# HAlg Note

## 1 Basic Knowledge

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

**Complement-wise Operations**: $\phi : V_1 \times V_2 \to V_1 \oplus V_2$ by I:$(\vec{v_1}, \vec{u_1}) + (\vec{v_2}, \vec{u_2}) := (\vec{v_1} + \vec{v_1}, \vec{u_1} + \vec{u_2})$, $\lambda(\vec{v}, \vec{u}) := (\lambda\vec{v}, \lambda\vec{u})$ (ps:$V_1, V_2$ 通过 $\phi$ 定义的 map 所形成的 vector space 记作 $V_1 \oplus V_2$)

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

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

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

$$A_{n\times m}B_{m\times n} = \begin{pmatrix} \mathbf{a}_{1*}^T \\ \vdots \\ \mathbf{a}_{n*}^T \end{pmatrix}B = \begin{pmatrix} \mathbf{a}_{1*}^T B \\ \vdots \\ \mathbf{a}_{n*}^T B \end{pmatrix} \qquad A_{n\times m} = A_{n\times m}I_m \begin{matrix} = A(\vec{e_1} & \vec{e_2} & \cdots & \vec{e_n}) \\ = (A\vec{e_1} & A\vec{e_2} & \cdots & A\vec{e_n}) \end{matrix} \qquad A_{n\times m}B_{m\times n} = \begin{pmatrix} \mathbf{a}_{*1} \cdots \mathbf{a}_{*m} \end{pmatrix}\begin{pmatrix} \mathbf{b}_{1*}^T \\ \vdots \\ \mathbf{b}_{m*}^T \end{pmatrix} = \sum_{k=1}^m \mathbf{a}_{*k}\mathbf{b}_{k*}^T$$

## 2 Summary

| Name | Group $(G, *)$ | Ring $(R, +, \cdot)$ | Vector Space $(F - V)$ | Module $(R - M)$ |
|---|---|---|---|---|
| Def | **Closure**: $g * h \in G$  $\forall g, h, k \in G$<br>**Associativity**: $(g * h) * k = g * (h * k)$<br>**Identity**: $\exists e \in G, e * g = g * e = g$<br>**Inverse**: $\exists g^{-1} \in G, g * g^{-1} = g^{-1} * g = e$ | $(R, +)$ is abelian group with $0_R$  $\forall a, b, c \in R$<br>$(R, \cdot)$ is **monoid** with $1_R$ (monoid is closure)<br>i.e. **Associativity**: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$<br>**Identity**: $1_R \cdot a = a \cdot 1_R = a$<br>**Distributive**: $a \cdot (b + c) = a \cdot b + a \cdot c$<br>$\qquad (b + c) \cdot a = b \cdot a + c \cdot a$ | $(V, \dot{+})$ is abelian group  $\forall \vec{v}, \vec{w} \in V$<br>$\exists$ map $F \times V \to V : (\lambda, \vec{v}) \to \lambda\vec{v}$  $\forall \lambda, \mu \in F$<br>**I**: $\lambda(\vec{v} + \vec{w}) = (\lambda\vec{v}) \dot{+} (\lambda\vec{w})$<br>**II**: $(\lambda + \mu)\vec{v} = (\lambda\vec{v}) \dot{+} (\mu\vec{v})$<br>**III**: $\lambda(\mu\vec{v}) = (\lambda\mu)\vec{v}$<br>**IV**: $1_F\vec{v} = \vec{v}$ | $(M, \dot{+})$ is abelian group  $\forall m_1, m_2 \in M$<br>$\exists$ map $R \times M \to M : (r, m) \to rm$  $\forall r_1, r_2 \in R$<br>**I**: $r(m_1 \dot{+} m_2) = (\lambda m_1) \dot{+} (\lambda m_2)$<br>**II**: $(r_1 + r_2)m_1 = (r_1 m_1) \dot{+} (r_1 m_1)$<br>**III**: $r_1(r_2 m_1) = (r_1 r_2)m_1$<br>**IV**: $1_R m_1 = m_1$ |
| Prop | **I**: $(gh)^{-1} = h^{-1}g^{-1}$ | **I**. $0 \cdot a = a \cdot 0 = 0$  $\forall a, b \in R$<br>**II**. $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$<br>**Commutative Ring**: add $\forall a, b \in R, ab = ba$ | **I**. $0\vec{v} = 0$ and $\vec{0}\lambda = \vec{0}$  $\forall \vec{v} \in V, \lambda \in F$<br>**II**. $(-1)\vec{v} = -\vec{v}$<br>**III**. $\lambda\vec{v} = \vec{0} \Leftrightarrow \lambda = 0$ or $\vec{v} = \vec{0} \star$ | **I**. $0_R m = 0_M ; r0_M = 0_M$  $\forall r \in R, m \in M$<br>**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 ($H$)**:  $\forall h_1, h_2 \in H$<br>**I**: $H \neq \emptyset$;<br>**II**: $h_1 * h_2 \in H$;<br>**III**: $h_1^{-1} \in H$. | **Subring ($R'$)**:  $\forall a, b \in R'$<br>**I**. $1_R \in R'$<br>**II**. $a - b \in R'$<br>**III**. $ab \in R'$ | **Subspace ($U$)**:  $\forall \vec{v}, \vec{u} \in U, \lambda, \mu \in F$<br>**I**. $\vec{0} \in U$<br>**II**. $\vec{u} + \vec{v} \in U$ and $\lambda\vec{u} \in U$<br>(or: $\lambda\vec{u} + \mu\vec{v} \in U$) | **Submodule ($M'$)**:  $\forall m_1, m_2 \in M'$<br>**I**. $0_M \in M'$  $\forall r_1, r_2 \in R$<br>**II**. $m_1 - m_2 \in M'$ and $r_1 m_1 \in M'$<br>(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 $\langle T \rangle$**:<br>$\langle T \rangle := \{g_1^{a_1} ... g_k^{a_k} \mid k \in \mathbb{N}, g_i \in T, a_i \in \mathbb{N}\}$ | **Generated Ideal $_R\langle T \rangle$**:  $R$ is *commutative ring*<br>$_R\langle T \rangle := \{\sum_{i=1}^n r_i t_i : n \in \mathbb{N}, r_i \in R, t_i \in T\}$ | **Generated subspaces $\langle T \rangle$**:<br>$\langle T \rangle := \{\alpha_1 \vec{v_1} + \cdots + \alpha_n \vec{v_n} : \alpha_i \in F, \vec{v_i} \in T, n \in \mathbb{N}\}$ | **Generated submodules $_R\langle T \rangle$**<br>$\langle T \rangle := \{r_1 t_1 + \cdots + r_t n : r_i \in R, t_i \in T, n \in \mathbb{N}\}$ |
| Special | **Cyclic Group**: $\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$ | **Principal Ideal**: $_R\langle a \rangle$  i.e. $aR$ | $\langle \emptyset \rangle := \{\vec{0}\}$ | **Cyclic submodule**: If $M =_R \langle t \rangle$ |
| Prop | | $\langle T \rangle$ is the smallest the {generated things} containing $T$.  ps: 默认 $^2 T \subseteq R$  $^4 T \subseteq M$ | | |
| Homo | **Homomorphism**:$\phi : G \to H$  $\forall g_1, g_2 \in G$<br>**I**. $\phi(g_1 * g_2) = \phi(g_1) * \phi(g_2)$ | $f : R \to S$ hom:  $\forall a, b \in R$<br>**I**. $f(a + b) = f(a) + f(b)$<br>**II**. $f(ab) = f(a)f(b)$ | $f : V \to W$  $\forall \vec{v_1}, \vec{v_2} \in V, \lambda \in F$<br>**I**. $f(\vec{v_1} + \vec{v_2}) = f(\vec{v_1}) + f(\vec{v_2})$<br>**II**. $f(\lambda\vec{v_1}) = \lambda f(\vec{v_1})$ | **R-Hom**: $f : M \to N$  $\forall a, b \in M, r \in R$<br>**I**. $f(a + b) = f(a) + f(b)$<br>**II**. $f(ra) = rf(a)$ |
| Prop A | **I**: $\phi(e_G) = e_H$<br>**II**: $\phi(g^{-1}) = \phi(g)^{-1}$<br><br>**III**. $\phi$ is 1-1 $\Leftrightarrow \ker \phi = \{e_G\}$ | **I**. $f(0_R) = 0_S$  $f(1_R) = 1_S$ NOT need<br>**II**. $f(x - y) = f(x) - f(y)$<br>**III**. $f(a^n) = (f(a))^n$  $f(mx) = mf(x)$<br>**IV**. $f$ is 1-1 $\Leftrightarrow \ker f = \{0_R\}$ | **I**. $f(\vec{0}) = \vec{0}$<br>**II**. $f(\lambda\vec{v} + \mu\vec{u}) = \lambda f(\vec{v}) + \mu f(\vec{u})$<br>**III**. $f \circ g$ is linear map.<br>**IV**. $f$ is 1-1 iff $\ker f = \{\vec{0}\}$ | **I**. $f(0_M) = 0_N$  $f(1_R) = 1_S$ NOT need<br>**II**. $f(a - b) = f(a) - f(b)$<br><br>**III**. $f$ is 1-1 iff $\ker f = \{0\}$ |
| Ker/Im | **I**. $Im(\phi)$ subgroup  $\ker(\phi) \triangleleft G$ normal.<br>**II**. $K \subseteq G$ is subgroup $\Rightarrow \phi(K) \subseteq H$ also.<br>**III**. $Ker(\phi)$ subgroup. | **I**. $Im(f)$ subring.  $\ker(f) \trianglelefteq R$ ideal .<br>**II**. $R' \subseteq R$ is subring $\Rightarrow f(R')$ also. | **I**. $\ker(f) ; Im(f)$ are subspaces.<br>**II**. Rank-Nullity Theorem... | **I**.$\ker f, Imf$ 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**: $\phi$ 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)$+ : F \times F \to F; (\lambda, \mu) \to \lambda + \mu$  (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  $\lambda(\mu + \nu) = \lambda\mu + \lambda\nu$  $e.g. Fields : \mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$

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

2. **Basis|max,min**: $B \Leftrightarrow B$ is minimal GS ($E$) $\Leftrightarrow B$ is maximal LI ($L$).  **Uniqueness|Basis**: 每个元素都可以由 basis 唯一表示.

3. **Proper Subspaces**: If $U \subset V$ is proper subspace, then $\dim U < \dim V$.  $\Rightarrow$  If $U \subseteq V$ is subspace and $\dim U = \dim V$, then $U = V$.

4. **Dimension Theorem**: If $U, W \subseteq V$ are subspaces of $V$, then $\dim(U + W) = \dim U + \dim W - \dim(U \cap W)$

**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 <span style="font-size:small">**ps:** 默认 $V, W$ $F$-Vector Spaces.</span>

## 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**: $\dim V = n \Leftrightarrow f : F^n \xrightarrow{\sim} V$ 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.

## 4.2 Matrices | Change of Basis | Similar Matrices | Trace

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

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

**Representing matrix of linear map** $_\mathcal{B}[f]_\mathcal{A}$: $f : V \to W$ be linear map, $\mathcal{A} = \{\vec{v_1}, ..., \vec{v_n}\}$ is basis of $V$, $\mathcal{B} = \{\vec{w_1}, ..., \vec{w_m}\}$ is basis of $W$.

1. $_\mathcal{B}[f]_\mathcal{A} := A$ (matrix) where $f(\vec{v}_{i \in \mathcal{A}}) = \sum_{j \in \mathcal{B}} A_{ji} \vec{w_j}$    $\exists M_\mathcal{B}^\mathcal{A} : Hom_F(V, W) \xrightarrow{\sim} Mat(n \times m; F)$

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**: $[f \circ g] = [f] \circ [g]$    $_\mathcal{C}[f \circ g]_\mathcal{A} =_\mathcal{C} [f]_\mathcal{B} \circ_\mathcal{B} [g]_\mathcal{A}$    $_\mathcal{B}[f(\vec{v})] =_\mathcal{B} [f] \circ_\mathcal{A} [\vec{v}]$    $_\mathcal{A}[f]_\mathcal{A} = I \Leftrightarrow f = id$

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 $\lambda$ 倍加到第 $i$ 行, 右乘代表 $j$ 列乘 $\lambda$ 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 $j$th 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.

# 5 Rings | Polynomials | Ideals | Subrings

## 5.1 Rings | Polynomial Rings

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

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

· **Lemma**: If $^1f : R \to S$ homo, $^2f(1_R) = 1_S, ^3x$ 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** $R[X]$: $R[X] := \{a_n X^n + \cdots + a_1 X + a_0 : a_i \in R, n \in \mathbb{N}\}$ where $X$ is **indeterminate** $\Leftarrow X \notin R$ and $\forall x \in R, Xa = aX$

1. **Degree**: $\deg(P) := \max\{n \in \mathbb{N} : a_n \neq 0\}$   **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. $a \neq 0$

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

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

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

**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 $f : X \to Z$ is a map s.t. $x \sim y \Leftrightarrow f(x) = f(y)$. ($\sim$ is Equivalence relation) **Important**

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

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

## 5.3 Factor Ring | First Isomorphism Theorem

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

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

1. By *well-defined* operators: $(x + I) \dot{+} (y + I) = (x + y) + I$ and $(x + I) \cdot (y + I) = xy + I \quad \Rightarrow \quad R/I$ is a ring.

2. $x + I = y + I \quad \Leftrightarrow \quad x \sim y \quad \Leftrightarrow \quad x - y \in I \quad || \quad$ $R$ is commutative $\Rightarrow R/I$ also. $\quad || \quad R/I \neq \{0 + I\}$ 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: $\overline{f}(x + I) = f(x)$

1. **can**: Mapping $can : R \to R/I$ by $x \mapsto x + I$ is [1] surjection, [2] $ker(can) = I$, [3] $can$ is ring homomorphism.

2. **f**: If [1] $f : R \to S$ is *ring homomorphism* and [2] $I \subseteq ker(f)$, then $\exists!$ [1] $\overline{f} : R/I \to S$ s.t. $f = \overline{f} \circ can$ is *ring homomorphism*.

3. **First Isomorphism Theorem**: If $f : R \to S$ is *ring homomorphism* $\Rightarrow \exists! \overline{f} : R/ker(f) \xrightarrow{\sim} im(f)$ is (*ring isomorphism*).

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

1. **can**: Mapping $can : G \to G/H$ by $x \mapsto xH$ is [1] surjection, [2] $ker(can) = H$, [3] $can$ is group homomorphism.

2. **f**: If [1] $f : G \to S$ is *group homomorphism* and [2] $H \subseteq ker(f)$, then $\exists!$ [1] $\overline{f} : G/H \to S$ s.t. $f = \overline{f} \circ can$ is *group homomorphism*.

3. **First Isomorphism Theorem**: If $f : G \to S$ is *group homomorphism* $\Rightarrow \exists! \overline{f} : G/ker(f) \xrightarrow{\sim} im(f)$ is (*group isomorphism*).

## 5.4 Modules | Submodules | All of That

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

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

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

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

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

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: $\overline{f}(x + N) = f(x)$

1. **can**: Mapping $can : M \to M/N$ by $x \mapsto x + N$ is [1] surjection, [2] $ker(can) = N$, [3] $can$ is module homomorphism.

2. **f**: If [1] $f : M \to S$ is *module homomorphism* and [2] $N \subseteq ker(f)$, then $\exists!$ [1] $\overline{f} : M/N \to S$ s.t. $f = \overline{f} \circ can$ is *module homomorphism*.

3. **First Isomorphism Theorem**: If $f : M \to S$ is *module homomorphism* $\Rightarrow \exists! \overline{f} : M/ker(f) \xrightarrow{\sim} im(f)$ is (*module isomorphism*).

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

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

$\ominus$ **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 $f : M/K \to M/N$ and then we can find $ker(f) = N/K$

# 6 Permutation | Determinants | Eigenvalues and Eigenvectors

## 6.1 Permutation | Determinants

**Permutation**: A bijection $\sigma : \{1, ..., n\} \xrightarrow{\sim} \{1, ..., n\}$ 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 $\sigma$ 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. $sgn(a_1 a_2) = -1 \quad sgn(a_1 ... a_n) = (-1)^{n-1} \quad sgn(\sigma\tau) = sgn(\sigma)sgn(\tau) \quad |$ **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 $A_{ij} = a_{ij}$.  $\det(A) := \sum_{\sigma \in \mathfrak{S}_n} \mathrm{sgn}(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)}$ (**Leibniz Formula**)  $\det(I_0) := 1$

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

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

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

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

1. $H(\lambda u, v) = \lambda H(u, v)$

2. $H(u + v, w) = H(u, w) + H(v, w)$

3. $H(u, \lambda v) = \lambda H(u, v)$

4. $H(u, v + w) = H(u, v) + H(u, w)$

 1. $H(u_1, ..., \lambda v_i, ..., u_n) = \lambda H(u_1, ..., v_i, ..., u_n)$  $\forall i$

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

 (左边 bilinear, 右边 multilinear)

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

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

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

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

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

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

1. **Unique on Field**: $\det : F^n \times \cdots \times F^n \to F$ or $\det : Mat(n; F) \to F$ is the $^1$*unique* $^2$*alternating* $^3$*multilinear form* s.t. $\det(I_n) = 1_F$

2. **Invertible on Field**: For $Mat(n; F)$, $A$ is invertible $\Leftrightarrow \det(A) \neq 0$   $\det(A^{-1}) = \det(A)^{-1}$   交换环, 结论成立如果 $\det(A)$ 在 $R$ 中有逆

3. **Similar on Field**: For $F$ field.   $A \sim B \Rightarrow \det(A) = \det(P^{-1}BP) = \det(B)$   Thus, we can define: $\det(f)$ for $f : V \to V$

4. **Operations**: If $R$ is *commutative ring*, then $\det(AB) = \det(A) \det(B)$   $\det(A^T) = \det(A)$   $\det(A^{-1}) = \det(A)^{-1}$

5. **Block Triangular**: If $A$ is block triangular, then $\det(A) = \prod_{i=1}^{n} \det(A_i)$   即矩阵分块后如果是对角阵, 行列式等于各个块的行列式乘积

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

1. **Cofactor**: In $R$, $C_{ij} := (-1)^{i+j} \det(A\langle i, j \rangle)$  where $A\langle i, j \rangle$ 是 $A$ 去掉第 $i$ 行第 $j$ 列的矩阵.  **Laplace's Expansion**: In $R$, $\det(A) = \sum_{j=1}^{n} a_{ij} C_{ij} = \sum_{i=1}^{n} a_{ij} C_{ij}$

2. **Adjugate Matrix**: In $R$ $\mathrm{adj}(A)$ matrix, $\mathrm{adj}(A)_{ij} := C_{ji}$  **Cramer's Rule**: In $R$ $A \cdot \mathrm{adj}(A) = (\det A) I_n$  In $F$, $x_i = \frac{\det(A_i)}{\det(A)}$ $A_i$ 代表 $A$ 的第 $i$ 列替换为 $b$

3. $^\ominus$ **Theorem|Need proof**: In $R$, $\mathrm{adj}(A^T) = \mathrm{adj}(A)^T$  Hint: $\mathrm{adj}(A^T)_{ij} = C_{ij}^{A^T} = (-1)^{i+j} \det(A^T\langle i, j \rangle) = (-1)^{i+j} \det(A\langle j, i \rangle^T) = (-1)^{i+j} \det(A\langle j, i \rangle) = C_{ji}^A = \mathrm{adj}(A)_{ji} = \mathrm{adj}(A)_{ij}^T$

4. $\star$ **Invertibility of Matrix**: In $R$, matrix $A$ is invertible $\Leftrightarrow \det(A) \in R^\times$  e.g. $\mathbb{Z}^\times = \{\pm 1\}$ ; $\mathbb{C}^\times, \mathbb{R}^\times, \mathbb{Q}^\times = \mathbb{C}^*, \mathbb{R}^*, \mathbb{Q}^*$ ; $\mathbb{F}_p^\times = \mathbb{F}_p \backslash \{0\}$ ; $\mathbb{Z}[i] = \{\pm 1, \pm i\}$

5. **Jacobi's Formula**, Let matrix $A$ s.t. $a_{ij}(t)$ are functions of $t$.   Then, $\frac{d}{dt} \det(A) = \mathrm{tr}\left(\mathrm{adj} A \cdot \frac{dA}{dt}\right)$

## 6.2 Eigenvalues | Eigenvectors | Diagonalization

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

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

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

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

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

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

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

Suppose $f(\vec{v}_k) = \sum_{i=1}^{m} c_{ik} \vec{w}_i + \sum_{j=m+1}^{n} b_{jk} \vec{v}_j$  Let $g : W \to W$ by $w \mapsto f(w)$  $h : V/W \to V/W$ by $v + W \mapsto f(v) + W$  $e : V/W \to W$ 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 $A \in Mat(n; F)$, it is *triangularisable* if $\exists P$ invertible s.t. $P^{-1} A P = U$ is upper triangular.

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

1. $\exists \mathcal{B} = (\vec{v}_1, ..., \vec{v}_n)$ basis s.t. $f(\vec{v}_i) = \sum_{j=1}^{i} a_{ji} \vec{v}_j$  (i.e. $_\mathcal{B}[f]_\mathcal{B}$ is upper triangular.)   we say $f$ is *triangularisable*

2. The characteristic polynomial $\chi_f(x)$ can be factored into <u>linear factors</u> over $F$.  (ps: If $F$ is algebraically closed, then $f$ is triangularisable)

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

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

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

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

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

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

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

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

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

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

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

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

# 8  Jordan Normal Form | Spectral Theorem

# 9  Appendix

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

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

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

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