HAlg Note

1 Basic Knowledge

Def of Group $(G,*)$: A set G with a operator $*$ is a group if: **Closure**: $\forall g,h \in G, g*h \in G$; **Associativity**: $\forall g,h,k \in G, (g*h)*k = g*(h*k)$; **Identity**: $\exists e \in G, \forall g \in G, e*g = g*e = g$; **Inverse**: $\forall g \in G, \exists g^{-1} \in G, g*g^{-1} = g^{-1}*g = e$. G,H groups, then $G \times H$ also.

Subgroup: $H \subseteq G$ is a subgroup if: $\forall h_1, h_2 \in H$ **I**: $H \neq \emptyset$; **II**: $h_1 * h_2 \in H$; **III**: $h_1^{-1} \in H$.

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 $\lambda(\mu+\nu) = \lambda\mu + \lambda\nu$ $e.g. Fields: \mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$

F**-Vector Space (V)**: A set V over a field F is a vector space if: V is an abelian group $V = (V, \dot{+})$ and $\forall \vec{v}, \vec{w} \in V$ $\lambda, \mu \in F$ e.g. $Poly: \mathbb{R}[x]_{<n}$ $\exists$ map $F \times V \to V : (\lambda, \vec{v}) \to \lambda\vec{v}$ satisfies: **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**: $1_F\vec{v} = \vec{v}$

Vector Subspaces Criterion: $U \subseteq V$ is a subspace of V if: **I**. $\vec{0} \in U$ **II**. $\forall \vec{u}, \vec{v} \in U, \forall \lambda \in F$: $\vec{u} + \vec{v} \in U$ and $\lambda\vec{u} \in U$ (or: $\lambda\vec{u} + \mu\vec{v} \in U$)

· **property**: If U, W are subspaces of V, then $U \cap W$ and $U + W$ are also subspaces of V. ps: $U + W := \{\vec{u} + \vec{w} : \vec{u} \in U, \vec{w} \in W\}$

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 $V_1 \oplus V_2$)

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 $x \mapsto (0, ..., 0, x, 0, ..., 0)$

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

Generating (subspaces) $\langle T \rangle$: $\langle T \rangle := \{\alpha_1\vec{v_1} + \cdots + \alpha_n\vec{v_n} : \alpha_i \in F, \vec{v_i} \in T, r \in \mathbb{N}\}$ $\langle \emptyset \rangle := \{\vec{0}\}$ If T is subspace $\Rightarrow \langle T \rangle = T$.

1. **Proposition**: $\langle T \rangle$ is the smallest subspace containing T. (i.e. $\langle T \rangle$ is the intersection of all subspaces containing T)
2. **Generating Set**: V is vector space, $T \subseteq V$. T is generating set of V if $\langle T \rangle = V$. **Finitely Generated**: $\exists$ finite set T, $\langle T \rangle = V$
3. **External Direct Sum**: 一个" 代数结构", 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
4. **Connect to Matrix**: Let $E = \{\vec{v_1}, ..., \vec{v_n}\}$, E is GS of V. Let $A = [\vec{v_1}, ..., \vec{v_n}] \Rightarrow \forall \vec{b} \in V, \exists \vec{x} = (x_1, ..., x_n)^T$ s.t. $A\vec{x} = \vec{b}$ (i.e. linear map:$\phi : \vec{x} \mapsto A\vec{x}$ is surjective)

Linearly Independent: $L = \{\vec{v_1}, \vec{v_2}, ..., \vec{v_r}\}$ is linearly independent if: $\forall c_1, ..., c_r \in F, c_1\vec{v_1} + \cdots + c_r\vec{v_r} = \vec{0} \Rightarrow c_1 = \cdots = c_r = 0$.

· **Connect to Matrix**: Let $L = \{\vec{v_1}, ..., \vec{v_n}\}$, L is LI of V. Let $A = [\vec{v_1}, ..., \vec{v_n}] \Rightarrow \forall \vec{x} \in F^n, A\vec{x} = 0\ (or\ \vec{0}) \Rightarrow \vec{x} = 0 (or\ \vec{0})$ (i.e. linear map ϕ:$\vec{x} \mapsto A\vec{x}$ is injective)

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

· **Connect to Matrix**: Let $B = \{\vec{v_1}, ..., \vec{v_n}\}$ is basis of V. Let $A = [\vec{v_1}, ..., \vec{v_n}] \Rightarrow \forall \vec{x} = (x_1, ..., x_n)^T$ s.t. $\phi : \vec{x} \mapsto A\vec{x}$ is 1-1 & onto (Bijection)

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**: $|L| \leq |E|$ (can get: dim unique) **LI→Basis**: If V finite generate $\Rightarrow \forall L$ can extend to a basis. If $L = \emptyset$, prove $\exists B$ $ker f \cap im f = \{0\}$
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 $\dim(U + W) = \dim U + \dim W - \dim(U \cap W)$

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

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

ps: 默认 V, W F**-Vector Spaces.**

3.1 Linear Mapping | Rank-Nullity

Linear Mapping/Homomorphism(Hom): $f : V \to W$ is *linear map* if: $\forall \vec{v}_1, \vec{v}_2 \in V, \forall \lambda \in F$. $f(\vec{v}_1 + \vec{v}_2) = f(\vec{v}_1) + f(\vec{v}_2)$ and $f(\lambda\vec{v}_1) = \lambda f(\vec{v}_1)$

· **Isomorphism**: = LM & Bij. **Endomorphism(End)**: = LM & $V = W$. **Automorphism(Aut)**: = LM & $V = W$ **Monomorphism**: = LM & 1-1. **Epimorphism**: = LM & onto.

· **Kernel**: $\ker f := \{\vec{v} \in V : f(\vec{v}) = \vec{0}\}$(It's subspace) **Image**: $Imf := \{f(\vec{v}) : \vec{v} \in V\}$(It's subspace) **Rank**:= $\dim(Imf)$ **Nullity**:= $\dim(\ker f)$ **Fixed Point** X^f: $X^f := \{x \in X : f(x) = x\}$

Property of Linear Map: Let $f, g \in Hom$: **a.**$f(\vec{0}) = \vec{0}$ **b.** f is 1-1 iff $\ker f = \{\vec{0}\}$ **c.** $f \circ g$ is linear map.

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 $\Rightarrow \dim V \leq \dim W$ **Surjection**: f is onto $\Rightarrow \dim V \geq \dim W$ 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.

3.2 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 $f(\vec{v}_{i \in \mathcal{A}}) = \sum_{j \in \mathcal{B}} A_{ji} \vec{w}_j$ $\exists M_{\mathcal{B}}^{\mathcal{A}} : Hom_F(V, W) \xrightarrow{\sim} Mat(n \times m; F)$
2. If $\vec{v} \in V$, then ${}_{\mathcal{A}}[\vec{v}] := \mathbf{b}$ (vector) where $\vec{v} = \sum_{i \in \mathcal{A}} \mathbf{b}_i \vec{v}_i$
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 $\tilde{\tilde{A}}$: $S(n,m,r)$ 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 *Endomorphism* 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.

4 Rings | Polynomials | Ideals | Subrings

4.1 Rings | Polynomial Rings

Ring $(R,+,\cdot)$: A set R with two operators $+,\cdot$ is a ring if: e.g. $Mat(n,F)$; $R[X]$; $\mathbb{Z}/m\mathbb{Z}$; $\mathbb{Z}$

1. $(R,+)$ is an *abelian group* with identity 0_R. **Commutative Ring**: add: $\forall a,b\in R, ab=ba$.
2. $(R,\cdot)$ is a **monoid** with identity 1_R. i.e. **Associativity**: $\forall a,b,c\in R,(a\cdot b)\cdot c=a\cdot(b\cdot c)$. **Identity**: $\forall a\in R, 1_R\cdot a=a\cdot 1_R=a$.
3. **Distributive**: $\forall a,b,c\in R$: $a\cdot(b+c)=a\cdot b+a\cdot c$ and $(b+c)\cdot a=b\cdot a+c\cdot a$. ps: 默认 monoid 是 closure 的

· If R is ring $\Rightarrow [1_R=0_R\Leftrightarrow R=\{0\}]$ i.e. For any non-zero ring, $1_R\neq 0_R$ **Field**: Commutative ring + multiplicative inverse = Field.

Properties of Ring: $\forall a,b\in R$. **I.** $0\cdot a=a\cdot 0=0$ **II.** $(-a)\cdot b=a\cdot(-b)=-(a\cdot b)$ **III.** $(-a)\cdot(-b)=a\cdot b$

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** $(R^\times,\cdot):=\{a\in R: a \text{ is unit}\}$

Zero-divisors: $a\in R$ is *zero-divisor* if $\exists b\in R, b\neq 0$ 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. $\mathbb{Z}/p\mathbb{Z},\mathbb{R},\mathbb{Q},\mathbb{Z},...$

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

· *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 $R[X]$: $R[X]:=\{a_nX^n+\cdots+a_1X+a_0: a_i\in R, n\in\mathbb{N}\}$ where X is **indeterminate** $\Leftarrow X\notin R$ and $\forall x\in R, Xa=aX$

1. **Degree**: $\deg(P):=\max\{n\in\mathbb{N}: a_n\neq 0\}$ **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. [2] *R integral domain or no zero-divisor* $\Rightarrow \deg(PQ)=\deg(P)+\deg(P)$
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. $a\neq 0$

4.2 Homomorphism | Ideals | Subrings

Ideal $(I\trianglelefteq R)$: A subset $I\subseteq R$ (ring) is an ideal if: **I.** $I\neq\emptyset$ **II.** $\forall a,b\in I, a-b\in I$ **III.** $\forall i\in I,\forall r\in R, ri, ir\in I$

1. **Generated Ideal** ${}_R\langle T\rangle$: $T\subseteq R$ (ring), where R is *commutative ring*. We define ${}_R\langle T\rangle:=\{\sum_{i=1}^n r_it_i: n\in\mathbb{N}, r_i\in R, t_i\in T\}$
   · **Lemma**: ${}_R\langle T\rangle$ is the smallest ideal containing T. **Principal Ideal**: ${}_R\langle a\rangle$ **Proper Ideal**: $I\neq R$ ps: R 一定是 commutative ring
2. If I,J are *ideals* of R. Then $I+J$; $I\cap J$ are also ideals.

Subring Test: $R'\subseteq R$ (ring) is a subring if: **I.** $1_R\in R'$ **II.** $\forall a,b\in R', a-b\in R'$ **III.** $\forall a,b\in R', ab\in R'$

· If $f:R\to S$ is *ring homomorphism*, and R' is subring of R. $\Rightarrow f(R')$ is subring of S.

Ring Homomorphism: R,S are rings, $f:R\to S$ is *ring homomorphism* if: **I.** $f(a+b)=f(a)+f(b)$ **II.** $f(ab)=f(a)f(b)$ $f(1_R)=1_S$ is NOT need

1. **Second Def**: f is ring homomorphism if: $f:(R,+)\to(S,+)$ is group homomorphism and $f(xy)=f(x)f(y)$.
2. **I.** $f(0_R)=0_S$ **II.** $f(-a)=-f(a)$ **III.** $f(a^n)=(f(a))^n$ **IV.** $f(x-y)=f(x)-f(y)$ **V.** $f(mx)=mf(x)$
3. **Kernel**: $\ker f:=\{a\in R: f(a)=0_S\}$ is an *ideal* **Image**: $Imf:=\{f(a): a\in R\}$ is a *subring.* **1-1**: f is 1-1 $\Leftrightarrow \ker f=\{0_R\}$
4. **Unit**: If [1] $f(1_R)=1_S$, [2] 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.*

4.3 Equivalence Relation

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

6 Jordan Normal Form | Spectral Theorem