

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: $\phi: V_1 \times V_2 \rightarrow V_1 \oplus V_2$ by $\mathbf{I}: (\vec{v}_1, \vec{u}_1) + (\vec{v}_2, \vec{u}_2) := (\vec{v}_1 + \vec{v}_2, \vec{u}_1 + \vec{u}_2)$, $\lambda(\vec{v}, \vec{u}) := (\lambda\vec{v}, \lambda\vec{u})$ (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 $V_1 \oplus \dots \oplus V_n := V_1 \times \dots \times V_n$ 且有一组运算法则 **component-wise operations**

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

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 <i>abelian group</i> 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: $a \cdot (b + c) = a \cdot b + a \cdot c$ $(b + c) \cdot a = b \cdot a + c \cdot a$	$(V, +)$ is <i>abelian group</i> $\forall \vec{v}, \vec{w} \in V$ $\exists \text{ map } F \times V \rightarrow V: (\lambda, \vec{v}) \rightarrow \lambda \vec{v} \quad \forall \lambda, \mu \in F$ I: $\lambda(\vec{v} + \vec{w}) = (\lambda\vec{v}) + (\lambda\vec{w})$ II: $(\lambda + \mu)\vec{v} = (\lambda\vec{v}) + (\mu\vec{v})$ III: $\lambda(\mu\vec{v}) = (\lambda\mu)\vec{v}$ IV: $1_F \vec{v} = \vec{v}$	$(M, +)$ is <i>abelian group</i> $\forall m_1, m_2 \in M$ $\exists \text{ map } R \times M \rightarrow M: (r, m) \rightarrow rm \quad \forall r_1, r_2 \in R$ I: $r(m_1 + m_2) = (\lambda m_1) + (\lambda m_2)$ II: $(r_1 + r_2)m_1 = (r_1 m_1) + (r_2 m_1)$ 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. $0_R m = 0_M; r 0_M = 0_M \quad \forall r \in R, m \in M$ 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; $GL_n; D_n; \mathbb{Z}$	$Mat(n, F); R[X]; \mathbb{Z}/m\mathbb{Z}; \mathbb{Z}$	$\mathbb{R}[x]_{<n}; Mat(n, F); Hom(V, W)$	
Sub objects	Subgroup (H): $\forall h_1, h_2 \in H$ I: $H \neq \emptyset$; II: $h_1 * h_2 \in H$; III: $h_1^{-1} \in H$.	Subring (R'): $\forall a, b \in R'$ I. $1_R \in R'$ II. $a - b \in R'$ III. $ab \in R'$	Subspace (U): $\forall \vec{v}, \vec{u} \in U, \lambda, \mu \in F$ 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'): $\forall m_1, m_2 \in M'$ I. $0_M \in M'$ $\forall r_1, r_2 \in R$ 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 $\langle T \rangle$: $\langle T \rangle := \{g_1^{a_1} \dots g_k^{a_k} \mid k \in \mathbb{N}, g_i \in T, a_i \in \mathbb{N}\}$	Generated Ideal $R\langle T \rangle$: R is commutative ring $R\langle T \rangle := \{\sum_{i=1}^n r_i t_i \mid n \in \mathbb{N}, r_i \in R, t_i \in T\}$	Generated subspaces $\langle T \rangle$: $\langle T \rangle := \{\alpha_1 \vec{v}_1 + \dots + \alpha_n \vec{v}_n \mid \alpha_i \in F, \vec{v}_i \in T, r \in \mathbb{N}\}$	
Special	Cyclic Group: $\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$	Principal Ideal: $R\langle a \rangle$	$\langle \vec{0} \rangle := \{\vec{0}\}$	
Prop	$\langle T \rangle$ is the smallest the {generated things} containing T . ps: 默认 ${}^2T \subseteq R \quad {}^4T \subseteq M$			
Homo	Homomorphism: $\phi: G \rightarrow H \quad \forall g_1, g_2 \in G$ I. $\phi(g_1 * g_2) = \phi(g_1) * \phi(g_2)$	$f: R \rightarrow S$ hom: $\forall a, b \in R$ I. $f(a + b) = f(a) + f(b)$ II. $f(ab) = f(a)f(b)$	$f: V \rightarrow W$ $\forall \vec{v}_1, \vec{v}_2 \in V, \lambda \in F$ I. $f(\vec{v}_1 + \vec{v}_2) = f(\vec{v}_1) + f(\vec{v}_2)$ II. $f(\lambda\vec{v}_1) = \lambda f(\vec{v}_1)$	
Prop A	I: $\phi(e_G) = e_H$ II: $\phi(g^{-1}) = \phi(g)^{-1}$ III. ϕ is injective $\Leftrightarrow \text{Ker } \phi = \{e_G\}$	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 $\Leftrightarrow \text{ker } f = \{0_R\}$	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 $\text{ker } f = \{\vec{0}\}$	
Ker/Im	I. $\text{Im}(\phi)$ subgroup $\text{Ker}(\phi) \triangleleft G$ normal. II. $K \subseteq G$ is subgroup $\Rightarrow \phi(K) \subseteq H$ also. III. $\text{Ker}(\phi)$ subgroup.	I. $\text{Im}(f)$ subring. $\text{Ker}(f) \trianglelefteq R$ ideal. II. $R' \subseteq R$ is subring $\Rightarrow f(R')$ also.	I. $\text{Ker}(f); \text{Im}(f)$ are subspaces. II. Rank-Nullity Theorem...	
Remark	Isomorphism: = LM & Bij. Endomorphism(End): = LM & $V = W$. Automorphism(Aut): = 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: $\text{Ker } \phi \triangleleft G$ **II:** ϕ is 1-1 $\Rightarrow G \cong \text{im } \phi$

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.** $\forall i \in I, \forall r \in R, ri, ir \in I$ e.g. $m\mathbb{Z}$

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) $+: F \times F \rightarrow F; (\lambda, \mu) \rightarrow \lambda + \mu$ (multiplication) $\cdot: F \times F \rightarrow F; (\lambda, \mu) \rightarrow \lambda\mu$ 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: $L = \{\vec{v}_1, \vec{v}_2, \dots, \vec{v}_r\}$ is linearly independent if: $\forall c_1, \dots, c_r \in F, c_1 \vec{v}_1 + \dots + c_r \vec{v}_r = \vec{0} \Rightarrow c_1 = \dots = c_r = 0$.

· **Connect to Matrix:** Let $L = \{\vec{v}_1, \dots, \vec{v}_n\}$, L is LI of V . Let $A = [\vec{v}_1, \dots, \vec{v}_n] \Rightarrow \forall \vec{x} \in F^n, A\vec{x} = 0$ (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 $B = \{\vec{v}_1, \dots, \vec{v}_n\}$ is basis of V . Let $A = [\vec{v}_1, \dots, \vec{v}_n] \Rightarrow \forall \vec{x} = (x_1, \dots, x_n)^T$ 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 \rightarrow Basis:** If V finite generate $\Rightarrow \forall L$ can extend to a basis. If $L = \emptyset$, prove $\exists B$ $\text{ker } f \cap \text{im } f = \{0\}$

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: $U, W \subseteq V, U, W$ subspaces are complementary ($V = U \oplus W$) if: $\exists \phi: U \times W \rightarrow V$ 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 -Vector Spaces.

4.1 Linear Mapping | Rank-Nullity

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

- Determined:** f is determined by $f(\vec{b}_i), \vec{b}_i \in \mathcal{B}_{basis}$ (* i.e. $f(\sum_i \lambda_i \vec{b}_i) := \sum_i \lambda_i f(\vec{b}_i)$)
- Classification of Vector Spaces:** $\dim V = n \Leftrightarrow f : F^n \xrightarrow{\sim} V$ by $f(\lambda_1, \dots, \lambda_n) \mapsto \sum_{i=1}^n \lambda_i \vec{v}_i$ is isomorphism.
- 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. $f \circ g = id$
- 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 $f : V \rightarrow W, \dim V = \dim(\ker f) + \dim(Im f)$

Following are properties:

- Injection:** f is 1-1 $\Rightarrow \dim V \leq \dim W$ **Surjection:** f is onto $\Rightarrow \dim V \geq \dim W$ Moreover, $\dim W = \dim Im f$ iff f is onto.
- Same Dimension:** f is isomorphism $\Rightarrow \dim V = \dim W$ **Matrix:** $\forall M$, column rank $c(M) = \text{row rank } r(M)$.
- 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 $AC = I$ || $\exists B, BA = I \Leftrightarrow \exists C, AC = I \Leftrightarrow \exists A^{-1}$ ${}_B[f^{-1}]_{\mathcal{A}} = {}_{\mathcal{A}}[f]_B^{-1}$

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

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

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!

- 交换 i, j 列/行: $P_{ij} = diag(1, \dots, 1, -1, 1, \dots, 1)(I + E_{ij})(I - E_{ji})(I + E_{ij})$ where -1 in j th place.
- Row Echelon Form|Smith Normal Form:** $\tilde{A}: REF$ 通过左乘初等矩阵可以实现 $\tilde{A}: S(n, m, r)$ 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 $f : V \rightarrow W$ can be representing by ${}_B[f]_{\mathcal{A}} = S(n, m, r)$ for some basis \mathcal{A}, \mathcal{B} of V, W .

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

- If $A \sim B$ iff A is similar to B , then \sim is an equivalence relation. ${}_{\mathcal{A}'}[f]_{\mathcal{A}'} \sim {}_{\mathcal{A}}[f]_{\mathcal{A}}$
- If $\mathcal{B} = \{p(\vec{v}_1), \dots, p(\vec{v}_n)\}$ and $\mathcal{A} = \{\vec{v}_1, \dots, \vec{v}_n\}$ where $p : V \xrightarrow{\sim} V$. Then ${}_{\mathcal{A}}[id_V]_{\mathcal{B}} = {}_{\mathcal{A}}[p]_{\mathcal{A}}$
- 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 $\mathcal{A}, \mathcal{B}; f : V \rightarrow V$
- 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.

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 ${}^1 f : R \rightarrow S$ homo, ${}^2 f(1_R) = 1_S, {}^3 x$ is unit of $R. \Rightarrow {}^1 f(x)$ is unit of $S. {}^2 f|_{R^\times} : R^\times \rightarrow S^\times$ 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. $\mathbb{Z}/p\mathbb{Z}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}, \dots$

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

· *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 $\forall x \in R, Xa = aX$

- 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
- Lemma:** ${}^1 R$ integral domain/no zero-divisors $\Rightarrow R[X]$ also. ${}^2 R$ integral domain or no zero-divisor $\Rightarrow \deg(PQ) = \deg(P) + \deg(Q)$
- 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 $\deg(B) < \deg(Q)$
- Function | Factorize:** If R is commutative ring $\Rightarrow {}^1 R[X] \rightarrow Maps(R, R)$ (可以视作函数) ${}^2 \lambda \in R$ is root of $P \Leftrightarrow (X - \lambda) | P(X)$
- 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