

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: $\phi: V_1 \times V_2 \rightarrow V_1 \oplus V_2$ by **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 $x \mapsto (0, \dots, 0, x, 0, \dots, 0)$

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

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

2 Summary

Name	Group $(G, *)$	Ring $(R, +, \cdot)$	Vector Space $(F - V)$	Module $(R - M)$
Def	Closure: $g * h \in G$ $\forall g, h, k \in G$ 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 $\forall a, b, c \in R$ (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> $\forall \vec{v}, \vec{w} \in V$ $\exists \text{ map } F \times V \rightarrow V: (\lambda, \vec{v}) \rightarrow \lambda \vec{v}$ $\forall \lambda, \mu \in F$ 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> $\forall m_1, m_2 \in M$ $\exists \text{ map } R \times M \rightarrow M: (r, m) \rightarrow rm$ $\forall r_1, r_2 \in R$ 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. $0 \cdot a = a \cdot 0 = 0$ $\forall a, b \in R$ 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 $\vec{0}\lambda = \vec{0}$ $\forall \vec{v} \in V, \lambda \in F$ II. $(-1)\vec{v} = -\vec{v}$ III. $\lambda\vec{v} = \vec{0} \Leftrightarrow \lambda = 0$ or $\vec{v} = \vec{0} *$	I. $0_R m = 0_M; r0_M = 0_M$ $\forall r \in R, m \in M$ 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): $\forall h_1, h_2 \in H$ 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 $\langle T \rangle$: $\langle T \rangle := \{\alpha_1 \vec{v}_1 + \dots + \alpha_n \vec{v}_n \mid \alpha_i \in F, \vec{v}_i \in T, n \in \mathbb{N}\}$	Generated submodules $_R \langle T \rangle$: $\langle T \rangle := \{r_1 t_1 + \dots + r_n t_n \mid r_i \in R, t_i \in T, n \in \mathbb{N}\}$
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 $^2 T \subseteq R$ $^4 T \subseteq M$			
Homo	Homomorphism: $\phi: G \rightarrow H$ $\forall g_1, g_2 \in G$ 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. $f(\lambda\vec{v}_1) = \lambda f(\vec{v}_1)$	R-Hom: $f: M \rightarrow N$ $\forall a, b \in M, r \in R$ 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. $f(0_R) = 0_S$ $f(1_R) = 1_S$ NOT need II. $f(x - y) = f(x) - f(y)$ III. $f(a^n) = (f(a))^n$ $f(mx) = mf(x)$ 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. $f(0_M) = 0_N$ $f(1_R) = 1_S$ 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 $\ker(\phi) \triangleleft G$ normal. II. $K \subseteq G$ is subgroup $\Rightarrow \phi(K) \subseteq H$ also. III. $Ker(\phi)$ subgroup.	I. $Im(f)$ subring. $\ker(f) \trianglelefteq R$ 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 $(H \triangleleft G)$: $H \subseteq G$ is normal if: $\forall g \in G, gH = Hg$

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

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 $\exists B$ $ker f \cap im f = \{0\}$

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: $\exists \phi: U \times W \rightarrow V$ by $(\vec{u}, \vec{w}) \mapsto \vec{u} + \vec{w}$ 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)

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 $f, g \in \text{Hom}$

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

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, $\dim W = \dim \text{Im} f$ 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 $AC = I$ || $\exists B, BA = I \Leftrightarrow \exists C, AC = I \Leftrightarrow \exists A^{-1}$ ${}_B[f^{-1}]_{\mathcal{A}} = {}_B[f]_{\mathcal{B}}^{-1}$

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

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: $P_{ij} = \text{diag}(1, \dots, 1, -1, 1, \dots, 1)(I + E_{ij})(I - E_{ji})(I + E_{ij})$ 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 $N = {}_B[f]_{\mathcal{B}}, M = {}_A[f]_{\mathcal{A}}$, then $N = T^{-1}MT$. where $T = {}_A[id_V]_{\mathcal{B}}$

- If $A \sim B$ iff A is similar to B , then \sim is an equivalence relation. ${}_A'[f]_{\mathcal{A}'} \sim {}_A[f]_{\mathcal{A}}$
- 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 ${}_A[id_V]_{\mathcal{B}} = {}_A[p]_{\mathcal{A}}$
- If V is a vector space over $F, [A, B]$ are similar matrices. $\Leftrightarrow A = {}_A[f]_{\mathcal{A}}, B = {}_B[f]_{\mathcal{B}}$ 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: $\text{tr}(A) := \sum_i a_{ii}$ and $\text{tr}(f) := \text{tr}({}_A[f]_{\mathcal{A}}) \mid \text{tr}(AB) = \text{tr}(BA) \quad \text{tr}(\lambda A + \mu B) = \lambda \text{tr}(A) + \mu \text{tr}(B) \quad \text{tr}(N) = \text{tr}(M)$ 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: $\forall a, b \in R$. 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 $\forall x \in R, Xa = aX$

- 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 $\Rightarrow {}^1 R[X] \rightarrow \text{Maps}(R, R)$ (可以视作函数) ${}^2 \lambda \in R$ is root of $P \Leftrightarrow (X - \lambda) \mid P(X)$
- 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

Equivalence Relation: A relation R on a set X is a subset $R \subseteq X \times X$. If $(x, y) \in R$, we write xRy , if R is Equivalence Relation, then:

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: A relation R on a set X, xRy . If R is partial order, then:

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. $x \sim y \Leftrightarrow E(x) = E(y) \Leftrightarrow E(x) \cap E(y) \neq \emptyset$.

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

Examples: ¹ If V F -vector space, W subspace. Then V/W is **quotient vector space**. ² If G group, H normal. Then G/H is **quotient group**. ³ If R ring, I ideal. Then R/I is **quotient ring**.

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

Then, $\exists!$ map $\bar{f} : (X/\sim) \rightarrow Z$ s.t. $f = \bar{f} \circ can$ with $\bar{f}(E(x)) = f(x)$ is **well-defined**. Further more, $\bar{f} : (X/\sim) \xrightarrow{\sim} Im(f)$
ps: Often, if we want to prove $g : (X/\sim) \rightarrow Z$ 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: $(x + I) + (y + I) = (x + y) + I$ and $(x + I) \cdot (y + I) = xy + I \Rightarrow R/I$ is a ring.
2. $x + I = y + I \Leftrightarrow x \sim y \Leftrightarrow x - y \in I$ || R is commutative $\Rightarrow R/I$ also. || $R/I \neq \{0 + I\}$ iff $I \neq R$
3. The Identity of R/I : $1_R + I$ The Zero of R/I : $0_R + I$

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

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

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

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

5.4 Modules | Submodules | All of That

Restrict with Scalar: Let $f : R \rightarrow S$ 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: $\forall m \in M, \exists! r_1, \dots, r_n \in R$ s.t. $m = r_1m_1 + \dots + r_nm_n$ ps: m_1, \dots, 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 .

ps: All properties of M/N are similar to R/I

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

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

[⊙]**Second Isomorphism Theorem for Modules:** Let N, K be submodules of R -module $M \Rightarrow N/(N \cap K) \cong (N + K)/K$

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

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

ps: consider $f : M/K \rightarrow M/N$ and then we can find $ker(f) = N/K$

6 Permutation | Determinants | Eigenvalues and Eigenvectors

6.1 Permutation | Determinants

Permutation: A bijection $\sigma : \{1, \dots, n\} \xrightarrow{\sim} \{1, \dots, n\}$ is a permutation.

All permutations of n elements form a group \mathfrak{S}_n .

1. **Transposition:** A transposition is a permutation that exchanges two elements. **Inversion:** A pair of elements (i, j) is an inversion of $\sigma \in \mathfrak{S}_n$ if $i < j$ but $\sigma(i) > \sigma(j)$
2. **Length:** The length of a permutation σ is the number of inversions. (i.e. $\ell(\sigma) := |\{(i, j) : i < j, \sigma(i) > \sigma(j)\}|$) **Sign:** $sgn(\sigma) := (-1)^{\ell(\sigma)}$ $sgn = 1, even ; sgn = -1, odd$
3. $sgn(a_1a_2) = -1$ $sgn(a_1 \dots a_n) = (-1)^{n-1}$ $sgn(\sigma\tau) = sgn(\sigma)sgn(\tau)$ | **Alternating Group:** $A_n := \{\sigma \in \mathfrak{S}_n : sgn(\sigma) = 1\}$
4. **Graph Meaning of Inversion:** Inversion is # edges that cross each other in the graph of permutation. (i.e. 画出的图中, 线段交叉的次数)

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

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 = $|\det(A)| \times area(U)$
2. $sgn(\det A)$ 决定了方向是否改变 (+1 不变, -1 变). (i.e. 顺时针变化, 左右 | 上下变化, 手性变化)

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

- $H(\lambda u, v) = \lambda H(u, v)$
 - $H(u + v, w) = H(u, w) + H(v, w)$
 - $H(u, \lambda v) = \lambda H(u, v)$
 - $H(u, v + w) = H(u, v) + H(u, w)$
- $H(u_1, \dots, \lambda v_i, \dots, u_n) = \lambda H(u_1, \dots, v_i, \dots, u_n) \quad \forall i$
 - $H(u_1, \dots, v_i + v_j, \dots, u_n) = H(u_1, \dots, v_i, \dots, u_n) + H(u_1, \dots, v_j, \dots, u_n) \quad \forall i$
- (左边 bilinear, 右边 multilinear)

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

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

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

if (multilinear): 1V_i same, ${}^2H(v_1, \dots, v_n) = 0 \quad \forall v_i = v_j$ (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 $H(u, v) = -H(v, u) \quad H(v_1, \dots, v_i, \dots, v_j, \dots, v_n) = -H(v_1, \dots, v_j, \dots, v_i, \dots, v_n)$ (\Leftarrow 不一定成立)

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

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

- Unique on Field:** $\det : F^n \times \dots \times F^n \rightarrow F$ or $\det : \text{Mat}(n; F) \rightarrow F$ is the ¹*unique* ²*alternating* ³*multilinear form* s.t. $\det(I_n) = 1_F$
- Invertible on Field:** For $\text{Mat}(n; F)$, A is invertible $\Leftrightarrow \det(A) \neq 0 \quad \det(A^{-1}) = \det(A)^{-1}$ 交换环, 结论成立如果 $\det(A)$ 在 R 中有逆
- Similar on Field:** For F field. $A \sim B \Rightarrow \det(A) = \det(P^{-1}BP) = \det(B)$ Thus, we can define: $\det(f)$ for $f : V \rightarrow V$
- Operations:** If R is *commutative ring*, then $\det(AB) = \det(A)\det(B) \quad \det(A^T) = \det(A) \quad \det(A^{-1}) = \det(A)^{-1}$
- 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. F be field. R be *commutative ring*.

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

6.2 Eigenvalues | Eigenvectors | Diagonalization

Eigenspace $E(\lambda, f)$: Let $f : V \rightarrow V$ linear map (End), $\lambda \in F$. $E(\lambda, f) := \{\vec{v} \in V : f(\vec{v}) = \lambda \vec{v}\}$. λ is *eigenvalue* if $E(\lambda, f) \neq \{0\}$
ps: $\ker(f - \lambda \text{id}_V)$ is the eigenspace of $E(\lambda, f)$ and it has a basis of eigenvectors $\{\vec{v}_1, \dots, \vec{v}_r\}$.

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

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

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

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

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

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

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

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

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

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

- $\exists \mathcal{B} = (\vec{v}_1, \dots, \vec{v}_n)$ 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) we say f is *triangularisable*
- The characteristic polynomial $\chi_f(x)$ can be factored into linear factors over F . (ps: If F is algebraically closed, then f is triangularisable)

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

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

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

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

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

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

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

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

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

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 $V \times V \rightarrow \mathbb{R}|\mathbb{C}$ s.t.

- Linear in 1st Variable:** $(\lambda \vec{x} + \mu \vec{y}, \vec{z}) = \lambda(\vec{x}, \vec{z}) + \mu(\vec{y}, \vec{z}) \quad \forall \lambda, \mu \in F, \vec{x}, \vec{y}, \vec{z} \in V$
- (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.
- 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 $(\vec{x}, \vec{y}) = \sum_{i,j} a_{ij} x_i \overline{y_j} = \vec{x}^T A \vec{y}$ where $A_{ij} = a_{ij}$

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

- Pythagoras' Theorem:** If $\vec{x} \perp \vec{y}$, then $\|\vec{x} + \vec{y}\|^2 = \|\vec{x}\|^2 + \|\vec{y}\|^2$. **Metric Space:** $d(\vec{x}, \vec{y}) := \|\vec{x} - \vec{y}\|$.
- Cauchy-Schwarz Inequality:** $|(x, y)| \leq \|x\| \|y\|$ **Triangle Inequality:** $\|\vec{x} + \vec{y}\| \leq \|\vec{x}\| + \|\vec{y}\|$ **Scalar:** $\|\lambda \vec{x}\| = |\lambda| \|\vec{x}\|$
Remark: *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: $\{\vec{v}_1, \dots, \vec{v}_n\}$ 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**.

- Observations: I.** For $\{\vec{v}_1, \dots, \vec{v}_n\}$ 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. \Rightarrow 证明 basis 只需要证 span.
- Theorem:** Every finite-dimensional inner product space has an orthonormal basis.
- Gram-Schmidt Process:** Let $\{\vec{v}_1, \dots, \vec{v}_n\}$ be basis of V . By using following way to get orthonormal basis:

a. $\vec{e}_1 = \frac{\vec{v}_1}{\ \vec{v}_1\ }$	$\text{Proj}_{\vec{e}_k} \vec{v}_j = (\vec{v}_j, \vec{e}_k) \vec{e}_k$	All-In-One: $\vec{e}_{k+1} = \frac{\vec{v}_{k+1} - \sum_{i=1}^k \text{Proj}_{\vec{e}_i} \vec{v}_{k+1}}{\ \vec{v}_{k+1} - \sum_{i=1}^k \text{Proj}_{\vec{e}_i} \vec{v}_{k+1}\ }$
b. $\vec{u}_2 = \vec{v}_2 - \text{Proj}_{\vec{e}_1} \vec{v}_2$	$\vec{e}_2 = \frac{\vec{u}_2}{\ \vec{u}_2\ }$	
c. $\vec{u}_3 = \vec{v}_3 - \text{Proj}_{\vec{e}_1} \vec{v}_3 - \text{Proj}_{\vec{e}_2} \vec{v}_3$	$\vec{e}_3 = \frac{\vec{u}_3}{\ \vec{u}_3\ }$	
d. $\vec{u}_n = \vec{v}_n - \sum_{i=1}^{n-1} \text{Proj}_{\vec{e}_i} \vec{v}_n$	$\vec{e}_n = \frac{\vec{u}_n}{\ \vec{u}_n\ }$	

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

- I.** A^\perp is always subspace of V . **II.** $A^\perp = \langle A \rangle^\perp$
- 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 $\{\vec{e}_1, \dots, \vec{e}_m\}$.

- Then: *orthogonal projection* $\pi_U : V \rightarrow V$ by $\vec{v} \mapsto \sum_{i=1}^m (\vec{v}, \vec{e}_i) \vec{e}_i$
- I.** $\pi_U^2 = \pi_U$ **II.** $\ker(\pi_U) = U^\perp$ and $\text{Im}(\pi_U) = U$ **III.** $\pi_U|_U = \text{id}_U$
- Orthogonal Decomposition:** For all $\vec{v} \in V$, $\vec{v} = (\vec{v} - \pi_U(\vec{v})) + \pi_U(\vec{v})$ where $(\vec{v} - \pi_U(\vec{v})) \perp \pi_U(\vec{v})$.
- 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 <i>orthogonal</i> if $A^T A = I_n$. (i.e. $A^{-1} = A^T$)	Unitary: matrix A is <i>unitary</i> if $\overline{A}^T A$ or $A^T \overline{A} = I_n$. (i.e. $A^{-1} = \overline{A}^T$)
Hermitian: matrix A is <i>Hermitian</i> if $\overline{A}^T = A$. (i.e. A is <i>self-adjoint</i> in \mathbb{C})	Symmetric: matrix A is <i>symmetric</i> if $A^T = A$. (i.e. A is <i>self-adjoint</i> in \mathbb{R})
Useful Tool: If $T : V \rightarrow W$ is linear map. For matrix ${}_B[T]_A$, The entry ${}_B[T]_A]_{ij} = (T \vec{e}_j, \vec{f}_i)$	
IPS isomorphism of V: A linear map $T : V \rightarrow W$ is <i>IPS isomorphism</i> of V (and W) if: ${}^1 T$ is isomorphism ${}^2 (T \vec{v}_1, T \vec{v}_2) = (\vec{v}_1, \vec{v}_2) \quad \forall \vec{v}_1, \vec{v}_2 \in V$	
Properties of IPS isomorphism: Let V, W be <i>inner product spaces</i> , $\mathcal{A} = \{\vec{e}_1, \dots, \vec{e}_m\}, \mathcal{B} = \{\vec{f}_1, \dots, \vec{f}_n\}$ are orthonormal basis of V, W .	
1. Linear map $T : V \rightarrow W$ is <i>IPS isomorphism</i> of V (i.e. T is iso & $(T \vec{v}_1, T \vec{v}_2) = (\vec{v}_1, \vec{v}_2)$) \Leftrightarrow Linear map $T : V \rightarrow W$ maps some orthonormal basis to another.	
2. $T : V \rightarrow V$ is <i>IPS isomorphism</i> $\Leftrightarrow {}_A[T]_A$ is <i>orthogonal</i> $_{\mathbb{R}}$ or <i>unitary</i> $_{\mathbb{C}}$ matrix.	
3. ★ Similar: If matrix $A = {}_A[f]_A$ and $B = {}_B[f]_B \Leftrightarrow B = P^{-1}AP$ and P is <i>orthogonal</i> $_{\mathbb{R}}$ or <i>unitary</i> $_{\mathbb{C}}$ matrix.	
Adjoint: V is inner product space. $T, S : V \rightarrow V$ are linear maps. T, S are called <i>adjoint</i> to one another if $(T \vec{v}, \vec{w}) = (\vec{v}, S \vec{w}) \quad \forall \vec{v}, \vec{w} \in V$.	
Self-adjoint: If $T = T^*$, then T is <i>self-adjoint</i> . (i.e. $(T \vec{v}, \vec{w}) = (\vec{v}, T \vec{w})$)	
Properties of Adjoint: Let V be <i>inner product spaces</i> , $\mathcal{A} = \{\vec{e}_1, \dots, \vec{e}_n\}$ are orthonormal basis of V . $T : V \rightarrow V$ is linear map.	
1. Then, $\exists!$ linear map $T^* : V \rightarrow V$ s.t. $(T \vec{v}, \vec{w}) = (\vec{v}, T^* \vec{w}) \quad \forall \vec{v}, \vec{w} \in V$.	
2. I. ${}_A[T^*]_A = \overline{({}_A[T]_A)}^T$ II. If $T = T^*$ (self-adjoint) $\Leftrightarrow {}_A[T]_A = \overline{({}_A[T]_A)}^T$ Hermitian/Symmetric III. $(T^*)^* = T$	
3. IPS isomorphism: $T : V \rightarrow V$ is <i>IPS isomorphism</i> $\Leftrightarrow TT^* = T^*T = \text{id}_V \Leftrightarrow {}_A[T]_A$ is <i>unitary</i> $_{\mathbb{C}}$ or <i>orthogonal</i> $_{\mathbb{R}}$ matrix.	
Normal: Linear map $T : V \rightarrow V$ is <i>normal</i> if $TT^* = T^*T$.	
Properties of Normal: Let V be <i>inner product spaces</i> , $\mathcal{A} = \{\vec{e}_1, \dots, \vec{e}_n\}$ are orthonormal basis of V . $T : V \rightarrow V$ is linear map.	
1. T is <i>normal</i> $\Leftrightarrow \overline{({}_A[T]_A)}^T {}_A[T]_A = {}_A[T]_A \cdot \overline{({}_A[T]_A)}^T$	
2. I. T is <i>self-adjoint</i> $\Rightarrow T$ is <i>normal</i> II. T is <i>IPS isomorphism</i> $\Rightarrow T$ is <i>normal</i> .	

7.3 Advanced Properties of Adjoint and Self-Adjoint

Properties of Self-adjoint: Let $T : V \rightarrow V$ 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**| λ : Eigenvectors of *distinct eigenvalues* are orthogonal.
3. **Orthogonal**| T : If $\vec{v} \perp \vec{w}$, and \vec{v} is *eigenvector* of T . Then, $T\vec{w} \perp \vec{v}$. \ominus 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* $\lambda_1, \dots, \lambda_n$ (can be repeated).

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

Real Quadratic forms: $Q(x_1, \dots, x_n) := \sum_{i=1}^n a_{ii}x_i^2 + 2 \sum_{1 \leq i < j \leq n} a_{ij}x_i x_j = \vec{x}^T A \vec{x}$ 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: $Q(\vec{x}) = (A\vec{x}, \vec{x}) \geq 0$ (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 $\sqrt{\frac{1}{\lambda_1}}, \dots, \sqrt{\frac{1}{\lambda_n}}$ 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 $\sqrt{\frac{1}{\lambda_1}}, \dots, \sqrt{\frac{1}{\lambda_n}}$.

8 Jordan Normal Form

9 Appendix

Vieta's formulas: For polynomial $P(x) = a_n x^n + \dots + a_1 x + a_0$. Let x_1, \dots, x_n be roots of $P(x)$.

$$x_1 + \dots + x_n = -\frac{a_{n-1}}{a_n} \quad x_1 \cdots x_n = (-1)^n \frac{a_0}{a_n} \quad x_1 x_2 + x_1 x_3 + \dots + x_{n-1} x_n = \frac{a_{n-2}}{a_n}$$

Determinant of Vandermonde Matrix: Let x_1, \dots, x_n be distinct elements of F . Then $\det \begin{pmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} \end{pmatrix} = \prod_{1 \leq i < j \leq n} (x_j - x_i)$

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