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: of g | |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 and ϕ \mathbb{R} λ in the prime λ is cyclic.

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

2 Summary

Name	Group $(G,*)$	Ring $(R, +, \cdot)$	Vector Space $(F - V)$	Module $(R - M)$
Def	Closure : $g * h \in G$ $\forall g, h, k \in G$	$(R,+)$ is abelian group with $0_R \forall a,b,c \in R$	$(V, \dot{+})$ is abelian group $\forall \vec{v}, \vec{w} \in V$	$(M, \dot{+})$ is abelian group $\forall m_1, m_2 \in M$
	Associativity : $(g * h) * k = g * (h * k)$	(R,\cdot) is monoid with 1_R (monoid is closure)	$\exists \operatorname{map} F \times V \to V : (\lambda, \vec{v}) \to \lambda \vec{v} \qquad \forall \lambda, \mu \in F$	$\exists \; \mathrm{map} \; R \times M \to M : (r,m) \to rm \qquad \qquad \forall \; r_1, r_2 \in R$
	Identity : $\exists e \in G, e * g = g * e = g$	i.e. Associativity : , $(a \cdot b) \cdot c = a \cdot (b \cdot c)$	$\mathbf{I}: \lambda(\vec{v} \dotplus \vec{w}) = (\lambda \vec{v}) \dotplus (\lambda \vec{w})$	$\mathbf{I}: r(m_1 \dotplus m_2) = (\lambda m_1) \dotplus (\lambda m_2)$
	Inverse : $\exists g^{-1} \in G, g * g^{-1} = g^{-1} * g = e$	Identity: $1_R \cdot a = a \cdot 1_R = a$	$\mathbf{II}: (\lambda + \mu)\vec{v} = (\lambda\vec{v}) \dotplus (\mu\vec{v})$	$\mathbf{II}: (r_1 + r_2)m_1 = (r_1m_1) \dotplus (r_1m_1)$
		Distributive : $a \cdot (b + c) = a \cdot b + a \cdot c$	$\mathbf{III} : \lambda(\mu \vec{v}) = (\lambda \mu) \vec{v}$	III: $r_1(r_2m_1) = (r_1r_2)m_1$
		$(b+c)\cdot a=b\cdot a+c\cdot a$	$\mathbf{IV}: 1_F \vec{v} = \vec{v}$	$IV: 1_R m_1 = m_1$
Prop	I: $(gh)^{-1} = h^{-1}g^{-1}$	$\mathbf{I.}\ 0 \cdot a = a \cdot 0 = 0 \qquad \forall a, b \in R$	$\mathbf{I}.\ 0\vec{v} = 0 \text{ and } \vec{0}\lambda = \vec{0} \qquad \forall \vec{v} \in V, \lambda \in F$	$\mathbf{I.} \ 0_R m = 0_M \ ; r 0_M = 0_M \qquad \forall r \in R, m \in M$
		$\mathbf{II.} (-a) \cdot b = a \cdot (-b) = -(a \cdot b)$	$II. (-1)\vec{v} = -\vec{v}$	II. (-r)m = r(-m) = -(rm)
		Commutative Ring: add $\forall a, b \in R, ab = ba$	III. $\lambda \vec{v} = \vec{0} \Leftrightarrow \lambda = 0 \text{ or } \vec{v} = \vec{0} *$	
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}	$\mathbb{R}[x]_{\leq n}$; $Mat(n,F)$; $Hom(V,W)$	
Sub	Subgroup (H): $\forall h_1, h_2 \in H$	Subring (R') : $\forall a, b \in R'$	Subspace (U) : $\forall \vec{v}, \vec{u} \in U, \lambda, \mu \in F$	Submodule (M') : $\forall m_1, m_2 \in M'$
objects	$\mathbf{I}: H \neq \emptyset;$	I. $1_R \in R'$	$\vec{I}. \vec{0} \in U$	$\mathbf{I.} \ 0_{M} \in M' \qquad \forall r_{1}, r_{2} \in R$
	$\mathbf{II}: h_1 * h_2 \in H;$	II. $a - b \in R'$	II. $\vec{u} + \vec{v} \in U$ and $\lambda \vec{u} \in U$	II. $m_1 - m_2 \in M'$ and $r_1 m_1 \in M'$
	III: $h_1^{-1} \in H$.	III. $ab \in R'$	(or: $\lambda \vec{u} + \mu \vec{v} \in U$)	(or: $r_1 m_1 - r_2 m_2 \in M'$)
Create	H, K subgroups $\Rightarrow H \cap K$ also.	$R, S \text{ subring} \Rightarrow R \cap S \text{ also.}$	V, W subspaces $\Rightarrow V \cap W, V + W$ also.	M, N submodules $\Rightarrow M \cap N, M + N$ also.
Generate	Generated Group $\langle T \rangle$:	Generated Ideal $_R\langle T\rangle$: R is commutative ring	Generated subspaces $\langle T \rangle$:	
objects	$\langle T \rangle := \{ g_1^{a_1} g_k^{a_k} k \in \mathbb{N}, g_i \in T, a_i \in \mathbb{N} \}$	$_R\langle T\rangle:=\{\sum_{i=1}^n r_it_i:n\in\mathbb{N},r_i\in R,t_i\in T\}$	$\langle T \rangle := \{\alpha_1 \vec{v_1} + \dots + \alpha_n \vec{v_n} : \alpha_i \in F, \vec{v_i} \in T, r \in \mathbb{N}\}$	
Special	Cyclic Group: $\langle g \rangle = \{ g^k k \in \mathbb{Z} \}$	Principal Ideal: $_R\langle a\rangle$	$\langle \emptyset \rangle := \{ \vec{0} \}$	
Prop		$\langle T \rangle$ is the smallest the {generated things} cont	caining T . ps: 默认 ${}^2T \subseteq R$ ${}^4T \subseteq M$	
Homo	Homomorphism: $\phi: G \to H$ $\forall g_1, g_2 \in G$	$f: R \to S$ hom: $\forall a, b \in R$	$f: V \to W \qquad \forall \vec{v}_1, \vec{v}_2 \in V, \lambda \in F$	
	I. $\phi(g_1 * g_2) = \phi(g_1) * \phi(g_2)$	$\mathbf{I}. f(a+b) = f(a) + f(b)$	$\mathbf{I}. f(\vec{v}_1 + \vec{v}_2) = f(\vec{v}_1) + f(\vec{v}_2)$	
		$\mathbf{II}.f(ab) = f(a)f(b)$	$\mathbf{II.}f(\lambda\vec{v}_1) = \lambda f(\vec{v}_1)$	
Prop A	$\mathbf{I}: \phi(e_G) = e_H$	$I. f(0_R) = 0_S \qquad f(1_R) = 1_S \text{ NOT need}$	$\mathbf{I}.f(\vec{0})=\vec{0}$	
	II: $\phi(g^{-1}) = \phi(g)^{-1}$	II. f(x - y) = f(x) - f(y)	II. $f(\lambda \vec{v} + \mu \vec{u}) = \lambda f(\vec{v}) + \mu f(\vec{u})$	
	III. ϕ is injective $\Leftrightarrow Ker \phi = \{e_G\}$	III. $f(a^n) = (f(a))^n$ $f(mx) = mf(x)$	III . $f \circ g$ is linear map.	
		Iv. f is 1-1 $\Leftrightarrow \ker f = \{0_R\}$	IV . f is 1-1 iff ker $f = {\vec{0}}$	
Ker/Im	I. $Im(\phi)$ subgroup $Ker(\phi) \lhd G$ normal.	I. $Im(f)$ subring. $Ker(f) \le R$ ideal.	I. $Ker(f)$; $Im(f)$ are subspaces.	
	II . $K \subseteq G$ is subgroup $\Rightarrow \phi(K) \subseteq H$ also.	II. $R' \subseteq R$ is subring $\Rightarrow f(R')$ also.	II. Rank-Nullity Theorem	
	III . $Ker(\phi)$ subgroup.			
Remark	Isomorphism: = LM & Bij. Endomorphis	m(End): = LM & $V = W$. Automorphism(A	ut): = LM & $V = W$ Monomorphism: =	LM & 1-1. Epimorphism : = LM & onto.

Normal $(H \triangleleft G)$: $H \subseteq G$ 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 $(I \subseteq R)$: 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.** $\forall i \in I, \forall r \in R, ri, ir \in I$

Property: If I, J are *ideals* of R. Then I + J; $I \cap J$ are also ideals.

Field (F): A set F is a field with two operators: (addition)+ : $F \times F \to F$; (λ, μ) $\to \lambda + \mu$ (multiplication)· : $F \times F \to F$; (λ, μ) $\to \lambda \mu$ if: (F, +) and $(F \setminus \{0_F\}, \cdot)$ are abelian groups with identity $0_F, 1_F$. and $\lambda(\mu + \nu) = \lambda \mu + \lambda \nu$ $e.g.Fields: \mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$

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: $\forall c_1, ..., c_r \in F, c_1\vec{v_1} + \cdots + c_r\vec{v_r} = \vec{0} \Rightarrow c_1 = \cdots = c_r = 0$.

• **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 $\phi: \vec{x} \mapsto A\vec{x}$ 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**: $|L| \le |E|$ (can get: dim unique) **LI** \to **Basis**: If V finite generate $\Rightarrow \forall L$ can extend to a basis. If $L = \emptyset$, prove $\exists B$ $ext{def} \cap imf = \{0\}$
- 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 $\dim(U + W) = \dim U + \dim W \dim(U \cap W)$

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.

4 Linear Mapping | Rank-Nullity | Matrices | Change of Basis ps. 默认 V, W F-Vect

4.1 Linear Mapping | Rank-Nullity

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

- 1. **Determined**: f is determined by $f(\vec{b_i})$, $\vec{b_i} \in \mathcal{B}_{basis}$ (* i.e. $f(\sum_i \lambda_i \vec{v_i}) := \sum_i \lambda_i f(\vec{v_i})$)
- 2. **Classification of Vector Spaces**: dim $V = n \Leftrightarrow f : F^n \stackrel{\sim}{\to} V$ 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. $^{\Theta}$ 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 $c(M) = \operatorname{row} \operatorname{rank} r(M)$.
- 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, $\mathcal{B} = \{\vec{w_1}, ..., \vec{v_m}\}$ is basis of W.

- 1. $_{\mathcal{B}}[f]_{\mathcal{A}} := A \text{ (matrix) where } f(\vec{v}_{i \in \mathcal{A}}) = \sum_{j \in \mathcal{B}} A_{ji} \vec{w}_j \qquad \exists M_{\mathcal{B}}^{\mathcal{A}} : Hom_F(V, W) \to Mat(n \times m; F)$
- 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**: $[f \circ g] = [f] \circ [g]$ $c[f \circ g]_{\mathcal{A}} = c[f]_{\mathcal{B}} \circ_{\mathcal{B}} [g]_{\mathcal{A}}$ $g[f(\vec{v})] = g[f]_{\mathcal{A}} \circ_{\mathcal{A}} [\vec{v}]$ $g[f]_{\mathcal{A}} = I \Leftrightarrow f = id$
- 4. Change of Basis: Define Change of Basis Matrix:= $_{\mathcal{A}}[id_V]_{\mathcal{B}}$ $_{\mathcal{B}'}[f]_{\mathcal{A}'}=_{\mathcal{B}'}[id_W]_{\mathcal{B}}\circ_{\mathcal{B}}[f]_{\mathcal{A}}\circ_{\mathcal{A}}[id_V]_{\mathcal{A}'}$ $_{\mathcal{A}'}[f]_{\mathcal{A}'}=_{\mathcal{A}}[id_V]_{\mathcal{A}'}$ $_{\mathcal{A}'}[f]_{\mathcal{A}'}\circ_{\mathcal{A}}[id_V]_{\mathcal{A}'}$ **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.

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. $A'[f]_{A'} \sim_{A} [f]_{A}$
- 2. If $\mathcal{B} = \{p(\vec{v_1}), ..., p(\vec{v_n})\}$ and $\mathcal{A} = \{\vec{v_1}, ..., \vec{v_n}\}$ where $p: V \stackrel{\sim}{\to} V$. Then $\mathcal{A}[id_V]_{\mathcal{B}} = \mathcal{A}[p]_{\mathcal{A}}$
- 3. If V is a vector space over F, $[A, B \text{ are } similar \text{ matrices.} \iff A =_{\mathcal{A}} [f]_{\mathcal{A}}, B =_{\mathcal{B}} [f]_{\mathcal{B}} \text{ for some basis } \mathcal{A}, \mathcal{B}; f : V \to V]$
- 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 $tr(f) := tr(_{\mathcal{A}}[f]_{\mathcal{A}}) \mid tr(AB) = tr(BA) \quad tr(\lambda A + \mu B) = \lambda tr(A) + \mu tr(B) \quad tr(N) = tr(M)$ 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: $(R, +) \rightarrow (S, +)$ 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 ${}^1f: R \to S$ homo, ${}^2f(1_R) = 1_{S_L} {}^3x$ is unit of R. $\Rightarrow {}^1f(x)$ is unit of S. ${}^2f|_{R^\times}: R^\times \to S^\times$ is group homomorphism.

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

- 1. **Degree**: $\deg(P) := \max\{n \in \mathbb{N} : a_n \neq 0\}$ **Leading Coefficient**: a_n **Monic**: $a_n = 1$ ps: Polynomial NOT a function
- 2. **Lemma**: 1R integral domain/no zero-divisors $\Rightarrow R[X]$ also. 2R integral domain or no zero-divisor $\Rightarrow \deg(PQ) = \deg(P) + \deg(P)$
- 3. **Division and Remainder**: If R is integral domain and P, $Q \in R[X]$, $Q \in R[X]$ s.t. P = AQ + B and $\deg(B) < \deg(Q)$
- 4. **Function** | **Factorize**: If R is *commutative ring* \Rightarrow $^1R[X] \rightarrow Maps(R,R)$ (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. $a \neq 0$

5.2 Equivalence Relation

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

7 Jordan Normal Form | Spectral Theorem