b \in R$ **I**. $f(a+b) = f(a) + f(b)$ **II**. $f(ab) = f(a)f(b)$	$f : V \to W$ $\quad \forall \vec{v}_1, \vec{v}_2 \in V, \lambda \in F$ **I**. $f(\vec{v}_1 + \vec{v}_2) = f(\vec{v}_1) + f(\vec{v}_2)$ **II**. $f(\lambda\vec{v}_1) = \lambda f(\vec{v}_1)$	**R-Hom**: $f : M \to N$ $\quad \forall a, b \in M, r \in R$ **I**. $f(a+b) = f(a) + f(b)$ **II**. $f(ra) = rf(a)$
Prop A	**I**: $\phi(e_G) = e_H$ **II**: $\phi(g^{-1}) = \phi(g)^{-1}$ **III**. ϕ is 1-1 $\Leftrightarrow \ker\phi = \{e_G\}$	**I**. $f(0_R) = 0_S$ $\quad f(1_R) = 1_S$ NOT need **II**. $f(x-y) = f(x) - f(y)$ **III**. $f(a^n) = (f(a))^n$ $\quad f(mx) = mf(x)$ **Iv**. f is 1-1 $\Leftrightarrow \ker f = \{0_R\}$	**I**. $f(\vec{0}) = \vec{0}$ **II**. $f(\lambda\vec{v} + \mu\vec{u}) = \lambda f(\vec{v}) + \mu f(\vec{u})$ **III**. $f \circ g$ is linear map. **IV**. f is 1-1 iff $\ker f = \{\vec{0}\}$	**I**. $f(0_M) = 0_N$ $\quad f(1_R) = 1_S$ NOT need **II**. $f(a-b) = f(a) - f(b)$ **III**. f is 1-1 iff $\ker f = \{0\}$
Ker/Im	**I**. $Im(\phi)$ subgroup $\quad \ker(\phi) \lhd G$ normal. **II**. $K \subseteq G$ is subgroup $\Rightarrow \phi(K) \subseteq H$ also. **III**. $Ker(\phi)$ subgroup.	**I**. $Im(f)$ subring. $\quad \ker(f) \unlhd R$ ideal . **II**. $R' \subseteq R$ is subring $\Rightarrow f(R')$ also.	**I**. $\ker(f)$; $Im(f)$ are subspaces. **II**. Rank-Nullity Theorem...	**I**. $\ker f, Im f$ are submodules.
Remark	**Isomorphism**: = LM & Bij. **Endomorphism(End)**: = LM & $V = W$. **Automorphism(Aut)**: = Iso & $V = W$ **Monomorphism**: = LM & 1-1. **Epimorphism**: = LM & onto.			

Normal $(H \lhd G)$: $H \subseteq G$ is normal if: $\forall g \in G, gH = Hg$

Property: **I**: $Ker\phi \lhd G$ **II**: ϕ is 1-1 $\Rightarrow G \cong im\phi$

Ideal $(I \unlhd R)$: A subset $I \subseteq R$ (ring) is an ideal if: **I.** $I \ne \emptyset$ **II.** $\forall a, b \in I, a - b \in I$ **III.** $\forall i \in I, \forall r \in R, ri, ir \in I$ e.g.$m\mathbb{Z}$

Property: If I, J are *ideals* of R. Then $I + J$; $I \cap J$ are also ideals. || Property of $m\mathbb{Z}$: $a\mathbb{Z} + b\mathbb{Z} = \gcd(a,b)\mathbb{Z}$; $a\mathbb{Z} \cap b\mathbb{Z} = \mathrm{lcm}(a,b)\mathbb{Z}$ Not Principal Ideal: $_{\mathbb{Z}[X]}\langle 2, X \rangle$

Field (F): A set F is a field with two operators: (addition)$+ : F \times F \to F; (\lambda, \mu) \to \lambda + \mu$ (multiplication)$\cdot : F \times F \to F; (\lambda, \mu) \to \lambda\mu$ if:

$(F, +)$ and $(F \setminus \{0_F\}, \cdot)$ are abelian groups with identity $0_F, 1_F$. and $\lambda(\mu + \nu) = \lambda\mu + \lambda\nu$ $\quad$ $e.g. Fields : \mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$

Field: For a ring R: Commutative ring + R has multiplicative inverse = Field.

3 Vector Spaces/Subspaces | Generating Set | Linear Independent | Basis

Linearly Independent: $L = \{\vec{v}_1, \vec{v}_2, ..., \vec{v}_r\}$ is linearly independent if: $\forall c_1, ..., c_r \in F, c_1\vec{v}_1 + \cdots + c_r\vec{v}_r = \vec{0} \Rightarrow c_1 = \cdots = c_r = 0$.

Basis & Dimension: If V is finitely generated. $\Rightarrow \exists$ subset $B \subseteq V$ which is both LI and GS. (B is basis) **Dim**: $\dim V := |B|$

Relation|GS,LI,Basis,dim: Let V be vector space. L is linearly independent set, E is generating set, B is basis set.

1. **GS|LI**: $|L| \le |E|$ (can get: dim unique) **LI→Basis**: If V finite generate $\Rightarrow \forall L$ can extend to a basis. If $L = \emptyset$, prove $\exists B$ $\quad kerf \cap imf = \{0\}$
2. **Basis|max,min**: $B \Leftrightarrow B$ is minimal GS $(E) \Leftrightarrow B$ is maximal LI (L). **Uniqueness|Basis**: 每个元素都可以由 basis 唯一表示.
3. **Proper Subspaces**: If $U \subset V$ is proper subspace, then $\dim U < \dim V$. $\Rightarrow$ If $U \subseteq V$ is subspace and $\dim U = \dim V$, then $U = V$.
4. **Dimension Theorem**: If $U, W \subseteq V$ are subspaces of V, then $\dim(U + W) = \dim U + \dim W - \dim(U \cap W)$ ↓特别同构于 F^n
5. **Isomorphism**: For *finitely generated* vector spaces V $\Rightarrow$ Two F-vector spaces V, W are isomorphic $\Leftrightarrow \dim V = \dim W$.

Complementary: $U, W \subseteq V$,U, V subspaces are complementary $(V = U \oplus W)$ if: $\exists\phi : U \times W \to V$ by $(\vec{u}, \vec{w}) \xrightarrow{\sim} \vec{u} + \vec{w}$ is isom.

i.e. $\forall\vec{v} \in V$, we have unique $\vec{u} \in U, \vec{w} \in W$ s.t. $\vec{v} = \vec{u} + \vec{w}$. ps: It's a linear map.

Criteria Lemma: If U, W are subspace of V, then $V = U \oplus W \Leftrightarrow V = U + W$ and $U \cap W = \{0\}$. (需要证明/只能两个向量空间)

4 Linear Mapping | Rank-Nullity| Matrices | Change of Basis

ps: 默认 V, W F-Vector Spaces.

4.1 Linear Mapping | Rank-Nullity

Property of Linear Map: Let $f, g \in Hom$

1. **Determined**: f is determined by $f(\vec{b}_i), \vec{b}_i \in \mathcal{B}_{basis}$ ($\star$ **i.e.** $f(\sum_i \lambda_i \vec{v}_i) := \sum_i \lambda_i f(\vec{v}_i)$)
2. **Classification of Vector Spaces**: $\dim V = n \Leftrightarrow f : F^n \xrightarrow{\sim} V$ by $f(\lambda_1, ..., \lambda_n) \mapsto \sum_{i=1}^n \lambda_i \vec{v}_i$ is isomorphism.
3. **Left/Right Inverse**: f is 1-1 $\Rightarrow \exists$ left inverse g s.t. $g \circ f = id$ 考虑 direct sum f is onto $\Rightarrow \exists$ right inverse g s.t. $f \circ g = id$
4. $^{\ominus}$ **More of Left/Right Inverse**: $f \circ g = id \Rightarrow g$ is 1-1 and f is onto. 使用 kernel=0 来证明

Rank-Nullity Theorem: For linear map $f : V \to W$, $\dim V = \dim(\ker f) + \dim(Imf)$ Following are properties:

1. **Injection**: f is 1-1 $\Rightarrow \dim V \le \dim W$ **Surjection**: f is onto $\Rightarrow \dim V \ge \dim W$ Moreover, $\dim W = \dim imf$ iff f is onto.
2. **Same Dimension**: f is isomorphism $\Rightarrow \dim V = \dim W$ **Matrix**: $\forall M$, column rank $c(M)$ = row rank $r(M)$.
3. **Relation**: If V, W finite generate, and $\dim V = \dim W$, Then: f is isomorphism $\Leftrightarrow f$ is 1-1 $\Leftrightarrow f$ is onto.

4.2 Matrices | Change of Basis | Similar Matrices | Trace

Matrix: For $A_{n\times m}, B_{m\times p}$, $AB_{n\times p} := (AB)_{ij} = \sum_{k=1}^m a_{ik} b_{kj}$ **Transpose**: $A_{m\times n}^T := (A^T)_{ij} = a_{ji}$

Invertible Matrices: A is invertible if $\exists B, C$ s.t. $BA = I$ and $AC = I$ || $\exists B,\ BA = I \Leftrightarrow \exists C, AC = I \Leftrightarrow \exists A^{-1}$ ${}_{\mathcal{B}}[f^{-1}]_{\mathcal{A}} = {}_{\mathcal{A}}[f]_{\mathcal{B}}^{-1}$

Representing matrix of linear map ${}_{\mathcal{B}}[f]_{\mathcal{A}}$: $f : V \to W$ be linear map, $\mathcal{A} = \{\vec{v}_1, ..., \vec{v}_n\}$ is basis of V, $\mathcal{B} = \{\vec{w}_1, ..., \vec{w}_m\}$ is basis of W.

1. ${}_{\mathcal{B}}[f]_{\mathcal{A}} := A$ (matrix) where $f(\vec{v}_i) = \sum_j A_{ji} \vec{w}_j$ $\exists M_{\mathcal{B}}^{\mathcal{A}} : Hom_F(V, W) \xrightarrow{\sim} Mat(n \times m; F)$
2. If $\vec{v} \in V$, then ${}_{\mathcal{A}}[\vec{v}] := \mathbf{b}$ (vector) where $\vec{v} = \sum_i b_i \vec{v}_i$
3. **Theorems**: $[f \circ g] = [f] \circ [g]$ ${}_{\mathcal{C}}[f \circ g]_{\mathcal{A}} = {}_{\mathcal{C}}[f]_{\mathcal{B}} \circ {}_{\mathcal{B}}[g]_{\mathcal{A}}$ ${}_{\mathcal{B}}[f(\vec{v})] = {}_{\mathcal{B}}[f]_{\mathcal{A}} \circ {}_{\mathcal{A}}[\vec{v}]$ ${}_{\mathcal{A}}[f]_{\mathcal{A}} = I \Leftrightarrow f = id$
4. **Change of Basis**: Define *Change of Basis Matrix*$:= {}_{\mathcal{A}}[id_V]_{\mathcal{B}}$ ${}_{\mathcal{B}'}[f]_{\mathcal{A}'} = {}_{\mathcal{B}'}[id_W]_{\mathcal{B}} \circ {}_{\mathcal{B}}[f]_{\mathcal{A}} \circ {}_{\mathcal{A}}[id_V]_{\mathcal{A}'}$ ${}_{\mathcal{A}'}[f]_{\mathcal{A}'} = {}_{\mathcal{A}}[id_V]_{\mathcal{A}'}^{-1} \circ {}_{\mathcal{A}}[f]_{\mathcal{A}} \circ {}_{\mathcal{A}}[id_V]_{\mathcal{A}'}$

Elementary Matrix: $I + \lambda E_{ij}$ (cannot $I - E_{ii}$) 就是初等矩阵, 左乘代表 j 行乘 λ 倍加到第 i 行, 右乘代表 j 列乘 λ 倍加到第 i 列 $\Rightarrow$ Invertible!

1. 交换 i, j 列/行: $P_{ij} = diag(1, ..., 1, -1, 1, ..., 1)(I + E_{ij})(I - E_{ji})(I + E_{ij})$ where -1 in jth place.
2. **Row Echelon Form|Smith Normal Form**: $\tilde{A}$: REF 通过左乘初等矩阵可以实现 $\approx A$: $S(n, m, r)$ 通过 $\tilde{A}$ 右乘初等矩阵可以实现

Smith Normal Form: $\forall A, \exists$ invertible P, Q s.t. $PAQ = S(n, m, r) := n \times m$ 的矩阵, 对角线前 r 个是 1, 后面 0. **Lemma**: $r = r(A) = c(A)$

· Every linear map $f : V \to W$ can be representing by ${}_{\mathcal{B}}[f]_{\mathcal{A}} = S(n, m, r)$ for some basis $\mathcal{A}, \mathcal{B}$ of V, W.

Similar Matrices: $N = T^{-1}MT \Leftrightarrow M, N$ are similar. *Special Case*: If $N = {}_{\mathcal{B}}[f]_{\mathcal{B}}, M = {}_{\mathcal{A}}[f]_{\mathcal{A}}$, then $N = T^{-1}MT$. where $T = {}_{\mathcal{A}}[id_V]_{\mathcal{B}}$

1. If $A \sim B$ iff A is similar to B, then $\sim$ is an equivalence relation. ${}_{\mathcal{A}'}[f]_{\mathcal{A}'} \sim {}_{\mathcal{A}}[f]_{\mathcal{A}}$
2. If $\mathcal{B} = \{p(\vec{v}_1), ..., p(\vec{v}_n)\}$ and $\mathcal{A} = \{\vec{v}_1, ..., \vec{v}_n\}$ where $p : V \xrightarrow{\sim} V$. Then ${}_{\mathcal{A}}[id_V]_{\mathcal{B}} = {}_{\mathcal{A}}[p]_{\mathcal{A}}$
3. If V is a vector space over F, $[A, B$ are *similar* matrices. $\Leftrightarrow$ $A = {}_{\mathcal{A}}[f]_{\mathcal{A}}, B = {}_{\mathcal{B}}[f]_{\mathcal{B}}$ for some basis $\mathcal{A}, \mathcal{B}; f : V \to V]$
4. Set of *End* is in a bijection correspondence with the equivalence class of matrices under $\sim$. 一个自同态 **End** 就对应一个相似矩阵的等价类

Trace: $tr(A) := \sum_i a_{ii}$ and $tr(f) := tr({}_{\mathcal{A}}[f]_{\mathcal{A}})$ | $tr(AB) = tr(BA)$ $tr(\lambda A + \mu B) = \lambda tr(A) + \mu tr(B)$ $tr(N) = tr(M)$ if M, N similar.

5 Rings | Polynomials | Ideals | Subrings

5.1 Rings | Polynomial Rings

2nd Def of Ring Homomorphism: f is ring homomorphism if: 1. $f : (R, +) \to (S, +)$ is group homomorphism and 2. $f(xy) = f(x)f(y)$.

Unit: $a \in R$ is unit if it's *Invertible*. i.e. $\exists a^{-1} \in R$ s.t. $aa^{-1} = a^{-1}a = 1_R$ **Group of Unit** $(R^\times, \cdot) := \{a \in R : a \text{ is unit}\}$

· **Lemma**: If ${}^1 f : R \to S$ homo, ${}^2 f(1_R) = 1_S$, ${}^3 x$ is *unit* of R. $\Rightarrow$ ${}^1 f(x)$ is *unit* of S. ${}^2 f|_{R^\times} : R^\times \to S^\times$ is *group homomorphism*.

Zero-divisors: $a \in R$ is *zero-divisor* if $\exists b \in R, b \ne 0$ s.t. $ab = 0$ or $ba = 0$ *Field has no zero-divisors.* · e.g. $\mathbb{Z}^\times = \{-1, 1\}$; 1_R is a unit.

Integral Domain: A *commutative* ring R is an integral domain if it has no zero-divisors. e.g. $\mathbb{Z}/p\mathbb{Z}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}, ...$ Cancellation Law: ↓

Properties of Integral Domain: $\forall a, b \in R$. **I.** $ab = 0 \Rightarrow a = 0$ or $b = 0$ **II.** $a, b \ne 0 \Rightarrow ab \ne 0$ **III.** $ab = ac, a \ne 0 \Rightarrow b = c$

· *Field is Integral Domain* **Every finite integral domain is a field** $\mathbb{Z}/p\mathbb{Z}$ is field iff p is prime. e.g.(integral domain) $\mathbb{Z}; \mathbb{Z}/p\mathbb{Z}$

Polynomial Ring $R[X]$: $R[X] := \{a_n X^n + \cdots + a_1 X + a_0 : a_i \in R, n \in \mathbb{N}\}$ where X is **indeterminate** $\Leftarrow X \notin R$ and $\forall x \in R, Xa = aX$

1. **Degree**: $\deg(P) := \max\{n \in \mathbb{N} : a_n \ne 0\}$ **Leading Coefficient**: a_n **Monic**: $a_n = 1$ ps: Polynomial NOT a function
2. **Lemma**: ${}^1 R$ *integral domain|no zero-divisors* $\Rightarrow R[X]$ also. and $\deg(PQ) = \deg(P) + \deg(Q)$ if $P, Q \ne 0$.
3. **Division and Remainder**: If R is *integral domain* and $P, Q \in R[X]$, Q **monic** $\exists!\, A, B \in R[X]$ s.t. $P = AQ + B$ and $\deg(B) < \deg(Q)$
4. **Function | Factorize**: If R is *commutative ring* $\Rightarrow$ ${}^1 R[X] \to Maps(R, R)$ (可以视作函数) ${}^2 \lambda \in R$ is root of $P \Leftrightarrow (X - \lambda) \mid P(X)$
5. **Roots**: If R is *Integral domain*: P has at most $\deg(P)$ roots.

Algebraically Closed: $R = F$ field is *algebraically closed* if every non-constant polynomial has a root in F. e.g. $\mathbb{C}$

· **Decomposes**: If F field is *algebraically closed* $\Rightarrow P$ decomposes into: $P(X) = a(X - \lambda_1) \cdots (X - \lambda_n), a \in F^\times$ i.e. $a \ne 0$

5.2 Equivalence Relation

Equivalence Relation: **Reflexive**: xRx $(x \sim x)$ **Symmetric**: $xRy \Rightarrow yRx$ $(x \sim y \Rightarrow y \sim x)$ **Transitive**: $xRy, yRz \Rightarrow xRz$ $(x \sim y, y \sim z \Rightarrow x \sim z)$

Partial Order: **Reflexive**: xRx $(x \sim x)$ **Anti-symmetric**: $xRy, yRx \Rightarrow x = y$ $(x \sim y, y \sim x \Rightarrow x = y)$ **Transitive**: $xRy, yRz \Rightarrow xRz$ $(x \sim y, y \sim z \Rightarrow x \sim z)$

Property of Equivalence Relation: If R $(\sim)$ is equivalence relation on X.

1. $\sim$ Define the **equivalence classes** of $x \in X$ as $E(x) := \{y \in X : x \sim y\}$
2. $\sim$ **Partition** X into disjoint subsets $X = \bigcup_i X_i$, X_i is equivalence class of $x \in X$.
3. $x \sim y \quad \Leftrightarrow \quad E(x) = E(y) \quad \Leftrightarrow \quad E(x) \cap E(y) \neq \emptyset$.

Set of Equivalence Classes $(X/\sim)$: $(X/\sim) := \{E(x) : x \in X\}$ **Canonical Projection**: $can : X \to (X/\sim)$ by $x \mapsto E(x)$

System of Representatives: $Z \subseteq X$ is a system of representatives if 每个等价类都恰好有一个元素代表在 Z 中

Universal Property of the set of Equivalence Classes: If $f : X \to Z$ is a map s.t. $x \sim y \Leftrightarrow f(x) = f(y)$. ($\sim$ is Equivalence relation) **Important**

Then, $\exists!$ map $\overline{f} : (X/\sim) \to Z$ s.t. $f = \overline{f} \circ can$ with $\overline{f}(E(x)) = f(x)$ is *well-defined*. Further more, $\overline{f} : (X/\sim) \xrightarrow{\sim} Im(f)$

ps: Often, if we want to prove $g : (X/\sim) \to Z$ is well-defined, we need to prove $x \sim y \Leftrightarrow g(x) = g(y)$ holds.

5.3 Factor Ring | First Isomorphism Theorem

Coset of Ideal: Let I be an ideal of R. Then $a + I$ is a coset of I. The $\sim$ is defined by $a \sim b \Leftrightarrow a - b \in I$ is an equivalence relation.

Factor Ring: Let I be ideal of R. $R/I := \{a + I : a \in R\}$ is the set of cosets of I. (i.e. R/I is the set of equivalence classes of R under $\sim$)

1. By *well-defined* operators: $(x + I) \dot{+} (y + I) = (x + y) + I$ and $(x + I) \cdot (y + I) = xy + I \quad \Rightarrow \quad R/I$ is a ring.
2. $x + I = y + I \quad \Leftrightarrow \quad x \sim y \quad \Leftrightarrow \quad x - y \in I$ || R is commutative $\Rightarrow R/I$ also. || $R/I \neq \{0 + I\}$ iff $I \neq R$
3. ⋆The <u>Identity</u> of R/I: $1_R + I$ The <u>Zero</u> of R/I: $0_R + I$

Universal Property of Factor Ring: Let R be a ring and I be an ideal of R. ps:$\overline{f}(x + I) = f(x)$

1. **can**: Mapping $can : R \to R/I$ by $x \mapsto x + I$ is ^{1} surjection, ^{2} $ker(can) = I$, ^{3} can is ring homomorphism.
2. **f**: If $^1 f : R \to S$ is *ring homomorphism* and $^2 I \subseteq ker(f)$, then $\exists!\, ^1\overline{f} : R/I \to S$ s.t. $f = \overline{f} \circ can$ is *ring homomorphism*.
3. **First Isomorphism Theorem**: If $f : R \to S$ is *ring homomorphism* $\Rightarrow \exists!\, \overline{f} : R/ker(f) \xrightarrow{\sim} im(f)$ is (*ring isomorphism*).

Universal Property of Quotient Group: Let G be a group and H be a normal subgroup of G. ps:$\overline{f}(g + N) = f(g)$

1. **can**: Mapping $can : G \to G/H$ by $x \mapsto xH$ is ^{1} surjection, ^{2} $ker(can) = H$, ^{3} can is group homomorphism.
2. **f**: If $^1 f : G \to S$ is *group homomorphism* and $^2 H \subseteq ker(f)$, then $\exists!\, ^1\overline{f} : G/H \to S$ s.t. $f = \overline{f} \circ can$ is *group homomorphism*.
3. **First Isomorphism Theorem**: If $f : G \to S$ is *group homomorphism* $\Rightarrow \exists!\, \overline{f} : G/ker(f) \xrightarrow{\sim} im(f)$ is (*group isomorphism*).

5.4 Modules | Submodules | All of That

Create Modules: Let $f : R \to S$ is a *ring homomorphism*, $f(1_R) = 1_S$ and M is a $S-$Module, then M is also a $R-$Module by:

Define the restrict our scalar: $rm := f(r)m \quad \forall r \in R, m \in M$ ps: $f(1_R) = 1_S$

Free Module: Let M be a $R-$Module. M is *free* if: $\forall m \in M, \exists!\, r_1, ..., r_n \in R$ s.t. $m = r_1 m_1 + \cdots + r_n m_n$ ps: $m_1, ..., m_n$ is basis of M

Coset of Submodule: Let N submodule of M. Then $m + N$ coset of N. $\sim$ is defined by $m \sim n \Leftrightarrow m - n \in N$ is an equivalence relation.

Factor Module: Let N submodule of M. $M/N := \{m + N : m \in M\}$ is the set of cosets of N.

Universal Property of Module Quotient: Let M be a module and N be a submodule of M. ps:$\overline{f}(x + N) = f(x)$

1. **can**: Mapping $can : M \to M/N$ by $x \mapsto x + N$ is ^{1} surjection, ^{2} $ker(can) = N$, ^{3} can is module homomorphism.
2. **f**: If $^1 f : M \to S$ is *module homomorphism* and $^2 N \subseteq ker(f)$, then $\exists!\, ^1\overline{f} : M/N \to S$ s.t. $f = \overline{f} \circ can$ is *module homomorphism*.
3. **First Isomorphism Theorem**: If $f : M \to S$ is *module homomorphism* $\Rightarrow \exists!\, \overline{f} : M/ker(f) \xrightarrow{\sim} im(f)$ is (*module isomorphism*).

$^{\ominus}$ **Second Isomorphism Theorem for Modules**: Let N, K be submodules of R-module $M \quad \Rightarrow \quad N/(N \cap K) \cong (N + K)/K$

ps: $\uparrow$ consider $f : N \to (N + K)/K$ and then we can find $ker(f) = N \cap K$ $\downarrow$ consider $f : M/K \to M/N$ and then we can find $ker(f) = N/K$

$^{\ominus}$ **Third Isomorphism Theorem for Modules**: Let N, K be submodules of R-module M ; $K \subseteq N \quad \Rightarrow \quad \frac{M/K}{N/K} \cong M/N$

$^{\ominus}$ **For Vector Space**: $\dim(V/U) = \dim V - \dim U$ Hint: Consider $can : V \to V/U$ by $v \mapsto v + U$ is surjection, $\ker(can) = U$

6 Permutation | Determinants | Eigenvalues and Eigenvectors

6.1 Permutation | Determinants

Review of Permutation: A bijection $\sigma : \{1, ..., n\} \xrightarrow{\sim} \{1, ..., n\}$ is a permutation. All permutations of n elements form a group $\mathfrak{S}_n$.

Transposition: 交换两个元素. **Inversion**: A pair of elements (i, j) is an inversion of $\sigma \in \mathfrak{S}_n$ if $i < j$ but $\sigma(i) > \sigma(j)$ $\operatorname{sgn}(a_1 a_2) = -1$ $\operatorname{sgn}(a_1 ... a_n) = (-1)^{n-1}$

$\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)$ **Alternating Group**: $A_n := \{\sigma \in \mathfrak{S}_n : \operatorname{sgn}(\sigma) = 1\}$ <u>**Graph Meaning of Inversion**</u>: Inversion is # 画出的图中, 线段交叉的次数

Determinant: For matrix $A_{n \times n}$, with $A_{ij} = a_{ij}$. $\det(A) := \sum_{\sigma \in \mathfrak{S}_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)}$ (**Leibniz Formula**) $\det(I_0) := 1$

or: $\det(A) := \sum_{\sigma^{-1} \in \mathfrak{S}_n} \operatorname{sgn}(\sigma^{-1}) a_{\sigma^{-1}(1)1} \cdots a_{\sigma^{-1}(n)n}$

Geometric Meaning of Determinant: Let area(U) denote the area|volume of U. Let A denote a matrix.

1. $\det(A)$ 对 U 操作后的面积 | 体积 = $|\det(A)| \times \text{area}(U)$ 2. $\operatorname{sgn}(\det A)$ 决定了方向是否改变 (+1 不变,-1 变). (i.e. 顺逆时针变化, 左右 | 上下变化, 手性变化)

Bilinear|Multilinear form: U, V, V_i, W be F-vector space. A mapping $H : U \times V \to W$ or $H : V_1 \times \cdots \times V_n \to W$ is *bilinear* | *multilinear* if:

1. $H(\lambda u, v) = \lambda H(u, v)$
2. $H(u + v, w) = H(u, w) + H(v, w)$
3. $H(u, \lambda v) = \lambda H(u, v)$
4. $H(u, v + w) = H(u, v) + H(u, w)$

1. $H(u_1, ..., \lambda v_i, ..., u_n) = \lambda H(u_1, ..., v_i, ..., u_n) \quad \forall i$
2. $H(u_1, ..., v_i + v_j, ..., u_n) = H(u_1, ..., v_i, ..., u_n) + H(u_1, ..., v_j, ..., u_n) \quad \forall i$

(左边 bilinear, 右边 multilinear)

H is **Symmetric** if (bilinear): $^1U = V$, $\quad ^2H(u,v) = H(v,u) \quad \forall u,v \in U$

if (multilinear): ^1V_i same, $\quad ^2H(v_1,...,v_n) = H(v_{\sigma(1)},...,v_{\sigma(n)}) \quad \forall \sigma \in \mathfrak{S}_n$

H is **Alternating|Antisymmetric** if (bilinear): $^1U = V$, $\quad ^2H(u,u) = 0 \quad \forall u \in U$

if (multilinear): ^1V_i same, $\quad ^2H(v_1,...,v_n) = 0 \quad \forall v_i = v_j$ (i.e. 只要存在两个及以上相同的, H 结果为 0)

Lemma I: If H is *alternating*, then $\quad H(u,v) = -H(v,u) \qquad H(v_1,...,v_i,...,v_j,...,v_n) = -H(v_1,...,v_j,...,v_i,...,v_n)$ ($\Leftarrow$ 不一定成立)

Lemma II: If H is *alternating*, then $\quad H(v_1,...,v_n) = \text{sgn}(\sigma)H(v_{\sigma(1)},...,v_{\sigma(n)})$ (σ is a permutation)

Example: If $H(\vec{u},\vec{v}) = \vec{u}^T A\vec{v} \Rightarrow$ multilinear form. $\quad$ If $A^T = A$, symmetric. $\quad$ If $A^T = -A$, antisymmetric.

Property of Determinant: Let A, B be $n \times n$ matrices. $\quad F$ be field. $\quad R$ be *commutative ring*.

1. **Unique on Field**: $\det : F^n \times \cdots \times F^n \to F$ *or* $\det : Mat(n;F) \to F$ is the ^{1}*unique* ^{2}*alternating* ^{3}*multilinear form* s.t. $\det(I_n) = 1_F$
2. **Invertible on Field**: For $Mat(n;F)$, A is invertible $\Leftrightarrow \det(A) \neq 0 \qquad \det(A^{-1}) = \det(A)^{-1}$ 交换环, 结论成立如果 $\det(A)$ 在 R 中有逆
3. **Similar on Field**: For F field. $\quad A \sim B \Rightarrow \det(A) = det(P^{-1}BP) = \det(B) \qquad$ Thus, we can define: $det(f)$ for $f : V \to V$
4. **Operations**: If R is *commutative ring*, then $\det(AB) = \det(A)\det(B) \qquad \det(A^T) = \det(A) \qquad \det(A^{-1}) = \det(A)^{-1} \qquad \det(\overline{A}) = \overline{\det(A)}$
5. **Block Triangular**: If A is block triangular, then $\det(A) = \prod_{i=1}^n \det(A_i)$ 即矩阵分块后如果是对角阵, 行列式等于各个块的行列式乘积

Common Theorems in Determinant: Let A be $n \times n$ matrix. $\quad F$ be field. $\quad R$ be *commutative ring*.

1. **Cofactor**: In R, $\; C_{ij} := (-1)^{i+j}\det(A\langle i,j\rangle)$ where $A\langle i,j\rangle$ 是 A 去掉第 i 行第 j 列的矩阵. **Laplace's Expansion**: In R, $\; \det(A) = \sum_{j=1}^n a_{ij}C_{ij} = \sum_{i=1}^n a_{ij}C_{ij}$
2. **Adjugate Matrix**: In R $\;$ adj(A) matrix, $\text{adj}(A)_{ij} := C_{ji}$ **Cramer's Rule**: In R $\; A \cdot \text{adj}(A) = (\det A)I_n$ $\quad$ In F, $x_i = \dfrac{\det(A_i)}{\det(A)}$ A_i 代表 A 的第 i 列替换为 b
3. $^\ominus$ **Theorem|Need proof**: In R, $\; \text{adj}(A^T) = \text{adj}(A)^T$ $\quad$ Hint: $\text{adj}(A^T)_{ij} = C_{ij}^{A^T} = (-1)^{i+j}\det(A^T\langle i,j\rangle) = (-1)^{i+j}\det(A\langle j,i\rangle^T) = (-1)^{i+j}\det(A\langle j,i\rangle) = C_{ji}^A = \text{adj}(A)_{ji} = \text{adj}(A)_{ij}^T$
4. **Invertibility of Matrix**: In R, matrix A is invertible $\Leftrightarrow \det(A) \in R^\times$ $\quad$ e.g. $\mathbb{Z}^\times = \{\pm 1\}$; $\mathbb{C}^\times, \mathbb{R}^\times, \mathbb{Q}^\times = \mathbb{C}^*, \mathbb{R}^*, \mathbb{Q}^*$; $\mathbb{F}_p^\times = \mathbb{F}_p \setminus \{0\}$; $\mathbb{Z}[i] = \{\pm 1, \pm i\}$
5. **Jacobi's Formula**, Let matrix A s.t. $a_{ij}(t)$ are functions of t. $\quad$ Then, $\dfrac{d}{dt}\det(A) = \text{tr}\left(\text{adj}A \cdot \dfrac{dA}{dt}\right)$

6.2 Eigenvalues | Eigenvectors | Diagonalization

Eigenspace $E(\lambda, f)$: Let $f : V \to V$ linear map (End), $\lambda \in F$. $\quad E(\lambda,f) := \{\vec{v} \in V : f(\vec{v}) = \lambda\vec{v}\}$. $\quad \lambda$ is *eigenvalue* if $E(\lambda,f) \neq \{0\}$

ps: $\ker(f - \lambda id_V)$ is the eigenspace of $E(\lambda,f)$ and it has a basis of eigenvectors $\{\vec{v}_1,...,\vec{v}_r\}$.

Existence of Eigenvalues: For all $f : V \to V$ linear map. ^1V is finite-dimensional. ^1F is *algebraically closed*. $\Rightarrow \; \exists$ eigenvalues.

Characteristic Polynomial $\chi_A(x)$: Let R be *commutative ring*. $A \in Mat(n;R)$. $\quad \chi_A(x) := \det(xI_n - A) \in R[x]$

Relation with Eigenvalues: If F is *field*, $\; A \in Mat(n;F)$. $\quad \lambda$ is eigenvalue of $A \Leftrightarrow \chi_A(\lambda) = 0$

Similar Matrix: If R is *commutative ring*, $\; A, B \in Mat(n;R)$ similar. $\quad \Rightarrow \quad \chi_A(x) = \chi_B(x) \qquad$ Thus: $\chi_f(x) := \chi_{{}_\mathcal{A}[f]_\mathcal{A}}(x)$

Moreover, if ${}_\mathcal{A}[f]_\mathcal{A} = A$ and A is similar to B. $\quad$ Then, $\exists$ basis $\mathcal{B}$ s.t. ${}_\mathcal{B}[f]_\mathcal{B} = B$

Remark: If $W \subseteq V$ is subspace. $f : V \to V$ is End. $f(W) \subseteq W$. $\quad$ Let $\mathcal{A} = (\vec{w}_1,...,\vec{w}_m)$ basis W. $\quad \mathcal{B} = (\vec{w}_1,...,\vec{w}_m, v_{m+1},...,\vec{v}_n)$ basis V. $\quad \mathcal{C} = (\vec{v}_{m+1} + W,...,\vec{v}_n + W)$ basis V/W.

Suppose $f(\vec{v}_k) = \sum_{i=1}^m c_{ik}\vec{w}_i + \sum_{j=m+1}^n b_{jk}\vec{v}_j$ $\quad$ Let $g : W \to W$ by $w \mapsto f(w)$ $\quad h : V/W \to V/W$ by $v + W \mapsto f(v) + W$ $\quad e : V/W \to W$ by $v_k + W \mapsto \sum_{i=1}^m c_{ik}\vec{w}_i$

Then: $\quad \chi_f(x) = \chi_g(x)\chi_h(x)$ $\quad$ and $\quad {}_\mathcal{B}[f]_\mathcal{B} = \begin{pmatrix} {}_\mathcal{A}[g]_\mathcal{A} & {}_\mathcal{A}[e]_\mathcal{C} \\ 0 & {}_\mathcal{C}[h]_\mathcal{C} \end{pmatrix} = \begin{pmatrix} a_{ij} & c_{ik} \\ 0 & b_{jk} \end{pmatrix}$ $\qquad$ ps: $f(\vec{w}_j) = \sum_{i=1}^m a_{ij}\vec{w}_i$

Triangularisability|A: Let $A \in Mat(n;F)$, it is *triangularisable* if $\exists P$ invertible s.t. $P^{-1}AP = U$ is upper triangular.

Triangularisability|f: Let $f : V \to V$ be End. V is finite-dimensional. the following are equivalent:

1. $\exists \mathcal{B} = (\vec{v}_1,...,\vec{v}_n)$ basis s.t. $f(\vec{v}_i) = \sum_{j=1}^i a_{ji}\vec{v}_j$ (i.e. ${}_\mathcal{B}[f]_\mathcal{B}$ is upper triangular.) $\qquad$ we say f is *triangularisable*
2. The characteristic polynomial $\chi_f(x)$ can be factored into <u>linear factors</u> over F. $\qquad$ (ps: If F is algebraically closed, then f is triangularisable)

Corollary I: Let $A, B \in Mat(n;F)$. $\quad$ *A is triangularisable* $\Leftrightarrow$ A is similar (Conjugate) to a *upper triangular* matrix B.

Corollary II: Let $f : V \to V$ be End. V is finite-dim. $\quad f$ *is triangularisable* $\Leftrightarrow \exists$ subspaces $V_0 = \{0\} \subset V_1 \subset \cdots \subset V_n = V$ s.t. $f(V_i) \subseteq V_i$.

Corollary III|nilpotent: For $A \in Mat(n;F)$. A is *nilpotent* (i.e. $A^k = 0$ for some k) $\Leftrightarrow \chi_A(x) = x^n$

Application: 将矩阵 A 进行三角化, 可以通过:1. 求特征值, 特征向量; 2. 选择一个特征向量为基 (通常选最大的); 3. 拓展为 V 的基; 4. 求 A 在新基下的矩阵 B, 此时 B 按分块矩阵看应有一部分三角化; 5. 对 B 未三角化的部分重复.

Diagonalisable|A: Let $A \in Mat(n;F)$. A is *diagonalisable* iff $\exists$ matrix P s.t. $P^{-1}AP = diag$

Diagonalisable|f: Let $f : V \to V$ be End, V is *diagonalisable* iff $\exists$ basis of V consisting of eigenvectors of f.

Diagonalisable|Finite: For V is finite-dimensional. $\quad V$ *is diagonalisable* $\Leftrightarrow \exists$ basis $\mathcal{B}$ s.t. ${}_\mathcal{B}[f]_\mathcal{B} = diag(\lambda_1,...,\lambda_n)$, $\quad$ where: $f(\vec{v}_i) = \lambda_i\vec{v}_i$

Property: In finite case, $\exists P$ consisting of eigenvectors s.t. $P^{-1}AP = diag(\lambda_1,...,\lambda_n)$

Corollary: If all roots of $\chi_f(x)$ are distinct, then f is *diagonalisable*.

LI of Eigenvectors: Let $f : V \to V$ be End. V is finite-dimensional. $\quad$ If $\lambda_1,...,\lambda_n$ are distinct $\Rightarrow$ Corresponding eigenvectors are linearly independent.

Cayley-Hamilton Theorem: Let R be *commutative ring*. $A \in Mat(n;R)$. $\quad$ Then: for $\chi_A(x)$ $\quad \chi_A(A) = 0$

对于 Jordan 块, 考虑 $J - \lambda I \to$ nilpotent. 可以得到一些多项式的性质 =0

$^\ominus$ 此框为一些有关前面 Ring 的性质: by Euclidean algorithm

Bézout's identity: if $gcd(f,g) = 1$, then $\exists\, a, b \in R[x]$ s.t. $af + bg = 1$.

About Ideal: ${}_{R[X]}\langle f,g\rangle = \gcd(f,g)R[X] \qquad {}_{R[X]}\langle f\rangle +_{R[X]} \langle g\rangle =_{R[X]} \langle\gcd(f,g)\rangle \qquad {}_{R[X]}\langle f\rangle \cap_{R[X]} \langle g\rangle =_{R[X]} \langle\text{lcm}(f,g)\rangle$

About Quotient: 通过欧几里得算法, 可以寻找到商空间中的元素的代表. $\quad$ e.g. $\mathbb{F}_2[X]/\langle X^2+1\rangle = \{I, 1+I, X+I, X+1+I\}$ (即所有小于 Ideal deg 元素 | 欧几里得算法得到的余数)

Find Units in Quotient: $g \in R/I$ is a unit iff $\gcd(f,g) = 1$

(Hint: ($\Rightarrow$) $fg + I = 1 + I \to fg - 1 \in I \to fg - 1 = h \cdot 1|h \cdot i \to$Euclidean algorithm; ($\Leftarrow$) Bézout's identity + Euclidean algorithm)

7 Inner Product Spaces | Orthogonal Complement / Proj | Adjoints and Self-Adjoint

7.1 Inner Product Spaces | Orthogonal Complement / Proj

Real|Complex Inner Product Space: Let V vector space over $F = \mathbb{R}|\mathbb{C}$. It is an *inner product space* if $\exists$ mapping $V \times V \to \mathbb{R}|\mathbb{C}$ s.t.

1. **Linear in 1st Variable**: $(\lambda\vec{x} + \mu\vec{y}, \vec{z}) = \lambda(\vec{x}, \vec{z}) + \mu(\vec{y}, \vec{z})$ $\forall \lambda, \mu \in F, \vec{x}, \vec{y}, \vec{z} \in V$
2. **(Conjugate) Symmetric**: $(\vec{x}, \vec{y}) = \overline{(\vec{y}, \vec{x})}$ for real, $(\vec{x}, \vec{y}) = (\vec{y}, \vec{x})$ | Real: *linear* in 2nd variable. Complex: *conjugate linear* in 2nd variable.
3. **Positive Definite**: $(\vec{x}, \vec{x}) \geq 0$ and $(\vec{x}, \vec{x}) = 0$ iff $\vec{x} = \vec{0}$ | Complex: $(\vec{z}, \lambda\vec{x} + \mu\vec{y}) = \overline{\lambda}(\vec{z}, \vec{x}) + \overline{\mu}(\vec{z}, \vec{y})$

   ps: **Standard Inner Product in $\mathbb{R}^n|\mathbb{C}^n$**: $(\vec{x}, \vec{y}) = \sum_{i=1}^n x_i y_i$ $(\vec{x}, \vec{y}) = \sum_{i=1}^n x_i \overline{y_i}$ (i.e. dot product $\vec{x} \cdot \vec{y} = \vec{x}^T \vec{y}$)

Special Inner Product: If $(\vec{x}, \vec{y}) = \sum_{i,j} a_{ij} x_i \overline{y_j} = \vec{x}^T A \overline{\vec{y}}$ where $A_{ij} = a_{ij}$

$\Rightarrow$ It is an inner product if: $^1\overline{A^T} = A$ $^2\vec{x}^T A \overline{\vec{x}} \geq 0, \forall \vec{x} \in \mathbb{R}^n|\mathbb{C}^n$ $^3(\vec{x}, \vec{x}) = 0$ iff $\vec{x} = \vec{0}$

Norms: For $\vec{x}, \vec{y} \in V$ in inner product space. $\|\vec{x}\| := \sqrt{(\vec{x}, \vec{x})} \geq 0$ **Orthogonal**: $\vec{x} \perp \vec{y}$ iff $(\vec{x}, \vec{y}) = 0$

1. **Pythagoras' Theorem**: If $\vec{x} \perp \vec{y}$, then $\|\vec{x} + \vec{y}\|^2 = \|\vec{x}\|^2 + \|\vec{y}\|^2$. **Metric Space**: $d(\vec{x}, \vec{y}) := \|\vec{x} - \vec{y}\|$.
2. **Cauchy-Schwarz Inequality**: $|(\vec{x}, \vec{y})| \leq \|\vec{x}\|\|\vec{y}\|$ **Triangle Inequality**: $\|\vec{x} + \vec{y}\| \leq \|\vec{x}\| + \|\vec{y}\|$ **Scalar**: $\|\lambda\vec{x}\| = |\lambda|\|\vec{x}\|$

   ps: *Cauchy-Schwarz Inequality*, "=" iff $\vec{x}, \vec{y}$ are linearly dependent. *Triangle Inequality*, "=" iff $\vec{x}, \vec{y}$ are linearly dependent, and they have same direction. (i.e. $\vec{x} = \lambda\vec{y}, \lambda \geq 0$)

Orthonormal Family: $\{\vec{v}_1, ..., \vec{v}_n\}$ is *orthonormal* if $^1\|\vec{v}_i\| = 1$ and $^2\vec{v}_i \perp \vec{v}_j$ for $i \neq j$. (i.e. $(\vec{v}_i, \vec{v}_j) = \delta_{ij}$) If it is basis, then it is **orthonormal basis**.

1. **Observations**: **I.** For $\{\vec{v}_1, ..., \vec{v}_n\}$ orthonormal basis. $\vec{v} = \sum_{i=1}^n (\vec{v}, \vec{v}_i)\vec{v}_i$. **II.** For orthonormal Family, 可直接用勾股定理, and 很明显 LI
2. **Theorem**: Every finite-dimensional inner product space has an orthonormal basis.
3. **Gram-Schmidt Process**: Let $\{\vec{v}_1, ..., \vec{v}_n\}$ be basis of V. By using following way to get orthonormal basis:

   a. $\vec{e}_1 = \frac{\vec{v}_1}{\|\vec{v}_1\|}$ $\mathrm{Proj}_{\vec{e}_k}\vec{v}_j = (\vec{v}_j, \vec{e}_k)\vec{e}_k$

   b. $\vec{u}_2 = \vec{v}_2 - \mathrm{Proj}_{\vec{e}_1}\vec{v}_2$ $\vec{e}_2 = \frac{\vec{u}_2}{\|\vec{u}_2\|}$

   c. $\vec{u}_3 = \vec{v}_3 - \mathrm{Proj}_{\vec{e}_1}\vec{v}_3 - \mathrm{Proj}_{\vec{e}_2}\vec{v}_3$ $\vec{e}_3 = \frac{\vec{u}_3}{\|\vec{u}_3\|}$

   d. $\vec{u}_n = \vec{v}_n - \sum_{i=1}^{n-1} \mathrm{Proj}_{\vec{e}_i}\vec{v}_n$ $\vec{e}_n = \frac{\vec{u}_n}{\|\vec{u}_n\|}$

   All-In-One:

   $$\vec{e}_{k+1} = \frac{\vec{v}_{k+1} - \sum_{i=1}^k \mathrm{Proj}_{\vec{e}_i}\vec{v}_{k+1}}{\left\|\vec{v}_{k+1} - \sum_{i=1}^k \mathrm{Proj}_{\vec{e}_i}\vec{v}_{k+1}\right\|}$$

Orthogonal Set: For subset T of vector space V. **Set Orthogonal to** A is $A^\perp := \{\vec{v} \in V : \vec{v} \perp \vec{a}, \forall \vec{a} \in A\}$

1. **I.** $A^\perp$ is always subspace of V. **II.** $A^\perp = \langle A \rangle^\perp$
2. **Orthogonal Decomposition Theorem**: Let V be inner product space. W be subspace of V. Then: $V = W \oplus W^\perp$

Orthogonal Projection: Let V be inner product space. U be subspace of V, with orthonormal basis $\{\vec{e}_1, ..., \vec{e}_m\}$.

1. Then: *orthogonal projection* $\pi_U : V \to V$ by $\vec{v} \mapsto \sum_{i=1}^m (\vec{v}, \vec{e}_i)\vec{e}_i$
2. **I.** $\pi_U^2 = \pi_U$ **II.** $\ker(\pi_U) = U^\perp$ and $\mathrm{Im}(\pi_U) = U$ **III.** $\pi_U|_U = id_U$
3. **Orthogonal Decomposition**: For all $\vec{v} \in V$, $\vec{v} = (\vec{v} - \pi_U(\vec{v})) + \pi_U(\vec{v})$ where $(\vec{v} - \pi_U(\vec{v})) \perp \pi_U(\vec{v})$.
4. **Closest Approximation**: Since $\|\vec{v} - \vec{u}\|^2 = \|\vec{v} - \pi_U(\vec{v})\|^2 + \|\pi_U(\vec{v}) - \vec{u}\|^2$ $\Rightarrow$ $\vec{u} = \pi_U(\vec{v})$ is the closest vector in U to $\vec{v}$.

7.2 Basic Properties of Adjoint and Self-Adjoint

Orthogonal: matrix A is *orthogonal* if $A^T A = I_n$. (i.e. $A^{-1} = A^T$) **Unitary**: matrix A is *unitary* if $\overline{A}^T A$ or $A^T \overline{A} = I_n$. (i.e. $A^{-1} = \overline{A}^T$)

Hermitian: matrix A is *Hermitian* if $\overline{A}^T = A$. (i.e. A is *self-adjoint* in $\mathbb{C}$) **Symmetric**: matrix A is *symmetric* if $A^T = A$. (i.e. A is *self-adjoint in* $\mathbb{R}$)

Useful Tool: If $T : V \to W$ is linear map. For matrix ${}_{\mathcal{B}}[T]_{\mathcal{A}}$, The entry $[{}_{\mathcal{B}}[T]_{\mathcal{A}}]_{ij} = (T\vec{e}_j, \vec{f}_i)$

IPS isomorphism of V: A linear map $T : V \to W$ is *IPS isomorphism* of V (and W) if: ^{1} T is isomorphism ^{2} $(T\vec{v}_1, T\vec{v}_2) = (\vec{v}_1, \vec{v}_2)$ $\forall \vec{v}_1, \vec{v}_2 \in V$

Properties of IPS isomorphism: Let V, W be *inner product spaces*, $\mathcal{A} = \{\vec{e}_1, ..., \vec{e}_m\}, \mathcal{B} = \{\vec{f}_1, ..., \vec{f}_n\}$ are orthonormal basis of V, W.

1. Linear map $T : V \to W$ is *IPS isomorphism* of V (i.e. T is iso & $(T\vec{v}_1, T\vec{v}_2) = (\vec{v}_1, \vec{v}_2)$) $\Leftrightarrow$ Linear map $T : V \to W$ maps some orthonormal basis to another.
2. **IPS isomorphism**: $T : V \to V$ is *IPS isomorphism* $\Leftrightarrow$ $TT^* = T^*T = \mathrm{id}_V$ $\Leftrightarrow$ ${}_{\mathcal{A}}[T]_{\mathcal{A}}$ is *unitary*$_{\mathbb{C}}$ or *orthogonal*$_{\mathbb{R}}$ matrix.

Adjoint: V is inner product space. $T, S : V \to V$ are linear maps. T, S are called *adjoint* to one another if $(T\vec{v}, \vec{w}) = (\vec{v}, S\vec{w})$ $\forall \vec{v}, \vec{w} \in V$.

Self-adjoint: If $T = T^*$, then T is *self-adjoint*. (i.e. $(T\vec{v}, \vec{w}) = (\vec{v}, T\vec{w})$)

Properties of Adjoint: Let V be *inner product spaces*, $\mathcal{A} = \{\vec{e}_1, ..., \vec{e}_n\}$ are orthonormal basis of V. $T : V \to V$ is linear map.

1. Then, $\exists!$ linear map $T^* : V \to V$ s.t. $(T\vec{v}, \vec{w}) = (\vec{v}, T^*\vec{w})$ $\forall \vec{v}, \vec{w} \in V$.
2. **I.** ${}_{\mathcal{A}}[T^*]_{\mathcal{A}} = \overline{({}_{\mathcal{A}}[T]_{\mathcal{A}})}^T$ **II.** $(T^*)^* = T$
3. **Self-Adjoint**: $\exists$ orthonormal basis of eigenvectors|Finite V (Spectral) $\Leftrightarrow$ If $T = T^*$ (self-adjoint) $\Leftrightarrow$ ${}_{\mathcal{A}}[T]_{\mathcal{A}} = \overline{({}_{\mathcal{A}}[T]_{\mathcal{A}})}^T$ Hermitian/Symmetric
4. ⋆ **Similar**: If matrix $A = {}_{\mathcal{A}}[f]_{\mathcal{A}}$ and $B = {}_{\mathcal{B}}[f]_{\mathcal{B}}$ $\Leftrightarrow$ $B = P^{-1}AP$ and P is *orthogonal*$_{\mathbb{R}}$ or *unitary*$_{\mathbb{C}}$ matrix.

Normal: Linear map $T : V \to V$ is *normal* if $TT^* = T^*T$.

Properties of Normal: Let V be *inner product spaces*, $\mathcal{A} = \{\vec{e}_1, ..., \vec{e}_n\}$ are orthonormal basis of V. $T : V \to V$ is linear map.

1. T is *normal* $\Leftrightarrow$ $\overline{{}_{\mathcal{A}}[T]_{\mathcal{A}}}^T \cdot {}_{\mathcal{A}}[T]_{\mathcal{A}} = {}_{\mathcal{A}}[T]_{\mathcal{A}} \cdot \overline{{}_{\mathcal{A}}[T]_{\mathcal{A}}}^T$
2. **I.** T is *self-adjoint* $\Rightarrow$ T is *normal* **II.** T is *IPS isomorphism* $\Rightarrow$ T is *normal*.

7.3 Advanced Properties of Adjoint and Self-Adjoint

Properties of Self-adjoint: Let $T : V \to V$ be a *self-adjoint* linear map on *inner product space* V. Then: 注意:inner product space 限制了 $F = \mathbb{R}|\mathbb{C}$

1. **Spectral Theorem**: If V is *finite-dimensional*, then T has *orthonormal basis* of *eigenvectors*. 存在特征值/向量, 且正交为基.
2. **Real**: Every eigenvalues of T are real. **Orthogonal**$|\lambda$: Eigenvectors of *distinct eigenvalues* are orthogonal.
3. **Orthogonal**$|T$: If $\vec{v} \perp \vec{w}$, and $\vec{v}$ is *eigenvector* of T. Then, $T\vec{w} \perp \vec{v}$. ⊖ also: $\vec{w} \perp T\vec{v}$

Spectral for $\mathbb{R}|\mathbb{C}$ **Matrix**: If $A \in \text{Mat}(n, \mathbb{R}|\mathbb{C})$ *symmetric*|*hermitian*. Then A has n *real* eigenvalues $\lambda_1, ..., \lambda_n$ (can be repeated).

Moreover, $\exists$ orthogonal|Unitary matrix P s.t. $P^TAP|\overline{P}^TAP = P^{-1}AP = diag(\lambda_1, ..., \lambda_n)$.

Real Quadratic forms: $Q(x_1, ..., x_n) := \sum_{i=1}^n a_{ii}x_i^2 + 2\sum_{1\le i<j\le n} a_{ij}x_ix_j = \vec{x}^TA\vec{x}$ where A is *real symmetric* matrix, variables $\vec{x} \in \mathbb{R}^n$

Can be written as $Q(\vec{x}) = (A\vec{x}, \vec{x})$ where $(\vec{x}, \vec{y}) = \vec{x}^T\vec{y}$ is *standard inner product*. **Corollary**: If A is real symmetric matrix. $\Rightarrow A = P^T\Lambda P \Rightarrow Q(\vec{x}) = \sum_{i=1}^n \lambda_i y_i^2$ where $\vec{y} = P\vec{x}$

Theorem: $Q(\vec{x}) = (A\vec{x}, \vec{x}) \ge 0$ (positive definite) $\Leftrightarrow$ all eigenvalues of A are positive. ps: A is real symmetric matrix.

Level Set: The set $\{\vec{x} \in \mathbb{R}^n : Q(\vec{x}) = (A\vec{x}, \vec{x}) = 1\} \Rightarrow$ is the image of ellipsoid, 轴为 $\sqrt{\frac{1}{\lambda_1}}, ..., \sqrt{\frac{1}{\lambda_n}}$ ps: A is real symmetric matrix,λ_i 为 A 的特征向量.

意思是: $A = P^T\Lambda P \Rightarrow Q(\vec{x}) = \sum_{i=1}^n \lambda_i y_i^2 \Rightarrow Q(\vec{x}) = 1$ 是一个 "椭圆" ellipsoid, "轴"(e.g. 半长轴, 半短轴) 为 $\sqrt{\frac{1}{\lambda_1}}, ..., \sqrt{\frac{1}{\lambda_n}}$.

8 Jordan Normal Form 默认 F:algebraically closed

2×2 **Matrices**: If $A \in \text{Mat}(2; F)$, F field. Then: A is diagonalisable $\Leftrightarrow A$ has distinct eigenvalues or $A = \lambda I$.

Matrix Exponential: $e^A = \sum_{n=0}^\infty \frac{1}{n!}A^n$ **Properties**: **I.**If $AB = BA \Rightarrow e^{A+B} = e^Ae^B$ **II.** $e^{P^{-1}AP} = P^{-1}e^AP$ **III.** $e^{\text{diag}(\lambda_1,...,\lambda_n)} = \text{diag}(e^{\lambda_1}, ..., e^{\lambda_n})$

Nilpotent Jordan Block: $J(r)^k = 0$

$$J(r) := \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}_{r\times r}$$

Superdiagonal: $x_{i,i+1}$ 对角线上面的元素

Useful Properties:

$$\begin{pmatrix} 0 & x_1 & 0 & \cdots & 0 \\ 0 & 0 & x_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & x_{r-1} \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}^2_{r\times r} = \begin{pmatrix} 0 & 0 & x_1x_2 & 0 & \cdots & 0 \\ 0 & 0 & 0 & x_2x_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 \end{pmatrix}_{r\times r}$$

Jordan Block of size r, eigenvalue λ:

$$J(r,\lambda) := \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda \end{pmatrix}_{r\times r}$$

$J(r,\lambda) = \lambda I_r + J(r) = D + N$ $DN = ND$ ps: 对于 J 也成立.

Generalised Eigenspace: For $\phi : V \to V$ linear map with eigenvalue λ. $E^{\text{gen}}(\lambda_i, \phi) := \{\vec{v} \in V : (\phi - \lambda_i\text{id}_V)^{a_i}(\vec{v}) = 0\}$

Arithmetic Multiplicity: $\dim E^{\text{gen}}(\lambda_i, \phi) \ge$ **Geometric Multiplicity**: $\dim E(\lambda_i, \phi)$ ps: If $\chi_\phi(x) = \prod_{i=1}^s (x - \lambda_i)^{a_i}$, then $\dim E^{\text{gen}}(\lambda_i, \phi) = a_i$

⊖ 对于 linear map/matrix, $\{0\} \subseteq \ker(f) \subseteq \ker(f^2) \subseteq \cdots \subseteq \ker(f^n)$. If $\ker(f^k) = \ker(f^{k+1})$, then $\ker(f^k) = \ker(f^{k+1}) = \cdots = \ker(f^n)$. 由此 E^{gen} 的 a_i 是一个上界 (当等于 characteristic 对应的), 但不一定是最小的.

Stable: Let $f : X \to X$ be mapping from a set X to itself. If $Y \subseteq X$ and $f(Y) \subseteq Y$, then Y is *stable* under f.

The Direct Sum Decomposition: For $\phi : V \to V$ linear map. The characteristic polynomial of ϕ is $\chi_\phi(x) = \prod_{i=1}^s (x - \lambda_i)^{a_i}$.

Then: **I.** $V = \bigoplus_{i=1}^s E^{\text{gen}}(\lambda_i, \phi)$ **II.** $\phi(E^{\text{gen}}(\lambda_i, \phi)) \subseteq E^{\text{gen}}(\lambda_i, \phi)$ (stable)

III. Let $\mathcal{B} = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_s$ where $\mathcal{B}_i$ is basis of $E^{\text{gen}}(\lambda_i, \phi) \Rightarrow {}_{\mathcal{B}}[\phi]_{\mathcal{B}} = \text{diag}({}_{\mathcal{B}_1}[\phi]_{\mathcal{B}_1}, ..., {}_{\mathcal{B}_s}[\phi]_{\mathcal{B}_s})$

⊖ **Properties of Nilpotent**: if $\phi : V \to V$ is linear map and $\phi^m\vec{v} = 0, \phi^{m-1}\vec{v} \ne 0$. Then: **I.** $\vec{v}, \phi\vec{v}, ..., \phi^{m-1}\vec{v}$ is linearly independent. **II.** ${}_{\mathcal{B}}[\phi]_{\mathcal{B}}$ is *nilpotent Jordan block* where $\mathcal{B} = \{\phi^{m-1}\vec{v}, \phi^{m-2}\vec{v}, ..., \vec{v}\}$

Jordan Normal Form: Let F be an algebraically closed field. Let V be finite dimensional vector space. Let $\phi : V \to V$ s.t. $\chi_\phi = \prod_{i=1}^s (x - \lambda_i)^{a_i}$.

I.$\exists$ basis $\mathcal{B}$ of V s.t. ${}_{\mathcal{B}}[\phi]_{\mathcal{B}} = \text{diag}(J(r_{11}, \lambda_1), ..., J(r_{1m_1}, \lambda_1), J(r_{21}, \lambda_2), ..., J(r_{s1}, \lambda_s), ..., J(r_{sm_s}, \lambda_s))$

II. $\exists! \phi_D : V \to V$ and $\phi_N : V \to V$ s.t. $\phi = \phi_D + \phi_N$ where ϕ_D is diagonalisable and ϕ_N is nilpotent. Furthermore, $\phi_D\phi_N = \phi_N\phi_D$.

III. $\exists$ basis $\mathcal{B}$ of V s.t. ${}_{\mathcal{B}}[\phi]_{\mathcal{B}} = D + N$ where D diagonalisable and N nilpotent, and $DN = ND$.

ps:Jordan form 的形状为一, 但里面的顺序不一定要一样. (J is unique up to reordering of the Jordan blocks.)

⊖ **Jordan Decomposition**: Let $A \in \text{Mat}(n; F)$, F algebraically closed field. Then: $\exists! D, N$ s.t. $A = D + N$, D diagonalisable, N nilpotent, $DN = ND$.

由 Direct Sum Decomposition $\to P^{-1}AP = \text{diag}(B_1, ..., B_S)$ where $B_i = {}_{\mathcal{B}_i}[\phi]_{\mathcal{B}_i} \to$ 根据 nilpotent 的性质, B_i 是 nilpotent + diag $\to B_i = D_i + N_i \to D = P\text{diag}(D_1, ..., D_S)P^{-1}$ $N = P\text{diag}(N_1, ..., N_S)P^{-1}$

Description of Jordan Normal Form: Let $A \in \text{Mat}(n; F)$, F algebraically closed field. The $\chi_A(x) = \prod_{i=1}^s (x - \lambda_i)^{a_i}$.

对于一个 λ_i, 考虑 $n_1, ..., n_{a_i}$:

$n_1 = \dim\ker(A - \lambda_i I)$

$n_2 = \dim\ker(A - \lambda_i I)^2 - n_1$

$\vdots$

$n_{a_i} = \dim\ker(A - \lambda_i I)^{a_i} - n_{a_i - 1}$

1. n_1 代表 size 不小于 1 的 Jordan block 个数
2. n_2 代表 size 不小于 2 的 Jordan block 个数
3. $\cdots$
4. n_{a_i} 代表 size 不小于 a_i 的 Jordan block 个数

1. exact $n_1 - n_2$ Jordan blocks of size 1
2. exact $n_2 - n_3$ Jordan blocks of size 2
3. $\cdots$
4. exact $n_{a_i - 1} - n_{a_i}$ Jordan blocks of size $a_i - 1$

Relate to Exponential: If $A = D + N$, D diagonalisable, N nilpotent, $DN = ND$.

Then: $e^A = e^De^N = P^{-1}\text{diag}(e^{\lambda_1}, ..., e^{\lambda_n})Pe^N$ and $e^{At} = P^{-1}\text{diag}(e^{t\lambda_1}, ..., e^{t\lambda_n})Pe^{tN}$

For Triangularisable/More Generally Case: For $f : V \to V$ linear map. V is finite dimensional vector space.

If $\chi_f(x)$ can be factored into linear factors over F. Then: f has a *Jordan normal form*.

Corollary: If f is triangularisable|Matrix A is triangularisable. Then: $f|M$ has a *Jordan normal form*.

9 Appendix

Vieta's formulas: For polynomial $P(x) = a_nx^n + \cdots + a_1x + a_0$. Let $x_1, ..., x_n$ be roots of $P(x)$.

$x_1 + \cdots + x_n = -\frac{a_{n-1}}{a_n}$ $x_1 \cdots x_n = (-1)^n\frac{a_0}{a_n}$ $x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n = \frac{a_{n-2}}{a_n}$

Determinant of Vandermonde Matrix: Let $x_1, ..., x_n$ be distinct elements of F. Then

$$\det\begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{pmatrix} = \prod_{1\le i<j\le n}(x_j - x_i)$$

Relate Matrix to Linear Map: For a Matrix A, define $T : F^n \to F^n$ by $T\vec{v} = A\vec{v}$. Then $[T] = A$

Def of Direct Sum: $U_1, ..., U_k$ subspaces of V. $V = U_1 \oplus \cdots \oplus U_k$ if $^1V = U_1 + U_2 + \cdots + U_k$ $^2u_1 + u_2 + \cdots + u_k = 0 \Rightarrow u_1 = u_2 = \cdots = u_k = 0$ $u_i \in U_i$

⋆**Useful Tool**: $A\vec{v} = \vec{0}$ for $\vec{v} \ne \vec{0} \Leftrightarrow \det(A) = 0$