线性代数笔记

章小明

2023 年 7 月 16 日

目录

前言

本书为本人自用的线性代数笔记, 因此省略了大量已学过或本人觉得无需加入 (赘述) 的内容, 如矩阵的基础运算, 向量空间的定义, 群环域的定义与基本性质, 矩阵与线性映射之间的自然联系, 因为本人认为这些都是易知而无需多番叙述的, 更非线性代数的重点.

本笔记中将尽量少地出现易知的定义, 如核与像或多重线性. 相应的, 本人将在本笔记中加入一些在一般的线性代数教材中不着重强调或不出现的内容.

本书蓝本为丘维声的《高等代数》, 参考书为李炯生的《线性代数》与 А.И.Кострикин 的《代数学引论》第二卷.

本书服从本人自身的排版意愿, 所有的外文人名也尽量使用源语言拼法.

符号表

$\mathbb{R}$ 表示实数域,$\mathbb{C}$ 表示复数域.$\mathbb{F}$ 一般表示一般的域, 有时表示 $\mathbb{R}$ 或 $\mathbb{C}$, 取决于章节前的说明.

$\mathbb{F}^{m\times n}$ 指数域 $\mathbb{F}$ 中的 $m\times n$ 阶矩阵全集,$M_n(\mathbb{F})=\mathbb{F}^{n\times n}$. 记 $\mathbb{F}^{m\times n}$ 中元素 $A=(a_{ij})_{m\times n}$, 这表明其有 m 行 n 列, 且默认记 a_{ij} 为其第 i 行第 j 列的交叉元. 记 $A^{(i)}$ 为矩阵 A 的第 i 列构成的向量,$A_{(i)}$ 为第 i 行构成的向量.

S_n 指 n 阶对称群,$\mathrm{GL}_n(\mathbb{F}):=\{A\in M_n(\mathbb{F}):\det A\neq 0\}$ 指数域 $\mathbb{F}$ 上的一般线性群,$\mathrm{SL}_n(\mathbb{F}):=\{A\in M_n(\mathbb{F}):\det A=1\}$ 指数域 $\mathbb{F}$ 上的特殊线性群.

方阵 A 的行列式可记作 $\det A$, 不作混淆的部分情况下也记作 $|A|$.

$\tau(\cdot)$ 为逆序数,$\varepsilon_\pi=(-1)^{\tau(\pi(1)\cdots\pi(n))}$ 为置换 $\pi\in S_n$ 的符号.

Chapter 1

预备知识

1.1 行列式

定义 1 (行列式)**.** 对 $A \in M_n(\mathbb{F})$ 有 $\det A := \sum_{\pi \in S_n} \varepsilon_\pi \prod_{i=1}^{n} a_{i,\pi(i)}$.

值得一提的是, 行列式概念源于对 n 个 n 维向量组成的平行多面体的**有向**体积的计算, 其中向量的坐标成为了行列式的元素. 因此也可以将行列式视为, 从单位 n 维立方体作线性变换 A(即对应的矩阵 A) 后有向体积的变换系数. 事实上我们后面会看到, 行列式即线性变换的特征值之积. 不难发现下面的基本性质在有向体积的计算中是显然的. 对行列式可以从下面的性质中取公理化定义, 即将行列式函数当作一个多重线性斜对称映射, 且满足下列的某些性质, 即可得到其他所有性质. 而行列式的上述置换定义实际上就是通过下面的性质对行列式中元素直接进行计算得来的, 在此我们不论述此处逆序数的出现的原因.

行列式的基本性质

1. 行列互换, 行列式不变
2. 可提取一行公因子
3. 若行列式中一行/列为两组数之和, 则行列式为对应的两个行列式之和
4. 两行/列互换, 行列式反号
5. 两行/列相同或成比例, 行列式为 0
6. 将一行的倍数加到另一行上, 行列式不变

行列式的展开 行列式 $\det A$ 的 $m \le n$ 阶子式记作 $A\begin{pmatrix} i_1 & \cdots & i_m \\ j_1 & \cdots & j_m \end{pmatrix}$, 其余子式记作 $A^c\begin{pmatrix} i_1 & \cdots & i_m \\ j_1 & \cdots & j_m \end{pmatrix}$, 代数余子式定义为 $(-1)^{\sum_{k=1}^{m}(i_k+j_k)} A^c\begin{pmatrix} i_1 & \cdots & i_m \\ j_1 & \cdots & j_m \end{pmatrix}$.$m = 1$ 时 $M_{ij} := A^c\begin{pmatrix} i \\ j \end{pmatrix}, A_{ij} := (-1)^{i+j} M_{ij}$.

定理 1.1 (Lapalce 展开定理)**.** *对于 $A \in M_n(\mathbb{F})$, 取定第 $i_1, \cdots, i_m$ 行 $(i_1 < \cdots < i_m)$, 则这 m 行形成的所有 m 阶子式与其对应的代数余子式之积的和 $= \det A$, 即*

$$\det A = \sum_{1 \le j_1 < j_2 < \cdots < j_m \le n} A\begin{pmatrix} i_1 & \cdots & i_m \\ j_1 & \cdots & j_m \end{pmatrix} (-1)^{\sum_{k=1}^{m}(i_k+j_k)} A^c\begin{pmatrix} i_1 & \cdots & i_m \\ j_1 & \cdots & j_m \end{pmatrix}.$$

特别地,

$$\det A = \sum_{i=1}^{n} a_{ki} A_{ki}, \qquad \sum_{i=1}^{n} a_{ki} A_{li} = 0 (k \ne l).$$

证明. 注意到 LHS 为 $n!$ 项的代数和, 因此仅需说明 RHS 加式也有在 $\det A$ 中不重复的 $n!$ 项. 注意到 k 阶子式及余子式分别有 $k!$ 项和 $(n-k)!$ 项, 因此 RHS 有 $\binom{n}{k} k!(n-k)! = n!$ 项, 下证其在 $\det A$ 中不重复.RHS 展开式中每一项形

如

$$(-1)^{\tau(\mu_1\cdots\mu_m)}\prod_{k=1}^{m}a_{i_k\mu_k}\cdot(-1)^{\sum_{k=1}^{m}(i_k+j_k)}\cdot(-1)^{\tau(\nu_1\cdots\nu_m)}\prod_{k=1}^{n-m}a_{i'_k\nu_k},$$

其中 $\{i'_1,\cdots,i'_{n-m}\}=[n]-\{i_1,\cdots,i_m\},\mu=(\mu_1\cdots\mu_m)$ 是 $j_1,\cdots,j_m$ 的排列, 而 $\nu=(\nu_1\cdots\nu_{n-m})$ 是 $[n]$ 中剩下元素的排列. 注意到 LHS 含有一项

$$(-1)^{\tau(i_1\cdots i_m i'_1\cdots i'_{n-m})+\tau(\mu_1\cdots\mu_m\nu_1\cdots\nu_{n-m})}\prod_{k=1}^{m}a_{i_k\mu_k}\prod_{k=1}^{n-m}a_{i'_k\nu_k}$$

故仅需考虑符号是否相同. 假设排列 $(\mu_1\cdots\mu_m\nu_1\cdots\nu_{n-m})$ 在 s 次对换变为 $(\mu'_1\cdots\mu'_m\nu_1\cdots\nu_{n-m})$, 且前 m 项单增, 则 s 与 $\tau(\mu)$ 同奇偶. 而另一方面,$(\mu'_1\cdots\mu'_m\nu_1\cdots\nu_{n-m})$ 中 μ'_k 后比其小的数有 μ'_k-k 个, 因此最终可知

$$(-1)^{\tau(\mu_1\cdots\mu_m\nu_1\cdots\nu_{n-m})}=(-1)^{\tau(\mu_1\cdots\mu_m)}(-1)^{\sum_{k=1}^{m}(\mu_k-k)+\tau(\nu_1\cdots\nu_{n-m})}=(-1)^{\tau(\mu)+\tau(\nu)+\sum\mu_k+\frac{m(m+1)}{2}}=(-1)^{\tau(\mu)+\tau(\nu)+\sum j_k+\frac{m(m+1)}{2}}$$

因此

$$\begin{aligned}(-1)^{\tau(i_1\cdots i_m i'_1\cdots i'_{n-m})+\tau(\mu_1\cdots\mu_m\nu_1\cdots\nu_{n-m})}=&(-1)^{\sum i_k+\frac{m(m+1)}{2}}(-1)^{\tau(\mu)+\tau(\nu)+\sum j_k+\frac{m(m+1)}{2}}\\=&(-1)^{\tau(\mu)+\tau(\nu)}(-1)^{\sum(i_k+j_k)}\end{aligned}$$

即符号相同, 故定理得证. □

Binet-Cauchy 公式给出了行列式在矩阵乘积上的推广.

定理 1.2 (Binet-Cauchy 公式)**.** *$A\in\mathbb{F}^{m\times n},B\in\mathbb{F}^{n\times m}$. 若 $m>n$ 则 $\det AB=0$, 否则则为 A 的所有 m 阶子式与 B 相应的 m 阶子式之积的和, 即*

$$\det AB=\sum_{1\le i_1<\cdots<i_m\le n}A\begin{pmatrix}1&\cdots&m\\i_1&\cdots&i_m\end{pmatrix}B\begin{pmatrix}i_1&\cdots&i_m\\1&\cdots&m\end{pmatrix}$$

证明. 我们将仅借助行列式的置换定义来解决这个问题. 由行列式的多重线性可知

$$\det AB=\begin{vmatrix}\sum_{k=1}^{n}a_{1k}b_{k1}&\cdots&\sum_{k=1}^{n}a_{1k}b_{km}\\\vdots&&\vdots\\\sum_{k=1}^{n}a_{mk}b_{k1}&\cdots&\sum_{k=1}^{n}a_{mk}b_{km}\end{vmatrix}=\sum_{k_1,\cdots,k_m\in[n]}\begin{vmatrix}a_{1k_1}&\cdots&a_{1k_m}\\\vdots&&\vdots\\a_{mk_1}&\cdots&a_{mk_m}\end{vmatrix}\prod_{i=1}^{m}b_{k_ii}$$

若 $m>n$ 则 $(k_1,\cdots,k_m)$ 中必然有两分量相同, 则和式中的行列式均为 0, 因此 $\det AB=0$. 因此, 我们需要求和下标 $(k_1,\cdots,k_m)$ 中分量各不相同.$m\le n$ 时, 因此注意到 $\sum_{(k_1,\cdots,k_m)\in[n]^m}=\sum_{1\le i_1<\cdots<i_m\le n}\sum_{\pi\in S_m}$, 此处 $\pi=\begin{pmatrix}i_1&\cdots&i_m\\k_1&\cdots&k_m\end{pmatrix}$, 因此我们有

$$\begin{aligned}\det AB=&\sum_{1\le i_1<\cdots<i_m\le n}\sum_{\pi\in S_m}\begin{vmatrix}a_{1k_1}&\cdots&a_{1k_m}\\\vdots&&\vdots\\a_{mk_1}&\cdots&a_{mk_m}\end{vmatrix}\prod_{i=1}^{m}b_{k_ii}=\sum_{1\le i_1<\cdots<i_m\le n}\begin{vmatrix}a_{1i_1}&\cdots&a_{1i_m}\\\vdots&&\vdots\\a_{mi_1}&\cdots&a_{mi_m}\end{vmatrix}\sum_{\pi\in S_m}\varepsilon_\pi\prod_{i=1}^{m}b_{k_ii}\\=&\sum_{1\le i_1<\cdots<i_m\le n}A\begin{pmatrix}1&\cdots&m\\i_1&\cdots&i_m\end{pmatrix}B\begin{pmatrix}i_1&\cdots&i_m\\1&\cdots&m\end{pmatrix}\end{aligned}$$

□

可以类似证明其有更一般的形式

定理 1.3 (Binet-Cauchy 公式的推广)**.** *$A\in\mathbb{F}^{m\times n},B\in\mathbb{F}^{n\times m}$, 正整数 $r\le m$. 若 $r>n$, 则 AB 的任一 r 阶子式为 0. 若 $r\le n$, 则 AB 的任一 r 阶子式*

$$AB\begin{pmatrix}i_1&\cdots&i_r\\j_1&\cdots&j_r\end{pmatrix}=\sum_{1\le k_1<\cdots<k_r\le n}A\begin{pmatrix}i_1&\cdots&i_r\\k_1&\cdots&k_r\end{pmatrix}B\begin{pmatrix}k_1&\cdots&k_r\\j_1&\cdots&j_r\end{pmatrix}$$

其有应用

命题 1.4. $A\in\mathbb{F}^{m\times n},m\le n$, 则 $\det AA^{\mathsf{H}}=\sum\limits_{M}|M|^2$, 其中 M 遍历 A 的 $\binom{n}{m}$ 个 m 阶子式.

命题 1.5 (Cauchy 恒等式). $\left(\sum\limits_{i=1}^{n}a_ic_i\right)\left(\sum\limits_{i=1}^{n}b_id_i\right)-\left(\sum\limits_{i=1}^{n}a_id_i\right)\left(\sum\limits_{i=1}^{n}b_ic_i\right)=\sum\limits_{1\le j<k\le n}(a_jb_k-a_kb_j)(c_jd_k-c_kd_j)$.

证明. 仅需对 $A=\begin{pmatrix}a_1&\cdots&a_n\\b_1&\cdots&b_n\end{pmatrix},B=\begin{pmatrix}c_1&\cdots&c_n\\d_1&\cdots&d_n\end{pmatrix}^{\mathsf{T}}$ 应用 Binet-Cauchy 公式. □

这一恒等式可直接导出 n 元 Cauchy 不等式.

经典行列式

1. Vandermonde 行列式 $\begin{vmatrix}1&1&\cdots&1\\x_1&x_2&\cdots&x_n\\\vdots&\vdots&&\vdots\\x_1^{n-1}&x_2^{n-1}&\cdots&x_n^{n-1}\end{vmatrix}=\prod\limits_{1\le j<i\le n}(x_i-x_j)$.
2. $\det(A+t1_{n\times n})=\det A+t\sum\limits_{i,j\in[n]}A_{ij}$.
3. $\begin{vmatrix}x&a_1&\cdots&a_{n-1}\\c_1&b_1&&\\\vdots&&\ddots&\\c_{n-1}&&&b_{n-1}\end{vmatrix}=$
4. 三对角线行列式 $\begin{vmatrix}a&b&0&\cdots&0&0&0\\c&a&b&\cdots&0&0&0\\0&c&a&\cdots&0&0&0\\\vdots&\vdots&\vdots&&\vdots&\vdots&\vdots\\0&0&0&\cdots&c&a&b\\0&0&0&\cdots&0&c&a\end{vmatrix}=\begin{cases}\dfrac{\alpha^{n+1}-\beta_{n+1}}{\alpha-\beta},&a^2\ne4bc\\\dfrac{2^n}{n+1}a^n,&a^2=4bc\end{cases}$, 其中 α,β 是 $x^2-ax+bc=0$ 的根.
   (a) $a=c=1,b=-1$ 时 $\det=f_{n+1}=\dfrac{\varphi^{n+1}-(-\varphi^{-1})^{n+1}}{\sqrt5},\varphi=\dfrac{1+\sqrt5}{2},-\varphi^{-1}=\dfrac{1-\sqrt5}{2}$.
   (b) $b=c=n,a=2n$ 时 $\det=(n+1)n^n$.
   (c) $b=c=1,a=2\cos\alpha$ 时 $\det=\begin{cases}\dfrac{\sin(n+1)\alpha}{\sin\alpha},&\alpha\ne k\pi\\n+1,&\alpha=2k\pi\\(-1)^n(n+1),&\alpha=(2k+1)\pi\end{cases}$.
5. $A\in M_m(\mathbb{F}),B\in M_n(\mathbb{F}),\begin{vmatrix}A&C\\O&B\end{vmatrix}=\det A\cdot\det B,\begin{vmatrix}O&A\\B&C\end{vmatrix}=(-1)^{mn}\det A\cdot\det B$,
6. $A\in M_m(\mathbb{F}),D\in M_n(\mathbb{F}),\begin{vmatrix}A&B\\C&D\end{vmatrix}=\begin{cases}\det A\cdot\det(D-CA^{-1}B),&A\text{可逆}\\\det D\cdot\det(A-BD^{-1}C),&D\text{可逆}\end{cases}$.
7. $A,B\in M_n(\mathbb{F}),\begin{vmatrix}A&B\\B&A\end{vmatrix}=\det(A+B)\det(A-B)$. 若 $[A,B]=O$, 则 $\begin{vmatrix}A&-B\\B&A\end{vmatrix}=\det(A^2+B^2)$.
8. $\det(I_m-AB)=\begin{vmatrix}I_n&B\\A&I_m\end{vmatrix}=\det(I_n-BA)$, 因此 $\det(A-\boldsymbol{\alpha}\boldsymbol{\alpha}^{\mathsf{T}})=(1-\boldsymbol{\alpha}^{\mathsf{T}}A^{-1}\boldsymbol{\alpha})\det A$.

1.2 线性方程组

Gauss-Jordan 算法

$$\text{增广矩阵} \xrightarrow{\text{初等行变换}} \text{阶梯形矩阵} \xrightarrow{\text{没有0=}d} \text{简化行} \begin{cases} \xrightarrow{\text{非零行=未知量}} \text{唯一解} \\ \xrightarrow{\text{非零行}\neq\text{未知量}} \text{通解} \end{cases}$$

例 1. 问 $\boldsymbol{\beta}$ 是否能被 $\{\boldsymbol{\alpha}_1,\cdots,\boldsymbol{\alpha}_n\}$ 线性表出, 即问 $\sum x_i\boldsymbol{\alpha}_i=\boldsymbol{\beta}$ 是否有解 *(不须唯一)*.

定理 1.6 (Kronecker-Capelli 可解性准则[1])**.** $Ax=b$ 有解 $\iff \operatorname{rank}A=\operatorname{rank}(A|b)$.

证明. 注意到 $Ax=b$ 有解等价于 $b\in\operatorname{span}(A^{(1)},\cdots,A^{(n)})$, 故 $\operatorname{span}(A^{(1)},\cdots,A^{(n)},b)\subset\operatorname{span}(A^{(1)},\cdots,A^{(n)})$, 故秩相等. □

若 $\sum x_i\boldsymbol{\alpha}_i=0$ 有非零解, 且其中有有限个解 $\{\boldsymbol{\eta}_1,\cdots,\boldsymbol{\eta}_t\}$, 其线性无关, 且方程组的每个解都能由该向量组线性表出, 则称这一组向量为该方程的一个基础解系. 换言之, 方程组 $\sum x_i\boldsymbol{\alpha}_i=0$ 的所有解构成了一个向量空间 $W=\left\{\sum_{i=1}^{t}k_i\boldsymbol{\eta}_i : k_i\in\mathbb{F}\right\}$, 而 $\{\boldsymbol{\eta}_1,\cdots,\boldsymbol{\eta}_t\}$ 是其一个基.

定理 1.7. $A\in M_n(\mathbb{F}), x\in\mathbb{F}^{n\times1}, Ax=0$ 的所有解构成的空间 $W=\left\{\sum_{i=1}^{t}k_i\boldsymbol{\eta}_i : k_i\in\mathbb{F}\right\}$ 的维数 $\dim W=n-\operatorname{rank}A$.

证明. $\operatorname{rank}A=n$ 时定理显然成立, 下证 $\operatorname{rank}A=r<n$ 的情形.

首先我们将 A 化为简化行阶梯形矩阵 J, 得到 $\begin{cases} x_1=b_{1,r+1}x_{r+1}+\cdots+b_{1n}x_n \\ x_2=b_{2,r+1}x_{r+1}+\cdots+b_{2n}x_n \\ \vdots \\ x_r=b_{r,r+1}x_{r+1}+\cdots+b_{rn}x_n \end{cases}$. 分别取 $\begin{pmatrix} x_{r+1}\\ \vdots\\ x_n\end{pmatrix}=\begin{pmatrix}1\\ \vdots\\ 0\end{pmatrix},\cdots,\begin{pmatrix}0\\ \vdots\\ 1\end{pmatrix}$

代入, 得到 $n-r$ 个解 $\boldsymbol{\eta}_1,\cdots,\boldsymbol{\eta}_{n-r}$, 其中可知 $\boldsymbol{\eta}_1=\begin{pmatrix} b_{1,r+1}\\ \vdots\\ b_{r,r+1}\\ 1\\ \vdots\\ 0\end{pmatrix},\cdots,\boldsymbol{\eta}_{n-r}=\begin{pmatrix} b_{1n}\\ \vdots\\ b_{rn}\\ 0\\ \vdots\\ 1\end{pmatrix}$.

我们再取方程组任一解 $\boldsymbol{\eta}=\begin{pmatrix}c_1\\ \vdots\\ c_n\end{pmatrix}$, 代入 J 的方程依然可得 $\begin{cases} c_1=b_{1,r+1}c_{r+1}+\cdots+b_{1n}c_n \\ c_2=b_{2,r+1}c_{r+1}+\cdots+b_{2n}c_n \\ \vdots \\ c_r=b_{r,r+1}c_{r+1}+\cdots+b_{rn}c_n \end{cases}$. 代回 $\boldsymbol{\eta}$ 可知 $\boldsymbol{\eta}=\sum_{i=1}^{n-r}c_{r+i}\boldsymbol{\eta}_i$. 由解的任意性以及 $\boldsymbol{\eta}_i$ 之间线性无关可知此时 $\dim W=n-r$, 得证. □

事实上对于非齐次的一般线性方程组也有类似的结论, 其解为一个 W 型的 $n-\operatorname{rank}A$ 维流形. 换言之, 即 "特解 + 通解", 在此不再赘叙证明过程.

例 2. 解 $\begin{pmatrix}3&1&-1&-2\\1&5&2&1\\2&6&-3&-3\\-1&-11&5&4\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix}=\begin{pmatrix}2\\-1\\3\\-4\end{pmatrix}$.

[1] 也称 Rouché-Capelli 定理.

将增广矩阵化为简化行阶梯形矩阵, 即 $\begin{pmatrix}1&0&-\frac{3}{16}&-\frac{9}{16}&\frac{9}{16}\\0&1&-\frac{7}{16}&-\frac{5}{16}&\frac{5}{16}\\0&0&0&0&0\\0&0&0&0&0\end{pmatrix}$, 因此我们得到解 $\begin{cases}x_1=\frac{3}{16}x_3+\frac{9}{16}x_4+\frac{9}{16}\\x_2=\frac{7}{16}x_3+\frac{5}{16}x_4+\frac{5}{16}\end{cases}$, 其中 x_3,x_4 为自由变量. 接下来赋值 $x_3=x_4=0$ 得到一个特解 $\boldsymbol{\gamma}_0=\begin{pmatrix}9/16\\5/16\\0\\0\end{pmatrix}$, 而该方程对应的齐次线性方程组 (即导出组) 的一般解即为 $\begin{cases}x_1=\frac{3}{16}x_3+\frac{9}{16}x_4\\x_2=\frac{7}{16}x_3+\frac{5}{16}x_4\end{cases}$. 分别代入 $x_3=16,x_4=0$ 与 $x_3=0,x_4=16$, 得到一个基础解系 $\boldsymbol{\eta}_1=\begin{pmatrix}3\\7\\16\\0\end{pmatrix},\boldsymbol{\eta}_2=\begin{pmatrix}9\\5\\0\\16\end{pmatrix}$. 因此最终本方程的全部解为 $W=\{\boldsymbol{\gamma}_0+k_1\boldsymbol{\eta}_1+k_2\boldsymbol{\eta}_2:k_1,k_2\in\mathbb{F}\}$.

Cramer 法则 由 Gauss-Jordan 算法可知, 对于 $A\in M_n(\mathbb{F})$[2],$Ax=b$ 有唯一解 $\iff \det A\neq 0$. 首先注意到阶梯型矩阵的对角线位置均非 0 时方程组有唯一解, 反之注意到非 0 行与未知量之间的关系即可. 事实上我们可以通过构造行列式来直接写出该唯一解. 我们记 A 的第 k 列被 b 替换得到的矩阵为 B_k, 我们有

定理 1.8 (Cramer 法则)**.** 对于 $A\in M_n(\mathbb{F})$,$\det A\neq 0 \iff Ax=b$ 有唯一解, 且解 $x=\left(\frac{\det B_1}{\det A},\cdots,\frac{\det B_n}{\det A}\right)^{\mathsf{T}}$.

证明. 注意到 $\det B_i=\sum_{k=1}^{n}b_kA_{ki}$(行列式展开) 且 $b_k=\sum_{j=1}^{n}a_{kj}x_j$ 即可. □

1.3 线性相关性

定义 2. 向量组 $\boldsymbol{\alpha}_1,\boldsymbol{\alpha}_2,\cdots,\boldsymbol{\alpha}_n$ 线性无关, 即 $\sum_{i\in[n]}k_i\boldsymbol{\alpha}_i=0 \iff k_i=0(\forall i\in[n])$.

向量组 $\boldsymbol{\alpha}_1,\boldsymbol{\alpha}_2,\cdots,\boldsymbol{\alpha}_n$ 线性相关, 即 $\exists(k_1,\cdots,k_n)\in\mathbb{F}^n-0:\sum_{i\in[n]}k_i\boldsymbol{\alpha}_i=0$.

向量组 $\{\boldsymbol{\alpha}_i\}_{i\in[n]}$ 线性相关

$\iff$ 1. 存在非零系数的线性组合为 0
2. $\forall i\in[n],\boldsymbol{\alpha}_i$ 可被向量组 $\{\boldsymbol{\alpha}_j\}_{j\in[n]-i}$ 线性表出. 换言之,$\forall i\in[n]:\boldsymbol{\alpha}_i\in\operatorname{span}\{\boldsymbol{\alpha}_j\}_{j\in[n]-i}$.
3. $\sum_{i=1}^{n}x_i\boldsymbol{\alpha}_i=0$ 有非零解
4. $\det(\boldsymbol{\alpha}_1,\cdots,\boldsymbol{\alpha}_n)=0$(若 $\boldsymbol{\alpha}_i\in\mathbb{F}^n$)
5. 若 $\boldsymbol{\beta}$ 可被 $\{\boldsymbol{\alpha}_i\}_{i\in[n]}$ 线性表出, 则有无穷种方式

$\impliedby$ 6. 向量组的部分组 $\{\boldsymbol{\alpha}_j\}_{j\in J\subset[n]}$ 线性相关
7. $\{\boldsymbol{\alpha}_i\}_{i\in[n]}$ 中每个 $\boldsymbol{\alpha}_i$ 去掉 m 个分量的缩短组也线性相关

上述七个命题也可以写成逆否形式从而作用在线性无关性上. 需要注意的是最后一条应该变为:

7' $\{\boldsymbol{\alpha}_i\}_{i\in[n]}$ 中每个 $\boldsymbol{\alpha}_i$ 加上 m 个分量的延长组也线性无关

命题 1.9. 若 $\{\boldsymbol{\alpha}_i\}_{i\in[n]}$ 线性无关, 且 $\begin{pmatrix}\boldsymbol{\beta}_1\\\vdots\\\boldsymbol{\beta}_n\end{pmatrix}=A^{\mathsf{T}}\begin{pmatrix}\boldsymbol{\alpha}_1\\\vdots\\\boldsymbol{\alpha}_n\end{pmatrix}$, 则 $\{\boldsymbol{\beta}_i\}_{i\in[n]}$ 线性无关 $\iff \det A\neq 0$.

[2]Cramer 法则适用于有限域吗? 否则此处需要填一笔说明 $\mathbb{F}=\mathbb{R}$或$\mathbb{C}$.

使用定义, 注意到本节性质 3', 以及 $Ax=b$ 有唯一解 $\iff \det A\neq 0$, 立得证.

命题 1.10. $\{\boldsymbol{\alpha}_i\}_{i\in[n]}$ 线性无关,$\boldsymbol{\beta}=\sum_{i\in[n]} b_i\boldsymbol{\alpha}_i$. 若 $b_i\neq 0$, 则用 $\boldsymbol{\beta}$ 替换 $\boldsymbol{\alpha}_i$ 得到的向量组线性无关.

证明. 使用上命题, 实质是 $\begin{vmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ b_1 & \cdots & b_{i-1} & b_i & b_{i+1} & \cdots & b_n \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{vmatrix} = b_i\neq 0.$ □

1.4 秩与维数

向量组的秩

定理 1.11 (Steinitz 替换定理)**.** 向量组 $\{\boldsymbol{\alpha}_i\}_{i\in[s]}$ 线性表出 $\{\boldsymbol{\beta}_i\}_{i\in[r]}$, 若 $\{\boldsymbol{\beta}_i\}_{i\in[r]}$ 线性无关, 则 $s\geq r$, 并且可以用 $\{\boldsymbol{\beta}_i\}_{i\in[r]}$ 替换 $\{\boldsymbol{\alpha}_i\}_{i\in[s]}$ 中的 r 个向量, 使之与 $\{\boldsymbol{\alpha}_i\}_{i\in[s]}$ 等价 *(即互相表出)*.

证明. 我们记 $\boldsymbol{\alpha}=(\boldsymbol{\alpha}_1,\cdots,\boldsymbol{\alpha}_s),\boldsymbol{\beta}=(\boldsymbol{\beta}_1,\cdots,\boldsymbol{\beta}_r),\boldsymbol{\beta}=\boldsymbol{\alpha}A$. 我们考虑逆否命题, 即设 $s<r$, 此时对 $A\in\mathbb{F}^{s\times r}, Ax=0$ 必有非零解, 因此 $\boldsymbol{\beta}x=\alpha Ax=0$ 必有非零解, 即 $\boldsymbol{\beta}$ 线性相关.

$s=r$ 时, 定理成立, 下考虑 $s>r$ 的情形. 我们设 $\boldsymbol{\gamma}$ 为用 β 替换 α 中第 $i_1,\cdots,i_r$ 个向量得到的向量组, 换言之 $\boldsymbol{\gamma}=(\boldsymbol{\beta}_1,\cdots,\boldsymbol{\beta}_r,\boldsymbol{\alpha}_{i'_1},\cdots,\boldsymbol{\alpha}_{i'_{s-r}})$, 其中 $\{i'_1,\cdots,i'_{s-r}\}=[s]-\{i_1,\cdots,i_r\}$. 设 $\boldsymbol{\alpha}B=\boldsymbol{\gamma}$, 即证 B 可逆. 实际上,$B=(A,C)$, 其中 $C\in\mathbb{F}^{s\times(s-r)}$, 且除了第 (k,i'_k) 元 $(k\in[s-r])$ 为 1 外其余元素为 0. 再用 Laplace 展开定理, 对此 $s-r$ 个元素展开, 可得 $\det B=A\begin{pmatrix} i_1 & \cdots & i_r \\ 1 & \cdots & r \end{pmatrix}$. 由于

$$r=\operatorname{rank}\boldsymbol{\beta}=\operatorname{rank}(\boldsymbol{\alpha}A^{(1)},\cdots,\boldsymbol{\alpha}A^{(r)})\leq\operatorname{rank}(A^{(1)},\cdots,A^{(r)})=\operatorname{rank}A\leq r,$$

因此必有 r 阶子式非零, 选取此子式对应的 $i_1,\cdots,i_r$ 列对应的向量即可, 此时 $\det B\neq 0$, 定理得证. □

事实上, 这个证明并不适合初学看, 因为其中的一些结论和定义会在后面展开, 尤其是向量组的秩这一概念本应由此定理得出, 却在此定理的证明中出现, 陷入了循环论证. 本证明的意图是给读者一个思路, 即用线性方程组, 矩阵和行列式解决基础的线性问题.

由此定理可知, 每个向量组中有极大的线性无关部分组 (不一定唯一), 但所有的极大线性无关组中都有相同个数的向量, 且等价, 即其张成的空间是一样的. 我们定义向量组的秩为向量组的极大线性无关组所含向量个数.

最后我们给出一些推论.

命题 1.12. 向量组 $\boldsymbol{\alpha}$ 线性表出 $\boldsymbol{\beta}$ 则 $\operatorname{rank}\boldsymbol{\alpha}\geq\operatorname{rank}\boldsymbol{\beta}$.

这一推论实际上相应于线性方程组是否有解与线性方程组的阶之间的关系.

命题 1.13. $\{\boldsymbol{\alpha}_i\}_{i\in[r]}$ 线性无关 $\iff \operatorname{rank}\boldsymbol{\alpha}=r$.

例 3. $\boldsymbol{\alpha}_1=(3,0,2)^{\mathsf{T}},\boldsymbol{\alpha}_2=(-2,5,4)^{\mathsf{T}},\boldsymbol{\alpha}_3=(6,15,8)^{\mathsf{T}}$. 由于 $\begin{vmatrix} 3 & -2 \\ 0 & 5 \end{vmatrix}=15\neq 0$, 因此其延长组 $\boldsymbol{\alpha}_1,\boldsymbol{\alpha}_2$ 线性无关. 但 $\det(\boldsymbol{\alpha}_1,\boldsymbol{\alpha}_2,\boldsymbol{\alpha}_3)=0$, 因此此向量组的秩为 *2*.

线性空间的维数 基即线性空间中的一个极大线性无关组, 线性空间的维数即基的秩. 需要注意的是, 不同的基本域下线性空间的维数不同. 有限维情形下有一般的结论 $\dim_{\mathbb{C}}V=2\dim_{\mathbb{R}}V$. 更一般地, 对于域 F 及其子域 E, 有 $\dim_E V=(\dim_F V)(\dim_E F)$.

可以注意到显然的结论: 对 V 的线性子空间 U,W, 若 $U\subset W$ 则 $\dim U\leq\dim W$. 这个命题可以导出一个显然但重要的结论:

命题 1.14. 对 V 的子空间 U,W, 若 $U\subset W$ 且 $\dim U=\dim W$ 则 $U=W$.

例 4. 如果要判断一些函数是否线性相关, 尤其是在 $\mathbb{R}^{\mathbb{R}}$ 上的函数, 我们一般只需要写出方程组然后考虑代入特殊根来判断.

矩阵的秩 我们给出十分重要的定理, 这一定理说明了矩阵存在一个内禀的不变量, 它就是秩.

定理 1.15. 矩阵的行列秩相等.

证明. $A\in\mathbb{F}^{m\times n}$ 可以被化为阶梯形矩阵 J, 其有 $r\leq m$ 个非零行, 即有 r 个主元, 记其在第 $j_1,\cdots,j_r$ 列, 即

$$J=\begin{pmatrix}
0 & \cdots & 0 & c_{1j_1} & \cdots & c_{1j_2} & \cdots & c_{1j_r} & \cdots & c_{1n}\\
0 & \cdots & 0 & 0 & \cdots & c_{2j_2} & \cdots & c_{2j_r} & \cdots & c_{2n}\\
\vdots & & \vdots & \vdots & & \vdots & & \vdots & & \vdots\\
0 & & 0 & 0 & & 0 & & c_{rj_n} & \cdots & c_{rn}\\
0 & \cdots & 0 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0\\
\vdots & & \vdots & \vdots & & \vdots & & \vdots & & \vdots\\
0 & \cdots & 0 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0
\end{pmatrix}$$

其中 $\prod\limits_{i=1}^{r}c_{ij_i}\neq 0$.

①要说明阶梯形矩阵 J 的行列秩相等, 仅需证明列秩等于 r, 行秩同理可证. 由于 $\det C=\begin{vmatrix}c_{1j_1} & c_{1j_2} & \cdots & c_{1j_r}\\ 0 & c_{2j_2} & \cdots & c_{2j_r}\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \cdots & c_{rj_r}\end{vmatrix}=\prod\limits_{i=1}^{r}c_{ij_i}\neq 0$, 因此 $C^{(1)},C^{(2)},\cdots,C^{(r)}$ 线性无关, 因此其延长组 $J^{(j_1)},J^{(j_2)},\cdots,J^{(j_r)}$ 线性无关, 因此 $\operatorname{rank}\left\{J^{(j_k)}\right\}_{k\in[r]}=r$.

设 $U=\left\{(a_1,\cdots,a_r,0,\cdots,0)^{\mathsf{T}}:a_i\in\mathbb{F}\right\}$, 其中元素可被分解为 $\{\boldsymbol{\varepsilon}_i\}_{i\in[r]}$ 的线性组合, 其中 $\boldsymbol{\varepsilon}_i$ 为第 i 分量为 1 其余为 0 的 n 阶列向量. 由于 $\{\boldsymbol{\varepsilon}_i\}_{i\in[n]}$ 线性无关, 因此 $\{\boldsymbol{\varepsilon}_i\}_{i\in[r]}$ 是 U 的基,$\dim U=r$. 注意到

$$r=\dim\operatorname{span}\left\{J^{(j_i)}\right\}_{i\in[r]}\leq\dim\operatorname{span}\left\{J^{(i)}\right\}_{i\in[n]}\leq\dim U=r,$$

因此列秩 $\operatorname{rank}\left\{J^{(i)}\right\}_{i\in[n]}=r$, 其中 $\left\{J^{(j_i)}\right\}_{i\in[r]}$ 是 J 列向量的极大线性无关组.

②可以注意到初等行变换不变矩阵的行秩, 下证其也不变矩阵的列秩.

考虑矩阵 C 经由初等行变换变为矩阵 D, 注意到 $\sum x_iC^{(i)}=0\iff\sum x_iD^{(i)}=0$, 因此可以认为 C 的列向量组的线性相关性与 D 的列向量组的相同, 这说明初等行变换不变化列向量组的线性相关性. 再设 A 初等行变换变为 B, 设 $B^{(j_1)},\cdots,B^{(j_r)}$ 为 B 列向量组的极大线性无关组, 因此 $A^{(j_1)},\cdots,A^{(j_r)}$ 线性无关. 另一方面, 取 $l\in[n]-\{j_i\}_{i\in[r]}$, 有 $A^{(j_1)},\cdots,A^{(j_r)},A^{(l)}$ 经由初等行变换变为 $B^{(j_1)},\cdots,B^{(j_r)},B^{(l)}$, 后者线性相关, 因此前者线性相关, 因此 $A^{(j_1)},\cdots,A^{(j_r)}$ 也为 A 列向量组的极大线性无关组. 综上, 初等行变换不变矩阵的列秩, 因为其将极大线性无关组变为极大线性无关组.

综上,A 的行秩 $\overset{②}{=}$ J 的行秩 $\overset{①}{=}$ J 的列秩 $\overset{②}{=}$ A 的列秩, 定理得证. □

定义 3 (秩)**.** 向量组的秩即其极大线性无关组所含向量个数, 矩阵的秩即矩阵行/列向量组的秩.

定理 1.16. $A\in\mathbb{F}^{m\times n},\operatorname{rank}A=A$ 非零子式的最高阶数.

证明. 设 $\operatorname{rank}A=r$,A 的 r 个主元组所在行组成矩阵 $A_1,\operatorname{rank}A_1=r$, 故 A_1 有 r 列线性无关, 其组成 r 阶非零行列式, 此即 A 的非零 r 阶子式.

设 $r<s\leq\min\{m,n\}$, 取 A 的 s 阶子式 $A\begin{pmatrix}i_1 & \cdots & i_s\\ j_1 & \cdots & j_s\end{pmatrix}$. 由 $\operatorname{rank}A=r<s$ 可知此子式可以由列向量组的线性相关性而计算为 0. 定理得证. □

由此证明可知,A 的非零 $\operatorname{rank} A$ 阶子式的行/列向量组线性无关, 故其延长组 (即对应的行/列) 线性无关, 且为 A 的行/列向量组的极大线性无关组. 也由上证明可知, 方阵满秩与行列式非零等价.

例 5. *如果要计算矩阵的秩, 仅需使用 Gauss 消元法. 如果需再去矩阵行/列向量组的极大线性无关组, 则在初等列/行变换后取非零行/列.*

命题 1.17. *$A \in \mathbb{F}^{m\times n}$ 的任 s 行组成的子阵 $A_1 \in \mathbb{F}^{s\times n}$ 有 $\operatorname{rank} A_1 \geq \operatorname{rank} A + s - m$.*

证明. 在 A_1 的行向量组中取极大线性无关组, 再将其扩充为 A 的行向量组中的极大线性无关组, 可见 A 的行向量组去掉该极大线性无关组所剩的向量组均不在 A_1 的行向量组中, 换言之,$\operatorname{rank} A - \operatorname{rank} A_1 \leq m - s$, 得证. □

1.5 线性空间的基础命题

本节不讲同构与外直和的定义, 这是代数中的基本概念, 不必多言.

基与坐标 基即线性空间中的一个极大线性无关组, 坐标即向量在此基下的线性分解. 由基的线性无关性, 分解是唯一的.

我们记有限维线性空间 V 上有两个基 $\boldsymbol{\alpha} = (\boldsymbol{\alpha}_1, \cdots, \boldsymbol{\alpha}_n), \boldsymbol{\beta} = (\boldsymbol{\beta}_1, \cdots, \boldsymbol{\beta}_n)$, 且前者表出后者有关系式 $\boldsymbol{\beta} = \boldsymbol{\alpha}A, A \in M_n(\mathbb{F})$, 此即 V 上由基 $\boldsymbol{\alpha}$ 到基 $\boldsymbol{\beta}$ 的基变换公式,A 为基 $\boldsymbol{\alpha}$ 到基 $\boldsymbol{\beta}$ 的过渡矩阵. 容易看出, 基 $\boldsymbol{\beta}$ 到基 $\boldsymbol{\alpha}$ 的过渡矩阵为 A^{-1}.

在 V 中固定一组基 $\boldsymbol{\alpha}$, 可见 $\eta : \boldsymbol{\beta} \mapsto A$(其中 A 是 $\boldsymbol{\alpha}$ 到 $\boldsymbol{\beta}$ 的过渡矩阵) 给出了 V 中所有基到 $\mathrm{GL}_n(\mathbb{F})$ 的同构.

最后, 任取向量 $\boldsymbol{x} \in V$ 有坐标 $x, y \in \mathbb{F}^n$ 满足 $\boldsymbol{x} = \boldsymbol{\alpha}x = \boldsymbol{\beta}y$, 我们有 $y = A^{-1}x$.

和与直和

命题 1.18. *V_1, V_2, V_3 均为 V 的子空间, 则有*

$$V_1 \cap (V_2 + V_3) \supset (V_1 \cap V_2) + (V_1 + V_3) \qquad V_1 + (V_2 \cap V_3) \subset (V_1 + V_2) \cap (V_1 + V_3)$$

定义 4 (直和)**.** *$\sum_{i=1}^{n} V_i$ 是直和则记为 $\bigoplus_{i=1}^{n} V_i$, 其有如下等价定义:*

1. *$\sum_{i=1}^{n} V_i$ 中的向量可被唯一分解为 V_i 向量之和*
2. *$\sum_{i=1}^{n} V_i$ 中 0 的分解方法唯一*
3. *$V_i \cap \left(\sum_{j\neq i} V_j\right) = 0, \forall i \in [n]$*
4. *$\dim \sum_{i=1}^{n} V_i = \sum_{i=1}^{n} \dim V_i$*
5. *所有 V_i 的基合起来即 $\sum_{i=1}^{n} V_i$ 的基*

定理 1.19. *V_1, V_2 是 V 的子空间, 则 $\dim V_1 + \dim V_2 = \dim(V_1 + V_2) + \dim(V_1 \cap V_2)$.*

证明. 取 $V_1 \cap V_2$ 的一个基扩展为 V_1, V_2 的基, 然后证明两基之和线性无关且构成 $V_1 + V_2$ 的基即可. □

商空间 商空间的定义不在此赘叙, 仅讨论商空间维数的重要公式.

定理 1.20. *对有限维线性空间 V 及其子空间 W, 则 $\dim(V/W) = \dim V - \dim W$.*

证明. 取 W 中的基 $\boldsymbol{\alpha}_1, \cdots, \boldsymbol{\alpha}_s$ 扩充为 V 的基 $\boldsymbol{\alpha}_1, \cdots, \boldsymbol{\alpha}_n$, 容易证明 $\boldsymbol{\alpha}_{s+1} + W, \cdots, \boldsymbol{\alpha}_n + W$ 是 V/W 的一个基. □

Chapter 2

多项式

多项式实际上也是线性代数的预备知识之一, 但其十分重要的地位使其单独成章, 多项式理论也是相当重要的理论, 在未来讨论带有纯量乘积的线性空间时将会回到这一主题. 本章我们讨论基础的多项式理论, 其最高不过涉及到 Newton 公式和 Sturm 定理. 本章内容要求基础的群, 环, 域知识, 以及了解由整环构造分式域的过程. 我们将在含幺交换环, 尤其是整环上讨论多项式.

2.1 多项式环

取含幺交换环 R 的含幺子环 A, 再取 $t \in R$, 可以构造扩环 $A[t]$, 其中元素 $a(t) = \sum_{k\geq 0}^{n} a_k t^k$ 即为一个 (单变元) 多项式. 类似的, 可以构造多变元多项式. 需要注意的是, 多变元也不过是有限个变元, 事实上此即一个超越扩张. 另一方面, 多项式仅有有限次幂, 无限个非零项 $a_k t^k$ 的代数和被称为形式幂级数, 这不是我们目前讨论的重点.

我们首先来讨论多项式环的构造. 取含幺交换环 A, 构造环 B, 其中元素为仅有限项非零的无穷序列, 且序列分量为 A 中元素. 为其自然地赋予加法和乘法, 其中乘法是按照分量为 $c_k = \sum_{i+j=k} a_i b_j$ 赋予的. 可以验证这是一个含幺交换环, 幺为 $(1, 0, \cdots)$. 我们记 $X = (0, 1, 0, \cdots), X^k$ 为仅第 $k+1$ 分量为 1 的序列, 因此我们可以以 $\sum_{k=0}^{n} a_k X^k$ 的形式给出 B 中的元素, 其中 $a_k \in A, n < +\infty, X^0 = 1$. 最后, 我们记这样构造的环为 $A[X]$, 它是 A 上的 (单变元) 多项式环.

我们可以认为 $A[X]$ 即 A 的扩环, 其上的运算与 A 上的运算是相容的. 我们定义多项式 $f \in A[X]$ 的次数 $\deg f$ 为其最高系数非零项的次数, 并规定 $\deg 0 = -\infty$. 容易发现,

命题 2.1. $\forall f, g \in A[X]$:

$$\deg(f+g) \leq \max\{\deg f, \deg g\}, \qquad \deg fg \leq \deg f + \deg g$$

后者在 f 与 g 的首项系数乘积非零时取等. 特别地,A 是整环时后者取等.

这一事实直接给出了

定理 2.2. *A 是整环, 则 A 上的多项式环也是.*

多变元的情形可以类似证明.

接下来我们可以返回到第一段讨论的内容, 即 $t \in R$ 的情形中.

定理 2.3. *含幺交换环 R 有含幺子环 $A, \forall t \in R$, 有唯一的环同态 $\Pi_t : A[X] \to R$ 使得 $\forall a \in A, \Pi_t(a) = a, \Pi_t(X) = t$.*

这样的同态是自然的, 更重要的是, 此同态联系了多项式的函数观点与代数观点, 也因此我们可以记 $\Pi_t(f) = f(t)$. 若存在 $f \in A[X]$ 使得 $\Pi_t(f) = 0$, 则称元素 $t \in R$ 为 A 上的代数元. 如果 $\Pi_t : A[X] \to R$ 是一个同构嵌入 (单同态), 则称 t 为 A 上的超越元. 当 $A = \mathbb{Q}, R = \mathbb{C}$ 时, 则简单地称之为代数数和超越数.

更一般地, 我们有

定理 2.4. *A, R 为任意含幺交换环,$t \in R$, 若 $\varphi : A \to R$ 是环同态, 则其可被唯一延拓为 $\varphi_t : A[X] \to R$ 且 $\varphi_t(X) = t$.*

这一定理证明与上同理, 不难证明.

2.2 多项式环上的因式分解

整除与唯一分解整环 我们考虑整环 R 上的多项式环 $R[X]$. 我们首先给出关于整除的一些定义:

1. $b \in R$ 被 $a \in R$ 整除 (即 $a|b$), 若 $\exists c \in R : b = ac$. 整除具有传递性和右线性.
2. 若 $a|b$ 且 $b|a$, 则称 a, b 为相伴元, 且 $b = ua, u$ 可逆, 换言之 $u|1$.
3. R 中的可逆元可以被认为是 1 的因子, 有时也被称为正则元.
4. $p \in R$ 被称为素元, 若其不可逆且不能被表为不可逆元之积.$A[X]$ 中的素元被称为既约多项式.

接下来我们给出定义

定义 5. *整环 R 被称为唯一分解整环 (Unique Factorization Domain, UFD), 若其中的任一非零元 a 可被分解为可逆元与素元之积, 且在重排和相伴意义下唯一. 换言之, 若 $a = u\prod_{i=1}^{r} p_i = v\prod_{j=1}^{s} q_j$, 其中 u, v 可逆,p_i, q_j 均为素元, 则 $r = s$ 且可适当选取 p_i, q_j 的下标, 使得 $p_i = u_i q_i, i \in [r]$, 其中 u_i 可逆.*

我们有

定理 2.5. *R 是整环且每个元素都有素因子分解, 则每个分解唯一 (即 R 是 UFD) $\iff$ $(p|ab \implies p|a \vee p|b)$, 其中 p 是素元.*

证明. $\implies$ 显然, $\impliedby$ 对可被分解的素因子个数归纳, 注意到整环具有消去律. □

最大公因与最小公倍

定义 6. *整环 R 中元素 a, b 的最大公因 (greatest common divisor, gcd)$\gcd(a, b)$ 指的是元素 $d \in R$, 若 $d|a, d|b, (c|a \wedge c|b \implies c|d)$; 最小公倍 (least common multiple, lcm)$\operatorname{lcm}(a, b)$ 指的是元素 $m \in R$, 若 $a|m, b|m, (a|n \wedge b|n \implies m|n)$. 若 $\gcd(a, b) = 1$, 则称 a, b 互素, 记为 $a \perp b$.*

注意到在此定义中我们对相伴元不加区分. 注意到它们都是结合的二元运算, 且具有乘性.

定理 2.6. *整环 R 中 $\forall a, b \in R$ 有 $ab = \gcd(a, b)\operatorname{lcm}(a, b)$.*

证明. 应用定义 (注意到 $\operatorname{lcm}(a, b) = a'a = b'b, a = \gcd(a, b)a'', b = \gcd(a, b)b''$) 代入并消去, 验证其满足定义即可. □

在 R 是 UFD 的情形下, 我们可以将分解写成素元幂的乘积的形式, 即 $a = u\prod_{i=1}^{r} p_i^{\alpha_i}, b = v\prod_{i=1}^{r} p_i^{\beta_i}, \alpha_i \geq 0, \beta_i \geq 0, p_i$ 是素元,u, v 是可逆元. 事实上我们有:$a|b \iff \forall i \in [r] : \alpha_i \leq \beta_i; \gcd(a, b) = \prod_{i=1}^{r} p_i^{\min\{\alpha_i, \beta_i\}}, \operatorname{lcm}(a, b) = \prod_{i=1}^{r} p_i^{\max\{\alpha_i, \beta_i\}}$.

Euclid 整环与辗转相除法

定义 7. *整环 R 是 Euclid 整环 (Euclidean Domain, ED), 若其上有映射 $\delta : R^* \to \mathbb{Z}_{\geq 0}$ 满足:*

1. *对任二非零元 a, b 有 $\delta(ab) \geq \delta(a)$.*
2. *$\forall a \in R, b \in R^* \exists q, r \in R$(前者被称为商元, 后者被称为余元) 使得 $a = qb + r$ 且 $\delta(r) < \delta(b)$ 或 $r = 0$.*

定理 2.7. *整环 $\mathbb{Z}$ 是 ED.*

证明. 取 $\delta(a) = |a|$, 显然 ED 的性质 1 成立, 下证性质 2. 设 $S = \{a - kb \in \mathbb{Z}_{\geq 0} : k \in \mathbb{Z}\} \subset \mathbb{Z}_{\geq 0}$, 由 $\mathbb{Z}_{\geq 0}$ 的良序性可知 S 含最小元 $r = a - bq \geq 0$. 若 $r \geq |b|$ 则 $r - |b|$ 为 S 最小元, 矛盾, 故 $r < |b|$, 性质 2 成立. □

引理 2.8. *整环 R 上多项式环 $R[X]$ 中多项式 g 首项系数可逆, 则 $\forall f \in R[X] \exists! q, r \in R[X] : f = qg + r, \deg r < \deg g$.*

证明. 若 $\deg g > \deg f$ 或 $\deg f = 0$ 定理显然成立. 对 $\deg f$ 归纳, 假设定理对所有次数 $< n$ 的多项式 f 成立, 且 $m = \deg g \leq \deg f = n$. 此时,$f = f_n g_m^{-1} X^{n-m} \cdot g + \tilde{f}, \deg \tilde{f} < n$, 因此可运用归纳假设, 有唯一的 $\tilde{q}, r \in A[X]$ 使得 $\tilde{f} = \tilde{q}g + r, \deg r < m$, 因此取 $q = f_n g_m^{-1} X^{n-m} + \tilde{q}$ 即可.q, r 的唯一性易证. □

定理 2.9. *多项式环 $\mathbb{F}[X]$ 是 ED.*

证明. 取 $\delta(f) = \deg f$, 由引理2.8立得. □

接下来我们讨论辗转相除法. 反复使用 ED 的性质 2, 可以得到一系列带余除法式

$$a = q_1 b + r_1, \qquad b = q_2 r_1 + r_2, \qquad r_1 = q_3 r_2 + r_3, \qquad \cdots$$

和降链 $\delta(b) > \delta(r_1) > \cdots$, 后者由 $\mathbb{Z}_{\geq 0}$ 的良序性必然会中断, 即降链有限, 且最终得到 $r_{k+1} = 0$, 换言之, 最后一式为 $r_{k-1} = q_{k+1} r_k$. 因此有 $r_k | r_{k-1}, r_k | r_{k-2}, \cdots, r | a$. 因此 r_k 是 a, b 的公因子. 另一方面若 c 是 a, b 的公因子, 则 $c | r_1 = a - bq, c | r_2, \cdots c | r_k$, 因此 $r_k = \gcd(a, b) = \gcd(b, r_1) = \cdots = \gcd(r_{k-1}, r_k)$. 此即辗转相除法.

注意到 r_i 为 r_{i-1}, r_{i-2} 的线性组合,r_2 是 b, r_1 的线性组合, 而 r_1 是 a, b 的线性组合, 合起来可知 r_k 是 a, b 的线性组合, 换言之

定理 2.10 (Bézout 引理)**.** *ED R 中任二元素 a, b 均存在 $\operatorname{lcm}(a, b), \gcd(a, b)$, 且存在 $u, v \in R$ 使得 $\gcd(a, b) = au + bv$. 特别地,$a \perp b$ 时有 $au + bv = 1$.*

其可以得到如下性质: 设 $a, b, c \in R, R$ 是 ED, 则

1. $(a \perp b) \wedge (a \perp c) \implies (a \perp bc)$
2. $(a | bc) \wedge (a \perp b) \implies (a | c)$
3. $(a | c) \wedge (b | c) \wedge (a \perp b) \implies (bc | a)$

最后我们来得到关于 ED 的重要结论.

定理 2.11. *ED 是 UFD.*

证明. 我们将使用定理2.5. 设 R 是 ED, 首先说明其上有因子分解. 若 $a = bc$, 其中 b, c 不可逆, 下面说明 $\delta(b) < \delta(a)$.

首先 $\delta(b) \leq \delta(bc) = \delta(a)$. 若 $\delta(b) = \delta(a)$, 则有 $b = qa + r, \delta(r) < \delta(a), r \neq 0$. 由 c 不可逆,$1 - qc \neq 0$, 则有 $\delta(a) = \delta(b) \leq \delta(b(1 - qc)) = \delta(b - aq) = \delta(r) < \delta(a)$, 矛盾.

接着, 设有分解 $a = a_1 \cdots a_n$, 则 $\delta(a) > \delta(a_1 \cdots a_{n-1}) > \cdots \delta(a_1) > \delta(1)$, 因此 $n \leq \delta(a) - \delta(1)$, 即元素 $a \in R$ 有一个长度最大的分解, 即其素因子分解.

下仅需证 $(p | ab \implies p | a \vee p | b), p$ 是素元. 若 $ab = 0$, 命题显然成立. 若 $ab \neq 0$, 则设 $d = \gcd(a, p) | p$. 由于 p 是素元, 因此 $d | 1$ 或相伴于 p, 前者即 $a \perp p, p | b$, 后者即 $p = ud | a$. □

因此我们有推论

命题 2.12 (算术基本定理)**.** *$\mathbb{Z}$ 和 $\mathbb{F}[X]$ 是 UFD.*

事实上, 多变元多项式环也是 UFD, 尽管它不是 ED.

既约多项式 容易发现,$\mathbb{F}[X]$ 中所有一次多项式都是既约多项式. 而另一方面, 我们有一个很强的结论:

定理 2.13. *UFD 中的素元有无限个.*

证明. 设仅有有限个素元 $p_1, \cdots, p_n$, 则取 $f = \prod_{i=1}^{n} p_i + 1$, 其有素因子 p_{n+1}, 这是一个与 $p_1, \cdots, p_n$ 均不相同的素元, 因为若有 $p_{n+1} = p_s, s \in [n]$, 则 $p_s \left| \left(f - \prod_{i=1}^{n} p_i \right) \right. = 1$, 即 p_s 可逆, 矛盾. 综上得证. □

因此,$\mathbb{F}[X]$ 中既约多项式有无限个. 由于在 $\mathbb{F}$ 有限的情况下指定次数的多项式仅有有限个, 因此有

命题 2.14. *在任意有限域上存在任意高次既约多项式.*

定义 8. 对于 *UFD* R 上的多项式环 $R[X]$ 中的元素 $f=\sum_{i=0}^{n}a_iX^i, a_i\in R$, 定义其容度 $d(f):=\gcd(a_0,\cdots,a_n)$. 若 $d(f)$ 可逆 (即 $d(f)|1$), 则称 f 为本原多项式.

定理 2.15 (Gauss 引理)**.** *UFD* R 上多项式环 $R[X]$ 中元素 $f,g\in R[X]$ 有 $d(fg)\approx d(f)d(g)$($\approx$ 指精确到相伴). 特别地, 本原多项式之积也为本原多项式.

证明. 记 $f=\sum_{i=0}^{n}a_iX_i, g=\sum_{j=0}^{m}b_jX^j$. 若 $d(f),d(g)$ 可逆而 $d(fg)$ 不可逆, 则可取素元 $p|d(fg)$, 而取最小的下标 s,t 使得 $p\nmid a_s, p\nmid b_t$, 而 fg 中 X^{s+t} 的系数为 $c_{s+t}=\sum_{i+j=s+t}a_ib_j=a_sb_t+(a_{s+1}b_{t-1}+a_{s+2}b_{t-2}+\cdots)+(a_{s-1}b_{t+1}+a_{s-2}b_{t+2}+\cdots)$, 由 s,t 的最小性可知 p 整除右端后两项. 而 $p|d(fg)|c_{s+t}$, 因此 $p|a_sb_t$. 由于 R 是 UFD, 因此 $p|a_s$ 或 $p|b_t$, 矛盾. 因此 $d(fg)$ 可逆.

考虑一般的多项式 $f=d(f)f_0, g=d(g)g_0, f_0,g_0$ 是本原多项式, 则 $d(fg)=d(f)d(g)d(f_0g_0)\approx d(f)d(g)$. □

命题 2.16. $f\in\mathbb{Z}[X]$, 若 f 在 $\mathbb{Z}$ 上既约, 则其在 $\mathbb{Q}$ 上既约.

证明. 若 f 在 $\mathbb{Q}$ 上不是既约的, 即 $f=gh, f\in\mathbb{Z}[X], g,h\in\mathbb{Q}[X]$, 则实际上其可被化为 $\mathbb{Z}[X]$ 上的等式 $af=bg_0h_0$, 其中 $g_0,h_0\in\mathbb{Z}[X]$ 是本原多项式. 由 Gauss 引理,$ad(f)=b$, 因此有 $f=d(f)g_0h_0$, 矛盾. □

定理 2.17 (Eisenstein 判别法)**.** $f=\sum_{i=0}^{n}a_iX^i\in\mathbb{Z}[X]$, 若存在素数 p 使得 $p\nmid a_n, p|a_i(i=0,\cdots,n-1), p^2\nmid a_0$, 则 f 在 $\mathbb{Q}$ 上是既约的.

证明. 反证, 若 f 在 $\mathbb{Q}$ 上不既约, 则由命题2.16知其可被分解为 $\mathbb{Z}$ 上两多项式之积, 即 $f=gh, g=\sum_{j=0}^{s}b_jX^j, h=\sum_{k=0}^{t}c_tX^t$. 将其模 p, 由条件可得 $\overline{a_n}X^n=\left(\sum_{j=0}^{s}\overline{b_j}X^j\right)\left(\sum_{k=0}^{t}\overline{c_k}X^k\right)$, 其中 $\overline{b_j},\overline{c_k}$ 是 b_j,c_k 模 p 后在 $\mathbb{Z}_p$ 中的剩余类. 比较系数, 注意到 $0=\overline{b_0}\overline{c_0}$, 即 $p^2|b_0c_0=a_0$, 矛盾, 故得证. □

2.3 分式域

我们将考虑如何将 $\mathbb{F}[X]$ 嵌入到一个域中, 实际上正如我们将 $\mathbb{Z}$ 嵌入 $\mathbb{Q}$ 中一样. 为保证问题的一般性, 我们将考虑任意整环 R.

构造过程是简单的. 在 $R\times R^*$ 上构造等价关系 $(a,b)\sim(c,d)\iff ad=bc$, 注意到整性使得其传递性成立. 令 $Q(R)=(R\times R^*)/\sim$, 仅需验证这是一个域即可, 记 (a,b) 所在其中的等价类为 $[a,b]$. 我们给定其上的加法运算 $[a,b]+[c,d]=[ad+bc,bd]$ 和乘法运算 $[a,b][c,d]=[ac,bd]$. 容易验证这些运算不依赖于代表元的选取, 并且在这些运算下 $Q(R)$ 成为一个域 (实际上即验证结合律, 分配律, 交换律, 含幺以及可逆). 最后, 可以给出一个环的单同态 $f:R\to Q(R), a\mapsto[a,1]$, 因此可以将 a 和 $[a,1]$ 等同看待, 即将 R 和 $f(R)$ 等同看待.

由于 $[b,1][a,b]=[a,1]$, 我们可以记 $[a,b]$ 为 a/b 或 $\frac{a}{b}$, 并称 $Q(R)$ 为 R 的分式域 (Field of fractions, 或分式环).

容易发现,$Q(\mathbb{Z})=\mathbb{Q}$, 而 $Q(\mathbb{F})\cong\mathbb{F}$. 可以证明,$R$ 是 $\mathbb{F}$ 的子环, 且 $\forall x\in\mathbb{F}: x=a/b, a\in R, b\in R^*$ 时,$Q(R)\cong\mathbb{F}$.

对于整环 $\mathbb{F}[X]$ 构成的分式域, 我们记其为 $\mathbb{F}(X)$, 称之为变元 X 在域 $\mathbb{F}$ 中的有理函数域, 其中的元素被称为有理函数. 可以证明,$\operatorname{char}\mathbb{F}(X)=\operatorname{char}\mathbb{F}$. 我们称其中的元素 f/g 的次数 $\deg f/g:=\deg f-\deg g$. 若 $\gcd(f,g)=1$, 则 f/g 被称为既约分式. 若 $\deg f/g<0$, 则称其为真分式. 实际上可以说明, 任一有理函数可被写作一多项式和一真分式的和. 最后,$\mathbb{F}(X)$ 中所有真分式连带其上的加法和乘法运算构成一个不含幺的环.

我们称 f/g 是最简分式, 若 $g=p^n, n\in\mathbb{Z}_{>0}, p\in\mathbb{F}[X]$ 是既约的. 我们有

定理 2.18. 真分式可被唯一表为最简分式的和.

证明. $f/g\in\mathbb{F}(X)$ 是给定真分式, 不失一般性地可以认为 g 首一.

①若 $g=g_1g_2$ 是互素首一多项式之积, 则 $\frac{f}{g}=\frac{f_1}{g_1}+\frac{f_2}{g_2}$, 右端两式均为真分式, 且分解唯一.

首先有 $u_1g_1+u_2g_2=1$, 再有带余除法 $fu_2=qg_1+f_1$, 则有 $f=f_1g_2+f_2g_1$, 即有此分解. 显然 f_1/g_1 是真分式, 而 $f_2/g_2=f/g-f_1/g_1$ 也是真分式 (由 $\deg fg_1<\deg g_1g_2, \deg f_1g<\deg g_1g_2$). 最后唯一性易证.

②若有标准分解 $g=\prod_{i=1}^{m}p_i^{\alpha_i}$, 则有唯一分解式 $\frac{f}{g}=\sum_{i=1}^{m}\frac{f_i}{p_i^{\alpha_i}}$, 其中 $\frac{f_i}{p_i^{\alpha_i}}$ 是真分式 (也称准素分式).

这一论断由上归纳可立即得到.

③所有真准素分式 $\frac{f}{p^n}$ 都可以被唯一表为最简分式的和.

由于 $\deg f<n\deg p$, 由辗转相除法给出一系列等式:$f=q_1p^{n-1}+r_1, r_1=q_2p^{n-2}+r_2,\cdots,r_{n-2}=q_{n-1}p+r_{n-1}, r_{n-1}=q_n$. 综上,$\frac{f}{p^n}=\frac{q_1}{p}+\frac{q_2}{p^2}+\cdots+\frac{q_n}{p^n}$. 由于 $\deg q_i<\deg p$(可以证明), 因此上式右端为最简分式之和. 根据带余除法, 这是唯一确定的.

综上, 定理得证. □

2.4 多项式根的一般性质

多项式的根 设整环 R 的子环 A 是含幺交换环.

定义 9 (多项式的根)**.** *$c\in R$ 被称为 $f\in A[X]$ 的根 (或零点), 若 $f(c)=0$.*

定理 2.19 (Bézout 定理)**.** *$c\in A$ 是 $f\in A[X]$ 的根 $\iff$ $X-c$ 在 $A[X]$ 中整除 f.*

证明. 仅需用 $X-c$ 除 f, 注意到余项为常数 (即为 $f(c)$) 即可. □

由此定理, 我们可以使用 Horner 方法 (又称综合除法) 来处理带余除法. 设 $f=\sum_{i=0}^{n}a_iX^i, q=\sum_{i=0}^{n-1}b_iX^i, f=(X-c)q+f(c)$, 则为计算 q 有一系列等式 $b_{n-1}=a_n, b_{k-1}=cb_k+a_k, f(c)=cb_0+a_0$.

由 Bézout 定理, 我们有

定义 10 (多重根)**.** *$c\in A$ 被称为 $f\in A[X]$ 的 k 重根, 若 $(X-c)^k|f$ 但 $(X-c)^{k+1}\nmid f$.*

定理 2.20. *R 是整环,$f\in R[X]^*, c_1,\cdots,c_r\in R$ 是 f 的 $k_1,\cdots,k_r$ 重根, 则 $f(X)=g(X)\prod_{i=1}^{r}(X-c_i)^{k_i}, g\in R[X], g(c_i)\neq 0$. 特别地,$\sum_{i=1}^{r}k_i\leq\deg f$.*

证明. 注意到 $Q(R)[X]$ 是 UFD 即可. □

命题 2.21. *R 是整环,$f,g\in R[X]$ 是次数 $\leq n$ 的多项式, 若其在 $n+1$ 个不同元素上取值相同, 则 $f=g$.*

多项式函数 注意到 $f\in A[X]$ 对应于一个函数 $\tilde{f}:A\to A, a\mapsto f(a)$, 后者全体构成环 A_{pol}, 称之为多项式函数环 (或整有理函数环), 这是 A^A 的子环.

对于 $A=\mathbb{F}_p$ 的情况,$f(X)=(X^p-X)g(X)\in A[X]$ 有 $\tilde{f}=0$, 有 Fermat 小定理易知. 仅当 $\deg f\leq p-1$ 时 $f\in\mathbb{F}_p(X)$ 才由自己的函数确定, 任意 $f\in\mathbb{F}_p[X]$ 可以用次数 $\leq p-1$ 的唯一确定的约化多项式 f^* 代替, 后者是 f 除以 X^p-X 得到的余式. 显然 $\tilde{f}=\tilde{f^*}$.

定理 2.22. *若 R 是无限的整环, 则 $R[X]\to R_{\mathrm{pol}}, f\mapsto\tilde{f}$ 是环同构.*

2.5 对称多项式

2.6 $\mathbb{C}$ 的代数封闭性

2.7 实系数多项式

Chapter 3

矩阵与线性映射

矩阵与线性映射之间的自然联系也是易知的, 在此不作赘叙. 用符号来写, 对于 $\dim U = m, \dim V = n$ 的线性空间,$\hom(U, V) \cong \mathbb{F}^{m\times n}$. 线性映射的矩阵表示是自然的, 在此不作赘叙.

需要注意的是, 尽管两者有如此紧密的联系, 但是两者在处理很多不同的内容时表现是相当不一样的, 如矩阵的打洞 (即灵活的分块矩阵) 与线性映射下的某些观点是完全不同的表现, 而后者常常在数学上更加深刻, 最起码在线性代数这门基础学科中. 这并不是说矩阵更差, 事实上, 矩阵分析在未来可能会填入或新增为一本笔记, 而那是十分重要的一门课程.

最后, 我们默认读者已经熟知矩阵的基础运算和矩阵的分块.

3.1 矩阵的基础命题

矩阵的基本性质

1. $[A, B] := AB - BA$ 是一个 Lie 括号, 即其是双线性反对称的, 且满足 Jacobi 恒等式 $\sum\limits_{cyc}[A, [B, C]] = O$.
2. $\begin{pmatrix} a & c \\ 0 & b \end{pmatrix}^n = \begin{pmatrix} a^n & \dfrac{a^n - b^n}{a - b}c \\ 0 & b^n \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^n = \begin{pmatrix} f_{n-1} & f_n \\ f_n & f_{n+1} \end{pmatrix}$.
3. 旋转矩阵
4. 奇数阶斜对称矩阵的行列式为 0, 偶数阶斜对称矩阵的行列式为 $\mathbb{F}$ 中某元素的平方.
5. $\operatorname{char}\mathbb{F} \neq 2$ 时斜对称矩阵的秩为偶数.(说明任一矩阵 A 的行/列向量组的极大线性无关组对应的 $\operatorname{rank} A$ 阶子式非零)
6. 若 A, B 均为斜对称矩阵, 则 $[A, B]$ 也为斜对称矩阵.
7. 上三角矩阵的积也为上三角矩阵. 特别地, 对角矩阵的积也为对角矩阵.
8. $\det AB = \det A \cdot \det B$.(计算分块矩阵的行列式)

特殊矩阵

1. 循环矩阵 $C = \begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & \ddots & \ddots & \\ & & & 0 & 1 \\ 1 & & & & 0 \end{pmatrix}, C^n = I_n$. 对 $f \in \mathbb{F}[x]_{n-1}, \det f(C) = \prod\limits_{k=0}^{n-1} f(\mathrm{e}^{\frac{2k\pi}{n}\mathrm{i}})$.
2. 矩阵 $J = \begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & \ddots & \ddots & \\ & & & 0 & 1 \\ & & & & 0 \end{pmatrix}, J^n = O$.
3. 基本矩阵 E_{ij}: 仅在 $a_{ij} = 1$ 处非零

4. 初等矩阵 $F_{ij}=I-E_{ii}-E_{jj}+E_{ij}+E_{ji}; F_{ij}(\lambda)=I+\lambda E_{ij}, F_i(\lambda)=I+(\lambda-1)E_{ii}$.
   将这些矩阵左/右乘上矩阵, 即对矩阵作相应的初等行/列变换: 交换 i,j 行; 将 λ 倍第 j 行加到第 i 行上, 或将 λ 倍第 i 列加到第 j 列上; 将第 i 行/列乘上 λ 倍.
5. 主对角占优矩阵行列式非零.

矩阵的秩

1. $\operatorname{rank}\begin{pmatrix}A & C\\ O & B\end{pmatrix}\geq \operatorname{rank}A+\operatorname{rank}B$, 且在 $C=O$ 时, 或在 A,B 均行/列满秩时取等.
2. $\max\{\operatorname{rank}A,\operatorname{rank}B\}\leq\operatorname{rank}(A|B)\leq\operatorname{rank}A+\operatorname{rank}B$.
3. $\operatorname{rank}AB\leq\min\{\operatorname{rank}A,\operatorname{rank}B\}$
4. $\operatorname{rank}(A+B)\leq\operatorname{rank}A+\operatorname{rank}B$
5. $\operatorname{rank}AA^{\mathsf{H}}=\operatorname{rank}A^{\mathsf{H}}A=\operatorname{rank}A$(用 Binet-Cauchy 公式)
6. (Sylvester 秩不等式)$\operatorname{rank}AB\geq\operatorname{rank}A+\operatorname{rank}B-n$
7. (Frobenius 秩不等式)$\operatorname{rank}ABC\geq\operatorname{rank}AB+\operatorname{rank}BC-\operatorname{rank}B$(考虑分块矩阵)
8. 幂等矩阵 (即 $A^2=A$) $\Longleftrightarrow$ $\operatorname{rank}A+\operatorname{rank}(I-A)=n$
9. 对合矩阵 (即 $A^2=I$) $\Longleftrightarrow$ $\operatorname{rank}(I-A)+\operatorname{rank}(I+A)=n$

可逆矩阵 我们定义 $A\in M_n(\mathbb{F})$ 的伴随矩阵 $A^\vee=(A_{ji})_{n\times n}\in M_n(\mathbb{F})$, 其中 A_{ij} 是相对 a_{ij} 元的代数余子式. 由行列式的展开结论可知:$A^\vee A=AA^\vee=(\det A)I_n$. 换言之,$A^{-1}=\dfrac{A^\vee}{\det A}$. 综合定理1.16的推论, 我们给出重要的结论

定理 3.1. *对于方阵, 满秩 $\Longleftrightarrow$ 可逆 $\Longleftrightarrow$ 行列式非零 $\Longleftrightarrow$ 对应的线性方程组有唯一解 $\Longleftrightarrow$ 对应的线性映射非退化 $\Longleftrightarrow$ 行/列向量组线性无关 (为 $\mathbb{F}^n$ 的一个基, 或者说张成空间为 $\mathbb{F}^n$).*

在此不加证明的给出一些伴随矩阵的性质:

1. A 可逆则 $A^\vee$ 可逆, 且 $(A^\vee)^{-1}=\dfrac{A}{\det A}$.
2. $\operatorname{rank}A^\vee=\begin{cases}n, & \operatorname{rank}A=n\\ 1, & \operatorname{rank}A=n-1\\ 0, & \operatorname{rank}A<n-1\end{cases}$, $\det A^\vee=(\det A)^{n-1}$.
3. $(A^\vee)^\vee=\begin{cases}(\det A)^{n-2}A, & n\geq 3\\ A, & n=2\end{cases}$
4. $(AB)^\vee=B^\vee A^\vee$

容易证明, 矩阵的逆矩阵是唯一的, 矩阵的逆运算也是对偶的. 换言之,$\mathrm{GL}_n(\mathbb{F})$ 是一个乘法群. 我们在此叙述一些可逆矩阵的性质.

1. $(A^{\mathsf{T}})^{-1}=(A^{-1})^{\mathsf{T}}$.
2. 可逆矩阵化为的简化行阶梯形矩阵为 I_n.
3. $P\in\mathrm{GL}_n(\mathbb{F}),\operatorname{rank}PA=\operatorname{rank}AP=\operatorname{rank}A$.

由最后一条性质, 可知将 A 变为 I_n 的初等行变换同样将 I_n 变为 A^{-1}. 因此可仅作初等行变换 $(A|I_n)\to(I_n|A^{-1})$. 这是重要的计算逆矩阵的方法. 值得一提的是这一基于 Gauss 消元法的方法的复杂度为 $O(n^3)$.

4. 上三角矩阵的逆矩阵也为上三角矩阵
5. $(aI_n+b1_{n\times n})^{-1}=\dfrac{1}{a}\left(I_n-\dfrac{b}{a+nb}1_{n\times n}\right),(aI_n+bJ_n)^{-1}=\dfrac{1}{a}\displaystyle\sum_{k=0}^{n-1}\left(-\frac{b}{a}J_n\right)^k$.
6. $f(A)=\displaystyle\sum_{k=0}^{m}a_kA^k=O,a_0\neq 0$, 则 $A^{-1}=-\displaystyle\sum_{k=0}^{m-1}\frac{a_{k+1}}{a_0}A^k$.
7. $A\in\mathbb{F}^{m\times n},B\in\mathbb{F}^{n\times m}$, 且 I_m-AB 可逆, 则 $(I_n-BA)^{-1}=I_n+B(I_m-AB)^{-1}A$.
8. $A,B,D\in M_n(\mathbb{F}),A,D$ 可逆且 $B^{\mathsf{T}}A^{-1}B+D^{-1}$ 可逆, 则 $(A+BDB^{\mathsf{T}})^{-1}=A^{-1}-A^{-1}B(B^{\mathsf{T}}A^{-1}B+D^{-1})^{-1}B^{\mathsf{T}}A^{-1}$.
9. $\begin{pmatrix}A & C\\ O & B\end{pmatrix}^{-1}=\begin{pmatrix}A^{-1} & -A^{-1}CB^{-1}\\ O & B^{-1}\end{pmatrix},\begin{pmatrix}A & B\\ C & D\end{pmatrix}^{-1}=\begin{pmatrix}A^{-1}+A^{-1}B(D-CA^{-1}B)^{-1}CA^{-1} & -A^{-1}B(D-CA^{-1}B)^{-1}\\ -(D-CA^{-1}B)^{-1}BA^{-1} & (D-CA^{-1}B)^{-1}\end{pmatrix}$

矩阵的相抵

3.2 线性映射的基本性质

3.3 矩阵的相似

3.4 特征值与特征向量

3.5 对角化

3.6 矩阵的分解

3.7 广义逆矩阵

Chapter 4

相似标准型

4.1 极小多项式与 Hamilton-Cayley 定理

4.2 λ 矩阵

4.3 Jordan 标准型

4.4 有理标准型

4.5 对偶空间

Chapter 5

双线性函数

Chapter 6

Euclid 空间

Chapter 7

酉空间

Chapter 8

张量

Chapter 9

仿射空间与 Euclid 点空间

Chapter 10

二次曲面