高等代数笔记：特征值到标准型

晨锦辉永生之语

2025 年 4 月 29 日

目录

1 初看特征值

1.1 特征值

给定线性空间 V 上的线性变换 $\mathcal{A}$，我们想找到 V 的一组基 $\{\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_n\}$，使线性变换 $\mathcal{A}$ 在这组基下的表示矩阵为对角矩阵：

$$\begin{pmatrix} a_1 & & & \\ & a_2 & & \\ & & \ddots & \\ & & & a_n \end{pmatrix}.$$

这时，若 $\boldsymbol{\alpha} = k_1\boldsymbol{e}_1 + k_2\boldsymbol{e}_2 + \cdots + k_n\boldsymbol{e}_n$，则

$$\mathcal{A}\boldsymbol{\alpha} = a_1k_1\boldsymbol{e}_1 + a_2k_2\boldsymbol{e}_2 + \cdots + a_nk_n\boldsymbol{e}_n.$$

线性变换 $\mathcal{A}$ 的表达式非常简单,线性变换 $\mathcal{A}$ 的许多性质也变得一目了然. 例如,若 $a_1, a_2, \cdots, a_r$ 不为零，而 $a_{r+1} = \cdots = a_n = 0$，则 $\mathcal{A}$ 的秩为 r，且 $\operatorname{Im}\mathcal{A}$ 就是由 $\{\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_r\}$ 生成的子空间，而 $\operatorname{Ker}\mathcal{A}$ 则是由 $\{\boldsymbol{e}_{r+1}, \cdots, \boldsymbol{e}_n\}$ 生成的子空间.

我们知道一个线性变换在不同基下的表示矩阵是相似的. 因此用矩阵的语言重述上面提到的问题就是：能否找到一类特别简单的矩阵，使任一定矩阵都与这类矩阵中的某一个相似？比如，我们可以问：是否所有的矩阵都相似于对角矩阵？若不然，哪一类矩阵可以相似于对角矩阵？

若线性空间 V 可分解为

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_m, \tag{1}$$

其中每个 V_i 都是线性变换 $\mathcal{A}$ 的不变子空间，那么 $\mathcal{A}$ 可以表示为分块对角阵. 我们希望 (1) 式中的 V_i 越小越好. 最小的非零子空间是一维子空间. 若 V_i 是一维子空间，x 是其中的任一非零向量，$\mathcal{A}$ 在 V_i 上的作用相当于一个数乘，于是存在 $\lambda_0 \in \mathbb{K}$，使

$$\mathcal{A}(x) = \lambda_0 x.$$

定义 1.1.1: 特征值与特征向量

设 $\mathcal{A}$ 是数域 $\mathbb{K}$ 上线性空间 V 上的线性变换，若 $\lambda_0 \in \mathbb{K}$，$x \in V$ 且 $x \neq 0$，使

$$\mathcal{A}(x) = \lambda_0 x, \tag{2}$$

则称 λ_0 是线性变换 $\mathcal{A}$ 的一个特征值，向量 x 称为 $\mathcal{A}$ 关于特征值 λ_0 的特征向量.

现在设 $\mathcal{A}$ 在某组基下的表示矩阵为 $\boldsymbol{A}$，向量 $\boldsymbol{x}$ 在这组基下可表示为一个列向量 $\boldsymbol{\alpha}$，这时(2)式等价于

$$\boldsymbol{A}\boldsymbol{\alpha} = \lambda_0\boldsymbol{\alpha} \iff (\lambda_0\boldsymbol{I}_n - \boldsymbol{A})\boldsymbol{\alpha} = 0. \tag{3}$$

因此，类似线性变换，我们可以定义矩阵的特征值、特征向量、特征子空间.

定义 1.1.2: 矩阵的特征值、特征向量和特征子空间

设 $\boldsymbol{A}$ 是数域 $\mathbb{K}$ 上的 n 阶方阵，若存在 $\lambda_0 \in \mathbb{K}$ 及 n 维非零列向量 $\boldsymbol{\alpha}$，使 $\boldsymbol{A}\boldsymbol{\alpha} = \lambda_0$ 成立，则称 λ_0 为矩阵 A 的一个**特征值**，$\boldsymbol{\alpha}$ 为 A 关于特征值 λ_0 的**特征向量**. 齐次线性方程组 $(\lambda_0\boldsymbol{I}_n - \boldsymbol{A})\boldsymbol{x} = 0$ 的解空间 V_{λ_0} 称为 A 关于特征值 λ_0 的**特征子空间**.

命题 1.1.1: 特征子空间

$\mathcal{A}$ 关于特征值 λ_0 的全体特征向量再加上零向量构成 V 的一个子空间.

证明. 若向量 $\boldsymbol{x}, \boldsymbol{y}$ 是关于特征值 λ_0 的特征向量，则

$$\mathcal{A}(\boldsymbol{x}+\boldsymbol{y}) = \mathcal{A}(\boldsymbol{x}) + \mathcal{A}(\boldsymbol{y}) = \lambda_0\boldsymbol{x} + \lambda_0\boldsymbol{y} = \lambda_0(\boldsymbol{x}+\boldsymbol{y}),$$

$$\mathcal{A}(c\boldsymbol{x}) = c\mathcal{A}(\boldsymbol{x}) = c\lambda_0\boldsymbol{x} = \lambda_0(c\boldsymbol{x}).$$

因此 $\mathcal{A}$ 的关于特征值 λ_0 的全体特征向量加上零向量构成 V 的子空间，记为 V_{λ_0}，称为 $\mathcal{A}$ 的关于特征值 λ_0 的**特征子空间**. □

显然 V_{λ_0} 是 $\mathcal{A}$ 的不变子空间.

我们已经定义了线性变换与矩阵的特征值，现在的问题是如果来求一个线性变换或一个矩阵的特征值？从 (6.1.4) 式可以看出，要使 α 非零，必须 $|\lambda_0 I_n - A| = 0$. 反过来，若 $\lambda_0 \in \mathbb{K}$ 且 $|\lambda_0 I_n - A| = 0$，则 (6.1.4) 式有非零解 α. 因此寻找矩阵 A 的特征值等价于寻找行列式 $|\lambda \boldsymbol{I}_n - A| = 0$ 时 λ 的值. 设 $A = (a_{ij})$，则

$$|\lambda \boldsymbol{I}_n - A| = \begin{vmatrix} \lambda - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & \lambda - a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & & \vdots \\ -a_{n1} & -a_{n2} & \cdots & \lambda - a_{nn} \end{vmatrix} \tag{6.1.5}$$

是一个以 λ 为未知数的 n 次首一多项式.

定义 1.1.3: 特征多项式

设 $\boldsymbol{A}$ 是 n 阶方阵，称 $|\lambda\boldsymbol{I}_n - \boldsymbol{A}|$ 为 A 的特征多项式.

由上面的讨论可得矩阵 A 的特征值就是它的特征多项式的根.

命题 1.1.2

设 $\boldsymbol{A}$ 是数域 K 上的 n 级矩阵，则 $\boldsymbol{A}$ 的特征多项式 $|\lambda\boldsymbol{I}-\boldsymbol{A}|$ 是一个 n 次多项式，λ^n 的系数是 1，λ^{n-1} 的系数等于 $-\mathrm{tr}(\boldsymbol{A})$，常数项为 $(-1)^n|\boldsymbol{A}|$，λ^{n-k} 的系数为 $\boldsymbol{A}$ 的所有 k 阶主子式的和乘以 $(-1)^k$，$1\leqslant k<n$.

证明. 设 $\boldsymbol{A}=(a_{ij})$ 的列向量组是 $\boldsymbol{a}_1,\boldsymbol{a}_2,\cdots,\boldsymbol{a}_n$.

$$|\lambda\boldsymbol{I}-\boldsymbol{A}|=\begin{vmatrix}\lambda-a_{11}&0-a_{12}&\cdots&0-a_{1n}\\0-a_{21}&\lambda-a_{22}&\cdots&0-a_{2n}\\\vdots&\vdots&\ddots&\vdots\\0-a_{n1}&0-a_{n2}&\cdots&0-a_{nn}\end{vmatrix}$$

利用行列式的性质，$|\lambda\boldsymbol{I}-\boldsymbol{A}|$ 可以拆成 2^n 个行列式的和，它们是

$$\begin{vmatrix}\lambda&0&\cdots&0\\0&\lambda&\cdots&0\\\vdots&\vdots&\ddots&\vdots\\0&0&\cdots&\lambda\end{vmatrix},\begin{vmatrix}-a_{11}&-a_{12}&\cdots&-a_{1n}\\-a_{21}&-a_{22}&\cdots&-a_{2n}\\\vdots&\vdots&\ddots&\vdots\\-a_{n1}&-a_{n2}&\cdots&-a_{nn}\end{vmatrix},$$

$$|(-\boldsymbol{a}_1,\cdots,-\boldsymbol{a}_{j_1-1},\lambda\boldsymbol{e}_{j_1},-\boldsymbol{a}_{j_1+1},\cdots,\lambda\boldsymbol{e}_{j_2},\cdots,-\boldsymbol{a}_n)|$$

其中 $1\leqslant j_1<\cdots<j_{n-k}\leqslant n,k=1,2,\cdots,n-1$.

上述第 1 个行列式等于 λ^n，第 2 个行列式等于 $(-1)^k|\boldsymbol{A}|$，对于第 3 种类型的行列式，按第 $j_1,j_2,\cdots,j_{n-k}$ 列展开，这 $n-k$ 列元素组成的 $n-k$ 阶子式只有一个不为 0：

$$\begin{vmatrix}\lambda&0&\cdots&0\\0&\lambda&\cdots&0\\\vdots&\vdots&\ddots&\vdots\\0&0&\cdots&\lambda\end{vmatrix}=\lambda^{n-k},$$

其余 $n-k$ 阶子式全为 0. 这个不等于 0 的 $n-k$ 阶子式的代数余子式为

$$(-1)^{(j_1+j_2+\cdots+j_{n-k})+(j_1+j_2+\cdots+j_{n-k})}(-\boldsymbol{A})_{j_1',j_2',\cdots,j_k'}=(-1)^k\boldsymbol{A}_{j_1',j_2',\cdots,j_k'}$$

其中 $(j_1',j_2',\cdots,j_k')=(1,2,\cdots,n)\setminus\{j_1,j_2,\cdots,j_{n-k}\}$，且 $j_1'<j_2'<\cdots<j_k'$. 因此第 3 种类型的行列式的值为

$$(-1)^k\boldsymbol{A}_{j_1',j_2',\cdots,j_k'}\lambda^{n-k}.$$

由于 $1\leqslant j_1'<j_2'<\cdots<j_k'\leqslant n$，因此 $|\lambda\boldsymbol{I}-\boldsymbol{A}|$ 中 λ^{n-k} 的系数为

$$(-1)^k\sum_{1\leqslant j_1'<j_2'<\cdots<j_k'\leqslant n}\boldsymbol{A}_{j_1',j_2',\cdots,j_k'},$$

其中 $k = 1, 2, \cdots, n-1$. 特别地，当 $k = 1$ 时，得到 $|\lambda \boldsymbol{I} - \boldsymbol{A}|$ 中 λ^{n-1} 的系数为

$$-(a_{11} + a_{22} + \cdots + a_{nn}) = -\operatorname{tr}(\boldsymbol{A}).$$

因此

$$|\lambda \boldsymbol{I} - \boldsymbol{A}| = \lambda^n - \operatorname{tr}(\boldsymbol{A})\lambda^{n-1} + \cdots + (-1)^k \sum_{1 \leqslant j_1' < j_2' < \cdots < j_k' \leqslant n} \boldsymbol{A}_{j_1', j_2', \cdots, j_k'} \lambda^{n-k} + \cdots + (-1)^n |\boldsymbol{A}|.$$

□

定义 1.1.4: 代数重数和几何重数

设 $\mathcal{A}$ 是 n 维线性空间 V 上的线性变换，λ_0 是 $\mathcal{A}$ 的一个特征值，V_0 是属于 λ_0 的特征子空间，称 $\dim V_0$ 为 λ_0 的**度数或几何重数**. λ_0 作为 $\mathcal{A}$ 的特征多项式根的重数称为 λ_0 的重数或代数重数.

命题 1.1.3: 几何重数小于等于代数重数

设 $\mathcal{A}$ 是 n 维线性空间 V 上的线性变换，λ_0 是 $\mathcal{A}$ 的一个特征值，则 λ_0 的度数总是小于等于 λ_0 的重数.

证明. 设特征值 λ_0 的重数为 m，度数为 t，又 V_0 是属于 λ_0 的特征子空间，则 $\dim V_0 = t$. 设 $\{\boldsymbol{e}_1, \cdots, \boldsymbol{e}_t\}$ 是 V_0 的一组基. 由于 V_0 中的非零向量都是 $\mathcal{A}$ 关于 λ_0 的特征向量，故

$$\mathcal{A}(\boldsymbol{e}_i) = \lambda_0 \boldsymbol{e}_i, \quad i = 1, \cdots, t.$$

将 $\{\boldsymbol{e}_1, \cdots, \boldsymbol{e}_t\}$ 扩充为 V 的一组基，记为 $\{\boldsymbol{e}_1, \cdots, \boldsymbol{e}_t, \boldsymbol{e}_{t+1}, \cdots, \boldsymbol{e}_n\}$，则 $\mathcal{A}$ 在这组基下的表示矩阵为

$$\boldsymbol{A} = \begin{pmatrix} \lambda_0 \boldsymbol{I}_t & * \\ O & \boldsymbol{B} \end{pmatrix},$$

其中 $\boldsymbol{B}$ 是一个 $n-t$ 阶方阵. 因此，线性变换 $\mathcal{A}$ 的特征多项式具有如下形状：

$$|\lambda I_V - \mathcal{A}| = |\lambda \boldsymbol{I}_n - \boldsymbol{A}| = (\lambda - \lambda_0)^t |\lambda \boldsymbol{I}_{n-t} - \boldsymbol{B}|,$$

这表明 λ_0 的重数至少为 t，即 $t \leqslant m$. □

定义 1.1.5: 特征向量系

设 $\mathcal{A}$ 是 n 维线性空间 V 上的线性变换，若 $\mathcal{A}$ 的任一特征值的度数等于重数，则称 $\mathcal{A}$ 有完全的特征向量系.

定理 1.1.1. *若 B 与 $\boldsymbol{A}$ 相似，则 B 与 $\boldsymbol{A}$ 具有相同的特征多项式，从而具有相同的特征值 (计重数).*

证明. 设 $\boldsymbol{B} = \boldsymbol{P}^{-1}\boldsymbol{A}\boldsymbol{P}$，其中 $\boldsymbol{P}$ 是可逆阵，则

$$|\lambda \boldsymbol{I}_n - \boldsymbol{B}| = |\boldsymbol{P}^{-1}(\lambda \boldsymbol{I}_n - \boldsymbol{A})\boldsymbol{P}| = |\boldsymbol{P}^{-1}||\lambda \boldsymbol{I}_n - \boldsymbol{A}||\boldsymbol{P}| = |\lambda \boldsymbol{I}_n - \boldsymbol{A}|.$$

因此相似矩阵必有相同的特征多项式，从而必有相同的特征值 (计重数). □

1.2 对角化

定义 1.2.1: 可对角化线性变换和矩阵

设 $n \in \mathbb{Z}_{\geq 0}$，若 n 维线性空间 V 有基 $\{\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_n\}$ 使得每个 $\boldsymbol{e}_i$ 都是 T 的特征向量，则称 T 在 $\mathbb{F}$ 上是**可对角化的**.

若将矩阵 $\boldsymbol{A} \in M_{n\times n}(\mathbb{F})$ 看作线性映射 $\mathbb{F}^n \to \mathbb{F}^n$，则 $\boldsymbol{A}$ 在 $\mathbb{F}$ 上可对角化相当于存在可逆矩阵 $\mathbb{P} \in M_{n\times n}(\mathbb{F})$，使得 $\boldsymbol{T} = \boldsymbol{P}^{-1}\boldsymbol{A}\boldsymbol{P}$ 为对角阵.

定理 1.2.1 (可对角化的条件 1)**.** *数域 $\mathbb{K}$ 上 n 级矩阵 A 可对角化的充分必要条件是 A 有 n 个线性无关的特征向量 $\boldsymbol{a}_1, \boldsymbol{a}_2, \cdots, \boldsymbol{a}_n$.*

证明. 若 n 维线性空间 V 上的线性变换 $\mathcal{A}$ 在某组基 $\{\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_n\}$ 下的表示矩阵为对角阵：$\mathrm{diag}\{\lambda_1, \lambda_2, \cdots, \lambda_n\}$, 此时 $\mathcal{A}(\boldsymbol{e}_i) = \lambda_i \boldsymbol{e}_i$，即 $\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_n$ 是 $\mathcal{A}$ 的特征向量，于是 $\mathcal{A}$ 有 n 个线性无关的特征向量.

反过来，若 n 维线性空间 V 上的线性变换 $\mathcal{A}$ 有 n 个线性无关的特征向量 $\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_n$，则这组向量构成了 V 的一组基，且 $\mathcal{A}$ 在这组基下的表示矩阵显然是一个对角阵. □

定理 1.2.2. 若 $\lambda_1,\lambda_2,\cdots,\lambda_k$ 为 n 维线性空间 V 上的线性变换 $\mathcal{A}$ 的不同的特征值，则

$$V_1+V_2+\cdots+V_k=V_1\oplus V_2\oplus\cdots\oplus V_k.$$

证明. 对 k 用数学归纳法. 若 $k=1$，结论显然成立. 现设对 $k-1$ 个不同的特征值 $\lambda_1,\lambda_2,\cdots,\lambda_{k-1}$，它们相应的特征子空间 $V_1,V_2,\cdots,V_{k-1}$ 之和是直和. 我们要证明 $V_1,V_2,\cdots,V_{k-1},V_k$ 之和为直和，这只需证明：

$$V_k\cap(V_1+V_2+\cdots+V_{k-1})=\{\mathbf{0}\} \tag{4}$$

即可，设 $\boldsymbol{v}\in V_k\cap(V_1+V_2+\cdots+V_{k-1})$，则

$$\boldsymbol{v}=\boldsymbol{v}_1+\boldsymbol{v}_2+\cdots+\boldsymbol{v}_{k-1}, \tag{5}$$

其中 $\boldsymbol{v}_i\in V_i(i=1,2,\cdots,k-1)$. 在 (5)式两边作用 $\mathcal{A}$，得

$$\mathcal{A}(\boldsymbol{v})=\mathcal{A}(\boldsymbol{v}_1)+\mathcal{A}(\boldsymbol{v}_2)+\cdots+\mathcal{A}(\boldsymbol{v}_{k-1}).$$

但 $\boldsymbol{v},\boldsymbol{v}_1,\boldsymbol{v}_2,\cdots,\boldsymbol{v}_{k-1}$ 都是 $\mathcal{A}$ 的特征向量或零向量，因此

$$\lambda_k\boldsymbol{v}=\lambda_1\boldsymbol{v}_1+\lambda_2\boldsymbol{v}_2+\cdots+\lambda_{k-1}\boldsymbol{v}_{k-1}. \tag{6}$$

在 (5) 式两边乘以 λ_k 减去 (6) 式得

$$\{\mathbf{0}\}=(\lambda_k-\lambda_1)\boldsymbol{v}_1+(\lambda_k-\lambda_2)\boldsymbol{v}_2+\cdots+(\lambda_k-\lambda_{k-1})\boldsymbol{v}_{k-1}.$$

由归纳假设，$V_1+V_2+\cdots+V_{k-1}$ 是直和，因此 $(\lambda_k-\lambda_i)\boldsymbol{v}_i=0$，而 $\lambda_k-\lambda_i\neq 0$，从而 $\boldsymbol{v}_i=0(i=1,2,\cdots,k-1)$. 这就证明了(4) 式. □

推论 1.1

线性变换 $\mathcal{A}$ 属于不同特征值的特征向量必线性无关.

推论 1.2

若 n 维线性空间 V 上的线性变换 $\mathcal{A}$ 有 n 个不同的特征值，则 $\mathcal{A}$ 必可对角化.

推论 1.3

若线性变换 $\mathcal{A}$ 的特征多项式没有重根，则 $\mathcal{A}$ 可对角化.

注意推论1.3只是可对角化的充分条件而非必要条件，比如说纯量变换 $\mathcal{A}=cI_V$ 当然可对角化，但 $\mathcal{A}$ 的 n 个特征值都是 c. 由定理1.2.2，我们还可以得到可对角化的另一个充分必要条件.

推论 1.4: 可对角化的充分必要条件

设 $\mathcal{A}$ 是 n 维线性空间 V 上的线性变换，$\lambda_1,\lambda_2,\cdots,\lambda_k$ 是 $\mathcal{A}$ 的全部不同的特征值，$V_i(i=1,2,\cdots,k)$ 是特征值 λ_i 的特征子空间，则 $\mathcal{A}$ 可对角化的充分必要条件是

$$V=V_1\oplus V_2\oplus\cdots\oplus V_k.$$

证明. 先证充分性. 设

$$V=V_1\oplus V_2\oplus\cdots\oplus V_k,$$

分别取 V_i 的一组基 $\{e_{i1},e_{i2},\cdots,e_{it_i}\}(i=1,2,\cdots,k)$，则这些向量拼成了 V 的一组基，并且它们都是 $\mathcal{A}$ 的特征向量. 因此 $\mathcal{A}$ 有 n 个线性无关的特征向量，从而 $\mathcal{A}$ 可对角化.

再证必要性. 设 $\mathcal{A}$ 可对角化，则 $\mathcal{A}$ 有 n 个线性无关的特征向量 $\{e_1,e_2,\cdots,e_n\}$，它们构成了 V 的一组基. 不失一般性，可设这组基中前 t_1 个是关于特征值 λ_1 的特征向量；接下去的 t_2 个是关于特征值 λ_2 的特征向量；……；最后 t_k 个是关于特征值 λ_k 的特征向量. 对任一 $\alpha\in V$，设 $\boldsymbol{\alpha}=a_1e_1+a_2e_2+\cdots+a_ne_n$，则 $\boldsymbol{\alpha}$ 可写成 $V_1,V_2,\cdots,V_k$ 中向量之和，因此由定理1.2.2可得

$$V=V_1+V_2+\cdots+V_k=V_1\oplus V_2\oplus\cdots\oplus V_k. \qquad \square$$

定理 1.2.3 (可对角化的充分必要条件). 设 $\mathcal{A}$ 是 n 维线性空间 V 上的线性变换，则 $\mathcal{A}$ 可对角化的充分必要条件是 $\mathcal{A}$ 有完全的特征向量系，即几何重数等于代数重数.

证明. 设 $\lambda_1,\lambda_2,\cdots,\lambda_k$ 是 $\mathcal{A}$ 的全部不同的特征值，它们对应的特征子空间、重数和度数分别记为 $V_i,m_i,t_i(i=1,2,\cdots,k)$. 由重数的定义1.1.4以及命题1.1.3可知

$$m_1+m_2+\cdots+m_k=n,\quad t_i\leqslant m_i,\quad i=1,2,\cdots,k.$$

由推论1.3，我们只要证明 $\mathcal{A}$ 有完全的特征向量系当且仅当 $V=V_1\oplus V_2\oplus\cdots\oplus V_k$. 若

$V = V_1 \oplus V_2 \oplus \cdots \oplus V_k$，则

$$n = \dim V = \dim(V_1 \oplus V_2 \oplus \cdots \oplus V_k) = \dim V_1 + \dim V_2 + \cdots + \dim V_k = \sum_{i=1}^{k} t_i \leqslant \sum_{i=1}^{k} m_i = n,$$

因此 $t_i = m_i (i = 1, 2, \cdots, k)$，即 $\mathcal{A}$ 有完全的特征向量系. 反过来，若 $\mathcal{A}$ 有完全的特征向量系，则

$$\dim(V_1 \oplus V_2 \oplus \cdots \oplus V_k) = \sum_{i=1}^{k} t_i = \sum_{i=1}^{k} m_i = n = \dim V,$$

从而 $V = V_1 \oplus V_2 \oplus \cdots \oplus V_k$ 成立. □

推论 1.5

n 维线性空间 V 上的线性变换 $\mathcal{A}$ 可对角化当且仅当 $\mathcal{A}$ 的属于不同特征值的特征子空间的维数之和等于 n.

2 环、域与多项式

2.1 环与域

非空集 S 上的 n 元运算（$n \in \mathbb{Z}_{\geqslant 1}$）无非是指一个映射 $S^n \to S$；譬如加法 $+$ 和乘法 $\cdot$ 都是 $\mathbb{Z}$ 上的二元运算. 对于一般的二元运算

$$\star : S \times S \to S;$$

习惯的做法是将 $\star(s_1, s_2)$ 写成 $s_1 \star s_2$. 对于可以理解为某种乘法的运算，通常以 $\cdot$ 标记；简写 $s_1 s_2 = s_1 \cdot s_2$ 也是常用的.

定义 2.1.1: 环

设 R 是非空集合，在 R 上定义了二元运算：$+ : R \times R \to R$ 和 $\cdot : R \times R \to R$，对任意的 $x, y, z \in R$，使得以下条件成立：

1. 加法运算满足以下条件：

   (1) 结合律：$(x + y) + z = x + (y + z)$;

   (2) 零元性质:$x + 0_R = x = 0_R + x$.

   (3) 交换律: $x + y = y + x$.

   (4) 加法逆元: 对所有 x 皆存在 $-x$ 使得 $x + (-x) = 0_R$.

2. 乘法运算 $x \cdot y$ 也简写为 xy，它满足以下条件：

(1) 结合律：$(xy)z = x(yz)$;

(2) 幺元性质[a]：$x \cdot 1_R = x = 1_R \cdot x$;

3. 乘法对加法满足

- 分配律: $(x+y)z = xz + yz, \quad z(x+y) = zx + zy$.

则称 $(R, +, \cdot, 0_R, 1_R)$ 为一个**环**. 不致混淆时，我们也把 $0_R, 1_R$ 简记为 $0, 1$，并以 R 代表 $(R, +, \cdot, 0_R, 1_R)$. 为了方便，我们也将 $x + (-y)$ 写作 $x - y$.

[a]不同的教材对环的定义不同体现在是否含有乘法幺元，例如参考书 [5] 中定义不含乘法幺元（即对乘法构成半群），而参考书 [6] 中定义含有乘法幺元. 含有乘法幺元的环具有更多好的性质，因此本笔记的环均指**含幺环**.

由环的定义不难推出如下性质：

1. 结合律确保任意有限多个元素的加法和乘法可以不带括号地写作 $x + y + z, xyz$ 等.

2. 分配律具有双边的版本:

$$a(x+y)b = (ax + ay)b = axb + ayb.$$

3. 加法和乘法幺元[1]都由各自的幺元性质唯一确定.

证明. 设 0_R 和 $0'_R$ 皆满足加法幺元性质, 1_R 和 $1'_R$ 皆满足乘法幺元性质, 则

$$0_R = 0_R + 0'_R = 0'_R, \quad 1_R = 1_R \cdot 1'_R = 1'_R.$$ □

4. 加法满足消去律: 若 $x + y = x' + y$, 等式两边同加 $-y$, 应用加法结合律得 $x = x + y + (-y) = x' + y + (-y) = x'$.

5. 任何 x 的加法逆元 $-x$ 皆唯一, 这是因为若 $x + x' = 0 = x + x''$, 则加法消去律蕴涵 $x' = x''$. 因此取加法逆元 $x \mapsto -x$ 也可以视为 R 上的一元运算.

6. 从加法逆元的唯一性和 $x + (-x) = 0 = (-x) + x$ 立见 $-(-x) = x$.

7. 恒等式 $x \cdot 0 = 0 = 0 \cdot x$ 成立. 以第一个等号为例, 我们有 $x \cdot 0 = x \cdot (0+0) = x \cdot 0 + x \cdot 0$, 对两端应用消去律可得 $x \cdot 0 = 0$.

8. 恒等式 $(-x)y = -xy = x(-y)$ 成立, 这是因为

$$(-x)y + xy = (-x+x)y = 0 \cdot y = 0, \quad x(-y) + xy = x(-y+y) = x \cdot 0 = 0$$

和加法逆元的唯一性.

[1]也就是单位元，加法幺元又称零元.

9. 作为上式的应用，我们有 $(-1)\cdot y = -y$ 和 $-x = x\cdot(-1)$; 特别地，代入 $x=-1$ 给出 $(-1)\cdot(-1)=1$.

注记. 最平凡的环是零环：这是只有单个元素 $1=0$ 的环. 另一方面，非零环必然满足 $1\neq 0$，否则任何 x 都满足 $x = x\cdot 1 = x\cdot 0 = 0$.

例 2.1.1: Gauss 整数环

我们经常遇到的很多数的集合，在数的普通加法和乘法下都构成环. 例如，任何数域都是环. 除此之外，很多本身不是域的数的集合也构成环. 例如，全体整数的集合 $\mathbb{Z}$ 在加法和乘法下也构成环. 现设 $m\in\mathbb{Z}$，令

$$\mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\}.$$

则 $\mathbb{Z}[\sqrt{m}]$ 也构成环. 特别地，当 $m=-1$ 时有

$$\mathbb{Z}[\sqrt{-1}] = \{a + b\sqrt{-1} \mid a, b \in \mathbb{Z}\}.$$

这是历史上非常著名的环的例子，称为 **Gauss 整数环**.

例 2.1.2: 多项式环与矩阵环

项式的集合和矩阵的集合都构成环. 具体来说，设 $\mathbb{P}$ 为一个数域，令 $\mathbb{P}[x]$ 为 $\mathbb{P}$ 上全体以 x 为文字的一元多项式的集合，则 $\mathbb{P}[x]$ 在多项式的加法和乘法下构成环，称为数域 $\mathbb{P}$ 上的 **一元多项式环**，或简称为 $\mathbb{P}$ 上的多项式环. 类似地，记 $\mathbb{P}^{n\times n}$ 为 $\mathbb{P}$ 上全体矩阵构成的集合，则 $\mathbb{P}^{n\times n}$ 在矩阵的加法和乘法下构成环，称为 $\mathbb{P}$ 上的 n 阶方阵环.

例 2.1.3: 某些函数构成的环

记实数轴上全体连续函数构成的集合为 $C(\mathbb{R})$，定义加法与乘法为

$$(f+g)(x) = f(x) + g(x),$$

$$(fg)(x) = f(x)g(x), \quad x\in\mathbb{R},\ f, g\in C(\mathbb{R}),$$

则容易验证 $C(\mathbb{R})$ 构成环. 同样地，记 $\mathbb{R}$ 上全体光滑函数（即具有任何阶的连续导数）的集合为 $C^\infty(\mathbb{R})$，则在上述两种运算下 $C^\infty(\mathbb{R})$ 构成环.

上述环有多种形式的推广. 例如，对任何闭区间 $[a,b]\subset\mathbb{R}$，设 $C([a,b])$ 为 $[a,b]$ 上全体连续函数构成的集合，则 $C([a,b])$ 在上述两种运算下构成环. 如果考虑多元函数，则欧几里得空间 $\mathbb{R}^n$ 上全体光滑函数的集合 $C^\infty(\mathbb{R}^n)$ 在上述加法和乘法下构成环. 对 $C^\infty(\mathbb{R}^n)$ 的研究在微分几何中具有重要意义.

对于任意 $n \in \mathbb{Z}_{\geqslant 0}$ 和 $r \in R$, 我们引入自明的写法

$$n \cdot r = nr := \underbrace{r + \cdots + r}_{n\ \text{项}}, \quad n \geqslant 1, \tag{7}$$
$$0 \cdot r := 0, \quad (-n) \cdot r = (-(n \cdot r)) := -(n \cdot r)$$

容易验证

$$\begin{aligned} n(r + r') = nr + nr', \quad (n + m)r = nr + mr, \\ (nm)r = n(mr), \quad (nr)r' = n(rr'), \\ r(n \cdot 1_R) = nr = (n \cdot 1_R)r \end{aligned} \tag{8}$$

对所有 $n, m \in \mathbb{Z}$ 和 $r, r' \in R$ 皆成立.

对于带有二元运算 $\star$ 的非空集 S 及其子集 S', 如果对所有 $s_1, s_2 \in S'$ 都有 $s_1 \star s_2 \in S'$, 则我们顺理成章地说 S' 对运算 $\star$ **封闭**, 对于一般的 n 元运算当然也有类似的说法. 封闭性可以用来定义代数结构的子结构, 以下仍以环为例.

定义 2.1.2: 子环

如果 R 的子集 R_0 包含 $0_R, 1_R$, 而且在加法, 乘法运算和加法取逆 $x \mapsto -x$ 之下封闭, 则 $(R_0, +, \cdot, 0_R, 1_R)$ 也是环, 称为 R 的**子环**.

例 2.1.4: 环的中心

环 R 的中心定义为

$$Z(R) := \{z \in R : \forall x \in R, zx = xz\}.$$

容易看出 $Z(R)$ 是 R 的子环.

定义 2.1.3: 逆

设 x 是环 R 的元素. 若存在 $y \in R$ 使得 $xy = 1$ (或 $yx = 1$), 则称 y 为 x 的**右逆** (或**左逆**), 而 x 右可逆 (或左可逆). 若 x 左右皆可逆, 则称 x **可逆**. 由 R 的可逆元构成的子集记为 $R^\times$.

我们可以证明:

引理 2.1

如果环 R 的元素 x 可逆, 则 x 的左逆也必然是右逆, 而且存在唯一的 $x^{-1} \in R$ 使得 $x^{-1}x = 1 = xx^{-1}$; 此时 $(x^{-1})^{-1} = x$.

证明. 设 x 可逆, x 为其左逆而 x_R 为其右逆. 由乘法结合律有

$$x_R = 1 \cdot x_R = (x_L \cdot x) \cdot x_R = x_L \cdot (x \cdot x_R) = x_L \cdot 1 = x_L.$$

这就说明左逆等于右逆, 反之亦然.

另一方面，如果 x_L 和 x'_L 都是 x 的左逆, x_R 和 x'_R 都是 x 的右逆, 则将左逆和右逆的四种组合代入上式, 可得

$$x_L = x_R, \quad x_L = x'_R, \quad x'_L = x_R, \quad x'_L = x'_R;$$

特别地, $x_L = x'_L$ 而 $x_R = x'_R$. 综上, 在 x 可逆的前提下, 左逆等于有右逆，并且唯一, 可以合理地记为 x^{-1}. □

注意到 $R^\times$ 包含 1 (显然 $1^{-1} = 1$), 而且对乘法运算封闭: 从 $y^{-1}x^{-1}xy = 1 = xyy^{-1}x^{-1}$ 可得

$$(xy)^{-1} = y^{-1}x^{-1}, \quad x, y \in R^\times.$$

进一步, 性质 $(x^{-1})^{-1} = x$ 说明 $R^\times$ 对取逆运算 $x \mapsto x^{-1}$ 也封闭. 对于环中的元素 $r \in R$ 及其 $n \in \mathbb{Z}_{\geqslant 1}$, 我们记

$$r^n = \underbrace{r \cdots r}_{n \text{ 项}};$$

此外 $r^0 := 1$. 若 $r \in R^\times$, 则进一步记

$$r^{-n} := (r^n)^{-1} = (r^{-1})^n, \quad n \in \mathbb{Z}_{\geqslant 1}.$$

我们总有等式 $r^{m+n} = r^m r^n$; 当 r 可逆时, 此式对 m 或 n 为负的情形同样成立. 同理, $r^{mn} = (r^m)^n$.

定义 2.1.4: 交换环

果环 R 的乘法满足交换律 $xy = yx$, 则称 R 为**交换环**.

因此 R 是交换环当且仅当 $Z(R) = R$.

定义 2.1.5: 交换环与域

满足 $R^\times = R \setminus \{0\}$ (换言之: 零不可逆, 而非零元皆可逆) 的环称为**除环**. 交换除环称为**域**. 域的子环如果也构成域, 则称之为**子域**.

由于域的乘法顺序可换, 在域中可以合理地将 xy^{-1} 写作 x/y 或 $\dfrac{x}{y}$, 前提是 $y \neq 0$.

例 2.1.5

对于寻常的乘法和加法运算, $\mathbb{C}$ 是域, 而 $\mathbb{R}, \mathbb{Q}$ 都是 $\mathbb{C}$ 的子域, 而子环 $\mathbb{Z}$ 不是域; 事实上 $\mathbb{Z}^\times = \{\pm 1\}$.

定义 2.1.6: 整环

非零交换环 R 若满足 $x, y \neq 0 \implies xy \neq 0$, 则称为**整环**.

整环的子环显然也是整环. 在整环中乘法对所有非零元都有消去律, 这是因为 $x \neq 0$ 和 $xy = xz$ 蕴涵 $x(y-z) = 0$, 因而蕴涵 $y = z$. 域自动是整环, 这是因为 $x \neq 0$ 和 $xy = 0$ 给出 $y = x^{-1}xy = x^{-1} \cdot 0 = 0$.

例 2.1.6: 同余类构成的环

设 $n \in \mathbb{Z}$. 选定 $n \in \mathbb{Z}$, 记 $\mathbb{Z}$ 对等价关系 $\bmod n$ 的商集[a]为 $\mathbb{Z}/n\mathbb{Z}$, 或简记为 $\mathbb{Z}n$; 其中的等价类也称为 $\bmod n$ **同余类**. 在 $\mathbb{Z}/n\mathbb{Z}$ 上定义加法和乘法运算如下

$$[x][y] := [xy], \quad [x] + [y] := [x + y],$$

其中 $x, y \in \mathbb{Z}$. 运算是良定义的, 也就是说运算产物仅依赖同余类 $[x]$ 和 $[y]$ 而不是 x 和 y 的具体取法, 这是容易由初等数论的知识证明的. 取 $0_{\mathbb{Z}/n\mathbb{Z}} := [0], 1_{\mathbb{Z}/n\mathbb{Z}} := [1]$, 立见 $\mathbb{Z}/n\mathbb{Z}$ 对此运算成为交换环. 注意到 $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}$ 而 $\mathbb{Z}/(-n)\mathbb{Z} = \mathbb{Z}/n\mathbb{Z}$, 因此以下不妨设 $n \in \mathbb{Z}_{\geqslant 1}$, 此时 $\mathbb{Z}/n\mathbb{Z}$ 恰有 n 个元素; 它是零环当且仅当 $n = 1$.

[a]请看笔者上一篇文章高等代数笔记 3：线性空间-> 线性映射 - 晨锦辉永生之语的文章 - 知乎`https://zhuanlan.zhihu.com/p/1890514261077381838`

注意到 $[x] \in (\mathbb{Z}/n\mathbb{Z})^\times$ 相当于说同余式 $xy \equiv 1 \pmod{n}$ 有解 $y \in \mathbb{Z}$. 根据 Bézout 定理, 此式有解等价于 x 和 n 互素; 换言之,

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{[x] : x \in \mathbb{Z}, x, n \text{ 互素}\};$$

基于 Euler 函数 $\mathcal{A}$ 的定义[2], 由此就得出 $|(\mathbb{Z}/n\mathbb{Z})^\times| = \mathcal{A}(n)$. 作为推论,

$$\mathbb{Z}/n\mathbb{Z} \text{ 为域} \iff \mathcal{A}(n) = n - 1 \iff n \text{ 为素数}.$$

我们也容易证明，$\mathbb{Z}/n\mathbb{Z}$ 为整环当且仅当它是域.

设 p 为素数. 域 $\mathbb{Z}/p\mathbb{Z}$ 是有限域的初步例子. 鉴于它的重要性, 我们另外引入符号

$$\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}.$$

定义 2.1.7: 环的直积

取一族环 $(R_i)_{i \in I}$, 下标 i 遍历某个非空集 I. 下面使用某种途径从已有的环构造新环，称作 $(R_i)_{i \in I}$ 的**直积**.

[2]$\mathcal{A}(n)$ 定义为不超过 n 而与 n 互素的正整数个数，也即正是与 n 互素的 mod n 同余类个数.

(1) 在 $\prod_{i\in I} R_i$ 上逐分量地定义加法和乘法, 分别写作

$$\underbrace{(r_i)_i + (r_i')_i := (r_i + r_i')_{i\in I}}_{\prod_i R_i \text{的加法}}, \quad \underbrace{(r_i)_i \cdot (r_i')_i := (r_i \cdot r_i')_{i\in I}}_{\prod_i R_i \text{的乘法}}.$$

(2) 定义零元 0 为 $(0_i)_i$, 幺元 1 为 $(1_i)_i$, 下标 i 代表它们分别是 R_i 中的零元和幺元.

这样我们就可以在每个 R_i 上来检验环的定义2.1.1, 就以加法结合律为例:

$$((r_i)_i + (r_i'')_i) + (r_i')_i = ((r_i + r_i'') + r_i')_i = (r_i + (r_i' + r_i''))_i = (r_i)_i + (r_i')_i + (r_i'')_i,$$

其他情形也是类似的. 容易看出 $-(r_i)_i = (-r_i)_i$. 若 $I = \{1, \ldots, n\}$, 对应的直积也写作 $R_1 \times \cdots \times R_n$ 的形式.

接着考虑每个 R_i 都是同一个环 R 的特例, 这时 $\prod_{i\in I} R_i$ 化为映射集 $R^I = \{f : I \to R\}$ 相对于逐点或逐元素的运算

$$(f + g)(i) := f(i) + g(i), \quad (fg)(i) := f(i)g(i), \quad i \in I$$

所成的环, 方式是让 f 对应 $(f(i))_{i\in I} \in \prod_{i\in I} R$; 特别地, 0_{R^I} 是常值映射 $i \mapsto 0_R$, 而 1_{R^I} 是常值映射 $i \mapsto 1_R$.

2.2 同态与同构

定义 2.2.1: 环同态

设 $f : R \to R'$ 为环之间的映射. 当以下条件成立时, 称 f 为**环同态**:

1. $f(x + y) = f(x) + f(y)$,
2. $f(xy) = f(x)f(y)$,
3. $f(1_R) = 1_{R'}$,

其中 x, y 取遍 R 的元素. 从环 R 映到其自身的同态也称为 R 的**自同态**.

由定义不难推出环同态的一些性质:

1. **保持零元:** $f(0_R) = 0_{R'}$.

证明. 从 $f(0_R) = f(0_R + 0_R) = f(0_R) + f(0_R)$, 配合 R' 中的加法消去律, 即得 $f(0_R) = 0_{R'}$. □

2. **保持加法逆元：** $f(-x) = -f(x)$. 这是 $0_{R'} = f(0_R) = f(x + (-x)) = f(x) + f(-x)$ 的推论.

3. **保持乘法逆元：** 若 $x \in R^\times$, 则 $f(x) \in (R')^\times$ 而 $f(x^{-1}) = f(x)^{-1}$, 这是因为 $1_{R'} = f(1_R) = f(xx^{-1}) = f(x)f(x^{-1})$.

4. **恒等自同态：** 任何环 R 到它自身的恒等映射 id_R 自动是环同态, 这是环同态的平凡例子.

5. **同态的合成：** 若 $f : R \to R'$ 和 $g : R' \to R''$ 为环同态, 则 $gf : R \to R''$ 也是环同态. 这是因为

$$
\begin{aligned}
gf(x+y) &= g(f(x)+f(y)) = gf(x) + gf(y),\\
gf(xy) &= g(f(x)f(y)) = gf(x)gf(y),\\
gf(1_R) &= g(1_{R'}) = 1_{R''}.
\end{aligned}
$$

6. **像与子环：** 对于环同态 $f : R \to R'$, 它的像 $f(R)$ 自然是 R' 的子环; 反过来说, 给定环 R' 及其子环 $R \subset R'$, 取 $\iota : R \to R'$ 为包含映射, 映 $r \in R$ 为 r, 则 ι 自然是环同态.

例 2.2.1: 同余类上的环同态

设 $n, m \in \mathbb{Z}$ 满足 $n \mid m$，考虑映射

$$
\begin{aligned}
p_n^m : \mathbb{Z}/m\mathbb{Z} &\to \mathbb{Z}/n\mathbb{Z}\\
[x]_m &\mapsto [x]_n.
\end{aligned}
$$

首先这是良定义的，对于任意 $x, y \in \mathbb{Z}$，成立

$$x \equiv y \pmod m \iff m \mid x - y \implies n \mid x - y \iff x \equiv y \pmod n.$$

根据同余类中加法和乘法的运算法则，我们有

$$p_m^n([x]_m + [y]_m) = p_m^n([x+y]_m) = [x+y]_n = [x]_n + [y]_n = p_m^n([x]_m) + p_m^n([y]_m).$$

同理容易验证

$$p_m^n([x]_m[y]_m) = p_m^n([x]_m)p_m^n([y]_m),$$

这表明 p_m^n 是环同态.

定义 2.2.2: 环同构

设 $f: R \to R'$ 为环同态. 如果存在环同态 $g: R' \to R$ 使得 $gf = \mathrm{id}_R$ 而 $fg = \mathrm{id}_{R'}$, 则称 f 为**环同构**, 而 g 为 f 的逆. 此时我们也说 R 和 R' **同构**.

可以用符号 $f: R \xrightarrow{\sim} R'$ 代表映射 $f: R \to R'$ 是环同构; 在不必指明 f 的场合, 我们也以符号 $R \simeq R'$ 代表环 R 和 R' 同构.

条件 $gf = \mathrm{id}_R$ 和 $fg = \mathrm{id}_{R'}$ 表明 f 的逆无非是 f 作为映射的逆 $g = f^{-1}$. 反过来说, 容易证环同态 f 如果作为映射是双射, 那么它也是环同构.

命题 2.2.1: 同态 + 双射 = 同构

设 $f: R \to R'$ 为环同态. 如果 f 是集合之间的双射, 则 f 是环同构.

证明. 问题归结为证 f 的逆映射 f^{-1} 也是环同态. 对 $f(1_R) = 1_{R'}$ 两边取 f^{-1} 可得 $1_R = f^{-1}(1_{R'})$. 对 $f(x+y) = f(x) + f(y)$ 两边取 f^{-1}, 并且记 $u = f(x)$, $v = f(y)$, 可得 $f^{-1}(u) + f^{-1}(v) = f^{-1}(u+v)$. 同理可见 $f^{-1}(uv) = f^{-1}(u)f^{-1}(v)$. 由于所有 $u, v \in R'$ 都能表作 $u = f(x)$ 和 $v = f(y)$ 的形式, 综上可见 f^{-1} 确实是环同态. □

恒等映射 id_R 是同构最简单的例子. 此外, 两个同构 f 和 g 的合成 gf 依然是同构, 以 $f^{-1}g^{-1}$ 为逆.

同构 $f: R \simeq R'$ 不但为集合 R 和 R' 建立了双射, 而且对应元素之间的一切环论运算 (加法, 乘法) 和幺元也在 f 之下相配对. 凡是以环论语言表达的一切性质, 对于同构的环 R 和 R' 都是等价的. 这是代数学中的一条基本原理.

命题 2.2.2

设 $\mathbb{F}$ 为域, R 为非零环, 而 $\mathcal{A}: F \to R$ 为环同态. 证明: $\mathcal{A}$ 为单射.

证明. 我们有 $\mathcal{A}(x) = \mathcal{A}(y) \iff \mathcal{A}(x-y) = 0$, 所以问题化为证 $x \neq 0 \implies \mathcal{A}(x) \neq 0$. 但是域 F 中的任意非零元都是可逆的, 而同态映可逆元为可逆元. □

定理 2.2.1 (中国剩余定理—同构版本). 设 $N = n_1 \cdots n_k$, 其中 $n_1, \ldots, n_k \in \mathbb{Z}_{\geqslant 1}$ 两两互素, 则有环同构

$$\begin{aligned} \mathcal{A} : \mathbb{Z}/N\mathbb{Z} &\xrightarrow{\sim} \prod_{i=1}^{k} \mathbb{Z}/n_i\mathbb{Z} \\ [x]_N &\longmapsto ([x]_{n_i})_{i=1}^{k}. \end{aligned}$$

证明. 例2.2.1业已说明 $[x]_N \mapsto [x]_{n_i}$ 对所有 i 都给出同态 $\mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/n_i\mathbb{Z}$. 既然直积的环结构是逐分量定义的, $\mathcal{A}$ 必保持环结构, 从而是同态.

此外, 映射两端作为集合都有 N 个元素, 基于抽屉原理, 证 $\mathcal{A}$ 是单射即可. 互素条件在此派上用场: 设 $x, y \in \mathbb{Z}$ 满足 $\mathcal{A}([x]_N) = \mathcal{A}([y]_N)$, 则对所有下标 i 都有

$$n_i \mid x - y.$$

既然 $n_1, \ldots, n_k$ 两两互素, 故 $N \mid x - y$, 亦即 $[x]_N = [y]_N$. 单性得证. □

2.3 分式域

设 R 为整环. 我们考虑集合

$$\mathrm{Ratio}(R) := \{(f, g) \in R^2 : g \neq 0\}.$$

在 $\mathrm{Ratio}(R)$ 上定义二元关系

$$(f_1, g_1) \sim (f_2, g_2) \iff f_1 g_2 = f_2 g_1.$$

这是一个等价关系. 反身性和对称性是显然的，只需简单验证传递性：设 $(f_1, g_1) \sim (f_2, g_2)$ 而 $(f_2, g_2) \sim (f_3, g_3)$，则 R 的交换性导致

$$(f_1 g_2) g_3 = (f_2 g_1) g_3 = (f_2 g_3) g_1 = (f_3 g_2) g_1.$$

因为 R 是整环，两边消去非零元 g_2 便得到 $f_1 g_3 = f_3 g_1$，亦即 $(f_1, g_1) \sim (f_3, g_3)$.

定义商集 $\mathrm{Frac}(R) := \mathrm{Ratio}(R)/\sim$. 接着来赋予 $\mathrm{Frac}(R)$ 环结构.

定义 2.3.1: Frac(R) 的环结构

(1) **加法和乘法.** 规定加法和乘法运算：

$$\frac{f_1}{g_1} + \frac{f_2}{g_2} := \frac{f_1 g_2 + g_1 f_2}{g_1 g_2}, \tag{9}$$

$$\frac{f_1}{g_1} \cdot \frac{f_2}{g_2} := \frac{f_1 f_2}{g_1 g_2}. \tag{10}$$

不难验证，(9)式和 (10) 式不依赖于等价类中代表的选择（即良定义的）. 以(9)式为例. 设 $\frac{f_1}{g_1} = \frac{f_1'}{g_1'}, \frac{f_2}{g_2} = \frac{f_2'}{g_2'}$，则

$$f_1 g_1' = g_1 f_1', \quad f_2 g_2' = g_2 f_2',$$

于是有

$$f_1 g_1'(g_2 g_2') = g_1 f_1'(g_2 g_2'), \tag{11}$$

$$f_2 g_2'(g_1 g_1') = g_2 f_2'(g_1 g_1'). \tag{12}$$

(11)式与 (12) 式相加，得

$$f_1 g_1' g_2 g_2' + f_2 g_2' g_1 g_1' = g_1 f_1' g_2 g_2' + g_2 f_2' g_1 g_1',$$

由此得出

$$\frac{f_1 g_2 + g_1 f_2}{g_1 g_2} = \frac{f_1' g_2' + g_1' f_2'}{g_1' g_2'},$$

即

$$\frac{f_1}{g_1} + \frac{f_2}{g_2} = \frac{f_1'}{g_1'} + \frac{f_2'}{g_2'}. \tag{13}$$

类似地可以证明，用 (10) 式规定 R 中的乘法运算是合理的. 容易验证，上述定义的加法和乘法都满足交换律、结合律，并且满足分配律.

(2) **零元.** $\frac{0}{1}$ 是 Frac(R) 中的零元，记作 0；根据环的性质，可以定义 $\frac{f}{g}$ 的负元 $\frac{-f}{g} = -\frac{f}{g}$.

(3) **乘法幺元.** $\frac{1}{1}$ 是 Frac(R) 的单位元，记作 1.

不难验证，在上述定义下，Frac(R) 成为**交换环**[3].

事实上，由定义2.1.5，Frac(R) 构成一个域，称为整环 R 的**分式域**.

[3]当然含幺.

命题 2.3.1: 分式域

交换（除）环 $\mathrm{Frac}(R)$ 的非零元皆可逆.

证明. 对于 $\mathrm{Frac}(R)$ 中每一个非零元 $\dfrac{f}{g}$，都存在 $\dfrac{g}{f} \in \mathrm{Frac}(R)$，使得

$$\frac{f}{g} \cdot \frac{g}{f} = \frac{fg}{gf} = \frac{1}{1} = 1, \quad \frac{g}{f} \cdot \frac{f}{g} = \frac{gf}{fg} = \frac{1}{1} = 1,$$

这表明 $\dfrac{f}{g}$ 是可逆的，$\dfrac{g}{f}$ 是 $\dfrac{f}{g}$ 的逆元，记作 $\left(\dfrac{f}{g}\right)^{-1}$，即

$$\left(\frac{f}{g}\right)^{-1} := \frac{g}{f}.$$

由于 $\mathrm{Frac}(R)$ 的每个非零元都可逆，因此可以在 $\mathrm{Frac}(R)$ 中定义除法如下：
设 $\dfrac{f_2}{g_2} \neq 0$，对于任意 $\dfrac{f_1}{g_1} \in \mathrm{Frac}(R)$，规定

$$\frac{f_1}{g_1} \Big/ \frac{f_2}{g_2} := \frac{f_1}{g_1} \cdot \left(\frac{f_2}{g_2}\right)^{-1}.$$

再将 $\mathrm{Frac}(R)$ 中的减法运算的定义取环中的减法定义即可. □

注记. 此时映射 $f \mapsto [f, 1]$ 将 R 自然地嵌入为 $Frac(R)$ 的子环.

分式的基本性质现在可以证明如下：设 $\dfrac{f}{g} \in R$. 任取 $h(x) \in R \setminus \{0\}$，由于 $fgh = gfh$，因此

$$\frac{f}{g} = \frac{fh}{gh}, \tag{14}$$

将 (14) 式从右到左看，即得到：分子与分母可以消去同一个非零公因式.

引理 2.2

对于一个非零的分式 $\dfrac{f}{g}$，分子的次数减去分母的次数所得的差 $\deg f - \deg g$ 不依赖于等价类的代表的选取.

证明. 设 $\dfrac{f}{g} = \dfrac{f_1}{g_1}$，则 $fg_1 = gf_1$，从而 $\deg f + \deg g_1 = \deg g + \deg f_1$. 因此

$$\deg f - \deg g = \deg f_1 - \deg g_1.$$

□

因此把 $\deg f - \deg g$ 称为分式 $\dfrac{f}{g}$ 的次数. 分式 $\dfrac{0}{1}$ 的次数为 $-\infty$.
类似于一元分式域的构造方法，我们还可以构造出 R 上的 n 元分式域.

2.4 多项式环与多项式函数

按照多项式的加法和乘法的具体定义，当下看出

$$(f+g)(x,y,\ldots)=f(x,y,\ldots)+g(x,y,\ldots),$$
$$(fg)(x,y,\ldots)=f(x,y,\ldots)g(x,y,\ldots),$$

(常数多项式 $c)(x,y,\ldots)=c$.

因此每个多项式 $f\in R[X,Y,\ldots]$ 都确定从 $R\times R\times\cdots$ (乘积项数 = 变元个数) 到 R 的映射，这是多项式 f 所确定的多项式函数。

例 3.3.5 对于一般的交换环 R，多项式未必由它对应的多项式函数确定。一个例子是取 $R=\mathbb{F}_p:=\mathbb{Z}/p\mathbb{Z}$，其中 p 是素数。根据 Fermat 小定理 2.8.6，单变元多项式

$$f(X)=X^p-X\in\mathbb{F}_p[X]$$

对所有 $x\in\mathbb{F}_p$ 都满足 $f(x)=0$，所以尽管 X^p-X 并非零多项式，它作为多项式函数却无异于零函数。推而广之，对于任意有限域 F，非零多项式 $f(X):=\prod_{a\in F}(X-a)$ 在任何 $a\in F$ 上取值皆为 0。

有鉴于此，对于一般的交换环，必须区分作为一个代数表达式的多项式以及相应的函数或映射，前者才是第一义的。我们将在 §3.6 说明何时可以等同一个多项式及它所对应的函数。

2.5 域的特征

我们用 0_R 代表环 R 的零元，用 1_R 代表 R 的幺元，作为区分.

我们常见的域（如 $\mathbb{Q},\mathbb{R},\mathbb{C}$ ）中，成立

$$(\forall)n\cdot 1_F=0_F \iff n=0, \tag{15}$$

而域 $F=\mathbb{F}_p$ 中成立

$$p\cdot 1_F=0_F; \tag{16}$$

这又蕴涵了对于任意 $x\in F$ 都有 $px=(p\cdot 1_F)\cdot x=0_F$.

性质(16)并非有限域独有. 考虑 $\mathbb{F}_p$ 上的有理函数域 $\mathbb{F}_p(X)$，它有无穷多个元素，但也满足 $p\cdot 1_{\mathbb{F}_p(X)}=0_{\mathbb{F}_p(X)}$，这点只须在其子域 $\mathbb{F}_p$ 里验证.

引理 2.3

对于任意环 R，存在唯一的环同态

$$\mathbb{Z}\longrightarrow R$$

$$n \longmapsto n \cdot 1_R.$$

证明. 唯一性：注意到环同态必然映 1 为 1_R，从而映 $n \geq 0$ 为 $1_R + \cdots 1_R = \underbrace{n \cdot 1_R}_{n\text{ 项}}$，而在 $n < 0$ 时映 $n = -|n|$ 为 $-(|n| \cdot 1_R) = n \cdot 1_R$.

存在性问题则归结为检验 $n \mapsto n \cdot 1_R$ 确实是环同态，这是容易验证的. □

定义 2.5.1: 特征

设 R 为整环，若存在唯一的 $\mathrm{char}(R) \in \mathbb{Z}_{\geq 0}$ 使得对所有 $n \in \mathbb{Z}$ 都有

$$n \cdot 1_R = 0_R \iff \mathrm{char}(R) \mid n,$$

称之为整环 R 的**特征**；它或者是 0，或者是素数.

证明. 记 $K_R := \{n \in \mathbb{Z} : n \cdot 1_R = 0_R\}$，它包含 0，对加法封闭，而且若 $n \in K_R$ 而 $m \in \mathbb{Z}$，则 $mn \cdot 1_R = (m \cdot 1_R)(n \cdot 1_R) = 0_R$ 蕴涵 $mn \in K_R$. 基于这两种封闭性，引理 2.3 遂说明存在唯一的 $\mathrm{char}(R) \in \mathbb{Z}_{\geq 0}$ 使得 $K_R = \mathrm{char}(R)\mathbb{Z}$. 设 $\mathrm{char}(R) \neq 0$，而且有因数分解 $\mathrm{char}(R) = ab$，则因为 $n \mapsto n \cdot 1_R$ 是环同态，故

$$\mathrm{char}(R) \cdot 1_R = (a \cdot 1_R)(b \cdot 1_R) = 0_R.$$

又因为 R 是整环，必有 $a \in K_R$ 或 $b \in K_R$，因此必有 $\mathrm{char}(R) \mid a$ 或 $\mathrm{char}(R) \mid b$；留意到 $\mathrm{char}(R) \neq 1$（否则将有 $1_R = 0_R$）. 这足以说明 $\mathrm{char}(R)$ 若非零则必为素数.

因此在特征为 $p > 0$ 的整环 R 中，任意 $x \in R$ 的 p 倍必然为零：$px = (p \cdot 1_R)x = 0_R x = 0_R$. □

例 2.5.1

设 p 为素数，而 R 为满足 $p \cdot 1_R = 0_R$ 的交换环（例如特征 p 的整环），则对所有 $x, y \in R$ 皆有

$$(x+y)^p = x^p + y^p.$$

证明. 利用二项式定理，只需证明二项式系数 $\binom{p}{k}$ 在 $0 < k < p$ 时总是 p 的倍数. 注意到

$$p \cdot \frac{(p-1)!}{(k-1)!(p-k)!} = k \cdot \frac{p!}{k!(p-k)!} = k\binom{p}{k},$$

且 $(k,p) = 1$，这就证明了 $p \mid \binom{p}{k}$. □

命题 2.5.1

若 R_0 是整环 R 的子环，则 $\mathrm{char}(R_0) = \mathrm{char}(R)$.

证明. 本书规定子环 R_0 必满足 $1_R = 1_{R_0}$，所以等式 $n \cdot 1_R = 0_R$ 成立与否可以在子环 R_0 中判定. □ □

整环 R 的特征和它的分式域的特征是一回事：诚然，根据命题 3.7.4，从 $R \subset \mathrm{Frac}(R)$ 可见 $\mathrm{char}(R) = \mathrm{char}(\mathrm{Frac}(R))$.

命题 2.5.2

设 E 和 F 为域，$\mathrm{char}(E) \neq \mathrm{char}(F)$，证明：不存在从 E 到 F 的环同态.

证明. 利用命题2.2.2. $\bullet sjjpj$ □

因此，不同特征的域无法直接沟通，除非通过一个较大的整环相联系，例如

$$\mathbb{F}_p \xleftarrow{\text{商映射}} \mathbb{Z} \xleftarrow{\text{包含}} \mathbb{Q},$$

或者是运用更复杂的代数或数论技术.

2.6 理想

2.6.1 理想

定义 2.6.1: 理想

环 R 的一个理想 I 是 R 的满足下列性质的非空子集[a]：

- I 在加法下封闭.
- 如果 $s \in I, r \in R$, 则 $rs \in I$，并且 $s \in I, t \in R$, 则 $st \in I$.

[a]不同的教材对理想的定义也不太一样，与环的定义有一定的关系.

注记. 由于定义中不要求 R 交换，所以乘法封闭性必须对双边来陈述；对于非交换环，我们也经常将上述定义中的理想称为 R 的 **双边理想**. 从上述定义中容易给出**左理想**、**右理想**的定义. 本笔记所指理想均为**双边理想**.

理想自动对加法逆元封闭：若 $x \in I$ 则 $-x \in I$，这是基于环论的等式 $-x = (-1) \cdot x$ 和理想的乘法封闭性. 理想的平凡例子有 $I = \{0\}$（零理想）和 $I = R$. 满足 $I \neq R$ 的理想 I 称为**真理想**.

命题 2.6.1

设 I 是 R 的理想，则 $I=R \iff 1\in I$.

证明. “$\implies$”显然. “$\impliedby$”. 若 $1\in I$，则 $\forall r\in R, r=1\cdot r\in I$. □

这表明，真理想不可能是 R 的子环，因为它不含乘法幺元 1.

例 2.6.1: 整数环的理想

整数环 $\mathbb{Z}$ 的任一子环必形如 $m\mathbb{Z}, m\geqslant 0$. 容易用理想的定义验证 $m\mathbb{Z}$ 是 $\mathbb{Z}$ 的理想，因此 $m\mathbb{Z}, m\geqslant 0$ 也是 $\mathbb{Z}$ 所有的理想.

例 2.6.2: 函数环的理想

考虑 $C(\mathbb{R})$. 取定 $x_0\in\mathbb{R}$，定义

$$Z_{x_0}(\mathbb{R})=\{f\in C(\mathbb{R}) \mid f(x_0)=0\},$$

则 $Z_{x_0}(\mathbb{R})$ 是 $C(\mathbb{R})$ 的理想.

函数环的另一个理想在微分几何中有重要作用. 设 x 为 $\mathbb{R}^n$ 中的一点，在 $C^\infty(\mathbb{R}^n)$ 中我们定义

$$O_x=\{f\in C^\infty(\mathbb{R}^n) \mid \text{存在}x\text{ 的一个邻域}U,\ \text{使得} f(y)=0,\ \forall y\in U\}.$$

则容易验证 O_x 是 $C^\infty(\mathbb{R}^n)$ 的一个理想.

给定了理想，如何构造新的理想呢？容易证明一个环的任意多个理想之交仍为理想. 现在设 S 为环 R 的非空子集，则 R 中所有包含 S 的理想（这样的理想是存在的，例如 R 本身就是一个）之交仍为 R 的理想，称为由 S 生成的理想，记为 $\langle S\rangle$. 我们断言 $\langle S\rangle$ 是 R 中包含集合 S 的最小理想. 事实上，由上面的定义，$\langle S\rangle$ 是理想，且包含 S. 另一方面，因为 $\langle S\rangle$ 是所有包含 S 的理想之交，因此任何包含 S 的理想一定包含 $\langle S\rangle$，因此 $\langle S\rangle$ 是最小的.

例 2.6.3: 包含理想的最小理想

我们证明

$$\langle S\rangle=\left\{\sum_{i=1}^n x_ia_i \,\middle|\, n\in\mathbb{N}, x_i\in R, a_i\in S, i=1,2,\cdots,n\right\}.$$

事实上，将上式右边的集合记为 I. 则对任何 $a\in S$, $a=1\cdot a\in I$（1 为 R 的幺元），故 $S\subseteq I$. 又由命题 2.2.11 容易看出 I 是 R 的理想. 另一方面，若 I_1 为 R 的一个理想且包含 S，则对任何 $x_i\in R$，以及 $a_i\in S, 1\leqslant i\leqslant n$，有 $x_ia_i\in I_1$，故 $\sum x_ia_i\in I_1$. 故 $I\subseteq I_1$，这说明 I 是包含 S 的最小理想，因此 $I=\langle S\rangle$.

定义 2.6.2: 主理想与生成元

设 I 为环 R 的理想，如果存在 $a \in I$ 使得 $I = \langle a \rangle$，则称 I 为主理想，而 a 称为 I 的一个生成元.

命题 2.6.2: 环同态的核

设 $f : R \to R'$ 为环同态，其核（又称零核）定义为

$$\ker(f) := f^{-1}(0) = \{x \in R : f(x) = 0\}.$$

这是 R 的理想.

证明. 首先验证加法封闭：若 $x, y \in \ker(f)$，则 $f(x+y) = f(x) + f(y) = 0 + 0 = 0$，故 $x + y \in \ker(f)$. 其次验证乘法双边封闭. 若 $x \in \ker(f)$ 而 $r \in R$，则

$$f(xr) = f(x)f(r) = 0 \cdot f(r) = 0 = f(r) \cdot 0 = f(r)f(x) = f(rx),$$

因此 $xr, rx \in \ker(f)$. □

2.6.2 商环

3 模

定义 3.0.1: 模

所谓左 R-模，是指

1. 加法群；
2. 映射 $R \times M \to M$，以乘法记号记为 $(r, m) \mapsto r \cdot m = rm$，也称为模的纯量乘法，满足如下条件：

   - $r(m_1 + m_2) = rm_1 + rm_2$,
   - $(r_1 + r_2)m = r_1 m + r_2 m$,
   - $(r_1 r_2)m = r_1(r_2 m)$,
   - $1_R m = m$.

   其中 $r_1, r_2 \in R$ 而 $m, m_i (i = 1, 2) \in M$.

类似可以定义右 R-模.

可以看出，模是线性空间定义的推广，相当于环上的线性空间.

4 有理标准形

4.1 线性映射和模结构

4.2 有理标准形

参考文献

[1] 谢启鸿, 姚慕生, 吴泉水. 高等代数学（第四版）. 上海：复旦大学出版社, 2022.

[2] 谢启鸿, 姚慕生. 高等代数（第四版）. 上海：复旦大学出版社, 2022.

[3] 丘维声. 高等代数（第二版，上册）. 北京：清华大学出版社, 2018. 上海：复旦大学出版社, 2022.

[4] 丘维声. 高等代数（第二版，下册）. 北京：清华大学出版社, 2018.

[5] 邓少强, 朱富海. 抽象代数. 北京：科学出版社，2017.

[6] 李文威. 代数学讲义. 网络版（编译日期: 2025-04-04），来自`https://www.wwli.asia/downloads/books/EAlg-Notes.pdf`