中国科学院大学课程讲义

线性代数 I

中国科学院大学　　数学科学学院

作者：支丽红

编者：禹天石

鸣谢：梁昊　刘俊杞　郑涛

2025 年 7 月 6 日

目录

第一章　代数的起源

1.1　简谈代数

Leoplod Kroncker(利奥波德 · 克罗内克，1823-1891，德国数学家) 曾说过：

“God made the integers, all else is the work of man.” 最基本的正整数的含义几乎是不言自明的 (虽然我们可以用皮亚诺公理的方法更形式化地构造它，有关内容参见习题课讲义)。

从

$$\text{”}1, 2, 3, \cdots\text{”}$$

到

$$\text{”}0, 1, 2, 3, \cdots\text{”}$$

是数学的一大进步 (印度人引入了 ”0”)。之后我们引入了负数 (加法可求逆)，有理数 (乘法可求逆)，实数 (极限运算封闭)，复数 (代数闭域)。对于数和数的运算是代数的基本任务之一。

代数最初起源于如下几个问题：

1. 解方程与数系的扩张：

   - $2x = 1 \Rightarrow x = 1/2$. 我们得到了有理数。
   - $x^2 = 2 \Rightarrow x = \pm\sqrt{2}$. 我们得到了无理数。
   - $x^2 = -1 \Rightarrow x = \pm i$. 我们得到了复数。

2. 几何：

   - $ax = b$. 一元一次方程，对应点。
   - $\begin{cases} ax + by = c \\ dx + ey = f \end{cases}$ 二元一次方程组表示平面上的直线的位置。

   Sophie Germain(索菲 · 热尔曼，法国女数学家，1776-1831) 曾说：
   “代数不外是符号的几何，而几何不外是图形的代数。”

3. 一元二次方程

   对 $ax^2 + bx + c = 0, a, b, c \in \mathbb{R}, a \neq 0$，我们做如下变形：

$$x^2 + px + q = 0, p = \frac{b}{a}, q = \frac{c}{a}.$$

$$\text{令} x = y - \frac{p}{2}, \text{得} (y - \frac{p}{2})^2 + p(y - \frac{p}{2}) + q = 0.$$

$$y^2 + (q - \frac{p^2}{4}) = 0.$$

即

$$y = \pm\sqrt{\frac{p^2}{4} - q}.$$

所以

$$x = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

代数：把含有符号的表达式恒等变形为所需要的形式。

4. 一元三次方程

   对于 $ax^3 + bx^2 + cx + d = 0, a, b, c, d \in \mathbb{Q}, a \neq 0$，我们需要作稍微复杂的处理。以下解法被称之为 Cardano formula 卡丹公式，关于这个公式有一段著名的知识产权公案。Tartaglia Nicolo(1500-1557 意大利数学家）塔尔塔利亚 1541 首先给出了三次方程求解公式，被 Girolanmo Cardano (1501-1576 意大利医生、代数和概率论家、赌徒《论赌博游戏》) 卡尔达诺 1545 年在自己的著作《大法》公布了三次方程求解的卡丹公式。

   首先，首项系数归一有：$x^3 + \frac{b}{a}x^2 + \frac{c}{a}x + \frac{d}{a} = 0.$

   令 $x = y - \frac{b}{3a}$，可以消去二次项，得到如下形式：

$$y^3 + py + q = 0.$$

   再令 $y = z - \frac{p}{3z}$，得

$$z^6 + qz^3 - \frac{p^3}{27} = 0(\text{预解式})$$

   这是一个关于 z^3 的二次方程，于是可以求出 z^3，进而通过复数开立方求出 z。然后，由 $y = z - \frac{p}{3z}$ 解出 y，由 $x = y - \frac{b}{3a}$ 解出 x。

5. 一元四次方程

   类似的求解公式由卡丹的学生费拉里得到，感兴趣的同学可以自行查阅。

6. 一元五次方程

   Niels Henrik Abel(尼尔斯 · 亨利克 · 阿贝尔，1802-1829，挪威数学家) 最早证明了一般的五次方程没有根式解。

   Évariste Galois(埃瓦里斯特 · 伽罗瓦，1811-1832，法国数学家) 用群论彻底解决了根式求解代数方程的问题，而且由此发展了一整套关于群和域的理论，称之为伽罗瓦理论。

   他得到结论：对于一般的 n 次有理系数方程，它可以根式求解等价于它对应的伽罗瓦群是可解群。例如，$x^5 - x - 1 = 0$ 不可以根式求解，而 $x^5 - 1 = 0$ 可以。

线性代数研究多元一次 (即线性) 方程或方程组，抽象代数研究一元高次方程 (组)，而一般方程组的解的情况则是代数几何研究的对象。

1.2 线性方程组初步

1.2.1 线性方程组与矩阵

现在我们讨论线性代数中最基本的研究对象：线性方程组。对

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \qquad\qquad\qquad\qquad \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \end{cases} \tag{L}$$

其中 a_{ij}, b_i 都是实数，$i = 1, 2 \ldots m, j = 1, 2 \ldots n$. $x_1 \ldots, x_n$ 都是未知数。

令

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

称为 (L) 的系数矩阵 (coefficient matrix)，而

$$B = \left(\begin{array}{c:c} & b_1 \\ A & \vdots \\ & b_m \end{array} \right) = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{pmatrix}$$

称为 A 关于 $\begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$ 的增广矩阵 (augmented matrix)。称 (L) 是由 B 确定的线性方程组。

关于矩阵的若干名词

我们将

$$A = (a_{ij})_{\substack{i=1,\ldots m \\ j=1,\ldots n}} = (a_{ij})_{m \times n}.$$

称为实数上 $m \times n$ 的矩阵，称 $\overrightarrow{A_i} = (a_{i1}, \ldots, a_{in})$ 为 A 的第 i 行，$\overrightarrow{A^{(j)}} = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix}$ 为 A 的第 j 列。为了书写简便，我们以后也用加粗的 $\mathbf{A}_i$ 和 $\mathbf{A}^{(j)}$ 来记行向量和列向量。a_{ij} 称为位于 A 中第 i 行第 j 列处的元素。$m = n$ 时 A 称为方阵。

关于行 (列) 的运算

记 $\overrightarrow{u} = (u_1, \ldots, u_n), \overrightarrow{v} = (v_1, \ldots, v_n)$，其中 $u_i, v_i, i = 1, \ldots, n$ 是实数，另外 $\alpha \in \mathbb{R}$。则

$$\overrightarrow{u} \pm \overrightarrow{v} = (u_1 \pm v_1, \ldots, u_n \pm v_n)$$
$$\alpha \overrightarrow{u} = (\alpha u_1, \ldots, \alpha u_n).$$

例 1.2.1. 求解

$$\begin{cases} x + 2y = 3 & (1.2.1) \\ 2x + 3y = 1 & (1.2.2) \end{cases}$$

解. (1.2.2)-2×(1.2.1) 得 $-y = -5 \Rightarrow y = 5$. 再代入 (1.2.1) 式得 $x = -7$. 于是方程组的解为

$$\begin{cases} x = -7 \\ y = 5 \end{cases}$$

用矩阵表示以上过程即：

$$\underbrace{\left(\begin{array}{cc:c} 1 & 2 & 3 \\ 2 & 3 & 1 \end{array}\right)}_{B} \xrightarrow{\mathbf{B}_2 - 2\mathbf{B}_1} \underbrace{\left(\begin{array}{cc:c} 1 & 2 & 3 \\ 0 & -1 & -5 \end{array}\right)}_{C} \xrightarrow{(-1)\times\mathbf{C}_2} \underbrace{\left(\begin{array}{cc:c} 1 & 2 & 3 \\ 0 & 1 & 5 \end{array}\right)}_{D} \xrightarrow{\mathbf{D}_1 - 2\mathbf{D}_2} \left(\begin{array}{cc:c} 1 & 0 & -7 \\ 0 & 1 & 5 \end{array}\right).$$

□

1.2.2 线性方程组的相容性

定义 1.2.1. 如果线性方程组 (L) 有解，则称 (L) 是相容的，否则称 (L) 是不相容的。

下面我们通过一个具体例子来说明这一概念。对方程组

$$\begin{cases} 2x_1 - x_2 + 3x_3 = 1 \\ 4x_1 - 2x_2 + 5x_3 = 5 \\ 2x_1 - x_2 + 4x_3 = -1 \end{cases}$$

用矩阵形式作如下变形：

$$\begin{pmatrix} 2 & -1 & 3 & 1 \\ 4 & -2 & 5 & 5 \\ 2 & -1 & 4 & -1 \end{pmatrix} \xrightarrow{r_2-2r_1} \begin{pmatrix} 2 & -1 & 3 & 1 \\ 0 & 0 & -1 & 3 \\ 2 & -1 & 4 & -1 \end{pmatrix}$$

$$\xrightarrow{r_3-r_1} \begin{pmatrix} 2 & -1 & 3 & 1 \\ 0 & 0 & -1 & 3 \\ 0 & 0 & 1 & -2 \end{pmatrix} \xrightarrow{r_3+r_2} \begin{pmatrix} 2 & -1 & 3 & 1 \\ 0 & 0 & -1 & 3 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

即得到 $0 \cdot x_3 = 1$，矛盾！于是原方程组无解，即不相容。

定义 1.2.2. 设 (L) 是相容的，若 (L) 有唯一解，则称 (L) 是确定的，否则称为不确定的。

例 1.2.2. 对方程组

$$\begin{cases} x_1 + x_2 + x_3 = 1 \\ ax_2 + x_3 = 0 \\ x_3 = b \end{cases}$$

其中 $a, b \in \mathbb{R}$. 则

1. $a \neq 0$：确定；

2. $a = 0, b \neq 0$：不相容；

3. $a = b = 0$：方程组可化为 $\begin{cases} x_1 + x_2 + x_3 = 1 \\ x_3 = 0 \end{cases}$ 显然是不确定的。

1.2.3 等价的线性方程组

定义 1.2.3. 设 (L) 和 (L') 是关于 $x_1, \ldots, x_n$ 的两个线性方程组，如果 (L) 和 (L') 都不相容，或者 (L) 和 (L') 同解，则称 (L) 和 (L') 是等价的。

定义 1.2.4. (**矩阵的初等行变换**) 设 M 是矩阵。

(I) 把 M 的两行互换位置，即：

$$M = \begin{pmatrix} \vdots \\ \mathbf{M}_i \\ \vdots \\ \mathbf{M}_j \\ \vdots \end{pmatrix} \longrightarrow \begin{pmatrix} \vdots \\ \mathbf{M}_j \\ \vdots \\ \mathbf{M}_i \\ \vdots \end{pmatrix}$$

(II) 设 $i \neq j, \alpha \in \mathbb{R}$. 把 M 的第 i 行乘以 α 后加到第 j 行，即：

$$M = \begin{pmatrix} \vdots \\ \mathbf{M}_i \\ \vdots \\ \mathbf{M}_j \\ \vdots \end{pmatrix} \longrightarrow \begin{pmatrix} \vdots \\ \mathbf{M}_i \\ \vdots \\ \mathbf{M}_j + \alpha\mathbf{M}_i \\ \vdots \end{pmatrix}$$

(III) 设 $\alpha \neq 0$，把 M 的第 i 行乘以 α，即：

$$M = \begin{pmatrix} \vdots \\ \mathbf{M}_i \\ \vdots \end{pmatrix} \longrightarrow \begin{pmatrix} \vdots \\ \alpha\mathbf{M}_i \\ \vdots \end{pmatrix}$$

引理 1.2.1. 设线性方程组 (L) 对应增广矩阵 B，对 B 做 (I)、(II) 或 (III) 类初等行变换得到矩阵 B'，B' 对应的线性方程组为 (L')，则 (L) 与 (L') 等价。

证明. (I) 类变换是调换两个方程的次序，(III) 类变换是对某一个方程乘以一个非零常数，显然不改变方程组的解的情况。下面考虑 (II) 类变换。

设

$$B = \begin{pmatrix} \vdots \\ \mathbf{B}_i \\ \vdots \\ \mathbf{B}_j \\ \vdots \end{pmatrix} \longrightarrow B' = \begin{pmatrix} \vdots \\ \mathbf{B}_i \\ \vdots \\ \mathbf{B}_j + \alpha\mathbf{B}_i \\ \vdots \end{pmatrix}$$

设 $\begin{cases} x_1 = \alpha_1 \\ \quad \vdots \\ x_n = \alpha_n \end{cases}$ 是 (L) 的解，由于 (L) 与 (L') 只有第 j 个方程不同，而将这个解代入第 j 个方程左侧有：

$$\begin{aligned} &(a_{j1} + \alpha a_{i1})\alpha_1 + \cdots + (a_{jn} + \alpha a_{in})\alpha_n \\ &= (a_{j1}\alpha_1 + \cdots + a_{jn}\alpha_n) + \alpha(a_{i1}\alpha_1 + \cdots + a_{in}\alpha_n) \\ &= b_j + \alpha b_i \\ &= \text{右侧}. \end{aligned}$$

于是 $\begin{cases} x_1 = \alpha_1 \\ \quad \vdots \\ x_n = \alpha_n \end{cases}$ 是 (L') 的解。

反过来，设 $\begin{cases} x_1 = \alpha'_1 \\ \vdots \\ x_n = \alpha'_n \end{cases}$ 是 (L') 的解，代入 (L) 的第 j 个方程，同理有：

$$\begin{aligned} \sum_{k=1}^{n} a_{jk}\alpha'_k &= \sum_{k=1}^{n}(a_{jk} + \alpha a_{ik} - \alpha a_{ik})\alpha'_k \\ &= \sum_{k=1}^{n}(a_{jk} + \alpha a_{ik})\alpha'_k - \alpha\sum_{k=1}^{n} a_{ik}\alpha'_k \\ &= b_j + \alpha b_i - \alpha b_i \\ &= b_i = \text{右侧}. \end{aligned}$$

于是命题成立。

□

1.2.4 解线性方程组：消元法

这一小节我们主要的任务是用矩阵的语言描述中学学过的消元法解线性方程组。

定义 1.2.5. 称矩阵 M 为行阶梯型 (row-echelon form) 矩阵，如果

$$M = \begin{pmatrix} * & \cdots & * & \square & \cdots & * & \cdots & * & \cdots & * \\ 0 & \cdots & 0 & 0 & \cdots & \square & \cdots & * & \cdots & * \\ \vdots & & \vdots & \vdots & & \vdots & \ddots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 & \cdots & \square & \cdots & * \\ 0 & \cdots & 0 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots & & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \end{pmatrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \end{matrix} \left.\begin{matrix} \\ \\ \\ \\ \end{matrix}\right\} r \text{ 行},$$

其中 $\square \neq 0$, $* \in \mathbb{R}$ 任意，$r \leqslant$ 行数。特别地，对于方阵 A，若 $\forall i > j, a_{ij} = 0$，则称 A 为上三角矩阵；若 $\forall i < j, a_{ij} = 0$，则称 A 为下三角矩阵。

例 1.2.3. $M = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$ 就是一个行阶梯型矩阵。

引理 1.2.2. 设 A 是矩阵，则通过有限次 (I) 和 (II) 类初等行变换可以将 A 化为阶梯型。

证明. 设 A 是 $m \times n$ 阶矩阵。对 m 作归纳。

$m = 1$ 时，A 本身是阶梯型。

设 $m > 1$ 且引理对 $m-1$ 行的矩阵成立。设 $A = (a_{ij})_{m\times n}$ 且 a_{ij} 不全为 0。不妨设 A 前 $k-1$ 列中的元素全为 0，但第 k 列中 $a_{lk} \neq 0$，则

(1) 交换 A 的第 l 行与第 1 行，得

$$A' = \begin{pmatrix} \overbrace{0 & \cdots & 0}^{k-1\text{列}} & a'_{1k} & \cdots & a'_{1n} \\ 0 & \cdots & 0 & a'_{2k} & \cdots & a'_{2n} \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & a'_{mk} & \cdots & a'_{mn} \end{pmatrix}$$

其中 $a'_{1k}=a_{lk}\neq 0$.

(2) $A' \xrightarrow{r_2-\frac{a'_{2k}}{a'_{1k}}r_1} A'' \xrightarrow{r_3-\frac{a'_{3k}}{a'_{1k}}r_1} A''' \longrightarrow \cdots \xrightarrow{r_m-\frac{a'_{mk}}{a'_{1k}}r_1} A^{(m)}$，则有：

$$A^{(m)}=\underbrace{\begin{pmatrix} 0 & \cdots & 0 & \square & * & \cdots & * \\ 0 & \cdots & 0 & 0 & * & \cdots & * \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & * & \cdots & * \end{pmatrix}}_{k\text{列}} \Bigg\} B$$

其中 B 是 $A^{(m)}$ 去掉第一行后得到的 $(m-1)\times n$ 矩阵。

(3) 由归纳假设，B 可以通过有限次 (I)、(II) 类初等变换得到行阶梯型矩阵：

$$B'=\underbrace{\begin{pmatrix} 0 & \cdots & 0 & \square & * & \cdots & * & * & \cdots & * \\ 0 & \cdots & 0 & 0 & * & \cdots & * & \square & \cdots & * \\ \vdots & & \vdots & & & & & & \vdots & \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix}}_{s\geqslant k}$$

(4) 由 (2) 和 (3) 立刻得到 A 可以通过有限次 (I)、(II) 类初等行变换化成行阶梯型。

□

定理 1.2.1. 设 (L) 是以 $\left(\begin{array}{c|c} & b_1 \\ A & \vdots \\ & b_m \end{array}\right)$ 为增广矩阵的线性方程组，则 (L) 等价于一个系数矩阵为行阶梯型的方程组 (L')，即 (L') 的增广矩阵为 $\left(\begin{array}{c|c} & b'_1 \\ A' & \vdots \\ & b'_m \end{array}\right)$，其中 A' 是行阶梯型矩阵。

证明. 对 A 作有限次初等行变换，由引理1.2.1及引理1.2.2，定理成立。 □

注 1.2.1. 我们把 $(L)\longrightarrow(L')$(阶梯型) 的方法称为 Gauss 消去法。

例 1.2.4. 令

$$A=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ 0 & a_{12} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_{nn} \end{pmatrix}_{n\times n}$$

其中 $a_{11},a_{12},\cdots,a_{nn}$ 都非零，另有 $b_1,b_2,\cdots,b_n$ 为任意实数。令

$$B=\left(\begin{array}{c|c} & b_1 \\ A & \vdots \\ & b_n \end{array}\right),$$

则 B 对应的线性方程组 (T) 有唯一解。

解. B 对应的线性方程组为

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ \qquad\quad a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \qquad\qquad\qquad\quad \vdots \\ \qquad\qquad\qquad\quad a_{nn}x_n = b_n \end{cases} \tag{T}$$

于是有

$$x_n = \frac{b_n}{a_{nn}},\ x_{n-1} = \frac{1}{a_{n-1,n-1}}(b_{n-1} - a_{n-1,n}x_n), \ldots, x_1 = \frac{1}{a_{11}}(b_1 - a_{12}x_2 - \cdots - a_{1n}x_n).$$

□

定理 1.2.2. 设线性方程组 (L) 的增广矩阵为 $\left(\begin{array}{c|c} & b_1 \\ A & \vdots \\ & b_m \end{array}\right)$ 其中 A 是 $m \times n$ 阶的阶梯形矩阵。A 中前 r 行含有非零元素，而后 $m-r$ 行全为 0。则

i) (L) 相容 $\Longleftrightarrow b_{r+1} = \cdots = b_m = 0$;

ii) (L) 确定 $\Longleftrightarrow r = n$且$b_{r+1} = \cdots = b_m = 0$;

证明. i) (L) 相容 $\Longrightarrow$ (L) 中不可能有矛盾方程 $\Longrightarrow b_{r+1} = \cdots = b_m = 0$; 另一方面，设增广矩阵的前 $r(r \leqslant n)$ 行对应方程组 (L')，则 (L') 相容 $\Longrightarrow$ (L) 相容。

ii) $(\Longrightarrow)$

(L) 解确定，则 (L) 显然相容，于是 $b_{r+1} = \cdots = b_m = 0$. 若 $r < n$，则对应的线性方程组形如

$$\begin{cases} \cdots + a_1x_{k_1} + *x_{k_1+1} + \cdots\cdots\cdots + *x_n = b_1 \\ \qquad\quad a_2x_{k_2} + *x_{k_2+1} + \cdots + *x_n = b_2 \\ \qquad\qquad\qquad\qquad\quad \vdots \\ \qquad\qquad\quad a_rx_{k_r} + \cdots + *x_n = b_r \end{cases}$$

其中 $k_1 < k_2 < \cdots < k_r$，$a_1, a_2, \cdots, a_r$ 非零，$*$ 为实数。

取任意的 $1 \leqslant i \leqslant n$，$i \neq k_1, k_2, \cdots k_r$，$x_i = 0$，得到解

$$\begin{cases} a_1x_{k_1} + *x_{k_2} + \cdots + *x_{k_r} = b_1 \\ \qquad a_2x_{k_2} + \cdots + *x_{k_r} = b_2 \\ \qquad\qquad\quad \vdots \\ \qquad\qquad a_rx_{k_r} = b_r \end{cases}$$

而取任意的 $1 \leqslant i \leqslant n,\ i \neq k_1, k_2, \ldots, k_r$ 时的 $x_i = 1$，则得到解

$$\begin{cases} a_1 x_{k_1} + *x_{k_2} + \cdots + *x_{k_r} = \widetilde{b_1} \\ a_2 x_{k_2} + \cdots + *x_{k_r} = \widetilde{b_2} \\ \vdots \\ a_r x_{k_r} = \widetilde{b_r} \end{cases}$$

其中 $\widetilde{b_1}, \widetilde{b_2}, \cdots, \widetilde{b_r}$ 为实数。于是方程组 (L) 有两组不同的解，矛盾！所以 $r = n$。

$(\Longleftarrow)$

若 $r = n$且$b_{r+1} = \cdots = b_m = 0$，则方程组形如例1.2.4中 (T) 的形式，于是由该例子的结论即知方程组有确定的解。

□

1.2.5 齐次线性方程组

定义 1.2.6. 设 $A = (a_{ij})_{m\times n}$，增广矩阵 $\left(\begin{array}{c:c} A & \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} \end{array}\right)$ 对应的线性方程组 (H) 称为齐次 (homogeneous) 线性方程组。即

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = 0 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = 0 \end{cases} \tag{H}$$

注 1.2.2. (1) (H) 有平凡解 $x_1 = \cdots = x_n = 0$.

(2) (H) 由系数矩阵 A 唯一确定。

(3) 对 (H) 作 (I)、(II)、(III) 类初等行变换仍得到齐次方程组。

(4) 几何意义：二元齐次方程 (组) 表示过原点的直线 (组)；三元齐次方程 (组) 表示过原点的平面 (组)。我们会在下册仿射空间一章中进一步阐述它们的几何意义。

定理 1.2.3. 设 A 是 $m\times n$ 阶的矩阵，其中 $m < n$，则以 A 为系数矩阵的齐次方程组 (H) 不确定。

证明. (H) 对应增广矩阵 $\left(\begin{array}{c:c} A & \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} \end{array}\right)$. 由定理 1.2.1，$(H)$ 等价于线性方程组 (H')，其增广矩阵为 $\left(\begin{array}{c:c} A' & \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} \end{array}\right)$. 其中 A' 是 $m\times n$ 阶的行阶梯型矩阵且 $m < n$。于是 A' 中含有非零元素的行数 $< n$。则由定理1.2.2，(H') 不确定，于是 (H) 不确定。 □

注 1.2.3. 几何意义：两个平面不可能只相交于一点。

命题 1.2.1. 设 A 是 $m\times n$ 阶矩阵，以 A 为系数矩阵的齐次方程组为 (H)，以 $\left(\begin{array}{c|c} & b_1 \\ A & \vdots \\ & b_m \end{array}\right)$ 为增广矩阵的线性方程组为 (L)，其中 $b_1,\dots,b_m\in\mathbb{R}$。设

$$\begin{cases} x_1=\alpha_1 \\ \quad\vdots \\ x_n=\alpha_n \end{cases},\quad \begin{cases} x_1=\beta_1 \\ \quad\vdots \\ x_n=\beta_n \end{cases}$$

都是 (L) 的解，

$$\begin{cases} x_1=\omega_1 \\ \quad\vdots \\ x_n=\omega_n \end{cases}$$

是 (H) 的解，则

(i)

$$\begin{cases} x_1=\alpha_1-\beta_1 \\ \quad\vdots \\ x_n=\alpha_n-\beta_n \end{cases} \tag{$*$}$$

是 (H) 的解；

(ii)

$$\begin{cases} x_1=\omega_1+\alpha_1 \\ \quad\vdots \\ x_n=\omega_n+\alpha_n \end{cases} \tag{$**$}$$

是 (L) 的解。

证明. $A=(a_{ij})_{m\times n}$.

(i) 由于

$$\begin{aligned}\sum_{j=1}^{n}a_{ij}(\alpha_j-\beta_j)&=\sum_{j=1}^{n}a_{ij}\alpha_j-\sum_{j=1}^{n}a_{ij}\beta_j\\&=b_i-b_i\\&=0.\end{aligned}$$

于是 $(*)$ 是 (H) 的解。

(ii) 由于

$$\sum_{j=1}^{n}a_{ij}(\omega_j+\alpha_j)=\sum_{j=1}^{n}a_{ij}\omega_j+\sum_{j=1}^{n}a_{ij}\alpha_j=b_j.$$

故 $(**)$ 是 (L) 的解。

□

命题 1.2.2. 设 A 是 $n\times n$ 阶矩阵，(H) 是以 A 为系数矩阵的齐次线性方程组，$b_1,\cdots,b_n$ 是实数。(L) 是以 $\left(\begin{array}{c|c} & b_1 \\ A & \vdots \\ & b_n \end{array}\right)$ 为增广矩阵的线性方程组。若 (H) 确定，则 (L) 确定。

证明. (H) 等价于增广矩阵为 $\left(\begin{array}{c|c} & 0 \\ A' & \vdots \\ & 0 \end{array}\right)$ 的线性方程组 (H')，其中 A' 是行阶梯型。由 (H) 确定知 (H') 确定。由定理1.2.2(ii)，A' 中有 n 行含有非零元素。

而 (L) 等价于 (L')，其增广矩阵为 $\left(\begin{array}{c|c} & b_1' \\ A' & \vdots \\ & b_n' \end{array}\right)$. 再由定理1.2.2(ii) 知 (L') 确定 $\longrightarrow$ (L) 确定。 □

注 1.2.4. 几何意义：

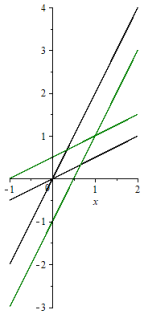


图 1.2-1 平移

最后，我们简单讨论一下 Gauss 消去法的算法复杂度。由于在计算机上做乘法 (除法) 比做加法 (减法) 要困难，因此分析一个算法时我们通常只考虑它做乘法的次数。我们不妨假设 n 个变量的线性方程组的解是确定的，则不难得到化成阶梯型的过程中我们需要做

$$\Gamma(n) = n(n-1) + (n-1)(n-2) + \cdots + 2\cdot 1 = \frac{n^3 - n}{3}$$

次乘法 (这个表达式的计算方法会在后面讲到)，而求解的过程需要做

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

次乘法。故总的算法复杂度为 $O(n^3)$。

Strassen 在 1969 年发现了降低这个复杂度的方法。关于 Strassen 算法，我们会在下册张量一章中进行介绍。

1.2.6 二阶行列式

我们首先介绍 2×2 矩阵的行列式 (determinant)。

定义 1.2.7. 设 $A = \left(\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right)$，定义 $\det A = a_{11}a_{22} - a_{12}a_{21}$ 为 A 的行列式，也记作 $|A|$。

例 1.2.5. $\det\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = 4 - 6 = -2.$

命题 1.2.3. 设 $A=\begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}$, (L_2) 是以 $\left(\begin{array}{c|c} A & \begin{matrix}b_1\\ b_2\end{matrix}\end{array}\right)$ 为增广矩阵的线性方程组，则

(i) (L_2) 确定 $\Longleftrightarrow |A|\neq 0$;

(ii) 设 (L_2) 确定，则 (L_2) 的解是

$$x_1=\frac{\begin{vmatrix}b_1 & a_{12}\\ b_2 & a_{22}\end{vmatrix}}{|A|},\ x_2=\frac{\begin{vmatrix}a_{11} & b_1\\ a_{21} & b_2\end{vmatrix}}{|A|}.$$

证明. 不妨设 $a_{11}\neq 0$，则

$$\left(\begin{array}{cc|c} a_{11} & a_{12} & b_1\\ a_{21} & a_{22} & b_2\end{array}\right)\xrightarrow{r_2-\frac{a_{21}}{a_{11}}r_1}\left(\begin{array}{cc|c} a_{11} & a_{12} & b_1\\ 0 & a_{22}-\dfrac{a_{21}a_{12}}{a_{11}} & b_2-\dfrac{a_{21}b_1}{a_{11}}\end{array}\right)$$

$$=\left(\begin{array}{cc|c} a_{11} & a_{12} & b_1\\ 0 & \dfrac{|A|}{a_{11}} & \dfrac{\begin{vmatrix}a_{11} & b_1\\ a_{21} & b_2\end{vmatrix}}{a_{11}}\end{array}\right)\xrightarrow{a_{11}r_2}\left(\begin{array}{cc|c} a_{11} & a_{12} & b_1\\ 0 & |A| & \begin{vmatrix}a_{11} & b_1\\ a_{21} & b_2\end{vmatrix}\end{array}\right)\triangleq M$$

(i) (L_2) 确定，则 a_{11},a_{21} 不全为 0，不妨设 $a_{11}\neq 0$(否则交换两行)，则由 M 和定理 1.2.2(ii) 知 $|A|\neq 0$。

反过来，若 $|A|\neq 0$，则 a_{11},a_{21} 不全为 0，不妨设 $a_{11}\neq 0$，同样由定理 1.2.2(ii) 知 (L_2) 确定。

(ii) 由 (i) 及矩阵 M 即可得到 (L_2) 的解为

$$x_1=\frac{\begin{vmatrix}b_1 & a_{12}\\ b_2 & a_{22}\end{vmatrix}}{|A|},\ x_2=\frac{\begin{vmatrix}a_{11} & b_1\\ a_{21} & b_2\end{vmatrix}}{|A|}.$$

□

类似地，有三阶行列式和三元一次方程组的解的形式，我们会在第三章中介绍更一般的结论。

置信编码问题

例 1.2.6. 为了传送 *PEACE* 一词，原则上利用四个基本信息单元

$$P=(0,0),\quad E=(1,0),\quad A=(0,1),\quad C=(1,1)$$

就够了，我们的译码可看作二元域 $\mathbb{F}_2\cong\mathbb{Z}_2=\{0,1\}$ 上的二维向量空间 $\mathbb{F}_2^2$ 的行向量。但是在传送过程中，可能发生干扰 (将 0 变为 1 或 1 变为 0)，结果终端得到的可能是，例如 *APACE*，根据香农 (Claude Elwood Shannon, 1916-2001, 美国信息论之父) 的基本定理，增加基本信息单元的长度 (即增加传送的行向量的长度) 可以清除干扰. 假设根据传送条件知道，在每个长为 5 的基本信息单元中最多出现一个失真。那么在向量空间 $S=\mathbb{F}_2^5$ 中取子集

$$S_0=\{P=(0,0,1,1,0),\quad E=(1,0,0,1,1),\quad A=(0,1,1,0,1),$$
$$C=(1,1,0,0,0)\},$$

称之为编码向量，其中的每个向量称为码字。码字之间的汉明（Richard Wesley Hamming, 1915-1998, 美国数学家）距离（数据传输中两个字对应位不同的的数量）大于等于 3. 以每个码字为中心，半径为 1 球，这些球互不相交。在 $\mathbb{F}_2^5$ 中找彼此汉明距离大于等于 3 的向量最多能找到 4 个，例子中的码字个数已经是最优的。

编码向量	00110	10011	01101	11000
得到的向量 编码向量失真后	00010	00011	00101	01000
	00100	10001	01001	10000
	00111	10010	01100	11100
	01110	10111	01111	11001
	10110	11011	11101	11010

可以恢复真实的信息：

1. 不同列中的失真向量的集合交为空。
2. 每一列向量到顶端向量的汉明距离为 1，即落在以顶端向量对应的码字为中心，半径为 1 的球面上。
3. 收到的向量落在哪个球上，就译码为球心对应的码字。

我们得到了可以纠正一个错误的编码 S_0，对于充分大的维数 n，利用向量空间 $\mathbb{F}_2^n$，可以构造类似的编码，没有错误地传送所有的字母，从而准确地传送任何文章，为了避免过长和过于缓慢的译码，S_0 要经过专门的选择。有许多办法可以做到这一点，其中包括利用有限域 $\mathbb{F}_q$ 的纯代数方法。[1]

[1]摘自《代数学引论》第一卷 §4.3，柯斯特利金著，高等教育出版社。

1.3 集合与映射

1.3.1 集合与子集

集合 (set) 是数学中的一个原始概念，是一些对象的总合。集合中的对象称为元素。我们在这里只介绍朴素集合论 (native set theory) 的一些基本内容，由格奥尔格康托尔 (Georg Cantor，1845-1918，德国数学家) 提出，有关公理化集合论的内容，可以参考相关领域的专门教材，如《Introduction to Axiomatic Set Theory》(GTM001) 或《代数学方法》第一章，李文威。

回到课程内容上来。例如，我们有 26 个小写英文字母的集合

$$S_1 = \{a, b, \ldots, z\},$$

也有所有正偶数的集合

$$S_2 = \{2, 4, 6, \ldots\} = \{a | a\text{是正整数且是 2 的倍数}\}.$$

我们显然有：a 在 S_1 中而 3 不在 S_2 中，记作 $a \in S_1$，$3 \notin S_2$。

一些常见的集合

集合	符号
正整数集	$\mathbb{Z}^+ = \{1, 2, 3, \ldots\}$
自然数集	$\mathbb{N} = \{0, 1, 2, \ldots\}$
整数集	$\mathbb{Z} = \{x \mid x \in \mathbb{N}\text{或} -x \in \mathbb{N}\}$
有理数集	$\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\}$
实数集	$\mathbb{R}, \mathbb{Q}$ 的完备化
复数集	$\mathbb{C} = \{x + y\sqrt{-1} \mid x, y \in \mathbb{R}\}$
空集	$\emptyset$

定义 1.3.1. 设 S, T 是两个集合，如果 S 中的元素都是 T 中的元素，则称 S 是 T 的子集 (subset)，记作 $S \subset T$(有的书上也记作 $S \subseteq T$)。若 $S \subset T$ 且 $T \subset S$，则称 $S = T$，否则称 $S \neq T$。若 $S \subset T$ 且 $S \neq T$，则称 S 是 T 的真子集，记作 $S \subsetneq T$。

例 1.3.1. $\mathbb{Z}^+ \subsetneq \mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R} \subsetneq \mathbb{C}$；空集 $\emptyset$ 是任意集合的子集。

例 1.3.2. $S = \{a, b, c\}$ 有且只有如下 8 个子集：

$$\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}.$$

思考题 1.3.1. 设集合 S 中有 n 个元素，试证明 S 共有 2^n 个子集。

1.3.2 集合的运算

这一小节我们介绍集合的交、并、差、直积等运算。

定义 1.3.2. 设 S 和 T 是两个集合，定义 S 和 T 的并：
$S \cup T = \{a | a \in S\text{或}a \in T\}$；$S$ 和 T 的交：$S \cap T = \{a | a \in S\text{且}a \in T\}$。

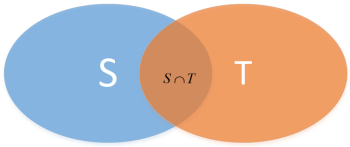


图 1.3-1 S 和 T 的并与交

更一般地，设 I 是一个指标集 (有限或无限)，对 $\forall i \in I, S_i$ 是集合，则

$$\bigcup_{i\in I} S_i = \{a | \exists j \in I, a \in S_j\}, \quad \bigcap_{i\in I} S_i = \{a | \forall j \in I, a \in S_j\}.$$

例 1.3.3. 设 S 是所有偶数的集合，T 是所有奇数的集合，则

$$S \cup T = \mathbb{Z}, \ S \cap T = \emptyset.$$

定义 1.3.3. 设 S 和 T 是两个集合，定义 S 和 T 的差集为

$$S \setminus T = \{a | a \in S \text{但} a \notin T\}.$$

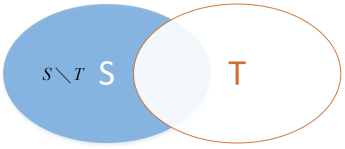


图 1.3-2 S 和 T 的差集

例 1.3.4. 设 $i \in \mathbb{N}$, $S_i = \mathbb{N} \setminus \{i\}$，证明 $\bigcap_{i\in\mathbb{N}} S_i = \emptyset$.

证明. 用反证法。设 $\bigcap_{i\in\mathbb{N}} S_i \neq \emptyset$，即 $\exists a \in \bigcap_{i\in\mathbb{N}} S_i$，则 $\forall i \in \mathbb{N}$, $a \in S_i$，即 $\forall i \in \mathbb{N}$, $a \neq i$，所以 $a \notin \mathbb{N}$，这与 $\bigcap_{i\in\mathbb{N}} S_i \subset \mathbb{N}$ 矛盾! □

命题 1.3.1. 设 R, S, T 是集合，则

$$\begin{aligned}
&(1) S \cup T = T \cup S, S \cap T = T \cap S;\\
&(2) (R \cup S) \cup T = R \cup (S \cup T),\\
&\quad (R \cap S) \cap T = R \cap (S \cap T);\\
&(3) (S \cup T) \cap R = (S \cap R) \cup (T \cap R),\\
&\quad (S \cap T) \cup R = (S \cup R) \cap (T \cup R).
\end{aligned}$$

证明留作练习。

下面我们定义集合的直积 (笛卡尔积)。为此我们先定义有序对。对于对象 x, y，我们定义 $(x, y) = \{\{x\}, \{x, y\}\}$，这样的定义满足 $(x_1, y_1) = (x_2, y_2) \Leftrightarrow x_1 = x_2, y_1 = y_2$. 归纳地我们可以定义长度为 n 的有序组。现在我们可以定义直积如下：

定义 1.3.4. 设 $S_1, S_2, \ldots, S_n$ 是 n 个集合，定义

$$S_1 \times \cdots \times S_n = \{(x_1, \ldots, x_n) | x_i \in S_i, i = 1, \ldots, n\}$$

为 $S_1, S_2, \cdots, S_n$ 的笛卡儿积 (Cartesian product)。特别地，当 $S_1 = S_2 = \cdots = S_n$ 时，记 $S_1 \times \cdots \times S_n = S_1^n$.

例 1.3.5.

- $\mathbb{R}^{1\times n} = \{(x_1, \ldots, x_n) | x_1, \ldots, x_n \in \mathbb{R}\}$，$n$ 维行向量空间；
- $\mathbb{R}^{n\times 1} = \{\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} | x_1, \cdots, x_n \in \mathbb{R}\}$，$n$ 维列向量空间；
- $S^1 = \{(x, y) \in \mathbb{R}^2 | x^2 + y^2 = 1\}$ 圆；
- $L = \{(x, y) \in \mathbb{R}^2 | ax + by = c\}$ 直线；
- $v = \left\{ (x_1, \ldots, x_n) \middle| \begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = 0 \\ \qquad\qquad\qquad\qquad \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = 0 \end{cases} \right\} \subset \mathbb{R}^n$ 线性子空间。

1.3.3 映射

有了集合，我们自然要考虑集合之间的“对应关系”，一种基本并且具有比较好的性质的“对应关系”就是映射。

定义 1.3.5. 设 S, T 是两个非空集合，$f \subset S \times T$，若 $\forall s \in S$，存在唯一$(\exists!)t \in T$，使得 $(s, t) \in f$，则称 f 是从 S 到 T 的映射 (mapping)，记为 $f : S \to T, s \mapsto f(s) = t$。我们把 $(s, t) \in f$ 记为 $t = f(s)$。称 S 为 f 的定义域 (domain)，T 为 f 的值域 (range)。特别地，当 $S = T$ 时，称 f 为 S 到自身的变换。

例 1.3.6. (1) $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$，即 $f(x) = x^2$ 是映射，即 $f = \{(x, x^2) | x \in \mathbb{R}\} \subset \mathbb{R}^2$.

(2) $S = \{1, 2, 3\}, T = \{a, b, c, d\}$，则 $f = \{(1, a), (2, b), (3, a)\}$ 是映射，而 $g = \{(1, a), (1, b), (2, d), (3, c)\}$ 不是映射，$h = \{(1, c), (2, d)\}$ 也不是映射。

定义 1.3.6. 设 $f : S \to T, S' \subset S$，则 $f(S') = \{f(s) | s \in S'\}$ 称为 S' 在 f 下的像集 (image)。

注 1.3.1. (i) $f(S') \subset T$.

(ii) $f(S)$ 称为 f 的像集，记为 $\mathrm{im}(f)$.

例 1.3.7. 设 $\sin : \mathbb{R} \to \mathbb{R}, x \mapsto \sin x$. 则 $\mathrm{im}(\sin) = [-1, 1]$，$\sin((0, \frac{\pi}{2})) = (0, 1)$.

一些重要的映射类型

定义 1.3.7. 设 $f : S \to T$ 是映射，若 $\mathrm{im}(f) = T$，则称 f 是满射 (surjection)；若 $\forall s_1, s_2 \in S, s_1 \neq s_2$，都有 $f(s_1) \neq f(s_2)$，则称 f 是单射 (injection)；若 f 既是单射又是满射，则称 f 为双射 (bijection)。

例 1.3.8. $\sin : \mathbb{R} \to \mathbb{R}$ 既不是单射又不是满射；
$\sin : \mathbb{R} \to [-1, 1]$ 是满射但不是单射；
$\sin : [0, \frac{\pi}{2}] \to \mathbb{R}$ 是单射但不是满射；
$\sin : [0, \frac{\pi}{2}] \to [0, 1]$ 是双射。

例 1.3.9. $\Pi : S \times T \to S,\ (s,t) \mapsto s$ 是满射，称为从 $S \times T$ 到 S 的投射 (投影,projection)。

定义 1.3.8. 设 $f : S \to T$ 是映射，$T' \subset T$，则

$$f^{-1}(T') = \{s \in S | f(s) \in T'\}$$

称为 T' 在 f 下的原像或逆像 (fiber)。特别地，如果 $T' \cap f(S) = \emptyset$，那么 $f^{-1}(T') = \emptyset$。于是，容易验证 $f^{-1}(T) = S$，这是因为任取 $s \in S$，我们总能找到 $f(s) \in T$，于是 $S \subset f^{-1}(T)$，而反过来的包含由定义即得。

例 1.3.10.

- $\sin^{-1}(\{0\}) = \{k\pi | k \in \mathbb{Z}\}$;
- $sin^{-1}((-1,1)) = \mathbb{R} \setminus \{\frac{(2k+1)\pi}{2} | k \in \mathbb{Z}\}$.

例 1.3.11.

- 恒同映射 (identity map) $\mathrm{id}_S : S \to S, s \mapsto s$ 是双射;
- $f : \mathbb{Z} \to \mathbb{Z}, x \mapsto x+1$ 是双射。

定义 1.3.9. 设 $f : S \to T$ 是映射，S' 是 S 的非空子集，则称 $f|_{S'} : S' \to T', s' \in S' \mapsto f(s')$ 为 f 在 S' 上的限制映射。

例 1.3.12. 设 $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$，则 $f|_{\mathbb{R}^+}, x \mapsto x^2$ 是单射。

定义 1.3.10. 设 $f : S \to T$, $t \in T$，则称 $f^{-1}(\{t\})$ 为 t 关于 f 的纤维 (fiber)。

例如，$\sin^{-1}(\{1\}) = \{2k\pi + \dfrac{\pi}{2} | k \in \mathbb{Z}\}$。显然我们有

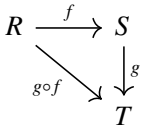
- f 是单射 $\iff \forall t \in T,\ f^{-1}(\{t\})$ 至多含有一个元素;
- f 是满射 $\iff \forall t \in T,\ f^{-1}(\{t\})$ 非空。

1.3.4 映射的复合

定义 1.3.11. 设 $f : R \to S, g : S \to T$ 是映射，则称

$$\begin{aligned} h :& R \to T \\ & r \mapsto g(f(r)) \end{aligned}$$

为 f 和 g 的复合 (乘积)，记为 $g \circ f$，在不引起混淆时也简记为 gf。



例 1.3.13. 设 $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$; $g : \mathbb{R} \to \mathbb{R}, x \mapsto x+1$. 则

$$\begin{aligned} g \circ f(x) &= g(x^2) = x^2 + 1; \\ f \circ g(x) &= f(x+1) = (x+1)^2. \end{aligned}$$

由以上例子可以看到，一般地，$f \circ g \neq g \circ f$。

命题 1.3.2. 设 $f : R \to S, g : S \to T$，则

(i) 若 f, g 是单射，则 $g \circ f$ 也是单射;

(ii) 若 f,g 是满射，则 $g\circ f$ 也是满射；

(iii) 若 f,g 是双射，则 $g\circ f$ 也是双射。

证明. 我们只证明 (i)，其余留作练习。

设 $r_1,r_2\in R$, $r_1\neq r_2$，则由 f 是单射知 $f(r_1)\neq f(r_2)$，再由 g 是单射知 $g(f(r_1))\neq g(f(r_2))$，即 $g\circ f$ 是单射。 □

定义 1.3.12. 设 $f:S\to T$，若存在 $g:T\to S$ 使得 $g\circ f=\mathrm{id}_S$，则称 f 有左逆 g；若存在 $h:T\to S$ 使得 $f\circ h=\mathrm{id}_T$，则称 f 有右逆 h；若 f 的左逆和右逆都存在 (则必然相等，见下面的推论 1.3.1)，则称 f 为可逆映射 (此时 $g=h:T\to S$ 也可逆，称为 f 的逆映射，记为 f^{-1})。

例 1.3.14. 设 $f:\mathbb{R}\to\mathbb{R},x\mapsto x+1$; $g:\mathbb{R}\to\mathbb{R},x\mapsto x-1$. 则

$$g\circ f(x)=g(x+1)=x;$$
$$f\circ g(x)=f(x-1)=x.$$

即 f,g 互为逆映射。

下面是可逆的等价条件。

定理 1.3.1. 设 $f:S\to T$，则 f 可逆 $\iff f$ 是双射。

证明. ($\Longrightarrow$)
设 $g:T\to S$ 满足 $g\circ f=\mathrm{id}_S$，$f\circ g=\mathrm{id}_T$，则对 $\forall s_1,s_2\in S,s_1\neq s_2$，有

$$s_1=g\circ f(s_1)=g(f(s_1))\neq s_2=g\circ f(s_2)=g(f(s_2)).$$

于是 $f(s_1)\neq f(s_2)$，即 f 是单射。
另一方面，设 $t\in T$，则 $t=\mathrm{id}_T(t)=f\circ g(t)=f(g(t))$，即 $g(t)$ 是 t 在 f 下的原像，即 f 是满射。综上 f 是双射。
($\Longleftarrow$)
由 f 是双射，对 $\forall t\in T,\exists!s\in S$ 使得 $f(s)=t$。于是可以定义 $g:T\to S,t\mapsto s$。首先 g 确实是一个映射 (用映射的定义验证之)，即 g 是**良定义** (well defined) 的。
其次，我们有

$$\forall s\in S,g\circ f(s)=g(f(s))=g(t)=s;$$
$$\forall t\in T,f\circ g(t)=f(s)=t.$$

于是 f 是可逆映射，且逆映射为 g。 □

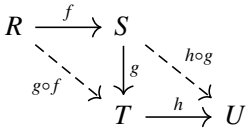
由定理的证明过程我们可以得到一个有用的结论：

命题 1.3.3. 设 $f:S\to T,g:T\to S$ 是映射，若 $g\circ f=\mathrm{id}_S$，则 g 是满射，f 是单射。

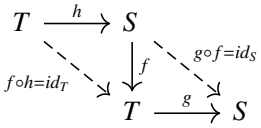
例 1.3.15. $\sin:[-\frac{\pi}{2},\frac{\pi}{2}]\to[-1,1]$ 是可逆映射。

定理 1.3.2 (结合律). 设 $f:R\to S,g:S\to T,h:T\to U$ 是映射，则 $h\circ(g\circ f)=(h\circ g)\circ f$.

证明可由下面的交换图表示，具体过程留给读者整理。



推论 1.3.1. 设 $f:S\to T, g:T\to S, h:T\to S$ 满足 $g\circ f=\mathrm{id}_S, f\circ h=\mathrm{id}_T$，则 $g=h$。



证明. 由结合律，$(gf)h=g(fh)$，即 $\mathrm{id}_S\circ h=g\circ\mathrm{id}_T$，即 $g=h$。 □

推论 1.3.2. 可逆映射的逆是唯一的。即若 $f:S\to T$ 可逆，$g,h:T\to S$ 满足 $gf=hf=\mathrm{id}_S, fg=fh=\mathrm{id}_T$，则 $g=h$。

由以上推论可知，若 f 是可逆映射，则 f^{-1} 是良定义的，且 $(f^{-1})^{-1}=f$。

推论 1.3.3. 设 $f:R\to S, g:S\to T$ 是可逆映射，则 gf 也可逆且 $(gf)^{-1}=f^{-1}\circ g^{-1}$。

证明. 由命题 1.3.2(iii) 知 gf 是双射，由定理 1.3.1 知 gf 可逆。故

$$(f^{-1}\circ g^{-1})\circ(g\circ f)=f^{-1}\circ(g^{-1}\circ g)\circ f=f^{-1}\circ f=\mathrm{id}_R.$$

同理 $(g\circ f)\circ(f^{-1}\circ g^{-1})=\mathrm{id}_T$. 于是 $(gf)^{-1}=f^{-1}\circ g^{-1}$。 □

需要注意的是，当映射不是双射时，它可以有单边逆，但没有逆映射，如下面的例子。

例 1.3.16. 设 $\Pi_x:\mathbb{R}^2\to\mathbb{R},(x,y)\mapsto x,\ i_x:\mathbb{R}\to\mathbb{R}^2, x\mapsto(x,0)$. 则

$$i_x\circ\Pi_x((x,y))=i_x(x)=(x,0),\ \Pi_x\circ i_x(x)=\Pi_x((x,0))=x.$$

即 $\Pi_x\circ i_x=\mathrm{id}_{\mathbb{R}}$，但 $i_x\circ\Pi_x\neq\mathrm{id}_{\mathbb{R}^2}$。

1.3.5 集合的势

最后我们简单地讨论一下集合中元素的“个数”。对于有限集，我们可以“数”出元素的个数，但对于无限集就不行了。为此，我们需要用映射的角度重新看待“数”这一过程。

定义 1.3.13. 设 S,T 是两个非空集合，若存在 $f:S\to T$ 是双射，则称 S 和 T 的势 (或基数,cardinality) 相等。

下面我们重新定义有限集与无限集。

定义 1.3.14. 若存在 $n\in\mathbb{N}$，使得集合 S 与 $\{1,\dots,n\}$ 等势，则称 S 是有限集；否则 S 是无限集。当 S 是有限集时，我们称集合 S 的势 (元素个数) 是 n，记为 $|S|=n$(或 $card(S)=n$)[1]。

注意到有限集和它的任意真子集一定不等势，而无限集一定存在某个真子集与它本身等势，这一点也可以作为有限集和无限集的定义。可以证明，这两个定义是等价的。

例 1.3.17. 注意到 $f:\mathbb{Z}^+\to\mathbb{N}, x\mapsto x-1$ 是双射，即 $\mathbb{Z}^+$与$\mathbb{N}$ 等势，但显然 $\mathbb{Z}^+\subsetneq\mathbb{N}$。

命题 1.3.4. 设 S,T 是集合，S 非空且有限，则 S,T 等势 $\iff T$ 中元素个数与 S 中元素个数相同。

[1]实际上，对无限集也可以定义集合的势，不过这不在本课程的范围内。

定理 1.3.3. 如果 S 是有限集，且变换 $f : S \to S$ 是单射，则 f 是双射。

证明. 只需证明 f 是满射。

对 $\forall x \in S$，$\exists! x' \in S$，使得 $f(x) = x'$。令 $f^k(x) = f(f \cdots f(x)), k = 0, 1, 2, \ldots$，则由 $f^k(x) \in S$ 及 S 是有限集可知 $\exists m, n, m > n$ 使得 $f^m(x) = f^n(x)$，即 $f(f^{m-1}(x)) = f(f^{n-1}(x))$(否则 $\{f^k(x) | k \in \mathbb{N}\} \subset S$ 是无限集，矛盾！) 于是由 f 是单射知 $f^{m-1}(x) = f^{n-1}(x)$。

重复以上过程，可知 $f^{m-n}(x) = f^0(x) = \mathrm{id}(x) = x$。令 $x' = f^{m-n-1}(x)$，则 $f(x') = x$，即 f 是满射。 □

这个定理对无限集不对，一个简单的反例是 $\sigma : \mathbb{N} \to \mathbb{N}, x \mapsto x + 1$，则 σ 是单射但不是满射 (0 没有原像)。

我们把与自然数集 $\mathbb{N}$ 等势的集合称为可数集或可列集，可以证明，$\mathbb{Z}, \mathbb{Q}$ 都是可数集，但 $\mathbb{R}$ 不是 (留作思考)。更一般地，我们可以证明一个集合 S 与它的所有子集构成的集合 (称为 S 的幂集，记作 2^S 或 $\mathcal{P}(S)$) 不等势。更一般的理论，读者可以参阅实变函数或点集拓扑学的标准教材。

1.4 等价关系和序关系

1.4.1 二元关系

定义 1.4.1. 设 S,T 是非空集合，$R\subset S\times T$，则称 R 是 S,T 上的一个二元关系。若 $(a,b)\in R$，则称 a与b 有关系 R，记为 aRb。若 $S=T$，则称 R 是 S 上的一个二元关系。

例 1.4.1. (1) 设 $S=\mathbb{R}$，则 "$\geqslant$" 是 $\mathbb{R}$ 上的二元关系。

(2) 设 L 是 $\mathbb{R}^2$ 上所有直线的集合，令 $C=\{(l_1,l_2)\in L^2|l_1\cap l_2\neq\emptyset\}$，则 C 是 L 上的二元关系，且

$$l_1Cl_2\Longleftrightarrow l_1与l_2相交或重合.$$

(3) 设 $f:S\to T$，定义

$$\sim_f=\{(s_1,s_2)|f(s_1)=f(s_2)\},$$

则 $s_1\sim_f s_2\Longleftrightarrow f(s_1)=f(s_2)$。

(4) 设 $S=\{a,b\}$，$R=\{(a,a)\}$。则 aRa 成立，但 aRb,bRb 都不成立。

1.4.2 等价关系

下面我们讨论一种特殊的二元关系，它是“相等”这一概念的自然推广。

定义 1.4.2. 设 $\sim$ 是集合 S 上的二元关系，满足

(i) 自反律，即 $\forall a\in S,a\sim a$;

(ii) 对称律，即对 $a,b\in S$，若 $a\sim b$，则 $b\sim a$;

(iii) 传递律，即对 $a,b,c\in S$，若 $a\sim b,b\sim c$，则 $a\sim c$.

则我们称 $\sim$ 是 S 上的等价关系。

下面是一些常用的等价关系。

(1) "="，即 $\{(a,a)|a\in S\}$。我们容易验证它满足自反、对称、传递三条性质。

(2) 设 L 是 $\mathbb{R}^2$ 上所有直线的集合，则 "$/\!/$" (平行关系) 是等价关系。

(3) 例 1.4.1 中定义的 "$\sim_f$" 是等价关系。验证如下：
$\forall s\in S,f(s)=f(s)\Longrightarrow s\sim_f s$ 自反；
$\forall s_1,s_2\in S,s_1\sim_f s_2\Longrightarrow f(s_1)=f(s_2)\Longrightarrow f(s_2)=f(s_1)\Longrightarrow s_2\sim_f s_1$ 对称；
$\forall s_1,s_2,s_3\in S,s_1\sim_f s_2,s_2\sim_f s_3\Longrightarrow f(s_1)=f(s_2),f(s_2)=f(s_3)\Longrightarrow f(s_1)=f(s_3)\Longrightarrow s_1\sim_f s_3$ 传递。

(4) "$\geqslant$" 不是等价关系，因为其显然不满足对称性；例1.4.1(2) 中两条直线的“相交或重合”也不是等价关系，因为其不满足传递性。

1.4.3 同余关系

这一小节我们讨论一种特殊的等价关系：$\mathbb{Z}$ 上的同余关系。同余在后续课程抽象代数和初等数论中都很重要。

定义 1.4.3. 设 $a,b\in\mathbb{Z}$，如果存在 $x\in\mathbb{Z}$ 使得 $a=xb$，则称 b 整除 a，记为 $b|a$。

下面我们定义 $\mathbb{Z}$ 上的带余除法。

定义 1.4.4. 设 $a,b\in\mathbb{Z},b\neq 0$，则 $\exists!q\in\mathbb{Z}$ 和 $r\in\{0,1,\dots,|b|-1\}$ 使得 $a=qb+r$ (我们会在第 4 章进一步讨论这一性质)，称这个操作为带余除法，其中 q 称作 a 关于 b 的商 (quotient)，记作 $q=\mathrm{quo}(a,b)$；r 称作 a 关于 b 的余 (remainder)，记作 $r=\mathrm{rem}(a,b)$。

引理 1.4.1. 设 $a,b\in\mathbb{Z},b\neq 0$，则 $b|a\iff \mathrm{rem}(a,b)=0$。

引理 1.4.2. 设 $n\in\mathbb{Z}\setminus\{0\}$, $a,b,\alpha,\beta\in\mathbb{Z}$，如果 $n|a,n|b$，则 $n|\alpha a+\beta b$。

这两个引理由定义即可证明。现在我们可以定义同余关系了。

定义 1.4.5. 设 $n\in\mathbb{Z}\setminus\{0\}$, $a,b\in\mathbb{Z}$，则我们称 a,b 模 n 同余 (congruent)，如果 $n|a-b$，记为 $a\equiv b \mod n$ 或者 $a\equiv_n b$。

下面我们验证同余是等价关系。

1. $n|(a-a)\Longrightarrow a\equiv_n a$;
2. $a\equiv_n b\Longrightarrow n|(a-b)\Longrightarrow n|(b-a)\Longrightarrow b\equiv_n a$;
3. $a\equiv_n b,b\equiv_n c\Longrightarrow n|(a-b),n|(b-c)\Longrightarrow n|(a-b+b-c)$, 即 $n|(a-c)\Longrightarrow a\equiv_n c$.

由以上三点我们就证明了同余是等价关系。下面我们介绍同余关系的一些简单性质。

命题 1.4.1. (1) 若 $a\equiv b \mod n$, $c\equiv d \mod n$，则 $a+c\equiv b+d \mod n$。

(2) 若 $a\equiv b \mod n$, $c\equiv d \mod n$，则 $ac\equiv bd \mod n$。

(3) 若 $a\equiv b \mod n$, $d|n$，则 $a\equiv b \mod d$。

(4) 设 $d\in\mathbb{Z}^+$，则 $a\equiv b \mod n\Longrightarrow da\equiv db \mod dn$。

这些性质的证明留作练习。同余还有许多性质，我们会在初等数论课程中深入学习。

1.4.4 等价类与商映射

将“等价”的东西放在一起讨论是一种十分自然的想法，这就产生了本节的内容。

定义 1.4.6. 设 $\sim$ 是集合 S 上的等价关系，$a\in S$，则定义

$$\overline{a}=\{b\in S|b\sim a\},$$

称 $\overline{a}$ 是 a 关于 $\sim$ 的等价类。

例 1.4.2. 对于 $\equiv_2$，有 $\overline{0}=\overline{2}=\cdots;\overline{1}=\overline{3}=\cdots$。可以证明只有这两个等价类 $\{\overline{0},\overline{1}\}$。更一般地，可以证明 $\equiv_n$ 有且只有 n 个等价类。

命题 1.4.2. 设 $\sim$ 是集合 S 上的等价关系，$a,b\in S$，则

(1) $a\sim b\iff \overline{a}=\overline{b}$;

(2) $a\nsim b\iff \overline{a}\cap\overline{b}=\emptyset$.

证明. (i) ($\Longrightarrow$)

设 $x\in\overline{a}$，则 $x\sim a$，因为 $a\sim b$，所以 $x\sim b$，即 $x\in\overline{b}$。故 $\overline{a}\subset\overline{b}$。同理 $\overline{b}\subset\overline{a}$。故 $\overline{a}=\overline{b}$。

($\Longleftarrow$)

由 $b\in\overline{b},\overline{a}=\overline{b}$ 知 $b\in\overline{a}$，即 $a\sim b$。

(ii) ($\Longrightarrow$)

用反证法。若 $\overline{a}\cap\overline{b}\neq\emptyset$，则存在 $x\in\overline{a}\cap\overline{b}$，即 $x\sim a, x\sim b$，所以 $a\sim b$，矛盾!

($\Longleftarrow$)

由定义立刻可证。

□

定义 1.4.7. 设 $\sim$ 是 S 上的等价关系，$a\in S$，则称 $\overline{a}$ 中的任意元素为 $\overline{a}$ 的代表元。

例如，关于 $\equiv_2$ 等价关系，任意偶数都是 $\overline{0}$ 的代表元，任意奇数都是 $\overline{1}$ 的代表元。

定义 1.4.8. 设 $\sim$ 是 S 上的等价关系，定义 $S/\sim=\{\overline{a}|a\in S\}$ 为 S 关于 $\sim$ 的商集。

例如，$\mathbb{Z}/\equiv_2=\{\overline{0},\overline{1}\}$，$\mathbb{Z}/\equiv_n=\{\overline{0},\ldots,\overline{n-1}\}$。我们通常把 $\{\overline{0},\ldots,\overline{n-1}\}$ 记为 $\mathbb{Z}_n$ 或 $\mathbb{Z}/n\mathbb{Z}$。

下面我们建立原集合和商集的联系。

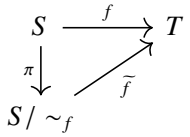
定义 1.4.9. 设 $\sim$ 是 S 上的等价关系，定义映射

$$\begin{aligned}\pi: S &\to S/\sim\\ a &\mapsto \overline{a}\end{aligned}$$

称为关于 $\sim$ 的商映射 (也称为自然投射或典范投影)。容易验证 π 是满射。

例 1.4.3. $\pi:\mathbb{Z}\to\mathbb{Z}_n, k\mapsto\overline{k}=\overline{\mathrm{rem}(k,n)}$ 是 $\mathbb{Z}$ 关于 $\equiv_n$ 的商映射。

定理 1.4.1. 设 $f:S\to T$，$\pi:S\to S/\sim_f$，则 $\exists!$单射$\widetilde{f}:S/\sim_f\to T$ 使得 $f=\widetilde{f}\circ\pi$。



证明. 我们定义

$$\begin{aligned}\widetilde{f}: S/\sim_f &\longrightarrow T\\ \overline{a} &\longmapsto f(a).\end{aligned}$$

首先 $\widetilde{f}$ 是良定义的：设 $\overline{a}=\overline{b}$，则 $a\sim_f b$，即 $f(a)=f(b)$，所以 $\widetilde{f}(\overline{a})=\widetilde{f}(\overline{b})$，即 $\widetilde{f}$ 的值与代表元的选取无关，这满足映射的定义。

其次 $\widetilde{f}$ 是单射：设 $\overline{a}\neq\overline{b}$，则 $a\nsim_f b$，即 $f(a)\neq f(b)$，所以 $\widetilde{f}(\overline{a})\neq\widetilde{f}(\overline{b})$，即 $\widetilde{f}$ 是单射。

最后验证 $f=\widetilde{f}\circ\pi$：对 $\forall a\in S$，$\widetilde{f}\circ\pi(a)=\widetilde{f}(\overline{a})=f(a)$，即 $f=\widetilde{f}\circ\pi$。 □

我们以后还会反复见到与这个定理类似的结论。

1.4.5 集合的分割

定义 1.4.10. 设 S 是集合，I 是一个指标集，且从 I 到 $2^S\setminus\{\emptyset\}$ 有一个单射 (即 $\forall i\in I$，S_i 是 S 的非空子集) 如果这个对应关系还满足：

(i) $\forall i,j\in I, i\neq j$，$S_i\cap S_j=\emptyset$;

(ii) $\bigcup\limits_{i\in I}S_i=S$.

则称 $\{S_i|i\in I\}$ 是 S 的一个分割 (partition)。

例 1.4.4. 设 $\sim$ 是 S 上的等价关系，则 $S/\sim$ 是 S 的一个分割。

证明. 设 $U \in S/\sim$，则 $\exists a \in S$ 使得 $U = \overline{a}$ 且 $U \subset S$ 非空；若 $\overline{a} \neq \overline{b}$，则 $\overline{a} \cap \overline{b} = \emptyset$。另外，$\forall a \in S,\ a \in \overline{a}$。综上，$S = \bigcup_{u \in S/\sim} U$。 □

下面的定理揭示了集合分割和等价关系之间的联系。

定理 1.4.2. 设 $T = \{S_i | i \in I\}$ 是集合 S 的一个分割，令

$$\sim_T = \{(a,b) \in S^2 | \exists i \in I, a, b \in S_i\}$$

则 $\sim_T$ 是 S 上的等价关系，且 $S/\sim_T = T$。

证明. 先验证 $\sim_T$ 是 S 是等价关系。
(1) 自反性。$\forall a \in S, \exists i \in I$，使得 $a \in S_i$，即 $a \sim_T a$。
(2) 对称性。若 $a \sim_T b$，则 $\exists i \in I$ 使得 $a, b \in S_i$，即 $b, a \in S_i$，故 $b \sim_T a$。
(3) 传递性。设 $a \sim_T b, b \sim_T c$，则 $\exists i, j \in I$ 使得 $a, b \in S_i$，$b, c \in S_j$，由于若 $i \neq j$ 则 $S_i \cap S_j = \emptyset$，与 $b \in S_i \cap S_j$ 矛盾，因此 $i = j$ 即 $a, c \in S_i$，故 $a \sim_T c$。
综上 $\sim_T$ 是 S 是等价关系。
设 $s \in S$，则 $\exists! \ i \in I,\ s \in S_i$，即 $\overline{s} = S_i$，所以 $S/\sim_T = T$。 □

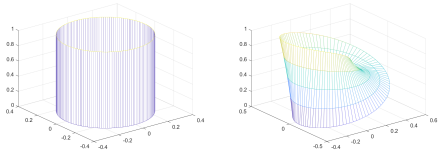
例 1.4.5. 考虑将正方形的对边“粘合”过程中的集合分割及对应的等价类。
设正方形为 $[0,1] \times [0,1]$，分割

$$T_1 = \{\{(0,y),(1,y)\} | y \in [0,1]\} \cup \{\{(x,y)\} | 0 < x < 1, y \in [0,1]\},$$

也就是说，任意的 $\{(0,y),(1,y)\}$ 是一个等价类，而 $0 < x < 1, y \in [0,1]$ 的单点集 $\{(x,y)\}$ 是一个等价类。我们把一个等价类中的元素视作一个点，即把一个等价类内的点“粘”到一起，则 $S/\sim_{T_1}$ 可以视作一个无底无盖的空心圆柱面；而分割

$$T_2 = \{\{(0,y),(1,1-y)\} | y \in [0,1]\} \cup \{\{(x,y)\} | 0 < x < 1, y \in [0,1]\},$$

则 $S/\sim_{T_2}$ 同理可以视作莫比乌斯 (Möbius) 带。



(a) $S/\sim_{T_1}$ 圆柱　　(b) $S/\sim_{T_2}$ 莫比乌斯带

图 1.4-1

1.4.6 序关系

等价关系是“相等”的推广，那么“小于等于”又该如何推广呢？这就是本小节将要讨论的序关系。

定义 1.4.11. 设 ”$\preceq$” 是集合 S 上的二元关系，并且满足
(1) 自反律：$\forall a \in S,\ a \preceq a$;
(2) 反对称律：设 $a, b \in S$，若 $a \preceq b$且$b \preceq a$，则 $a = b$;

(3) 传递律：设 $a,b,c \in S$，若 $a \preceq b$且$b \preceq c$，则 $a \preceq c$.
则称 "$\preceq$" 是一个序关系。

例 1.4.6. 在 $\mathbb{Z}$ 上 $\leqslant$ 和 $\geqslant$ 都是序关系；在 $\mathbb{Z}^+$ 上整除关系 "$|$" 也是序关系 (试验证之)。

定义 1.4.12. 设 $\preceq$ 是集合 S 上的序关系，如果对 $\forall a,b \in S$，有 $a \preceq b$ 或 $b \preceq a$ 成立，则称 $\preceq$ 是全序 (total order)，否则称为偏序 (partial order)。

例如，在 $\mathbb{Z}$ 上 $\leqslant$ 和 $\geqslant$ 都是全序；而 $\mathbb{Z}^+$ 上的整除关系 "$|$" 是偏序。

下面我们把 "极大值" 和 "最大值" 的概念推广开来。类似地，我们也可以定义极小元和最小元。

定义 1.4.13. 设 $\preceq$ 是集合 S 上的序关系 (偏序或全序)，$a \in S$，则

(i) 如果不存在 $b \in S$ 使得 $a \preceq b$ 且 $a \neq b$，则称 a 是关于序 "$\preceq$" 的极大元；

(ii) 如果 $\forall b \in S, b \preceq a$，则称 a 是关于序 "$\preceq$" 的最大元。

可以证明，最大元一定是极大元，但极大元不一定是最大元。极大元可以有多个，但如果最大元存在，则一定唯一。下面的例子具体展示了这一点。

例 1.4.7. 令 $S = \{a,b,c\}$，$T = 2^S$ (幂集)，$T_0 = T \setminus \{S\}$，则 "$\subset$" 是 T 和 T_0 上的序关系，S 是 T 中的最大元，而 T_0 中没有最大元，极大元有三个，分别是 $\{a,b\},\{a,c\},\{b,c\}$。

借此机会我们引入最大公因数和最小公倍数的定义。

定义 1.4.14. 设 $a,b \in \mathbb{Z}^+, S = \{c \in \mathbb{Z}^+ \big| c|a且c|b\}$，则集合 S(其中元素称为公因数) 在 $\mathbb{Z}^+$ 上通常的序关系的最大元就是最大公因数 (greatest common divisor)，记为 $\gcd(a,b)$；同理定义集合 $T = \{c \in \mathbb{Z}^+ \big| a|c且b|c\}$(其中元素称为公倍数)，则 T 在 $\mathbb{Z}^+$ 上通常的序关系下的最小元称为最小公倍数 (least common multiple)，记为 $\mathrm{lcm}(a,b)$。同理我们也可以定义 $a_1,\ldots,a_n \in \mathbb{Z}^+$ 的最大公因数和最小公倍数，我们不再赘述。

最后我们介绍著名的 Zorn 引理，它与集合论中的选择公理是等价的，证明可参考《代数学方法》，李文威，高等教育出版社 的第一章。我们在后续的代数和泛函分析课程中还会用到它。

定理 1.4.3 (Zorn 引理). 设 $(S,\preceq)$ 是一个偏序集，如果 $(S,\preceq)$ 中的任意全序子集皆有上界，则 $(S,\preceq)$ 中必有极大元。

1.5 置换

这一节我们讨论一种基本的映射，即有限集 $X=\{1,2,\cdots n\}$ 上的双射变换。

我们记 $S_n=\{\sigma: X\to X|\sigma是双射\}$，在第四章我们会看到，$S_n$ 在映射复合下形成群结构。下面我们具体讨论 S_n 中元素的性质。

通常我们将 S_n 中的元素 σ 称为**置换**，并表示为

$$\sigma=\begin{pmatrix}1 & 2 & \cdots & n\\ i_1 & i_2 & \cdots & i_n\end{pmatrix}或\sigma=\begin{pmatrix}1 & 2 & \cdots & n\\ \sigma(1) & \sigma(2) & \cdots & \sigma(n)\end{pmatrix}.$$

其中 $(i_1,i_2,\cdots,i_n)$ 是 $(1,2,\cdots,n)$ 的一个全排列。显然 S_n 中有 $n!$ 个元素。容易验证 S_n 中的置换满足结合律 (但一般不满足交换律)。特别地，恒同映射 $e=\begin{pmatrix}1 & 2 & \cdots & n\\ 1 & 2 & \cdots & n\end{pmatrix}$ 在 S_n 中，满足 $\forall\sigma\in S_n,\ \sigma e=e\sigma=\sigma$，并且对 $\forall\sigma\in S_n,\exists!\tau\in S_n$ 使得 $\sigma\tau=\tau\sigma=e$，称 τ 是 σ 的逆元，记作 σ^{-1}。

例 1.5.1. 令 $\sigma=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 3 & 4 & 1\end{pmatrix},\ \tau=\begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 3 & 2 & 1\end{pmatrix}$，则

$$\sigma\tau=\begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 4 & 3 & 2\end{pmatrix},\ \tau\sigma=\begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 2 & 1 & 4\end{pmatrix}$$

显然 $\sigma\tau\neq\tau\sigma$。

此外，对 $\forall\sigma\in S_n$，我们记

$$\sigma^k=\underbrace{\sigma\cdots\sigma}_{k个},k\in\mathbb{Z}^+,$$

并特别规定 $\sigma^0=e,\ \sigma^{-k}=\underbrace{\sigma^{-1}\cdots\sigma^{-1}}_{k个},k\in\mathbb{Z}^+$，则对 $\forall\sigma,\tau\in S_n$ 及 $i,j\in\mathbb{Z}^+$ 满足

$$\sigma^{i+j}=\sigma^i\sigma^j,\ (\sigma^i)^j=\sigma^{ij},\ (\sigma\tau)^{-1}=\tau^{-1}\sigma^{-1}.$$

引理 1.5.1. 设 $\sigma\in S_n$，则 $\exists m\in\mathbb{Z}^+$ 使得 $\sigma^m=e$。

证明. 注意到 $\sigma,\sigma^2,\ldots,\sigma^n,\ldots$ 都在 S_n 中，而 S_n 是有限集，故 $\exists i,j\in\mathbb{Z}^+,i<j,\ \sigma^i=\sigma^j$，则 $\sigma^{j-i}=e$。令 $m=j-i$ 即可。 □

由此我们可以引入置换的阶的定义。

定义 1.5.1. 设 $\sigma\in S_n$，则满足 $\sigma^k=e$ 的最小的正整数 k 称为 σ 的阶，记为 $\mathrm{ord}(\sigma)$。

注 1.5.1. 设 $\sigma\in S_n$，则 $\mathrm{ord}(\sigma)=1\Longleftrightarrow\sigma=e$。

例 1.5.2. 设 $\sigma=\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}$，求 $\mathrm{ord}(\sigma)$。

解. 由于 $\sigma^2=\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}=e\ ,\sigma\neq e$，故 $\mathrm{ord}(\sigma)=2$。 □

引理 1.5.2. 设 $\sigma\in S_n,\ \mathrm{ord}(\sigma)=k,\ m\in\mathbb{Z}$，则 $\sigma^m=e\Longleftrightarrow k|m$。

证明. ($\Longleftarrow$)
设 $m = kq, q \in \mathbb{Z}$，则 $\sigma^m = \sigma^{kq} = (\sigma^k)^q = e^q = e$.
($\Longrightarrow$)
做带余除法 $m = kq + r,\ r \in \{0, 1, \ldots, k-1\}$，则 $e = \sigma^m = \sigma^{kq+r} = \sigma^r$，若 $r > 0$ 则与 $\mathrm{ord}(\sigma) = k$ 矛盾，故 $r = 0$。 □

下面我们将置换分解成更“基本”的置换的乘积 (复合)。

定义 1.5.2. 设 $i_1, \ldots, i_k \in X$ 两两不同，$\pi \in S_n$，如果

$$\pi(i_1) = i_2,\ \pi(i_2) = i_3, \ldots,\ \pi(i_{k-1}) = i_k,\ \pi(i_k) = i_1.$$

且对 $\forall j \in X \setminus \{i_1, \ldots, i_k\}$，有 $\pi(j) = j$，则称 π 是一个循环 (cycle)，k 是 π 的长度。此时我们简记为 $\pi = (i_1\ i_2 \cdots i_k) = (i_1\ \pi(i_1) \cdots \pi^{k-1}(i_1))$。

例 1.5.3. 循环 $(123) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ 的长度是 3，阶也是 3。

引理 1.5.3. 循环 $\sigma = (i_1 \cdots i_k)$ 的阶是 k。

证明. 对 $\forall m \in \{1, 2, \ldots, k-1\}$，有 $\sigma^m(i_1) = i_{m+1} \neq i_1$，于是 $\sigma^m \neq e$。
而 $\sigma^k(i_1) = \sigma(\sigma^{k-1}(i_1)) = \sigma(i_k) = i_1$，注意到 σ 也可以写成 $(i_2\ i_3 \cdots i_k\ i_1)$，于是 $\sigma^k(i_2) = i_2$。
同理可得 $\forall j \in \{1, \cdots k\},\ \sigma^k(i_j) = i_j$。 □

定义 1.5.3. 设 $\sigma = (i_1\ i_2 \cdots i_k),\ \tau = (j_1 \cdots j_l)$ 是 S_n 中的两个循环，如果 $\{i_1, \ldots, i_k\} \cap \{j_1, \ldots, j_l\} = \emptyset$，则称 σ 与 τ 不相交。

引理 1.5.4. 设 $\sigma = (i_1\ i_2 \cdots i_k),\ \tau = (j_1 \cdots j_l)$ 是 S_n 中的两个不相交的循环，则 $\sigma\tau = \tau\sigma$。

证明. 设 $I = \{i_1, \cdots, i_k\},\ J = \{j_1, \cdots, j_l\},\ M = X \setminus (I \cup J)$，则
$\forall m \in M, \sigma\tau(m) = \sigma(m) = m,\ \tau\sigma(m) = \tau(m) = m.$
$\forall i \in I, \sigma\tau(i) = \sigma(i),\ \tau\sigma(i) = \tau(\sigma(i)) = \sigma(i).$ (因为 $\sigma(i) \notin J$)
同理 $\forall j \in J, \sigma\tau(j) = \tau\sigma(j) = \tau(j)$. 验证完毕。 □

上面我们介绍了循环的基本性质，现在我们需要把一般的置换分解成不相交循环的乘积，为此我们需要更精细地考虑置换作用到集合上的效果。

定义 1.5.4. 设 $\sigma \in S_n$，$\mathrm{ord}(\sigma) = m$，若存在 $s \in \mathbb{Z}$ 使得 $j = \sigma^s(i)$，则称点 $i, j \in X$ 为 σ 等价的，记为 $i \sim_\sigma j$。容易验证 σ 等价是一个等价关系，于是作商 $X/\sim_\sigma$ 可以得到等价类 $X_1, \cdots, X_p$，满足 $X = \bigcup\limits_{1 \leqslant i \leqslant p} X_i$ 及 $X_i \cap X_j = \emptyset, i \neq j$。我们把每个等价类 X_i 称为 σ 的一个轨道，X_i 中元素的个数 l_i 称为这个轨道的长度。

容易验证，$\sigma\big|_{X_i}$ 恰好是一个 l_i 阶的循环 (留作思考)，这样我们几乎已经完成了分解，下面我们正式地写出这个分解并证明其唯一性。

定理 1.5.1. 设 $\sigma \in S_n \setminus \{e\}$，则 σ 可以写成有限个互不相交的循环的乘积，即 $\sigma = \pi_1 \cdots \pi_p$($\pi_i$ 是循环)，并且这个分解在不计次序的意义下是唯一的，即若 $\sigma = \tau_1 \cdots \tau_q$ (τ_j 也都是循环)，则 $p = q$ 且 $\tau_1, \ldots, \tau_p$ 是 $\pi_1, \ldots, \pi_p$ 的一个排列。

证明. 先证分解的存在性，我们用数学归纳法[1]。设 $I_\sigma = \{i \in X | \sigma(i) \neq i\}$，我们对 $|I_\sigma|$ 进行归纳。

(1) 当 $|I_\sigma| = 2$ 时，不妨设 $I_\sigma = \{i_1, i_2\}$，则 $\sigma(i_1) = i_2$，$\sigma(i_2) = i_1$，而 $\forall j \in X \setminus I_\sigma$，$\sigma(j) = j$，于是 $\sigma = (i_1\ i_2)$ 本身就是循环。

(2) 下面设 $|I_\sigma| = l > 2$ 且对 $|I_\sigma| < l$ 的所有置换，这种分解都存在。则对 $|I_\sigma| = l$ 的情形，我们设 $i_1 \in I_\sigma$，则 $\sigma^{\mathrm{ord}(\sigma)}(i_1) = i_1$，于是存在 $k \in \mathbb{Z}^+$ 使得

$$\sigma^k(i_1) = i_1, \text{ 且} \forall m \in \{1, 2, \dots k-1\},\ \sigma^m(i_1) \neq i_1.$$

于是记 $i_2 = \sigma(i_1),\ i_3 = \sigma(i_2) = \sigma^2(i_1), \dots,\ i_k = \sigma(i_{k-1}) = \sigma^{k-1}(i_1)$ 两两不同，即 $\pi = (i_1\ i_2 \cdots i_k)$ 是一个循环。令 $J = X \setminus \{i_1, \dots, i_k\}$，取置换 τ 满足

$$\begin{aligned} \tau : & X \longrightarrow X \\ & i \longmapsto i, \quad i \in \{i_1, \dots, i_k\}; \\ & j \longmapsto \sigma(j), \quad j \in J. \end{aligned}$$

下面验证 $\sigma = \pi \circ \tau$。

$\forall i \in \{i_1, \dots, i_k\},\ \pi\tau(i) = \pi(i) = \sigma(i)$;

$\forall j \in J,\ \pi(\tau(j)) = \tau(j) = \sigma(j)$.

即 $\sigma = \pi \circ \tau$ 成立。另一方面，$|I_\tau| < l$，于是由归纳假设，τ 可以分解成若干个不相交循环的乘积，并且由 τ 的取法可知 τ 与 π 也不相交。于是由数学归纳法，分解的存在性证毕。

下面验证分解的唯一性。

设 $\sigma = \pi_1 \cdots \pi_p = \tau_1 \cdots \tau_q$ 都是 σ 的不相交的循环分解。取 i 使得 τ_1 改变 i，则由于分解互不相交，$\tau_2, \cdots, \tau_q$ 都不改变 i。同样的，$\pi_1, \dots, \pi_p$ 中也只有一个循环改变 i，设为 π_a，则 $\sigma(i) = \pi_a(i) = \tau_1(i)$，反复运用引理1.5.4，可得

$$\sigma\pi_a = \pi_1 \cdots \pi_a \cdots \pi_p\pi_a = \pi_1 \cdots \pi_a \cdots \pi_a\pi_p = \cdots = \pi_a\pi_1 \cdots \pi_a \cdots \pi_p = \pi_a\sigma,$$

即 σ 与 π_a 交换。同理 σ 与 τ_1 也交换。于是

$$\sigma^2(i) = \sigma(\sigma(i)) = \sigma(\pi_a(i)) = \pi_a(\sigma(i)) = \pi_a^2(i), \text{ 同理} \sigma^2(i) = \tau_1^2(i).$$

重复以上做法可得对任意的正整数 h 有 $\sigma^h(i) = \pi_a^h(i) = \tau_1^h(i)$ [2]。设 c 是使得 $\sigma^c(i) = i$ 的最小正整数，那么 $\pi_a = \left(i\ \sigma(i)\ \sigma^2(i) \cdots \sigma^{c-1}(i)\right) = \tau_1$。于是 $\tau_1^{-1}\sigma = \pi_a^{-1}\sigma$ 有两个分解式：$\pi_1\pi_2 \cdots \pi_{a-1}\pi_{a+1} \cdots \pi_p$ 和 $\tau_2\tau_3 \cdots \tau_q$。于是由数学归纳法 (对 p 或 q 归纳) 可知结论成立。

□

这个证明过程同时也给出了寻找这种分解的方法。

例 1.5.4. (1)$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix}$，则 $\sigma = (1\ 3\ 2\ 5\ 4)$;

(2)$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 4 & 1 \end{pmatrix}$，则 $\sigma = (1\ 5)(2\ 3)(4)$.

[1] 关于数学归纳法，我们会在习题课讲义中详细介绍。

[2] 注意这里不能直接由 $\sigma(i) = \pi_a(i) = \tau_1(i)$ 得到 $\sigma^h(i) = \pi_a^h(i) = \tau_1^h(i)$，因为这里的幂次表示映射的复合，我们并没有条件 σ 作用在 $\sigma(i)$ 上和 π_a 作用在 $\sigma(i)$ (等于$\pi_a(i)$) 上相等。

下面的定理利用循环分解给出了置换的阶的求法。

定理 1.5.2. 设 $\sigma \in S_n$ 且 $\sigma = \pi_1 \cdots \pi_s, \pi_i$ 是两两不相交的循环，则 $\operatorname{ord}(\sigma) = \operatorname{lcm}(\operatorname{ord}(\pi_1), \ldots, \operatorname{ord}(\pi_s))$。

证明. 设 $k = \operatorname{ord}(\sigma)$, $k_i = \operatorname{ord}(\pi_i)$, $i = 1, \ldots, s$, $l = \operatorname{lcm}(k_1, \ldots, k_s)$。则 $\exists q_i \in \mathbb{Z}^+$，使得 $l = k_i q_i$, $i = 1, \ldots, s$。于是有

$$\begin{aligned} \sigma^l &= (\pi_1 \cdots \pi_s)^l \\ &= \pi_1^l \cdots \pi_s^l \quad \text{(引理1.5.4)} \\ &= \pi_1^{k_1 q_1} \cdots \pi_s^{k_s q_s} \\ &= e. \end{aligned}$$

即 $k \leqslant l$。下证 $k = l$。
用反证法，若 $k < l$，则 $\exists k_i$ 使得 $k_i \nmid k$。不妨设 $i = 1$，则 $k = m_1 k_1 + r_1$，其中 $r_1 \in \{1, 2, \ldots, k_1 - 1\}$。则

$$\sigma^k = \pi_1^k \pi_2^k \cdots \pi_s^k = \pi_1^{r_1} \pi_2^k \cdots \pi_s^k.$$

由 r_1 的取值范围知 $\pi_1^{r_1} \neq e$，即存在 $j \in X$ 使得 $\pi_1^{r_1}(j) \neq j$，而 $\pi_2^k, \ldots, \pi_s^k$ 与 $\pi_1^{r_1}$ 都不相交，故 $j = \sigma^k(j) = \pi_1^{r_1}(j) \neq j$，这与 $\sigma^k = e$ 矛盾！故 $k = l$。 □

例 1.5.5. 设 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 5 & 4 & 6 & 10 & 8 & 2 & 9 & 1 & 7 \end{pmatrix}$，求 $\operatorname{ord}(\sigma)$。

解. $\sigma = (1\ 3\ 4\ 6\ 8\ 9)(2\ 5\ 10\ 7)$，则 $\operatorname{ord}(\sigma) = \operatorname{lcm}(6, 4) = 12$。 □

下面我们转而关注长度为 2 的循环，我们把它们称为对换。

命题 1.5.1. 设 $\forall \sigma \in S_n \setminus \{e\}$，$\sigma$ 总可以写成有限个对换的乘积。

只需注意到置换可以写成有限个循环的乘积，而对任意的循环 $\pi = (i_1\ i_2 \cdots i_k) = (i_1\ i_k) \cdots (i_1\ i_3)(i_1\ i_2)$，即任意置换都可以写成有限个对换的乘积。

例 1.5.6. 将 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 1 & 6 & 5 \end{pmatrix}$ 写成对换的乘积。

解. $\sigma = (1\ 2\ 4)(5\ 6) = (1\ 4)(1\ 2)(5\ 6) = (2\ 1)(2\ 4)(5\ 6)$. □

需要注意的是，将置换分解成对换乘积的形式并不是唯一的，但不同分解中对换个数的奇偶性是一致的。下面我们将证明这一点。

引理 1.5.5. 设 $\alpha = (s\ t)$, $\beta = (u\ v) \in S_n$ 是对换，$\alpha \neq \beta$，则存在对换 α', β' 使得 $\alpha'(s) \neq s$, $\beta'(s) = s$, $\beta\alpha = \alpha'\beta'$。

证明. (1) 若 $\{s, t\} \cap \{u, v\} = \emptyset$，则 $\alpha\beta = \beta\alpha$，于是令 $\alpha' = \alpha$, $\beta' = \beta$ 即可。

(2) 若 $u = s$，则 $v \neq s$, $v \neq t$，则 $\beta\alpha = (s\ v)(s\ t) = (s\ t)(v\ t)$，令 $\alpha' = \alpha$, $\beta' = (v\ t)$ 即可。

(3) 若 $u = t$，则 $v \neq s$, $v \neq t$，则 $\beta\alpha = (v\ t)(s\ t) = (s\ v)(v\ t)$，令 $\alpha' = (s\ v)$, $\beta' = \beta$ 即可。

□

引理 1.5.6. 设 $\tau_1, \cdots, \tau_k$ 是对换，且 $e = \tau_1 \cdots \tau_k$，则 k 是偶数。

证明. 显然 $k \neq 1$，若 $k = 2$，则结论成立。下面我们证明：若 $k > 2$，则 e 能写成 $k-2$ 个对换的乘积。
设 $\tau_k = (s\ t)$，由引理1.5.5，存在对换 τ'_{k-1}，τ'_k，使得

$$\tau'_k(s) = s,\ \tau'_{k-1}(s) \neq s,\ \tau_{k-1}\tau_k = \tau'_{k-1}\tau'_k.$$

则 $e = \tau_1 \cdots \tau_{k-2}\tau'_{k-1}\tau'_k$。若 $\tau_{k-2}\tau'_{k-1} = e$，则 e 是 $k-2$ 个对换的乘积，证明结束。否则 $\tau_{k-2} \neq \tau'_{k-1}$。对 τ_{k-2}，τ'_{k-1} 再用引理1.5.5得：存在对换 τ'_{k-2}，τ''_{k-1} 使得

$$\tau''_{k-1}(s) = s,\ \tau'_{k-2}(s) \neq s,\ \tau_{k-2}\tau'_{k-1} = \tau'_{k-2}\tau''_{k-1},\ \text{且} e = \tau_1 \cdots (\tau_{k-3}\tau'_{k-2})\tau''_{k-1}\tau'_k.$$

重复以上步骤，我们或者在某次重复中结束证明，得到 e 是 $k-2$ 个对换的乘积；或者得到

$$e = \delta_1\delta_2 \cdots \delta_k,$$

其中 $\delta_1, \delta_2, \cdots, \delta_k$ 是对换，且 $\delta_2(s) = \cdots = \delta_k(s) = s$，而 $\delta_1(s) \neq s$，则 $s = e(s) = \delta_1(s) \neq s$，这是一个矛盾！故后一种情况不会发生，于是 e 可以写成 $k-2$ 个对换的乘积，归纳即可证明原命题。 □

定理 1.5.3. 设 $\sigma \in S_n \setminus \{e\}$，$\sigma = \lambda_1 \cdots \lambda_k = \mu_1 \cdots \mu_m$，其中 $\lambda_1, \ldots, \lambda_k, \mu_1, \ldots, \mu_m$ 都是对换，则 k 和 m 具有相同的奇偶性。

证明. 只需注意到 $\lambda_1 \cdots \lambda_k = \mu_1 \cdots \mu_m$，于是

$$\begin{aligned} e &= (\lambda_1 \cdots \lambda_k)^{-1}\mu_1 \cdots \mu_m \\ &= \lambda_k \cdots \lambda_1\mu_1 \cdots \mu_m \end{aligned}$$

所以 $k+m$ 是偶数，即 k, m 具有相同的奇偶性。 □

有了以上定理，我们就可以定义置换的符号了。

定义 1.5.5. 设 $\sigma \in S_n$，若 σ 是偶数个对换之积，则定义 σ 的符号为 1；若 σ 是奇数个对换之积，则定义 σ 的符号为-1。特别地，e 的符号为 1。我们把 σ 的符号记为 ε_σ，则 $\varepsilon_\sigma = (-1)^k$，其中 k 是对换的个数。

推论 1.5.1. 设 $\sigma \in S_n$，且 $\sigma = \pi_1 \cdots \pi_s$，其中 $\pi_1, \ldots, \pi_s$ 是不相交的循环，则

$$\varepsilon_\sigma = (-1)^{\sum_{i=1}^{s}[\mathrm{ord}(\pi_i)-1]}.$$

利用命题1.5.1下面的说明即可证明这一推论。

例 1.5.7. 求 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 5 & 7 & 3 & 1 & 6 \end{pmatrix}$ 的符号。

解. $\sigma = (1\ 2\ 4\ 7\ 6)(3\ 5)$，则 $\mathrm{ord}(\sigma) = \mathrm{lcm}(5, 2) = 10$，$\varepsilon_\sigma = (-1)^{4+1} = -1$. □

命题 1.5.2. 设 $\sigma, \tau \in S_n$，则 $\varepsilon_{\sigma\tau} = \varepsilon_\sigma\varepsilon_\tau$.

证明. 将 σ, τ 都写成对换乘积即可证明。 □

当 $\varepsilon_\sigma = 1$ 时，我们称 σ 为偶置换；当 $\varepsilon_\sigma = -1$ 时，我们称 σ 为奇置换。我们把所有偶置换构成的集合记作 A_n，所有奇置换构成的集合记作 $\overline{A_n}$。于是 $S_n = A_n \cup \overline{A_n}$。在第四章我们会知道，$A_n$ 也构成了一个群结构。下面我们讨论 A_n 中元素的个数。任取 $\sigma \in S_n$，作映射

$$L_\sigma : S_n \to S_n,\ \pi \mapsto \sigma\pi; \qquad R_\sigma : S_n \to S_n,\ \pi \mapsto \pi\sigma.$$

容易验证 L_σ, R_σ 都是双射 (利用 $L_\sigma \circ L_{\sigma^{-1}} = e$, $L_{\sigma^{-1}} \circ L_\sigma = e$ 可得 L_σ 是双射，R_σ 同理)。我们可以计算出：

(1) 如果 σ 是偶置换, 那么

$$L_\sigma(A_n) = R_\sigma(A_n) = A_n.$$
$$L_\sigma\left(\overline{A_n}\right) = R_\sigma\left(\overline{A_n}\right) = \overline{A_n}.$$

(2) 如果 σ 是奇置换, 那么

$$L_\sigma(A_n) = R_\sigma(A_n) = \overline{A_n}.$$
$$L_\sigma\left(\overline{A_n}\right) = R_\sigma\left(\overline{A_n}\right) = A_n$$

于是, S_n 中的偶置换的数量等于奇置换的数量, 从而

$$|A_n| = \left|\overline{A_n}\right| = \frac{1}{2}|S_n| = \frac{n!}{2}.$$

最后我们简单介绍一下对称函数和斜对称 (反对称) 函数。在下册张量一章中我们会更深入地讨论。

定义 1.5.6. 设 $\pi \in S_n$，f 是 n 个自变量的函数 (值域是数集)，令

$$f_\pi(x_1, \ldots, x_n) = f(x_{\pi(1)}, \ldots, x_{\pi(n)}).$$

称函数 f_π 是由 π 作用到 f 上得到的。若 $\forall \pi \in S_n$，$f_\pi = f$，则我们称一个函数是对称 (symmetric) 的；若 $\forall \pi \in S_n$，$f_\pi = \varepsilon_\pi f$，则称一个函数是斜对称 (反对称, anti-symmetric) 的。

置换作用到函数上有以下的结合律。

引理 1.5.7. 设 $\alpha, \beta \in S_n$，f 是 n 个自变量的函数，则 $f_{\alpha\beta} = (f_\beta)_\alpha$。

利用定义验证即可。

引理 1.5.8. 交换任意两个自变量的位置，斜对称函数变号。

由斜对称函数的定义可以直接得到上面的引理，它也可以作为斜对称函数的定义。

例 1.5.8. $\Delta_n = \Delta_n(x_1, x_2, \cdots, x_n) = \prod\limits_{1 \leqslant i < j \leqslant n} \left(x_j - x_i\right)$ 是斜对称函数 (试验证之)。这是一个十分常用的例子。当 $x_1, \ldots, x_n$ 两两不同时，$\Delta_n(x_1, x_2, \ldots, x_n) \neq 0$。

利用斜对称函数 (用引理1.5.8作为定义) 可以给出定理1.5.3的另一个证明。设 $\sigma \in S_n$, $\sigma = \sigma_1 \cdots \sigma_k$ 是置换的对换分解，f 是 n 元斜对称函数，则

$$f_\sigma = (f_{\sigma_k})_{\sigma_1 \cdots \sigma_{k-1}} = -f_{\sigma_1 \cdots \sigma_{k-1}} = \cdots = (-1)^k f = \varepsilon_\sigma f.$$

由于 f_σ 与 σ 的对换分解无关，所以当 f 不是零函数时，可知 ε_σ 也与分解无关。

1.6 整数的算术与辗转相除法

我们在中学时就已经知道，整数的素因子分解在不计次序下是唯一的 (这个结论称之为算术基本定理)，但我们并没有严格证明过它 (我们会在第六章证明它)。本节的主要任务是，尽量绕开算术基本定理而讲清楚最大公因数的性质和求最大公因数的算法。

定义 1.6.1. 设 $a,b\in\mathbb{Z}^+, S=\{c\in\mathbb{Z}^+\big|c|a且c|b\}$，则集合 S(其中元素称为公因数) 在 $\mathbb{Z}^+$ 通常的序下的最大元就是最大公因数 (greatest common divisor)，记为 $\gcd(a,b)$；同理定义集合 $T=\{c\in\mathbb{Z}^+\big|a|c且b|c\}$(其中元素称为公倍数)，则 T 在通常的序下的最小元称为最小公倍数 (least common multiple)，记为 $\mathrm{lcm}(a,b)$。如果 $a,b\in\mathbb{Z}$，那么我们定义 a,b 的最大公因数是它们绝对值的最大公因数，最小公倍数同理。

给定任意整数 $a,b\in\mathbb{Z},\ b\neq 0$，$a,b$ 的最大公因子 $\gcd(a,b)$ 和最小公倍数 $\mathrm{lcm}(a,b)$ 满足

1. $\gcd(a,b)|a,\gcd(a,b)|b$，$\forall d,d|a,d|b$ 则 $d|\gcd(a,b)$;
2. $a|\mathrm{lcm}(a,b),b|\mathrm{lcm}(a,b)$，$\forall u,a|u,b|u$ 则 $\mathrm{lcm}(a,b)|u$.

首先我们介绍辗转相除法 (Euclidean's Algorithm)。设 $a,b\in\mathbb{Z}^+,\ b\neq 0$，我们欲求出 $\gcd(a,b)$。为此我们进行如下操作：

(1) 设 $r_0=a,\ r_1=b$，作带余除法 $r_0=q_2r_1+r_2$，即 $q_2=\mathrm{quo}(r_0,r_1),\ r_2=\mathrm{rem}(r_0,r_1)$。如果 $r_2=0$，则 $r_1|r_0$，即 $r_1=\gcd(a,b)$，否则进行 (2)。

(2) 作带余除法 $r_1=q_3r_2+r_3$，即 $q_3=\mathrm{quo}(r_1,r_2),\ r_3=\mathrm{rem}(r_1,r_2)$。如果 $r_3=0$，则易证 $r_2=\gcd(a,b)$(思考)，否则进行 (3)。

(3) 反复作带余除法 $r_2=q_4r_3+r_4,\cdots,r_{k-2}=q_kr_{k-1}+r_k,\ r_{k-1}=q_{k+1}r_k$，由于 $r_2,\ r_3,\cdots$ 都是非负整数，且 $r_2>r_3>\cdots$，因此这个操作必然在有限步内终止 (即遇到 $r_{k+1}=0$)，此时 $r_k=\gcd(a,b)$。

下面我们证明这个算法的正确性。为此只需证 $\gcd(r_{i-2},r_{i-1})=\gcd(r_{i-1},r_i)$ 对任意 $i=2,3,\cdots,k$ 成立。设

$$x=\gcd(r_{i-2},r_{i-1}),\quad y=\gcd(r_{i-1},r_i),$$

则由 $r_{i-2}=q_ir_{i-1}+r_i$ 及 $x|r_{i-1},\ x|r_{i-2}$ 知 $x|r_i$，于是 $x|y$。类似地可以得到 $y|x$，即 $x=y$ (注意 $x>0,\ y>0$)。因此，

$$\gcd(a,b)=\gcd(r_0,r_1)=\gcd(r_1,r_2)=\cdots=\gcd(r_{k-1},r_k)=r_k.$$

综上所述，我们有以下定理：

定理 1.6.1. 设 $a,b\in\mathbb{Z},\ b\neq 0$，则

(i) $\gcd(a,b)$ 存在；

(ii) $\exists u,v\in\mathbb{Z}$ 使得 $ua+vb=\gcd(a,b)$ (Bezout 关系)。

证明. (i) 由辗转相除法即可得到。
(ii) 设 $\gcd(a,b)=g$，由辗转相除法可得：

$$g = r_K = r_{k-2} + (-q_k)r_{k-1},$$

因为

$$r_{k-3} = q_{k-1}r_{k-2} + r_{k-1},$$

所以

$$g = r_{k-2} + (-q_k)(r_{k-3} - q_{k-1}r_{k-2}) = (-q_k)r_{k-3} + (1 + q_kq_{k-1})r_{k-2}.$$

令 $u_{k-2} = -q_k$, $v_{k-2} = 1 + q_kq_{k-1}$。再由 $r_{k-4} = q_{k-2}r_{k-3} + r_{k-2}$ 得

$$g = u_{k-2}r_{k-3} + v_{k-2}(r_{k-4} - q_{k-2}r_{k-3}) = v_{k-2}r_{k-4} + (u_{k-2} - q_{k-2}v_{k-2})r_{k-3}$$

再令 $u_{k-3} = v_{k-2}$, $v_{k-3} = u_{k-2} - q_{k-2}v_{k-2}$。重复这样的回代操作即可得到存在 $u_1, v_1 \in \mathbb{Z}$，使得 $g = u_1a + v_1b$。 □

例 1.6.1. 计算 $\gcd(18, 4)$。

解. $18 = 4 \times 4 + 2$, $4 = 2 \times 2$. 所以 $\gcd(18, 4) = 2$。 □

定义 1.6.2. 设 $a, b \in \mathbb{Z}$, $b \neq 0$，若 $\gcd(a, b) = 1$，则称 a, b 互素。

下面是互素的充要条件。

定理 1.6.2. 设 $a, b \in \mathbb{Z}$, $b \neq 0$，则 a, b 互素 $\iff \exists u, v \in \mathbb{Z}$ 使得 $ua + vb = 1$。

证明. ($\Longrightarrow$) 由定理1.6.1(ii) 即得结论。
($\Longleftarrow$) 设 $g = \gcd(a, b)$，则 $g|a$, $g|b$，于是 $g|(ua + vb)$ 即 $g|1$。又 $1|g$，故 $g = 1$。 □

下面我们考虑最小公倍数与最大公因数的关系。

引理 1.6.1. 设 $a, b \in \mathbb{Z} \setminus \{0\}$，如果 a, b 互素，则 $\operatorname{lcm}(a, b) = ab$。

证明. 显然 ab 是 a, b 的公倍数，设 m 是 a, b 的一个公倍数，则 $\exists s, t \in \mathbb{Z}$ 使得 $m = sa = tb$。又因为 $\gcd(a, b) = 1$，由定理1.6.2知 $\exists u, v \in \mathbb{Z}$ 使得 $ua + vb = 1$，所以 $uam + vbm = m$，即 $ab(ut + vs) = m$，即 $ab|m$。所以 ab 是 a 和 b 的最小公倍数。 □

定理 1.6.3. 设 $a, b \in \mathbb{Z} \setminus \{0\}$，则 $\operatorname{lcm}(a, b) = \dfrac{ab}{\gcd(a, b)}$。

证明. 设 $g = \gcd(a, b)$，则 $\exists c, d \in \mathbb{Z}$ 使得 $a = cg$, $b = dg$ 且 $\gcd(c, d) = 1$ (前者由 gcd 的定义，后者由 Bezout 关系)。则

$$\frac{ab}{g} = \frac{cg \cdot dg}{g} = cdg.$$

则我们的目标是证明 $\operatorname{lcm}(a, b) = cdg$。显然 cdg 是 a, b 的公倍数，设 m 是 ab 的公倍数，则 $\exists s, t$ 使得 $m = sa = scg$, $m = tb = tdg$。于是 $sc = td$，我们记为 $sc = td = w$，则 w 是 c, d 的公倍数，而由 c, d 互素知 $w = rcd$, $r \in \mathbb{Z}$ (引理 1.6.1)。所以 $m = wg = rcdg$，即 $cdg|m$。综上，$\operatorname{lcm}(a, b) = cdg = \frac{ab}{\gcd(a,b)}$。 □

下面我们介绍一些素数的性质。

定义 1.6.3. 设 $p \in \mathbb{Z}^+ \setminus \{1\}$，若 p 不能写成两个小于 p 的正整数之积，则称 p 为素数或质数 (prime number)；反之称为合数 (composite number)。[1]

[1] 1 既不是素数也不是合数。

例如，2，3，5，7，11，13，17，19，23，29 都是素数；除 2 以外，素数都是奇数，但反过来不对 (如 9，15)。

定理 1.6.4. *设 $m \in \mathbb{Z}^+ \setminus \{1\}$，则 m 可以写成若干个素数之积。*

证明. 用数学归纳法。定理对 $m = 2$ 显然成立。下设 $m > 2$ 且定理对一切 2 和 $m-1$ 之间的正整数成立，则对于数 m 来说，若 m 是素数，则定理直接成立；否则 $\exists k, l \in \{2, \cdots, m-1\}$ 使得 $m = kl$，对 k, l 应用归纳假设可知定理成立。 □

例如，$24 = 2^3 \times 3$。

例 1.6.2. *求证素数有无穷多个。*

证明. 用反证法。假设只有有限个素数 $p_1, \cdots, p_k$，则令 $m = p_1 \cdots p_k + 1 > p_i$, $i \in \{1, \cdots, k\}$，于是 m 不是素数。即 $\exists j \in \{1, \cdots, k\}$ 使得 $p_j | m$，于是 $p_j | 1$ ，矛盾！故素数有无穷多个。 □

引理 1.6.2. *设 $a, b \in \mathbb{Z}$，p 是素数，若 $p | ab$，则必有 $p | a$ 或 $p | b$。*

证明. 设 $p \nmid a$，我们只需证 $p | b$ 即可。由 p 是素数，故 $p \nmid a \Longrightarrow \gcd(p, a) = 1$，于是 $\exists u, v$ 使得 $ua + vp = 1$，则 $uab + vpb = b$，则由 $p | ab$, $p | vpb$ 知 $p | b$。 □

例 1.6.3. *设 p 是素数，$k \in \mathbb{Z}$ 且 $1 < k < p$，求证 $p | \binom{p}{k}$.*

证明. 由于 $\binom{p}{k} = \dfrac{p!}{k!(p-k)!}$，故 $p! = \binom{p}{k} k!(p-k)!$。于是 $p | \binom{p}{k} k!(p-k)!$。若 $p | k!$，则必存在 $i \in \{1, \cdots, k\}$ 使得 $p | i$，这是不可能的！即 $p \nmid k!$。同理 $p \nmid (p-k)!$。故 $p | \binom{p}{k}$。 □

最后我们介绍一下著名的中国剩余定理。这个定理可以推广到一般的交换环上，我们会在抽象代数课程中遇到它。

定理 1.6.5 (中国剩余定理, Chinese Remainder Theorem). *设 $m, n \in \mathbb{Z}^+$ 且 $\gcd(m, n) = 1$，则对任意整数 a, b，存在整数 x 满足同余方程组*

$$\begin{cases} x \equiv a \mod m \\ x \equiv b \mod n \end{cases}$$

并且若 y 也是该同余方程组的解，则 $x \equiv y \mod mn$。

证明. 由 $\gcd(m, n) = 1$，故存在 $u, v \in \mathbb{Z}$ 使得 $um + vn = 1$，即

$$\begin{cases} um \equiv 1 \mod n \\ vn \equiv 1 \mod m \end{cases}.$$

令 $x = avn + bum$，则

$$\begin{cases} x \equiv avn \equiv a \mod m \\ x \equiv bum \equiv b \mod n \end{cases}$$

即为所求。设另有整数 $y \neq x$ 也满足同余方程组，则 $m | x - y$, $n | x - y$，于是 $x - y$ 是 m, n 的公倍数，由引理1.6.1，m, n 的最小公倍数是 mn，故 $mn | x - y$，即 $x \equiv y \mod mn$。 □

这个定理也可以推广到 $m_1, \ldots, m_s$ 两两互素的情形，证明留作思考。

1.7 习题

线性方程组初步

1. 如果方程组 (L) 是确定的, 证明它相伴的齐次线性方程组 (H) 只有零解. 举例说明反之不对.

2. 设 A 是 $m\times n$ 阶矩阵，$m<n$, $b_1,\dots,b_m\in\mathbb{R}$。试证明：以 $\left(\begin{array}{c|c} & b_1\\ A & \vdots\\ & b_m\end{array}\right)$ 为增广矩阵的线性方程组或者不相容，或者不确定。

3. 试判断下列线性方程组是否有解, 在有解时求出它的解:

(1)
$$\begin{cases} x_1+x_2-3x_3=-1,\\ 2x_1+x_2-2x_3=1,\\ x_1+x_2+x_3=3,\\ x_1+2x_2-3x_3=1.\end{cases}$$

(2)
$$\begin{cases} \lambda x_1+x_2+x_3=1,\\ x_1+\lambda x_2+x_3=1,\\ x_1+x_2+\lambda x_3=1.\end{cases}$$

4. 证明

(1) $\begin{vmatrix} a & b\\ c & d\end{vmatrix}=\begin{vmatrix} a & c\\ b & d\end{vmatrix}=-\begin{vmatrix} b & a\\ d & c\end{vmatrix}=-\begin{vmatrix} c & d\\ a & b\end{vmatrix}$.

(2) $\begin{vmatrix} a+a' & b\\ c+c' & d\end{vmatrix}=\begin{vmatrix} a & b\\ c & d\end{vmatrix}+\begin{vmatrix} a' & b\\ c' & d\end{vmatrix}$.

(3) $\begin{vmatrix} a & b+b'\\ c & d+d'\end{vmatrix}=\begin{vmatrix} a & b\\ c & d\end{vmatrix}+\begin{vmatrix} a & b'\\ c & d'\end{vmatrix}$.

5. 计算行列式. (1) $\begin{vmatrix} 3 & -4\\ 4 & 3\end{vmatrix}$;

(2) $\begin{vmatrix} \cos\alpha & -\sin\alpha\\ \sin\alpha & \cos\alpha\end{vmatrix}$;

(3) $\begin{vmatrix} \log_b a & 1\\ 1 & \log_a b\end{vmatrix}$;

(4) $\begin{vmatrix} 3 & 2 & 1\\ 4 & 5 & 6\\ -2 & 1 & 5\end{vmatrix}$;

(5) $\begin{vmatrix} a & b & c\\ b & c & a\\ c & a & b\end{vmatrix}$.

集合与映射

1. 证明命题1.3.1和1.3.2.

2. 设 $\Omega = \{+, -, ++, +-, -+, --, +++, \cdots\}$ 是加号和减号的有限序列的集合, 而 $f : \Omega \to \Omega$ 是一个变换, 将元素 $\omega = \omega_1\omega_2\cdots\omega_n \in \Omega$ 对应到 $\omega' = \omega_1\dot{\omega}_1\omega_2\dot{\omega}_2\cdots\omega_n\dot{\omega}_n$, 其中若 $\omega_k = +$, 则 $\dot{\omega}_k = -$, 若 $\omega_k = -$, 则 $\dot{\omega}_k = +$. 证明在 $f(f\omega)$ 的长度 > 4 的任意区间内包含 $++$ 或 $--$.

3. 由法则 $n \to n^2$ 给出的映射 $f : \mathbb{N} \to \mathbb{N}$ 有右逆吗? 给出 f 的两个左逆.

4. 设 $f : X \to Y$ 是一个映射, 且 S, T 都是 X 的子集. 证明

$$f(S \cup T) = f(S) \cup f(T), \quad f(S \cap T) \subset f(S) \cap f(T).$$

   试举一例, 说明后一个式子中的包含关系一般来说不能换成相等关系.

5. 集合 S 的全体子集的集合记作

$$\mathcal{P}(S) = \{T \mid T \subset S\}.$$

   例如若 $S = \{s_1, s_2, \cdots, s_n\}$ 是 n 个元素的有限集, 则 $\mathcal{P}(S)$ 由空集 $\varnothing, n$ 个单元集 $\{s_1\}, \{s_2\}, \cdots, \{s_n\}, n(n-1)/2$ 个二元集 $\left\{s_i, s_j\right\}, 1 \leqslant i < j \leqslant n$, 等等, 直到全集 $T = S$ 组成. 集合 $\mathcal{P}(S)$ 的基数是多少?

6. 设 $f : X \to Y$ 是一个映射, 且设对某个元素 $a \in X, b = f(a)$. 原像

$$f^{-1}(b) = f^{-1}(f(a)) = \{x \mid f(x) = f(a)\}$$

   叫作元素 $b \in \mathrm{im}(f)$ 上的纤维. 证明集合 X 是互不相交的纤维的并 (也就是说, 给出了 X 的一个划分). 注意: 符号 $f^{-1}(b)$ 不能联想到逆映射, 后者可能并不存在.

7. 证明有限个可数集的笛卡尔积也是可数集.

8. 符号 $S \triangle T$ 表示两个集合 S 与 T 的对称差: $S \triangle T = (S \setminus T) \cup (T \setminus S)$. 证明 $S \triangle T = (S \cup T) \setminus (S \cap T)$.

9. 对有限集合 $A_1, A_2, \cdots, A_n$, 证明

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i| - \sum_{1 \leqslant i < j \leqslant n} \left|A_i \cap A_j\right| + \cdots + (-1)^{k-1} \sum_{1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant n} \left|A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}\right| + \cdots + (-1)^{n-1} \left|A_1 \cap A_2 \cap \cdots \cap A_n\right| .$$

等价关系和序关系

1. 证明命题1.4.1.

2. 证明集合 $T = \left\{(a, b) \in \mathbb{R}^2 \mid a - b \in \mathbb{Z}\right\}$ 是实数集 $\mathbb{R}$ 上的等价关系 (几何上 $\mathbb{R}$ 关于这个等价关系的商集可以和圆周等同起来).

3. 对 $\mathbb{R}^2$ 中的元素, 定义关系如下: $(a,b) \sim (c,d)$ 当且仅当 $a-c$ 和 $b-d$ 都是整数. 证明这个关系 $\sim$ 是 $\mathbb{R}^2$ 上的等价关系 (几何上 $\mathbb{R}^2$ 关于这个等价关系的商集可以和环面 (形如汽车轮胎) 等同起来).

4. 定义 $\mathbb{R}^2$ 上的二元关系 $\leqslant$ 如下:

$$(a,b) \leqslant (c,d) \Longleftrightarrow a < c, \text{ 或} a = c \text{ 但} b \leqslant d.$$

证明: 这个二元关系是 $\mathbb{R}^2$ 上的全序.

5. 定义 $\mathbb{R}^2$ 上的二元关系 $\leqslant$ 如下:

$$(a,b) \leqslant (c,d) \Longleftrightarrow a \leqslant c, \text{ 且} a+b \leqslant c+d.$$

证明: 这个二元关系是 $\mathbb{R}^2$ 上的偏序但不是全序.

6. 令实坐标平面 $\mathbb{R}^2$ 上的两点 $P(x,y) \sim P(x',y')$, 当且仅当 $y = y'$. 设 l : $\{(x,y) \mid y = kx+b,\ k \neq 0\}$ 是与 X 轴相交的任意直线, 试给出 $\mathbb{R}^2/\sim$ 的元素与 l 的点之间的一一对应.

7. 证明 2 元、3 元和 4 元集分别有 2,5 和 15 个不同的商集.

置换

1. 将置换

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 6 & 8 \end{pmatrix}$$

和置换

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 8 & 2 & 1 & 4 & 5 & 7 \end{pmatrix}$$

分解成不交循环的乘积, 并求出它们的阶.

2. 设 $\sigma = \pi_1 \cdots \pi_p \in S_n$, 其中 π_k 是互不相交的循环, $k \in \{1,\ldots,p\}$. 记 $l_k = \mathrm{ord}(\pi_k)$. 令

$$p' = n - \sum_{k=1}^{p} l_k,$$

则 σ 使 p' 个点保持不变. 数 $d(\sigma) = n-(p+p')$ 叫作置换 σ 的减量. 验证 $\varepsilon_\sigma = (-1)^{d(\sigma)}$.

3. 计算置换

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ n & n-1 & n-2 & \cdots & 2 & 1 \end{pmatrix}$$

的符号.

4. 设 $\sigma \in S_n$ 是长度为 k 的循环, 证明: 对于任意的 $\tau \in S_n$, 置换 $\tau\sigma\tau^{-1}$ 仍是长度为 k 的循环.

5. 设 $\sigma \in S_n$. 称整数对 $\langle i,j\rangle$ 是 σ 的一个反序如果 $1 \leqslant i < j \leqslant n$ 且 $\sigma(i) > \sigma(j)$, 整数对 $\langle i,j\rangle$ 是 σ 的一个顺序如果 $1 \leqslant i < j \leqslant n$ 且 $\sigma(i) < \sigma(j)$. 显然没有反序的置换是单位变换 e. 假设 $\langle i,j\rangle$ 是 σ 的反序, 命 τ 和 τ' 分别为对换 $(\sigma(j)\sigma(i))$ 和对换 (ij). 证明:

(1) 整数对 $\langle i, j\rangle$ 是 $\tau\sigma$ 的顺序, 也是 $\sigma\tau'$ 的顺序.

(2) 如果整数对 $\langle a, i\rangle$ 和 $\langle a, j\rangle$ 都是 σ 的反序, 那么它们也都是 $\tau\sigma$ 的反序.

(3) 如果整数对 $\langle a, j\rangle$ 和 $\langle a, i\rangle$ 中只有一个是 σ 的顺序, 则它们中也只有一个是 $\tau\sigma$ 的反序.

(4) 如果整数对 $\langle a, i\rangle$ 和 $\langle a, j\rangle$ 都是 σ 的顺序, 则它们也都是 $\tau\sigma$ 的顺序.

(5) 如果整数对 $\langle i, b\rangle$ 和 $\langle j, b\rangle$ 都是 σ 的顺序, 则它们也都是 $\tau\sigma$ 的顺序.

(6) 如果整数对 $\langle i, b\rangle$ 和 $\langle j, b\rangle$ 中只有一个是 σ 的反序, 则它们中也只有一个是 $\tau\sigma$ 的反序.

(7) 如果整数对 $\langle i, b\rangle$ 和 $\langle j, b\rangle$ 都是 σ 的反序, 则它们也都是 $\tau\sigma$ 的反序.

(8) 如果整数对 $\langle i, c\rangle$ 和 $\langle c, j\rangle$ 中只有一个是 σ 的反序, 则它们中也只有一个是 $\tau\sigma$ 的反序.

(9) 如果整数对 $\langle i, c\rangle$ 和 $\langle c, j\rangle$ 都是 σ 的反序, 则它们都是 $\tau\sigma$ 的顺序.

于是 $\tau\sigma$ 的反序总数比 σ 的反序总数少一个奇数. 由此可知, 存在对换 $\tau_m, \cdots, \tau_1$ 使得

$$\tau_m \cdots \tau_1 \sigma = e,$$

其中 m 与 σ 的反序总数 k 有相同的奇偶性. 所以 σ 的符号 $\varepsilon_\sigma = (-1)^m = (-1)^k$ 也可以通过 σ 的反序数计算.

6. 利用上题的结论计算置换

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & . & . & . & \cdots & n-1 & n \\ 2 & 4 & 6 & \cdots & 1 & 3 & 5 & \cdots & . & . \end{pmatrix}$$

和

$$\begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n-1 & n \\ n & 1 & n-1 & 2 & \cdots & . & . \end{pmatrix}$$

的符号.

7. 证明: $n \geqslant 3$ 时 S_n 中的每个**偶置换**都可以写成长度为 3 的循环的乘积.

整数的算术

1. 利用辗转相除法求 252 和 198 的最大公因数.

2. 利用中国剩余定理求解同余方程组

$$\begin{cases} x \equiv 1 \mod 5 \\ x \equiv 3 \mod 12 \end{cases}.$$

3. 每一个不等于 2 的素数都可以写成 $4k+1$ 或 $4k-1$ 的形式. 试证明形如 $4k-1$ 的素数有无穷多个.

4. 下述论断是非平凡的:
若 $n, m \in \mathbb{Z}, \gcd(n, m) = 1$, 如果 p 是整除 $n^2 + m^2$ 的一个素数, 则 $p = 4k+1$.
试用该论断证明存在无穷多个形如 $4k+1$ 的素数.

5. 如果自然数 n 恰可被 r 个不同的素数 $p_1, \cdots, p_r$ 整除, 则小于 n 且与 n 互素的整数的个数

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\cdots\left(1 - \frac{1}{p_r}\right).$$

函数 $\varphi : \mathbb{N} \to \mathbb{N}$ 叫作欧拉函数. 证明公式当 $n \leqslant 25$ 时, 以及当 $n = p^m$ 时成立. 思考: 如何证明一般情况下该公式成立?

6. 运用二项式定理, 对 n 作归纳证明: 若 p 是素数, 则 $n^p - n$ 对任意 $n \in \mathbb{Z}$ 可以被 p 整除.

第二章　矩阵

2.1　向量

我们在第一章 §1.2 已经介绍过了矩阵的行和列，现在我们称 $\mathbf{a}=(a_1,\dots,a_m)$，$a_i\in\mathbb{R}$ 为 m 维行向量，$\mathbf{b}=\begin{pmatrix}b_1\\ \vdots\\ b_n\end{pmatrix}$ 为 n 维列向量。

2.1.1　向量空间（坐标空间）

我们记 $\mathbb{R}^{1\times n}=\{(a_1,\dots,a_n)|a_i\in\mathbb{R}\}$，$\mathbb{R}^{n\times 1}=\left\{\begin{pmatrix}b_1\\ \vdots\\ b_n\end{pmatrix}|b_i\in\mathbb{R}\right\}$，并将后者简记成 $\mathbb{R}^n$。为了节省空间，我们把 $\mathbb{R}^n$ 中的列向量简记为 $(b_1,\dots,b_n)^t$，即列向量写成行向量的转置。我们在 $\mathbb{R}^n$ 上定义如下的加法和数乘运算：

(1) 设 $\mathbf{x}=(x_1,\dots,x_n)^t$，$\mathbf{y}=(y_1,\dots,y_n)^t$，定义加法 $\mathbf{x}+\mathbf{y}=(x_1+y_1,\dots,x_n+y_n)^t$；

(2) 设 $\mathbf{x}=(x_1,\dots,x_n)^t$，$\alpha\in\mathbb{R}$，定义数乘 $\alpha\mathbf{x}=(\alpha x_1,\dots,\alpha x_n)^t$。

另外我们记 $\mathbf{0}=(0,\dots,0)^t$，显然 $\forall\mathbf{x}\in\mathbb{R}^n$，$\mathbf{x}+\mathbf{0}=\mathbf{x}$。以上定义对行向量同理。

向量的加法和数乘满足以下运算律：

(1) 加法交换律：$\mathbf{x}+\mathbf{y}=\mathbf{y}+\mathbf{x}$；

(2) 加法结合律：$(\mathbf{x}+\mathbf{y})+\mathbf{z}=\mathbf{x}+(\mathbf{y}+\mathbf{z})$；

(3) 加法单位元：$\forall\mathbf{x}\in\mathbb{R}^n$，$\mathbf{x}+\mathbf{0}=\mathbf{x}$；

(3) 加法逆元：$\forall\mathbf{x}\in\mathbb{R}^n$，$\exists\mathbf{y}\in\mathbb{R}$，$\mathbf{x}+\mathbf{y}=\mathbf{0}$；

(5) 数乘结合律：$\alpha,\beta\in\mathbb{R}$，则 $(\alpha\beta)\mathbf{x}=\alpha(\beta\mathbf{x})$；

(6) 数乘单位元：$1\cdot\mathbf{x}=\mathbf{x}$；

(7) 数乘对向量加法的两个分配律：$\alpha(\mathbf{x}+\mathbf{y})=\alpha\mathbf{x}+\alpha\mathbf{y}$；$(\alpha+\beta)\mathbf{x}=\alpha\mathbf{x}+\beta\mathbf{x}$。

例 2.1.1. 设

$$\begin{cases}a_{11}x_1+a_{12}x_2+\cdots+a_{1n}x_n=b_1\\ a_{21}x_1+a_{22}x_2+\cdots+a_{2n}x_n=b_2\\ \qquad\qquad\vdots\\ a_{m1}x_1+a_{m2}x_2+\cdots+a_{mn}x_n=b_m\end{cases}\tag{L}$$

记 $A=(a_{ij})_{m\times n}$，$\mathbf{b}=(b_1,\dots,b_m)^t$，则 (L) 可以表示为

$$x_1\mathbf{A}^{(1)}+\cdots+x_n\mathbf{A}^{(n)}=\mathbf{b}.$$

其中 $\mathbf{A}^{(1)},\dots,\mathbf{A}^{(n)},\mathbf{b}\in\mathbb{R}^m$。即线性方程组可以视作列向量的线性组合。

2.1.2　线性相关性

设 $\mathbf{v}_1,\dots,\mathbf{v}_k\in\mathbb{R}^n$，$\alpha_1,\dots,\alpha_k\in\mathbb{R}$，则 $\alpha_1\mathbf{v}_1+\cdots+\alpha_k\mathbf{v}_k$ 称为 $\mathbf{v}_1,\dots,\mathbf{v}_k$ 的一个线性组合，$\alpha_1,\dots,\alpha_k\in\mathbb{R}$ 称为该线性组合的系数。

例 2.1.2. 在例2.1.1中，(L) 相容 $\Longleftrightarrow$ $\mathbf{b}$ 是 $\mathbf{A}^{(1)},\dots,\mathbf{A}^{(n)}$ 的线性组合。

例 2.1.3. 设 $\mathbf{u}=(1,1,1)^t$, $\mathbf{v}_1=(1,2,3)^t$, $\mathbf{v}_2=(1,0,0)^t$, 再设 $\mathbf{u}=\alpha_1\mathbf{v}_1+\alpha_2\mathbf{v}_2$, 则

$$\begin{pmatrix}\alpha_1+\alpha_2\\ 2\alpha_1\\ 3\alpha_1\end{pmatrix}=\begin{pmatrix}1\\1\\1\end{pmatrix}.$$

即

$$\begin{cases}\alpha_1+\alpha_2=1\\ 2\alpha_1=1\\ 3\alpha_1=1\end{cases}$$

不相容。所以 $\mathbf{u}$ 不是 $\mathbf{v}_1$, $\mathbf{v}_2$ 的线性组合。

定义 2.1.1. 设 $\mathbf{v}_1,\dots,\mathbf{v}_k\in\mathbb{R}^n$, 如果存在不全为 0 的 $\alpha_1,\dots,\alpha_k\in\mathbb{R}$, 使得 $\alpha_1\mathbf{v}_1+\cdots+\alpha_k\mathbf{v}_k=\mathbf{0}$ 成立, 则称 $\mathbf{v}_1,\dots,\mathbf{v}_k$ 线性相关; 反之, 若 $\alpha_1\mathbf{v}_1+\cdots+\alpha_k\mathbf{v}_k=\mathbf{0}\Longrightarrow\alpha_1=\cdots=\alpha_k=0$, 则称 $\mathbf{v}_1,\dots,\mathbf{v}_k$ 线性无关。

例 2.1.4. 对齐次方程组

$$\begin{cases}a_{11}x_1+a_{12}x_2+\cdots+a_{1n}x_n=0\\ a_{21}x_1+a_{22}x_2+\cdots+a_{2n}x_n=0\\ \qquad\qquad\qquad\vdots\\ a_{m1}x_1+a_{m2}x_2+\cdots+a_{mn}x_n=0\end{cases}\tag{H}$$

记 $A=(a_{ij})$。则 (H) 有非平凡解 $\Longleftrightarrow\mathbf{A}^{(1)},\dots,\mathbf{A}^{(n)}$ 线性相关。

例 2.1.5. 判断 $\mathbf{v}_1=(1,0,1)^t$, $\mathbf{v}_2=(0,1,1)^t$, $\mathbf{v}_3=(1,1,1)^t$ 是否线性相关。

解. 设 $\alpha_1\mathbf{v}_1+\alpha_2\mathbf{v}_2+\alpha_3\mathbf{v}_3=\mathbf{0}$, 则

$$\begin{cases}\alpha_1+\alpha_3=0\\ \alpha_2+\alpha_3=0\\ \alpha_1+\alpha_2+\alpha_3=0\end{cases}$$

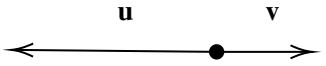
解得 $\alpha_1=\alpha_2=\alpha_3=0$。即 $\mathbf{v},\mathbf{v}_2,\mathbf{v}_3$ 线性无关。 □

线性相关的几何意义:

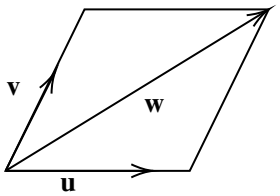
(1)$\mathbf{u}\in\mathbb{R}^n$ 线性相关即 $\mathbf{u}=\mathbf{0}$。

(2)$\mathbf{u},\mathbf{v}\in\mathbb{R}^n$ 线性相关, 则 $\mathbf{u},\mathbf{v}$ "同向" 或 "反向" 共线 (平行)。

(3)$\mathbf{u},\mathbf{v},\mathbf{w}\in\mathbb{R}^3$ 线性相关, 则 $\mathbf{u},\mathbf{v},\mathbf{w}$ 共面。



(2) 共线



(3) 共面

命题 2.1.1. 设 $\mathbf{v}_1,\dots,\mathbf{v}_k\in\mathbb{R}^n$, $1\leqslant i\leqslant k$, 则

(i) 如果 $\mathbf{v}_1,\dots,\mathbf{v}_i$ 线性相关, 则 $\mathbf{v}_1,\dots,\mathbf{v}_k\in\mathbb{R}^n$ 线性相关;

(ii) 如果 $\mathbf{v}_1,\dots,\mathbf{v}_i,\dots,\mathbf{v}_k$ 线性无关，则 $\mathbf{v}_1,\dots,\mathbf{v}_i$ 线性无关；

(iii) $\mathbf{v}_1,\dots,\mathbf{v}_k$ 线性相关 $\Longleftrightarrow$ $\mathbf{v}_1,\dots,\mathbf{v}_k$ 中某个向量是其它向量的线性组合；

(iv) 设 $\mathbf{v}\in\mathbb{R}^n$ 且 $\mathbf{v}_1,\dots,\mathbf{v}_k$ 线性无关，则 $\mathbf{v},\mathbf{v}_1,\dots,\mathbf{v}_k$ 线性相关 $\Longleftrightarrow$ $\exists!$一组$\alpha_1,\dots,\alpha_k\in\mathbb{R}$ 使得 $\mathbf{v}=\alpha_1\mathbf{v}_1+\cdots+\alpha_k\mathbf{v}_k$。

证明. 只证 (iv)，(i)(ii)(iii) 留作练习。
($\Longleftarrow$) 方向是显然的，下面证明 ($\Longrightarrow$) 方向。
由于 $\mathbf{v},\mathbf{v}_1,\dots,\mathbf{v}_k$ 线性相关，故存在不全为 0 的 $\alpha_0,\alpha_1,\dots,\alpha_k\in\mathbb{R}$ 使得

$$\alpha_0\mathbf{v}+\alpha_1\mathbf{v}_1+\cdots+\alpha_k\mathbf{v}_k=\mathbf{0}. \tag{2.1.1}$$

若 $\alpha_0=0$，则 $\alpha_1,\dots,\alpha_k$ 不全为 0 且 $\alpha_1\mathbf{v}_1+\cdots+\alpha_k\mathbf{v}_k=\mathbf{0}$，这与 $\mathbf{v}_1,\dots,\mathbf{v}_k$ 线性无关矛盾！故 $\alpha_0\neq 0$，则移项并在 (2.1.1) 式两边同时除以 α_0 得

$$\mathbf{v}=\left(-\frac{\alpha_1}{\alpha_0}\right)\mathbf{v}_1+\cdots+\left(-\frac{\alpha_k}{\alpha_0}\right)\mathbf{v}_k. \tag{2.1.2}$$

将 $(-\frac{\alpha_i}{\alpha_0})$ 视作新的 α_i 即可。
下证唯一性。若另有 $\mathbf{v}=\lambda_1\mathbf{v}_1+\cdots+\lambda_k\mathbf{v}_k$，则将它与 (2.1.2) 式相减得 $(-\frac{\alpha_1}{\alpha_0}-\lambda_1)\mathbf{v}_1+\cdots+(-\frac{\alpha_k}{\alpha_0}-\lambda_k)\mathbf{v}_k=\mathbf{0}$，则由 $\mathbf{v}_1,\dots,\mathbf{v}_k$ 线性无关可得 $-\frac{\alpha_i}{\alpha_0}-\lambda_i=0,\ i=1,\dots,k$，即唯一性得证。 □

例 2.1.6. 记 $\mathbf{e}^{(j)}=(0,\dots,1,\dots,0)^t\in\mathbb{R}^n$(第 j 个位置是 1，其他为 0)，则
(1)$\mathbf{e}^{(1)},\dots,\mathbf{e}^{(n)}$ 线性无关；
(2)$\forall\mathbf{x}\in\mathbb{R}^n$，$\exists!$一组$\alpha_1,\dots,\alpha_n\in\mathbb{R}$ 使得 $\mathbf{x}=\alpha_1\mathbf{e}^{(1)}+\cdots+\alpha_n\mathbf{e}^{(n)}$，即 $\mathbf{x}=(\alpha_1,\dots,\alpha_n)^t$。

例 2.1.7. 求证：$\mathbb{R}^n$ 中任意 $n+1$ 个向量一定线性相关。

证明. 设 $\mathbf{v}_j=(v_{1j},\dots,v_{nj})^t$，其中 $j=1,2,\dots,n+1$，若有 $\alpha_1,\dots,\alpha_{n+1}\in\mathbb{R}$，使得 $\alpha_1\mathbf{v}_1+\cdots+\alpha_{n+1}\mathbf{v}_{n+1}=\mathbf{0}$，则

$$\begin{cases} v_{11}\alpha_1+\cdots+v_{1,n+1}\alpha_{n+1}=0\\ v_{21}\alpha_1+\cdots+v_{2,n+1}\alpha_{n+1}=0\\ \qquad\qquad\qquad\vdots\\ v_{n1}\alpha_1+\cdots+v_{n,n+1}\alpha_{n+1}=0 \end{cases}$$

即 $\alpha_1,\dots,\alpha_{n+1}$ 是该齐次方程组的解。由定理 1.2.3 可得该方程组有非平凡解，即 $\mathbf{v}_1,\dots,\mathbf{v}_{n+1}$ 线性相关。

□

引理 2.1.1 (线性组合引理). 设 $\mathbf{u}_1,\dots,\mathbf{u}_k,\mathbf{v}_1,\dots,\mathbf{v}_l\in\mathbb{R}^n$ 且每个 $\mathbf{u}_i$ 都是 $\mathbf{v}_1,\dots,\mathbf{v}_l$ 的线性组合，如果 $k>l$，则 $\mathbf{u}_1,\dots,\mathbf{u}_k$ 线性相关。

证明. 设

$$\begin{aligned}\mathbf{u}_1 &= a_{11}\mathbf{v}_1 + \cdots + a_{1l}\mathbf{v}_l\\ \mathbf{u}_2 &= a_{21}\mathbf{v}_1 + \cdots + a_{2l}\mathbf{v}_l\\ &\vdots\\ \mathbf{u}_k &= a_{k1}\mathbf{v}_1 + \cdots + a_{kl}\mathbf{v}_l\end{aligned}$$

其中 $a_{ij} \in \mathbb{R}$ 都是已知的。我们想要证明 $\mathbf{u}_1, \ldots, \mathbf{u}_k$ 线性相关，即存在不全为 0 的 $\alpha_1, \ldots, \alpha_k \in \mathbb{R}$ 使得 $\sum_{i=1}^{k} \alpha_i \mathbf{u}_i = \mathbf{0}$。由于

$$\begin{aligned}&\sum_{i=1}^{k} \alpha_i \mathbf{u}_i\\ =& \sum_{i=1}^{k} \alpha_i (\sum_{j=1}^{l} a_{ij}\mathbf{v}_j)\\ =& \sum_{j=1}^{l} (\sum_{i=1}^{k} a_{ij}\alpha_i)\mathbf{v}_j\end{aligned}$$

只要对每个 $j = 1, \ldots, l$，都有 $\sum_{i=1}^{k} a_{ij}\alpha_i = 0$，则 $\sum_{i=1}^{k} \alpha_i \mathbf{u}_i = \mathbf{0}$ 成立。于是目标变为寻找以 $\alpha_1, \ldots, \alpha_k$ 为变元的方程组

$$\sum_{i=1}^{k} a_{ij}\alpha_i = 0, \quad j = 1, \ldots, l.$$

的非零解。由于方程组有 k 个变元，l 个方程，$k > l$，故由定理1.2.3，该方程组有非零解。于是我们证明了原命题。 □

例 2.1.8. 设 $\mathbf{u}_1 = \lambda_1 \mathbf{v}$, $\mathbf{u}_2 = \lambda_2 \mathbf{v}$，则 $\mathbf{u}_1, \mathbf{u}_2$ 线性相关。

2.1.3 极大线性无关组

我们也把向量的集合称为向量组。这一节我们将阐明向量集的一个基本性质：$\mathbb{R}^n$ 的一个向量的集合中一定存在“极大”的线性无关的子集，并且这种子集的元素个数是一个不变量。

定义 2.1.2. 设 $T \subset \mathbb{R}^n$ 非空，若 T 中每个非空有限子集都是线性无关的，则称 T 是线性无关集。由例 2.1.7 知 $|T| < n + 1$。

定义 2.1.3. 设 $S \subset \mathbb{R}^n$ 非空，$T \subset S$ 是线性无关 (子) 集，如果 $\forall \sigma \in S \setminus T$, $T \cup \{\sigma\}$ 是线性相关的，则称 T 是 S 中的极大线性无关集。

引理 2.1.2 (扩充引理). 设 $S \subset \mathbb{R}^n$ 且 $T \subset S$ 是一个线性无关集，则存在 S 的一个极大线性无关组 $\widetilde{T}$ 满足 $T \subset \widetilde{T}$。

证明. 若 T 本身是极大的，则证明结束。
否则，存在 $\mathbf{v}_1 \in S \setminus T$ 使得 $T_1 = T \cup \{\mathbf{v}_1\}$ 是 S 中的线性无关集。若 T_1 是极大的，则证明结束。
否则，存在 $\mathbf{v}_2 \in S \setminus T$ 使得 $T_2 = T_1 \cup \{\mathbf{v}_2\}$ 是 S 中的线性无关集。

…… 一直这样重复下去，例2.1.7保证了这个过程一定在有限步内终止，于是整个证明完成。 □

以后我们会知道，扩充引理对抽象向量空间中的向量集也成立，但终止性由 Zorn 引理保证。

命题 2.1.2. 设 $S \subset \mathbb{R}^n$ 且 $S \neq \emptyset$, $S \neq \{\mathbf{0}\}$，则

(i) S 中有极大线性无关组；

(ii) 设 T_1, T_2 是两个极大线性无关组，则 $|T_1| = |T_2|$。

证明. (i) 由条件可得存在向量 $\mathbf{v} \in S$, $\mathbf{v} \neq \mathbf{0}$，对 $\{\mathbf{v}\}$ 应用扩充引理即可。
(ii) 设 $T_1 = \{\mathbf{u}_1, \ldots, \mathbf{u}_k\}$, $T_2 = \{\mathbf{v}_1, \ldots, \mathbf{v}_l\}$，则由极大线性无关组的定义，$\forall \mathbf{u}_i \in T_1$, $i = 1, \ldots, k$，有 $\mathbf{u}_i$ 是 $\mathbf{v}_1, \ldots, \mathbf{v}_l$ 的线性组合。于是由线性组合引理，$k \leqslant l$。同理 $l \leqslant k$，因此 $k = l$。 □

推论 2.1.1. 设 $S \subset \mathbb{R}^n, T = \{\mathbf{v}_1, \ldots, \mathbf{v}_m\} \subset S$ 是 S 的极大线性无关组，则对 $\forall \mathbf{v} \in S$, $\exists!$一组$\alpha_1, \ldots, \alpha_m \in \mathbb{R}$，使得 $\mathbf{v} = \sum_{i=1}^m \alpha_i \mathbf{v}_i$。

证明. 由于 T 是极大线性无关组，故 $\mathbf{v}, \mathbf{v}, \cdots \mathbf{v}_m$ 线性相关，于是由命题2.1.1(iv) 知结论成立。 □

推论 2.1.2. 设 $S \subset \mathbb{R}^n$, $T = \{\mathbf{v}_1, \ldots, \mathbf{v}_m\} \subset S$，如果对 $\forall \mathbf{v} \in S$, $\exists!$一组$\alpha_1, \ldots, \alpha_m \in \mathbb{R}$，使得 $\mathbf{v} = \sum_{i=1}^m \alpha_i \mathbf{v}_i$，则 T 是 S 的极大线性无关组。

证明. 只需证 $\{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$ 线性无关。用反证法。若 $\{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$ 线性相关，由命题2.1.1(iii)，不妨设 $\mathbf{v}_1 = \alpha_2 \mathbf{v}_2 + \cdots + \alpha_m \mathbf{v}_m$，则

$$\mathbf{v}_1 = 0 \cdot \mathbf{v}_1 + \alpha_2 \mathbf{v}_2 + \cdots + \alpha_m \mathbf{v}_m = 1 \cdot \mathbf{v}_1$$

即 $\mathbf{v}_1$ 有两种表出方式，这与存在唯一的表出方式矛盾！ □

推论 2.1.3. 设 $S \subset \mathbb{R}^n$, r 是 S 中极大线性无关组中元素的个数，T 是 S 中的线性无关子集，如果 $|T| = r$，则 T 是极大线性无关组。

证明. 由扩充引理，存在极大线性无关组 $\widetilde{T}$ 满足 $T \subset \widetilde{T}$，又由 $|T| = |\widetilde{T}| = r$ 知 $T = \widetilde{T}$。 □

2.1.4 子空间

定义 2.1.4. 设 $V \subset \mathbb{R}^n$ 非空，如果对 $\forall \mathbf{x}, \mathbf{y} \in V$ 及 $\alpha \in \mathbb{R}$，有 $\mathbf{x} + \mathbf{y} \in V$, $\alpha \mathbf{x} \in V$ (即 V 对加法和数乘封闭)，则称 V 是 $\mathbb{R}^n$ 的子空间。

注 2.1.1. (1)V 是子空间，则必有 $\mathbf{0} \in V$；
(2)V 是子空间 $\Longleftrightarrow \forall \mathbf{x}, \mathbf{y} \in V$, $\alpha, \beta \in \mathbb{R}$，有 $\alpha \mathbf{x} + \beta \mathbf{y} \in V$。

例 2.1.9. 齐次方程组

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = 0 \\ \qquad\qquad\qquad\qquad \cdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = 0 \end{cases} \tag{H}$$

的所有解的集合 V 是 $\mathbb{R}^n$ 的子空间。

证明. 由 $\mathbf{0} \in V$，故 $V \neq \emptyset$。v 另一方面，若 $\mathbf{u} = (\alpha_1, \ldots, \alpha_n)^t$，$\mathbf{v} = (\beta_1, \ldots, \beta_n)^t \in V$，则对 $\forall \alpha, \beta \in \mathbb{R}$，有

$$\sum_{j=1}^{n} a_{ij}(\alpha\alpha_j + \beta\beta_j) = \alpha(\sum_{j=1}^{n} a_{ij}\alpha_j) + \beta(\sum_{j=1}^{n} a_{ij}\beta_j) = 0.$$

即 $\alpha\mathbf{u} + \beta\mathbf{v}$ 也是 (H) 的解，即封闭性成立。 □

命题 2.1.3. 任意多个子空间的交仍然是子空间。

证明. 设 $U_i \subset \mathbb{R}^n$ 是子空间，其中 $i \in I$ 是指标集，由于每个 U_i 都对加法和数乘封闭，因此 $\forall \mathbf{x}, \mathbf{y} \in \cap_{i\in I} U_i$，我们有 $\forall i \in I$，$\mathbf{x} + \mathbf{y} \in U_i$，即 $\mathbf{x} + \mathbf{y} \in \cap_{i\in I} U_i$；同理 $\forall a \in \mathbb{R}$，$a\mathbf{x} \in\in \cap_{i\in I} U_i$。此即子空间的任意交还是子空间。 □

但两个子空间的并一般不是子空间 (除非一个包含另一个，试证明之)。因此我们需要考虑同时包含两个子空间的最小的子空间，这就是和空间。

定义 2.1.5. 设 $S, T \subset \mathbb{R}^n$ 非空，我们定义集合 $U = \{\mathbf{x} + \mathbf{y} | \mathbf{x} \in S, \mathbf{y} \in T\}$，则称 U 是 S, T 的和，记为 $U = S + T$。

命题 2.1.4. 设 $U, V \subset \mathbb{R}^n$ 是子空间，则 $U + V$ 也是子空间。

证明. 设 $\mathbf{x}, \mathbf{y} \in U + V$，则 $\exists \mathbf{u}_1, \mathbf{u}_2 \in U$，$\mathbf{v}_1, \mathbf{v}_2 \in V$，使得 $\mathbf{x} = \mathbf{u}_1 + \mathbf{v}_1$，$\mathbf{y} = \mathbf{u}_2 + \mathbf{v}_2$。下面验证封闭性。对 $\forall \alpha, \beta \in \mathbb{R}$，有

$$\alpha\mathbf{x} + \beta\mathbf{y} = \alpha(\mathbf{u}_1 + \mathbf{v}_1) + \beta(\mathbf{u}_2 + \mathbf{v}_2) = \underbrace{(\alpha\mathbf{u}_1 + \beta\mathbf{u}_2)}_{\in U} + \underbrace{(\alpha\mathbf{v}_1 + \beta\mathbf{v}_2)}_{\in V}$$

即 $\alpha\mathbf{x} + \beta\mathbf{y} \in U + V$。由注2.1.1(2) 即得结论。

□

命题 2.1.5. 设 $\mathbf{v}_1, \ldots, \mathbf{v}_k \in \mathbb{R}^n$，定义它们的线性包络 (linear span):

$$\text{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_k\} = \{\alpha_1\mathbf{v}_1 + \cdots + \alpha_k\mathbf{v}_k | \alpha_i \in \mathbb{R},\ i = 1, \ldots, k\}.$$

则容易验证 $\text{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ 是子空间 (留作练习，它也称为由 $\mathbf{v}_1, \ldots, \mathbf{v}_k$ 生成的子空间)。在很多书上 $\text{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ 也被记作 $< \mathbf{v}_1, \ldots, \mathbf{v}_k >$，我们在讲义的上册也是混用这两个记号。(在讲义的下册我们只使用 span，以免和内积的记号混淆。)

证明. 设 $\mathbf{u}, \mathbf{v} \in \text{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$，则存在 $\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_k$ 使得

$$\mathbf{u} = \alpha_1\mathbf{v}_1 + \cdots + \alpha_k\mathbf{v}_k$$
$$\mathbf{v} = \beta_1\mathbf{v}_1 + \cdots + \beta_k\mathbf{v}_k$$

则对 $\forall \lambda, \mu \in \mathbb{R}$，有

$$\lambda\mathbf{u} + \mu\mathbf{v} = \lambda(\alpha_1\mathbf{v}_1 + \cdots + \alpha_k\mathbf{v}_k) + \mu(\beta_1\mathbf{v}_1 + \cdots + \beta_k\mathbf{v}_k) = \sum_{i=1}^{k}(\lambda\alpha_i + \mu\beta_i)\mathbf{v}_i \in \text{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}.$$

即结论成立。 □

推论 2.1.4. 设 $\mathbf{v}_1, \ldots, \mathbf{v}_k \in \mathbb{R}^n$，$V$ 是含有 $\mathbf{v}_1, \ldots, \mathbf{v}_k$ 的子空间，则 $\text{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_k\} \subset V$。

证明留作练习。这个推论表明 $\mathrm{span}\{\mathbf{v}_1,\dots,\mathbf{v}_k\}$ 是含有 $\mathbf{v}_1,\dots,\mathbf{v}_k$ 的最小子空间。

定义 2.1.6. 设 U,V 是 $\mathbb{R}^n$ 的子空间，如果 $U\cap V=\{\mathbf{0}\}$，则称 $U+V$ 是直和，记为 $U\oplus V$。

命题 2.1.6. 设 $U,V\subset\mathbb{R}^n$ 是子空间，则 $U+V$ 是直和 $\Longleftrightarrow$ 对 $\forall\mathbf{x}\in U+V$, $\exists!\mathbf{u}\in U$和$\mathbf{v}\in V$ 使得 $\mathbf{x}=\mathbf{u}+\mathbf{v}$。

证明. ($\Longrightarrow$) 若 $\mathbf{x}$ 有两种表出方式：$\mathbf{x}=\mathbf{u}+\mathbf{v}=\mathbf{u}_1+\mathbf{v}_1$，则 $\mathbf{u}-\mathbf{u}_1=\mathbf{v}_1-\mathbf{v}\in U\cap V=\{\mathbf{0}\}$，即 $\mathbf{u}=\mathbf{u}_1$, $\mathbf{v}=\mathbf{v}_1$。
($\Longleftarrow$) 设 $\mathbf{w}\in U\cap V$，则 $\mathbf{w}$ 有两种表出方式：$\mathbf{w}=\mathbf{w}+\mathbf{0}=\mathbf{0}+\mathbf{w}$，由唯一性即得 $\mathbf{w}=\mathbf{0}$。 □

注 2.1.2. 设 U_1,U_2 是子空间，则 $U_1\cap U_2\subset U_1\subset U_1+U_2$，但 $(U_1+U_2)\cap U_3\neq U_1\cap U_3+U_2\cap U_3$，即分配律一般不成立。例如，设在 $\mathbb{R}^2$ 中 $U_1=\mathrm{span}\{\mathbf{e}_1\}$, $U_2=\mathrm{span}\{\mathbf{e}_2\}$，则 $U_1\cap U_2=\{\mathbf{0}\}$, $U_1+U_2=\mathrm{span}\{\mathbf{e}_1,\mathbf{e}_2\}$。令 $U_3=\mathrm{span}\{\mathbf{e}_1+\mathbf{e}_2\}$，则 $(U_1+U_2)\cap U_3=U_3$，而 $U_1\cap U_3+U_2\cap U_3=\{\mathbf{0}\}$。

2.1.5 基底与维数

这一小节的内容和下册抽象向量空间的内容是一脉相承的。

定义 2.1.7. 设 $V\subset\mathbb{R}^n$ 是子空间，且 $V\neq\{\mathbf{0}\}$，再设 $\mathbf{b}_1,\dots,\mathbf{b}_d$ 线性无关，并满足 $V=<\mathbf{b}_1,\dots,\mathbf{b}_d>$，则称 $\mathbf{b}_1,\dots,\mathbf{b}_d$ 是 V 的一组基 (basis)。

命题 2.1.7. 设 $V\subset\mathbb{R}^n$ 是子空间，且 $V\neq\{\mathbf{0}\}$，$\mathbf{b}_1,\dots,\mathbf{b}_d\in V$，则 $\mathbf{b}_1,\dots,\mathbf{b}_d$ 是 V 的一组基 $\Longleftrightarrow$ $\mathbf{b}_1,\dots,\mathbf{b}_d$ 是 V 的一个极大线性无关组。

证明. ($\Longrightarrow$) 由于 $\mathbf{b}_1,\dots,\mathbf{b}_d$ 是 V 的一组基，即 $\mathbf{b}_1,\dots,\mathbf{b}_d$ 线性无关，假设它们不是极大线性无关的，则存在 $\mathbf{v}\in V$ 使得 $\mathbf{b}_1,\dots,\mathbf{b}_d,\mathbf{v}$ 线性无关。另一方面，由基的定义有 $\mathbf{v}\in<\mathbf{b}_1,\dots,\mathbf{b}_d>$，即存在 $\alpha_1,\dots,\alpha_d\in\mathbb{R}$，使得 $\mathbf{v}=\alpha_1\mathbf{b}_1+\cdots+\alpha_d\mathbf{b}_d$，移项即可得到 $\mathbf{b}_1,\dots,\mathbf{b}_d,\mathbf{v}$ 线性相关，矛盾！
($\Longleftarrow$) 设 $\mathbf{b}_1,\dots,\mathbf{b}_d$ 是 V 中的极大线性无关组，即 $\forall\mathbf{v}\in V$, $\mathbf{b}_1,\dots,\mathbf{b}_d,\mathbf{v}$ 线性相关，又因为 $\mathbf{b}_1,\dots,\mathbf{b}_d$ 线性无关，由命题2.1.1(iv) 及线性包络的定义 (命题 2.1.5) 知 $\mathbf{v}\in<\mathbf{b}_1,\dots,\mathbf{b}_d>$，由 $\mathbf{v}$ 的任意性即有 $V\subset<\mathbf{b}_1,\dots,\mathbf{b}_d>$，而另一个方向的包含关系是显然的，因此 $V=<\mathbf{b}_1,\dots,\mathbf{b}_d>$。 □

注 2.1.3. 若 V 有一组基 $\mathbf{b}_1,\dots,\mathbf{b}_d$，则 $\forall\mathbf{v}\in V$, $\exists!$一组$\alpha_1,\dots,\alpha_d\in\mathbb{R}$ 使得 $\mathbf{v}=\sum_{i=1}^d\alpha_i\mathbf{b}_i$。此时称 $(\alpha_1,\dots,\alpha_d)^t$ 是 V 在 $\mathbf{b}_1,\dots,\mathbf{b}_d$ 下的**坐标**。另外，由命题2.1.2，V 中两组基含有的元素个数相同。

定义 2.1.8. 设 $V\subset\mathbb{R}^n$ 是子空间，且 $V\neq\{\mathbf{0}\}$，$\mathbf{b}_1,\dots,\mathbf{b}_d\in V$ 是 V 的一组基，则称 d 为 V 的维数 (dimension)，简记为 $\dim V=d$。特别地，$\{\mathbf{0}\}$ 的维数为 0。

例 2.1.10. $\mathbb{R}^n$ 有自然的基底 $\mathbf{e}^{(1)}=(1,0,\dots,0)^t$, $\mathbf{e}^{(2)}=(0,1,\dots,0)^t,\cdots\cdots,\mathbf{e}^{(n)}=(0,\dots,0,1)^t$。于是 $\dim\mathbb{R}^n=n$。

定理 2.1.1 (基扩充定理). 设 $V\subset\mathbb{R}^n$ 是子空间，$\dim V=d>0$, $\mathbf{v}_1,\dots,\mathbf{v}_k\in V$ 线性无关，则存在 $\mathbf{v}_{k+1},\dots,\mathbf{v}_d\in V$ 使得 $\mathbf{v}_1,\dots,\mathbf{v}_k,\mathbf{v}_{k+1},\dots,\mathbf{v}_d$ 是一组基。

证明. 由扩充引理 (引理2.1.2)，存在 $\mathbf{v}_{k+1},\dots,\mathbf{v}_d\in V$ 使得 $\mathbf{v}_1,\dots,\mathbf{v}_d$ 是 V 的极大线性无关组。再由命题2.1.7可知 $\mathbf{v}_1,\dots,\mathbf{v}_d$ 是 V 的一组基。 □

定理 2.1.2 (包含定理). 设 U,V 是 $\mathbb{R}^n$ 的子空间且 $U\subset V$，则 $U\subsetneq V\Longleftrightarrow\dim U<\dim V$。

证明. ($\Longleftarrow$) 显然，下面证明 ($\Longrightarrow$) 方向。
若 $V = \{\mathbf{0}\}$，则结论显然；否则设 $\mathbf{u}_1, \ldots, \mathbf{u}_d$ 是 U 的基，则存在 $\mathbf{v} \in V \setminus U$ 使得 $\mathbf{v} \notin < \mathbf{u}_1, \ldots, \mathbf{u}_d >$。由命题2.1.1(iv) 可知 $\mathbf{u}_1, \ldots, \mathbf{u}_d, \mathbf{v}$ 线性无关。再用定理2.1.1即可得到 $\dim V \geqslant d + 1 > \dim U$。 □

注 2.1.4. 该结论对非线性的情形不对。例如，设 S 是方程 $x(x^2 + y^2 - 1) = 0$ 的解集，则 y轴 $\subsetneq S$，但 $\dim($y 轴$) = 1 = \dim S$。

定理 2.1.3 (维数公式). 设 $U_1, U_2 \subset \mathbb{R}^n$ 是子空间，则

$$\dim(U_1 + U_2) + \dim(U_1 \cap U_2) = \dim U_1 + \dim U_2.$$

证明. 若 $U_1 = \{\mathbf{0}\}$ 或 $U_2 = \{\mathbf{0}\}$，则结论显然成立。
下设 $U_1 \cap U_2 \neq 0$, $\mathbf{w}_1, \ldots, \mathbf{w}_m$ 是 $U_1 \cap U_2$ 的一组基。则由基扩充定理，$\exists \mathbf{u}_1, \ldots, \mathbf{u}_s \in U_1$及$\mathbf{v}_1, \ldots, \mathbf{v}_t \in U_2$ 使得：
(A)$\mathbf{w}_1, \ldots, \mathbf{w}_m, \mathbf{u}_1, \ldots, \mathbf{u}_s$ 是 U_1 的一组基；
(B)$\mathbf{w}_1, \ldots, \mathbf{w}_m, \mathbf{v}_1, \ldots, \mathbf{v}_t$ 是 U_2 的一组基。
下面证明 $\mathbf{w}_1, \ldots, \mathbf{w}_m, \mathbf{u}_1, \ldots, \mathbf{u}_s, \mathbf{v}_1, \ldots, \mathbf{v}_t$ 是线性无关的。
如果存在 $\alpha_1, \ldots, \alpha_m, \lambda_1, \ldots, \lambda_s, \mu_1, \ldots, \mu_t \in \mathbb{R}$ 满足

$$\sum_{i=1}^{m} \alpha_i \mathbf{w}_i + \sum_{i=1}^{s} \lambda_i \mathbf{u}_i + \sum_{i=1}^{t} \mu_i \mathbf{v}_i = \mathbf{0}, \tag{$*$}$$

则令 $\mathbf{w} = \sum_{i=1}^{m} \alpha_i \mathbf{w}_i$, $\mathbf{u} = \sum_{i=1}^{s} \lambda_i \mathbf{u}_i$, $\mathbf{v} = \sum_{i=1}^{t} \mu_i \mathbf{v}_i$。显然 $\mathbf{w} \in U_1 \cap U_2$, $\mathbf{u} \in U_1$, $\mathbf{v} \in U_2$。又因为 $\mathbf{w}+\mathbf{u} = -\mathbf{v}$, 故也有 $\mathbf{v} \in U_1$, 于是 $\mathbf{v} \in U_1 \cap U_2$。则存在 $\beta_1, \ldots, \beta_m \in \mathbb{R}$ 使得 $\mathbf{v} = \beta_1 \mathbf{w}_1 + \cdots + \beta_m \mathbf{w}_m$。即

$$(\alpha_1 + \beta_1)\mathbf{w}_1 + \cdots + (\alpha_m + \beta_m)\mathbf{w}_m + \lambda_1 \mathbf{u}_1 + \cdots + \lambda_s \mathbf{u}_s = \mathbf{0}.$$

由 (A) 知 $\lambda_1 = \cdots = \lambda_s = 0$，代回 ($*$) 式得到

$$\sum_{i=1}^{m} \alpha_i \mathbf{w}_i + \sum_{i=1}^{t} \mu_i \mathbf{v}_i = \mathbf{0}$$

再由 (B) 可知 $\alpha_1 = \cdots = \alpha_m = \mu_1 = \cdots = \mu_t = 0$。
即 $\mathbf{w}_1, \ldots, \mathbf{w}_m, \mathbf{u}_1, \ldots, \mathbf{u}_s, \mathbf{v}_1, \ldots, \mathbf{v}_t$ 是线性无关的。
再证 $\mathbf{w}_1, \ldots, \mathbf{w}_m, \mathbf{u}_1, \ldots, \mathbf{u}_s, \mathbf{v}_1, \ldots, \mathbf{v}_t$ 的线性包络是 $U_1 + U_2$。
设 $\mathbf{x} = \mathbf{x}_1 + \mathbf{x}_2 \in U_1 + U_2$，其中 $\mathbf{x}_1 \in U_1$, $\mathbf{x}_2 \in U_2$，则有：

$$\mathbf{x}_1 = a_1 \mathbf{w}_1 + \cdots + a_m \mathbf{w}_m + c_1 \mathbf{u}_1 + \cdots + c_s \mathbf{u}_s;$$
$$\mathbf{x}_2 = b_1 \mathbf{w}_1 + \cdots + b_m \mathbf{w}_m + d_1 \mathbf{v}_1 + \cdots + d_t \mathbf{v}_t.$$

于是

$$\mathbf{x} = (a_1+b_1)\mathbf{w}_1+\cdots+(a_m+b_m)\mathbf{w}_m+c_1\mathbf{u}_1+\cdots+c_s\mathbf{u}_s+d_1\mathbf{v}_1+\cdots+d_t\mathbf{v}_t \in < \mathbf{w}_1, \ldots, \mathbf{w}_m, \mathbf{u}_1, \ldots, \mathbf{u}_s, \mathbf{v}_1, \ldots, \mathbf{v}_t >$$

即 $\mathbf{w}_1, \ldots, \mathbf{w}_m, \mathbf{u}_1, \ldots, \mathbf{u}_s, \mathbf{v}_1, \ldots, \mathbf{v}_t$ 是 $U_1 + U_2$ 的基。
因此，$\dim(U_1 + U_2) = m + s + t = (m + s) + (m + t) - m = \dim U_1 + \dim U_2 - dim(U_1 \cap U_2)$。特

别的。当 $U_1 \cap U_2 = \{\mathbf{0}\}$ 时，令 $m = 0$ 即可得到结论。这样我们就完成了证明。 □

推论 2.1.5. 设 $U_1, U_2 \subset \mathbb{R}^n$ 是子空间，则 $U_1 + U_2$ 是直和 $\Longleftrightarrow \dim(U_1 + U_2) = \dim U_1 + \dim U_2$。

证明留作练习。

注 2.1.5. 设 $A \in \mathbb{R}^{m\times n}$，我们有方程组：

$$x_1\mathbf{A}^{(1)} + \cdots + x_n\mathbf{A}^{(n)} = \mathbf{0} \tag{H}$$

$$x_1\mathbf{A}^{(1)} + \cdots + x_n\mathbf{A}^{(n)} = \mathbf{b} \tag{L}$$

则 (H) 有非平凡解 $\Longleftrightarrow \mathbf{A}^{(1)}, \ldots, \mathbf{A}^n$ 线性相关；(L) 有解 (相容)$\Longleftrightarrow \mathbf{b} \in < \mathbf{A}^{(1)}, \ldots, \mathbf{A}^n >$。

命题 2.1.8. 设 $V \subset \mathbb{R}^n$ 是非零子空间，$\mathbf{v}_1, \ldots, \mathbf{v}_k$ 是 V 的一组生成元，则 $\mathbf{v}_1, \ldots, \mathbf{v}_k$ 中的任何极大线性无关组是 V 的一组基。

例 2.1.11. 求 $V = < (1,2,1)^t, (1,0,1)^t, (2,2,2)^t >$ 的一组基。

解. 将三个向量按顺序命名为 $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$。设 $\alpha_1(1,2,1)^t + \alpha_2(1,0,1)^t = \mathbf{0}$，解得 $\alpha_1 = \alpha_2 = 0$。于是 $\mathbf{v}_1, \mathbf{v}_2$ 线性无关。又 $\mathbf{v}_3 = \mathbf{v}_1 + \mathbf{v}_2$，故 $\{\mathbf{v}_1, \mathbf{v}_2\}$ 是 $< (1,2,1)^t, (1,0,1)^t, (2,2,2)^t >$ 的极大线性无关组，因此是 V 的一组基。 □

2.2 矩阵的秩

这一节我们讨论矩阵的第一个重要的不变量：矩阵的秩。

2.2.1 秩定理

设 $A \in \mathbb{R}^{m\times n}$，我们称矩阵 A 的行向量生成的子空间 $< \mathbf{A}_1, \dots, \mathbf{A}_m >$ 为 A 的行空间，记作 $V_r(A)$；称矩阵 A 的列向量生成的子空间 $< \mathbf{A}^{(1)}, \dots, \mathbf{A}^{(n)} >$ 为 A 的列空间，记作 $V_c(A)$。

定义 2.2.1. 称行空间的维数 $\dim V_r(A)$ 为矩阵 A 的行秩；列空间的维数 $\dim V_c(A)$ 为 A 的列秩。

本小节的主要结果是下面的秩定理。

定理 2.2.1. 设 $A \in \mathbb{R}^{m\times n}$，则 $\dim V_r(A) = \dim V_c(A)$。即矩阵的行秩等于列秩。

下面我们用初等行列变换的工具证明这一结论。

引理 2.2.1. 设 B 是 A 通过有限次 (I)、(II) 类初等行变换得到的矩阵，则 $V_r(B) = V_r(A)$。

证明. 设 B 是 A 通过 (I) 类初等行变换得到的矩阵，则

$$\begin{aligned} V_r(A) &=< \mathbf{A}_1, \dots, \mathbf{A}_i, \dots, \mathbf{A}_j, \dots, \mathbf{A}_m > \\ &=< \mathbf{A}_1, \dots, \mathbf{A}_j, \dots, \mathbf{A}_i, \dots, \mathbf{A}_m > \\ &= V_r(B) \end{aligned}$$

设 B 是 A 通过 (II) 类初等变换得到的矩阵，则

$$V_r(B) =< \mathbf{A}_1, \dots, \mathbf{A}_i, \dots, \mathbf{A}_j + \lambda\mathbf{A}_i, \cdots, \mathbf{A}_m >$$

因为 $i \neq j$，故 $\mathbf{A}_j = (\mathbf{A}_j + \lambda\mathbf{A}_i) - \lambda\mathbf{A}_i$ ，即 $\mathbf{A}_j \in V_r(B)$，所以 $V_r(A) \subset V_r(B)$。
反之，$\mathbf{A}_j + \lambda\mathbf{A}_i \in V_r(A)$，即 $V_r(B) \subset V_r(A)$。
由于一步变换下行空间不变，故经过有限步后行空间仍不变。综上，$V_r(B) = V_r(A)$。 □

我们将初等行变换中对行的操作改成相应的对列的操作，则可以定义三类初等列变换。与上面的证明过程类似，我们可以得到：

引理 2.2.2. 设 B 是 A 通过有限次 (I)、(II) 类初等列变换得到的矩阵，则 $V_c(B) = V_c(A)$。

引理 2.2.3. 设 B 由 A 经过有限步 (I)、(II) 类初等行变换得到，则 $\dim V_c(B) = \dim V_c(A)$。

证明. 由引理2.2.2，我们可以通过同样的初等列变换先调整 A, B 的列，使得 A 的前 d 列是极大线性无关组，而在这个过程中 $V_c(A), V_c(B)$ 都不变。于是不妨设 $\mathbf{A}^{(1)}, \dots, \mathbf{A}^{(d)}$ 是 $\mathbf{A}^{(1)}, \dots, \mathbf{A}^{(d)}, \dots, \mathbf{A}^{(n)}$ 的一个极大线性无关组，下面我们证明 $\mathbf{B}^{(1)}, \dots, \mathbf{B}^{(d)}$ 一定是 $\mathbf{B}^{(1)}, \dots, \mathbf{B}^{(d)}, \dots, \mathbf{B}^{(n)}$ 的一个极大线性无关组。
设 $(H_A), (H_B)$ 分别是以 A, B 为系数矩阵的齐次线性方程组，由引理1.2.1知 $(H_A), (H_B)$ 等价。
设有 $\alpha_1, \dots, \alpha_d \in \mathbb{R}$ 使得

$$\alpha_1\mathbf{B}^{(1)} + \cdots + \alpha_d\mathbf{B}^{(d)} = \mathbf{0},$$

则

$$\alpha_1\mathbf{B}^{(1)} + \cdots + \alpha_d\mathbf{B}^{(d)} + 0 \cdot \mathbf{B}^{(d+1)} + \cdots + 0 \cdot \mathbf{B}^{(n)} = \mathbf{0}$$

即 $(\alpha_1,\ldots,\alpha_d,0,\ldots,0)^t$ 是 (H_B) 的解，从而是 (H_A) 的解。于是

$$\alpha_1\mathbf{A}^{(1)}+\cdots+\alpha_d\mathbf{A}^{(d)}=\mathbf{0},$$

再由 $\mathbf{A}^{(1)},\ldots,\mathbf{A}^{(d)}$ 线性无关知 $\alpha_1=\cdots=\alpha_d=0$，即 $\mathbf{B}^{(1)},\ldots,\mathbf{B}^{(d)}$ 线性无关。
下证极大性。设 $k\in\{d+1,\ldots,n\}$，由于 $\mathbf{A}^{(1)},\ldots,\mathbf{A}^{(d)}$ 是极大线性无关组，故 $\exists\beta_1,\ldots,\beta_d\in\mathbb{R}$ 使得

$$\beta_1\mathbf{A}^{(1)}+\cdots+\beta_d\mathbf{A}^{(d)}-\mathbf{A}^{(k)}=\mathbf{0}.$$

即 $(\beta_1,\ldots,\beta_d,\ldots,0,\ldots,0,-1,0,\ldots,0)^t$ 是 (H_A) 的解，所以它也是 (H_B) 的解，即

$$\beta_1\mathbf{B}^{(1)}+\cdots+\beta_d\mathbf{B}^{(d)}-\mathbf{B}^{(k)}=\mathbf{0}.$$

所以 $\mathbf{B}^{(k)}\in<\mathbf{B}^{(1)},\ldots,\mathbf{B}^{(d)}>$。
故由命题2.1.8可得 $\dim V_c(B)=\dim V_c(A)=d$。 □

有了以上的准备工作，我们现在可以来证明定理2.2.1了。

证明. 对 A 作以下初等行列变换：

$$A\xrightarrow{(I),(II)\text{类初等行变换}}B=\begin{pmatrix}0&\cdots&0&\square_1&\cdots&*&\cdots&*&\cdots&*\\0&\cdots&0&0&\cdots&\square_2&\cdots&*&\cdots&*\\\vdots&&\vdots&\vdots&&\vdots&\ddots&\vdots&&\vdots\\0&\cdots&0&0&\cdots&0&\cdots&\square_k&\cdots&*\\0&\cdots&0&0&\cdots&0&\cdots&0&\cdots&0\\\vdots&&\vdots&\vdots&&\vdots&&\vdots&&\vdots\\0&\cdots&0&0&\cdots&0&\cdots&0&\cdots&0\end{pmatrix}\left.\begin{matrix}\\\\\\\\\\\\\end{matrix}\right\}k\text{行}$$

$$\xrightarrow{(I)\text{类初等列变换}}C=\begin{pmatrix}\square_1&*&*&\cdots&\cdots&*\\&\square_2&*&\cdots&\cdots&*\\&&\ddots&&&\vdots\\&&&\square_k&\cdots&*\\0&0&\cdots&0&\cdots&0\\&&\cdots&&&\\0&0&\cdots&0&\cdots&0\end{pmatrix}\left.\begin{matrix}\\\\\\\\\\\\\end{matrix}\right\}k\text{行}$$

$$\underbrace{\qquad\qquad}_{k\text{列}}$$

$$\xrightarrow{(II)\text{类初等列变换}}D=\begin{pmatrix}\square_1&0&0&\cdots&\cdots&0\\&\square_2&0&\cdots&\cdots&0\\&&\ddots&&&\vdots\\&&&\square_k&\cdots&0\\0&0&\cdots&0&\cdots&0\\&&\cdots&&&\\0&0&\cdots&0&\cdots&0\end{pmatrix}\left.\begin{matrix}\\\\\\\\\\\\\end{matrix}\right\}k\text{行}$$

$$\underbrace{\qquad\qquad}_{k\text{列}}$$

显然 $k=\dim V_c(D)$，于是由引理2.2.2，$k=\dim V_c(C)=\dim V_c(B)$，再由引理2.2.3，$k=$

$\dim V_c(A)$。
另一方面，由于 B 是行阶梯型矩阵，容易证明 $\dim V_r(B) = k$，而由引理2.2.1 即有 $\dim V_r(A) = \dim V_r(B) = k$。
综上，$\dim V_r(A) = \dim V_c(A)$。 □

于是我们就可以定义矩阵的秩如下：

定义 2.2.2 (矩阵的秩). 设 $A \in \mathbb{R}^{m\times n}$，则称 $\dim V_r(A)$ 为 A 的秩，记作 $\operatorname{rank}(A)$。

以上的证明过程也告诉了我们一种求矩阵的秩的方法：用初等变换将矩阵化成阶梯型。我们看下面的例子。

例 2.2.1. 设 $A = \begin{pmatrix} 1 & 0 & 4 & 5 \\ 2 & 1 & -1 & 3 \\ 4 & 1 & 7 & 13 \end{pmatrix}$，求 $\operatorname{rank}(A)$。

解.

$$A \xrightarrow{r_2-2r_1} \begin{pmatrix} 1 & 0 & 4 & 5 \\ 0 & 1 & -9 & -7 \\ 4 & 1 & 7 & 13 \end{pmatrix} \xrightarrow{r_3-4r_1} \begin{pmatrix} 1 & 0 & 4 & 5 \\ 0 & 1 & -9 & -7 \\ 0 & 1 & -9 & -7 \end{pmatrix} \xrightarrow{r_3-r_2} \begin{pmatrix} 1 & 0 & 4 & 5 \\ 0 & 1 & -9 & -7 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

即 $\operatorname{rank}(A) = 2$。 □

例 2.2.2. 设 $A \in \mathbb{R}^{m\times n}$，求证 $\operatorname{rank}(A) \leqslant \min(m, n)$。

证明. 由于 $V_r(A) \subset \mathbb{R}^{1\times n}$，故 $\dim V_r(A) \leqslant n$。同理 $V_c(A) \subset \mathbb{R}^{m\times 1} \Longrightarrow \dim V_c(A) \leqslant m$。
于是 $\operatorname{rank}(A) \leqslant \min(m, n)$。 □

最后，设 $A \in \mathbb{R}^{m\times n}$，我们称 $\operatorname{rank}(A) = m$ 的矩阵 A 为行满秩的；称 $\operatorname{rank}(A) = n$ 的矩阵 A 为列满秩的。若 $A \in \mathbb{R}^{n\times n}$ 且 $\operatorname{rank}(A) = n$，则称 A 是满秩的。

2.2.2 秩的应用

定理 2.2.2. 设 $A \in \mathbb{R}^{m\times n}$，$(H_A)$ 是以 A 为系数矩阵的齐次线性方程组。则

$$(H_A) \text{ 有非平凡解} \Longleftrightarrow \operatorname{rank}(A) < n.$$

证明. 设 (H_A) 为 $x_1\mathbf{A}^{(1)} + \cdots + x_n\mathbf{A}^{(n)} = \mathbf{0}$。
($\Longrightarrow$) 设 $(x_1, \ldots, x_n)^t = (\alpha_1, \ldots, \alpha_n)^t$ 是 (H_A) 的非平凡解，则 $\alpha_1\mathbf{A}^{(1)} + \cdots + \alpha_n\mathbf{A}^{(n)} = \mathbf{0}$，即 $\mathbf{A}^{(1)}, \ldots, \mathbf{A}^{(n)}$ 线性相关，于是 $\dim V_c(A) < n$，即 $\operatorname{rank}(A) = \dim V_c(A) < n$。
($\Longleftarrow$) 由 $\dim V_c(A) < n$ 知 $\mathbf{A}^{(1)}, \ldots, \mathbf{A}^{(n)}$ 线性相关，即存在不全为 0 的 $\beta_1, \ldots, \beta_n$ 使得 $\beta_1\mathbf{A}^{(1)} + \cdots + \beta_n\mathbf{A}^{(n)} = \mathbf{0}$，则 $(\beta_1, \ldots, \beta_n)$ 是 (H_A) 的非平凡解。 □

下面的定理是定理1.2.2的向量表述。

定理 2.2.3. 设 $A \in \mathbb{R}^{m\times n}$，$\mathbf{b} \in \mathbb{R}^m$，(L) 是以 $(A|\mathbf{b})$ 为增广矩阵的线性方程组，则 (L) 相容 $\Longleftrightarrow \operatorname{rank}(A) = \operatorname{rank}(A|\mathbf{b})$。

证明留作练习。

例 2.2.3. 判断方程组

$$\begin{cases} x+y=1 \\ 2x-y=2 \\ 5x+2y=5 \end{cases} \tag{L}$$

是否相容。

解. 对 (L) 的增广矩阵作如下初等行变换：

$$B=\underbrace{\left(\begin{array}{cc:c} 1 & 1 & 1 \\ 2 & -1 & 2 \\ 5 & 2 & 5 \end{array}\right)}_{A} \xrightarrow{r_2-2r_1} \left(\begin{array}{cc:c} 1 & 1 & 1 \\ 0 & -3 & 0 \\ 5 & 2 & 5 \end{array}\right) \xrightarrow{r_3-5r_1} \left(\begin{array}{cc:c} 1 & 1 & 1 \\ 0 & -3 & 0 \\ 0 & -3 & 0 \end{array}\right) \xrightarrow{r_3-r_2} \left(\begin{array}{cc:c} 1 & 1 & 1 \\ 0 & -3 & 0 \\ 0 & 0 & 0 \end{array}\right)$$

即 $\operatorname{rank}(A)=\operatorname{rank}(B)=2$，于是 (L) 相容。 □

在本节的最后，我们考虑齐次线性方程组的解集。例2.1.9已经告诉我们该解集是 $\mathbb{R}^n$ 的子空间。那么，这个子空间的维数与方程组的系数矩阵有什么关系呢？这就是下面的对偶定理。

定义 2.2.3. 设 $A\in\mathbb{R}^{m\times n}$，以 A 为系数矩阵的齐次线性方程组的解空间记为 V_A。

定理 2.2.4 (对偶定理 (方程版)). 设 $A\in\mathbb{R}^{m\times n}$，则 $\operatorname{rank}(A)+\dim(V_A)=n$。

证明. 不妨设 $r=\operatorname{rank}(A)$, $\mathbf{A}^{(1)},\dots,\mathbf{A}^{(r)}$ 是 $V_c(A)$ 的一组基，则 $\forall j\in\{r+1,\dots,n\}$, $\exists\alpha_{1j},\dots,\alpha_{rj}\in\mathbb{R}$ 使得

$$\alpha_{1j}\mathbf{A}^{(1)}+\cdots+\alpha_{rj}\mathbf{A}^{(r)}-\mathbf{A}^{(j)}=\mathbf{0}.$$

即 $\mathbf{v}_j=(\alpha_{1j},\dots,\alpha_{rj},0,\dots,0,-1,0,\dots,0)^t$ (第 j 个位置是-1) 是 A 对应的齐次线性方程组的一个解，又注意到 $\mathbf{v}_{r+1},\dots,\mathbf{v}_n\in V_A$ 是线性无关的 (注意 "-1" 的位置)，所以 $\dim V_A\geqslant n-r$。下面任取 $\mathbf{u}=(\beta_1,\dots,\beta_n)^t\in V_A$，我们的目标是证明 $\mathbf{u}$ 是 $\mathbf{v}_{r+1},\dots,\mathbf{v}_n$ 的线性组合，从而说明 $\mathbf{v}_{r+1},\dots,\mathbf{v}_n$ 是 V_A 的一组基。 由于 V_A 是子空间，故 $\mathbf{u}+\beta_{r+1}\mathbf{v}_{r+1}+\cdots+\beta_n\mathbf{v}_n\in V_A$，即形如 $(\lambda_1,\dots,\lambda_r,0\cdots,0)^t$ (后 $n-r$ 个位置全为 0) 的向量是以 A 为系数矩阵的齐次线性方程组的解，具体写出来就是：

$$\lambda_1\mathbf{A}^{(1)}+\cdots+\lambda_r\mathbf{A}^{(r)}=\mathbf{0}.$$

再由 $\mathbf{A}^{(1)},\dots,\mathbf{A}^{(r)}$ 线性无关可知 $\lambda_1=\cdots=\lambda_r=0$，即

$$\mathbf{u}=-(\beta_{r+1}\mathbf{v}_{r+1}+\cdots+\beta_n\mathbf{v}_n).$$

于是我们证明了 $\mathbf{v}_{r+1},\dots,\mathbf{v}_n$ 是 V_A 的一组基，即 $\dim V_A=n-r$。

□

例 2.2.4. 设 $A=\begin{pmatrix}1&1&-1&0\\1&-1&0&1\\5&-1&-2&3\end{pmatrix}$，求 V_A 的一组基。

解. 作如下初等行变换：

$$A\xrightarrow[r_3-5r_1]{r_2-r_1}\begin{pmatrix}1&1&-1&0\\0&-2&1&1\\0&-6&-3&3\end{pmatrix}\xrightarrow{r_3-3r_2}\begin{pmatrix}1&1&-1&0\\0&-2&1&1\\0&0&0&0\end{pmatrix}$$

于是 $\mathrm{rank}(A) = 2$。由对偶定理，$\dim V_A = 4 - \mathrm{rank}(A) = 4 - 2 = 2$。下面求解此齐次方程组。由于方程组等价于

$$\begin{cases} x_1 + x_2 - x_3 = 0 \\ -2x_2 + x_3 + x_4 = 0 \end{cases}$$

即

$$\begin{cases} x_1 = -x_2 + x_3 \\ x_4 = 2x_2 - x_3 \end{cases}$$

分别取 $x_2 = 1,\ x_3 = 0$ 和 $x_2 = 0,\ x_3 = 1$ 得 $V_A = <(-1, 1, 0, 2)^t,\ (1, 0, 1, -1)^t>$。 □

2.3 线性映射

用线性映射的观点来看待矩阵是十分重要和基本的。

2.3.1 定义和例子

这一小节我们的主要任务是定义线性映射并讨论它的一些基本的性质。

定义 2.3.1. 设 $\varphi:\mathbb{R}^n\to\mathbb{R}^m$ 是映射，如果对 $\forall\mathbf{x},\mathbf{y}\in\mathbb{R}^n$ 及 $\alpha\in\mathbb{R}$，有 $\varphi(\mathbf{x}+\mathbf{y})=\varphi(\mathbf{x})+\varphi(\mathbf{y})$ 及 $\varphi(\alpha\mathbf{x})=\alpha\varphi(\mathbf{x})$ 成立，则称 φ 是线性映射。

注 2.3.1. (1) 对于线性映射 φ，一定有 $\varphi(\mathbf{0})=\mathbf{0}$。这是因为 $\varphi(\mathbf{0}+\mathbf{0})=2\varphi(\mathbf{0})=\varphi(\mathbf{0})$。
(2)$\varphi:\mathbb{R}^n\to\mathbb{R}^m$ 是线性映射 $\Longleftrightarrow\forall\mathbf{x},\mathbf{y}\in\mathbb{R}^n$ 及 $\alpha,\beta\in\mathbb{R}$，有 $\varphi(\alpha\mathbf{x}+\beta\mathbf{y})=\alpha\varphi(\mathbf{x})+\beta\varphi(\mathbf{y})$。
其中，$(\Longrightarrow)$ 方向利用定义即可证明，$(\Longleftarrow)$ 方向分别取 $\alpha=\beta=1$ 和 $\alpha=1,\beta=0$ 即可验证。

下面来看几个例子。

例 2.3.1. (1)$\varphi:\mathbb{R}^m\to\mathbb{R}^m$，$\mathbf{x}\mapsto\mathbf{x}$ 恒同映射是线性的。
(2)$\varphi:\mathbb{R}^n\to\mathbb{R}^m$，$\mathbf{x}\mapsto\mathbf{0}$ 零映射是线性的。
(3)$\varphi:\mathbb{R}^n\to\mathbb{R}^n$，$\mathbf{x}\mapsto\mathbf{x}+\mathbf{v}$，其中 $\mathbf{v}\in\mathbb{R}^n\setminus\{\mathbf{0}\}$，非平凡的平移映射**不是**线性的。(不满足 $\varphi(\mathbf{0})=\mathbf{0}$.)

命题 2.3.1. 设 $\varphi:\mathbb{R}^n\to\mathbb{R}^m$ 是线性映射，$\mathbf{v}_1,\dots,\mathbf{v}_k\in\mathbb{R}^n$，$\alpha_1,\dots,\alpha_k\in\mathbb{R}$，则

(i) $\varphi(\alpha_1\mathbf{v}_1+\cdots+\alpha_k\mathbf{v}_k)=\alpha_1\varphi(\mathbf{v}_1)+\cdots+\alpha_k\varphi(\mathbf{v}_k)$;

(ii) 如果 $\mathbf{v}_1,\dots,\mathbf{v}_k$ 线性相关，则 $\varphi(\mathbf{v}_1),\dots,\varphi(\mathbf{v}_k)$ 也线性相关。

(iii) 如果 $\varphi(\mathbf{v}_1),\dots,\varphi(\mathbf{v}_k)$ 线性无关，则 $\mathbf{v}_1,\dots,\mathbf{v}_k$ 也线性无关。

证明. (i) 对 k 作归纳。$k=1$ 时即线性映射的定义。
设 $k-1$ 时结论成立，则

$$\begin{aligned}&\varphi(\alpha_1\mathbf{v}_1+\cdots+\alpha_{k-1}\mathbf{v}_{k-1}+\alpha_k\mathbf{v}_k)\\=&\varphi(\alpha_1\mathbf{v}_1+\cdots+\alpha_{k-1}\mathbf{v}_{k-1})+\alpha_k\varphi(\mathbf{v}_k)\\=&\alpha_1\varphi(\mathbf{v}_1)+\cdots+\alpha_{k-1}\varphi(\mathbf{v}_{k-1})+\alpha_k\varphi(\mathbf{v}_k)\quad\text{(归纳假设)}\end{aligned}$$

(ii) 设 $\beta_1\mathbf{v}_1+\cdots+\beta_k\mathbf{v}_k=\mathbf{0}$，其中 β_i，$i=1,\dots,k$ 不全为 0，则

$$\mathbf{0}=\varphi(\mathbf{0})=\varphi(\beta_1\mathbf{v}_1+\cdots+\beta_k\mathbf{v}_k)=\beta_1\varphi(\mathbf{v}_1)+\cdots+\beta_k\varphi(\mathbf{v}_k)$$

即 $\varphi(\mathbf{v}_1),\dots,\varphi(\mathbf{v}_k)$ 线性相关。

(iii) 即 (ii) 的逆否命题。

□

例 2.3.2. 设有映射 (函数)$f:\mathbb{R}^n\to\mathbb{R}$，则 f 是线性映射 $\Longleftrightarrow\exists\alpha_1,\dots,\alpha_n\in\mathbb{R}$，使得对 $\forall\mathbf{x}=(x_1,\dots,x_n)^t\in\mathbb{R}^n$，有 $f(\mathbf{x})=\alpha_1x_1+\cdots+\alpha_nx_n$。

证明. $(\Longrightarrow)$ 设 $\alpha_j=f(\mathbf{e}^{(j)})$，$j=1,\dots,n$。则由 $\mathbf{x}=x_1\mathbf{e}^{(1)}+\cdots+x_n\mathbf{e}^{(n)}$ 可得

$$f(\mathbf{x})=x_1f(\mathbf{e}^{(1)})+\cdots+x_nf(\mathbf{e}^{(n)})=\alpha_1x_1+\cdots+\alpha_nx_n$$

即得结论。
($\Longleftarrow$) 用定义验证。设 $\mathbf{y} = (y_1, \ldots, y_n)^t$, $\lambda \in \mathbb{R}$, 则

$$f(\mathbf{x} + \mathbf{y}) = \alpha_1(x_1 + y_1) + \cdots + \alpha_n(x_n + y_n) = f(\mathbf{x}) + f(\mathbf{y})$$
$$f(\lambda\mathbf{x}) = \alpha_1(\lambda x_1) + \alpha_n(\lambda x_n) = \lambda(\alpha_1 x_1 + \cdots + \alpha_n x_n) = \lambda f(\mathbf{x})$$

即得到 f 是线性映射。 □

例 2.3.3. $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$ 不是线性映射。

定理 2.3.1 (线性映射基本定理). 设 $\mathbf{b}_1, \ldots, \mathbf{b}_n$ 是 $\mathbb{R}^n$ 的一组基, $\mathbf{v}_1, \ldots, \mathbf{v}_n$ 是 $\mathbb{R}^m$ 中任意 n 个向量, 则存在唯一的线性映射 $\varphi : \mathbb{R}^n \to \mathbb{R}^m$ 使得 $\varphi(\mathbf{b}_i) = \mathbf{v}_i$, $i = 1, 2, \ldots, n$。

证明. (分三步, 一是构造映射 φ 并说明其良定义, 二是证明 φ 的线性性, 三是证明唯一性。)
(1) 由基的定义, 对 $\forall \mathbf{x} \in \mathbb{R}^n$, 存在唯一一组 $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$ 使得 $\mathbf{x} = \alpha_1\mathbf{b}_1 + \cdots + \alpha_n\mathbf{b}_n$。于是我们可以定义

$$\begin{aligned} \varphi : &\mathbb{R}^n \longrightarrow \mathbb{R}^m \\ &\mathbf{x} \longmapsto \sum_{i=1}^{n} \alpha_i \mathbf{v}_i. \end{aligned}$$

注意 $\alpha_1, \ldots, \alpha_n$ 的存在唯一性保证了 φ 是良定义的, 且 $\varphi(\mathbf{b}_i) = \mathbf{v}_i$, $i = 1, 2, \ldots, n$ 成立。
(2) 设另有 $\mathbf{y} = \sum_{i=1}^{n} \beta_i \mathbf{b}_i \in \mathbb{R}^n$ 及 $\lambda, \mu \in \mathbb{R}$, 则

$$\begin{aligned} \varphi(\lambda\mathbf{x} + \mu\mathbf{y}) &= \varphi(\lambda \sum_{i=1}^{n} \alpha_i \mathbf{b}_i + \mu \sum_{i=1}^{n} \beta_i \mathbf{b}_i) \\ &= \varphi(\sum_{i=1}^{n} (\lambda\alpha_i + \mu\beta_i)\mathbf{b}_i) \\ &= \sum_{i=1}^{n} (\lambda\alpha_i + \mu\beta_i)\mathbf{v}_i \\ &= \lambda \sum_{i=1}^{n} \alpha_i \mathbf{v}_i + \mu \sum_{i=1}^{n} \beta_i \mathbf{v}_i \\ &= \lambda\varphi(\mathbf{x}) + \mu\varphi(\mathbf{y}) \end{aligned}$$

即 φ 的线性性得证。
(3) 设另有 $\psi : \mathbb{R}^n \to \mathbb{R}^m$ 是线性映射并且也满足 $\psi(\mathbf{b}_i) = \mathbf{v}_i$, 则对 $\forall \mathbf{x} \in \mathbb{R}^n$, 有

$$\psi(\mathbf{x}) = \psi(\sum_{i=1}^{n} \alpha_i \mathbf{b}_i) = \sum_{i=1}^{n} \alpha_i \psi(\mathbf{b}_i) = \sum_{i=1}^{n} \alpha_i \mathbf{v}_i = \varphi(\mathbf{x}).$$

即 $\psi = \varphi$。于是唯一性成立。 □

例 2.3.4. 下面我们考虑两种特殊的线性映射: 嵌入与投影。设 $\mathbb{R}^n$ 的标准基为 $\mathbf{e}^{(1)}, \ldots, \mathbf{e}^{(n)}$, $\mathbb{R}^m$ 的标准基为 $\mathcal{E}^{(1)}, \ldots, \mathcal{E}^{(m)}$。则有:

情形 1：$n \leqslant m$(嵌入)，作线性映射 $\varphi : \mathbb{R}^n \to \mathbb{R}^m$ 且满足：$\varphi(\mathbf{e}^{(j)}) = \mathcal{E}^{(j)},\ j = 1, \ldots, n$。于是有：

$$\begin{aligned}\varphi((x_1, \ldots, x_n)^t) &= \varphi(x_1\mathbf{e}^{(1)} + \cdots + x_n\mathbf{e}^{(n)}) \\ &= x_1\varphi(\mathbf{e}^{(1)}) + \cdots + x_n\varphi(\mathbf{e}^{(n)}) \\ &= x_1\mathcal{E}^{(1)} + \cdots + x_n\mathcal{E}^{(n)} \\ &= (x_1, \ldots, x_n, \underbrace{0, \ldots, 0}_{n-m\text{个}})^t.\end{aligned}$$

情形 2：$n \geqslant m$(投影)。类似上面的推导可以得到：

$$\varphi((x_1, \ldots, x_n)^t) = ((x_1, \ldots, x_m)^t).$$

例 2.3.5. 设线性映射 $\varphi : \mathbb{R}^2 \to \mathbb{R}^2$ 满足

$$\varphi(\mathbf{e}^{(1)}) = \begin{pmatrix}\cos\theta \\ \sin\theta\end{pmatrix}, \quad \varphi(\mathbf{e}^{(2)}) = \begin{pmatrix}-\sin\theta \\ \cos\theta\end{pmatrix}.$$

那么，对 $\forall \mathbf{x} \in \mathbb{R}^2,\ \mathbf{x} = (x_1, x_2)^t$，有 $\varphi(\mathbf{x}) = (x_1\cos\theta - x_2\sin\theta,\ x_1\sin\theta + x_2\cos\theta)^t$。
此即 $\mathbb{R}^2$ 上的旋转变换。

2.3.2 线性映射下的子空间

这一小节我们讨论子空间在线性映射下的“变与不变”。

命题 2.3.2. 设 $\varphi : \mathbb{R}^n \to \mathbb{R}^m$ 是线性映射，则
(i) 如果 $U \subset \mathbb{R}^n$ 是子空间，则 $\varphi(U) \subset \mathbb{R}^m$ 也是子空间，并且 $\dim(U) \geqslant \dim(\varphi(U))$；
(ii) 如果 $V \subset \mathbb{R}^m$ 是子空间，则 $\varphi^{-1}(V)$ 是 $\mathbb{R}^n$ 中的子空间。

证明. (i) 设 $\mathbf{x}, \mathbf{y} \in \varphi(U)$，则存在 $\mathbf{u}, \mathbf{v} \in U$ 使得 $\varphi(\mathbf{u}) = \mathbf{x},\ \varphi(\mathbf{v}) = \mathbf{y}$。于是对 $\forall \alpha, \beta \in \mathbb{R}$，有

$$\alpha\mathbf{x} + \beta\mathbf{y} = \alpha\varphi(\mathbf{u}) + \beta\varphi(\mathbf{v}) = \varphi(\alpha\mathbf{u} + \beta\mathbf{v}).$$

即 $\varphi(U)$ 是子空间。另设 $\mathbf{x}_1, \ldots, \mathbf{x}_d$ 是 $\varphi(U)$ 的一组基，则存在 $\mathbf{u}_1, \ldots, \mathbf{u}_d \in U$ 使得 $\varphi(\mathbf{u}_i) = \mathbf{x}_i$。于是由命题 2.3.1(iii) 可得 $\mathbf{u}_1, \ldots, \mathbf{u}_d$ 线性无关，所以 $\dim U \geqslant d = \dim(\varphi(U))$。
(ii) 对 $\forall \mathbf{x}, \mathbf{y} \in \varphi^{-1}(V)$，即 $\varphi(\mathbf{x}), \varphi(\mathbf{y}) \in V$，则任取 $\alpha, \beta \in \mathbb{R}$，有 $\alpha\varphi(\mathbf{x}) + \beta\varphi(\mathbf{y}) \in V$，即

$$\varphi(\alpha\mathbf{x} + \beta\mathbf{y}) = \alpha\varphi(\mathbf{x}) + \beta\varphi(\mathbf{y}) \in V.$$

即 $\alpha\mathbf{x} + \beta\mathbf{y} \in \varphi^{-1}(V)$。即 $\varphi^{-1}(V)$ 是 $\mathbb{R}^n$ 中的子空间。 □

定义 2.3.2. 设 $\varphi : \mathbb{R}^n \to \mathbb{R}^m$ 是线性映射，称 $\varphi^{-1}(\mathbf{0})$ 为 φ 的核空间，记作 $\ker(\varphi)$；称 $\varphi(\mathbb{R}^n)$ 为 φ 的像空间，记作 $\mathrm{im}(\varphi)$。由上面的命题，$\ker(\varphi) \subset \mathbb{R}^n,\ \mathrm{im}(\varphi) \subset \mathbb{R}^m$ 都是子空间。

下面的命题十分常用。

命题 2.3.3. 设 $\varphi : \mathbb{R}^n \to \mathbb{R}^m$ 是线性映射，则 φ 是单射 $\iff \ker(\varphi) = \{\mathbf{0}\}$。

证明. ($\Longrightarrow$) 由于 $\varphi(\mathbf{0}) = \mathbf{0}$，而 φ 是单射，故 $\ker(\varphi) = \{\mathbf{0}\}$。
($\Longleftarrow$) 设 $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ 且 $\varphi(\mathbf{x}) = \varphi(\mathbf{y})$，则 $\varphi(\mathbf{x} - \mathbf{y}) = \mathbf{0}$，即 $\mathbf{x} - \mathbf{y} \in \ker(\varphi)$，故由 $\ker(\varphi) = \{\mathbf{0}\}$ 立刻得到 $\mathbf{x} - \mathbf{y} = \mathbf{0}$，即 $\mathbf{x} = \mathbf{y}$。 □

下面我们用线性映射的观点重写对偶定理。

定理 2.3.2 (对偶定理 (映射版)). 设 $\varphi:\mathbb{R}^n\to\mathbb{R}^m$ 是线性映射, 则 $\dim(\ker(\varphi))+\dim(\mathrm{im}(\varphi))=n$。

证明. 设 $\mathbf{u}_1,\dots,\mathbf{u}_d$ 是 $\ker(\varphi)$ 的一组基, 则由基扩充定理, $\mathbb{R}^n$ 有一组基为:

$$\mathbf{u}_1,\dots,\mathbf{u}_d,\mathbf{u}_{d+1},\dots,\mathbf{u}_n.$$

下面我们证明如下的断言: $\varphi(\mathbf{u}_{d+1}),\dots,\varphi(\mathbf{u}_n)$ 是 $\mathrm{im}(\varphi)$ 的一组基。
(1)$\varphi(\mathbf{u}_{d+1}),\dots,\varphi(\mathbf{u}_n)$ 线性无关。下面是验证过程。
设 $\beta_{d+1}\varphi(\mathbf{u}_{d+1})+\cdots+\beta_n\varphi(\mathbf{u}_n)=\mathbf{0}$, 即 $\varphi(\beta_{d+1}\mathbf{u}_{d+1}+\cdots+\beta_n\mathbf{u}_n)=\mathbf{0}$。于是 $\beta_{d+1}\mathbf{u}_{d+1}+\cdots+\beta_n\mathbf{u}_n\in\ker(\varphi)$。
那么, 由 $\ker(\varphi)$ 的基的定义, 存在 $\beta_1,\dots,\beta_d\in\mathbb{R}$ 使得 $\beta_{d+1}\mathbf{u}_{d+1}+\cdots+\beta_n\mathbf{u}_n=\beta_1\mathbf{u}_1+\cdots+\beta_d\mathbf{u}_d$,
于是由 $\mathbf{u}_1,\dots,\mathbf{u}_d,\mathbf{u}_{d+1},\dots,\mathbf{u}_n$ 线性无关知 $\beta_1=\cdots=\beta_n=0$。特别地, $\beta_{d+1}=\cdots=\beta_n=0$, 即 $\varphi(\mathbf{u}_{d+1}),\dots,\varphi(\mathbf{u}_n)$ 线性无关。
(2) 对 $\forall\mathbf{x}\in\mathrm{im}(\varphi)$, $\exists\mathbf{u}\in\mathbb{R}^n$ 使得 $\varphi(\mathbf{u})=\mathbf{x}$。由 $\mathbb{R}^n$ 的基可得 $\exists!$一组$\alpha_1,\cdots,\alpha_n$ 使得 $\mathbf{u}=\sum_{i=1}^n\alpha_i\mathbf{u}_i$。
用 φ 作用在上面的等式两边, 得到

$$\varphi(\mathbf{u})=\sum_{i=d+1}^{n}\alpha_i\varphi(\mathbf{u}_i).$$

即 $\mathrm{im}(\varphi)\subset<\varphi(\mathbf{u}_{d+1}),\dots,\varphi(\mathbf{u}_n)>$。由 (1), (2) 可知断言成立, 即 $\dim(\mathrm{im}(\varphi))=n-d$。 □

推论 2.3.1. 设 $\varphi:\mathbb{R}^n\to\mathbb{R}^m$ 是线性映射, 则
(i)φ 是单射 $\iff\dim(\mathrm{im}(\varphi))=n$;
(ii) 当 $m=n$ 时 φ 是单射 $\iff$ φ 是满射。

证明. (i)φ 是单射 $\iff\dim(\ker(\varphi))=0\iff\dim(\mathrm{im}(\varphi))=n$;
(ii) 由 (i) 知 φ 是单射 $\iff$ $\mathrm{im}(\varphi))=\mathbb{R}^n\iff$ φ 是满射。 □

2.3.3 线性映射在标准基下的矩阵表示

在本小节中, 我们设 $\mathbb{R}^n$ 的标准基为 $\mathbf{e}^{(1)},\dots,\mathbf{e}^{(n)}$, $\mathbb{R}^m$ 的标准基为 $\boldsymbol{\mathcal{E}}^{(1)},\dots,\boldsymbol{\mathcal{E}}^{(m)}$。

定义 2.3.3. 设 $\varphi:\mathbb{R}^n\to\mathbb{R}^m$ 是线性映射, $\varphi(\mathbf{e}^{(j)})=(a_{ij},\dots,a_{mj})^t$, $j=1,\dots,n$。我们称矩阵

$$A=\begin{pmatrix}a_{11}&a_{12}&\cdots&a_{1n}\\ \vdots&\vdots&&\vdots\\ a_{m1}&a_{m2}&\cdots&a_{mn}\end{pmatrix}_{m\times n}=(\varphi(\mathbf{e}^{(1)}),\dots,\varphi(\mathbf{e}^{(n)}))$$

为 φ 在标准基下的矩阵。注意, 由定理2.3.1, A 是由 φ 唯一确定的, 记为 A_φ。

例 2.3.6. (1)$\varphi:\mathbb{R}^n\to\mathbb{R}^m$, $\mathbf{u}\mapsto\mathbf{0}$ 零映射对应的矩阵是零矩阵;
(2)$\varphi:\mathbb{R}^n\to\mathbb{R}^n$, $\mathbf{u}\mapsto\mathbf{u}$ 恒同映射对应的矩阵是单位矩阵

$$A_\varphi=\begin{pmatrix}1&0&\cdots&0\\ 0&1&\cdots&0\\ \vdots&\vdots&\ddots&\vdots\\ 0&0&\cdots&1\end{pmatrix}_{n\times n}=E_n.$$

命题 2.3.4. 设 $\varphi:\mathbb{R}^n\to\mathbb{R}^m$ 是线性映射，φ 在标准基下的矩阵为 $A=(a_{ij})_{m\times n}$，则对 $\forall\mathbf{x}=(x_1,\dots,x_n)\in\mathbb{R}^n$，有

$$\varphi(\mathbf{x})=x_1\mathbf{A}^{(1)}+\cdots+x_n\mathbf{A}^{(n)}=\begin{pmatrix}a_{11}x_1+\cdots+a_{1n}x_n\\ \vdots\\ a_{m1}x_1+\cdots+a_{mn}x_n\end{pmatrix}.$$

证明. 由 $\varphi(\mathbf{e}^{(j)})=\mathbf{A}^{(j)},\ j=1,2,\dots,n$ 得

$$\begin{aligned}\varphi(\mathbf{x})&=\varphi(x_1\mathbf{e}^{(1)}+\cdots+x_n\mathbf{e}^{(n)})\\&=x_1\varphi(\mathbf{e}^{(1)})+\cdots+x_n\varphi(\mathbf{e}^{(n)})\\&=x_1\mathbf{A}^{(1)}+\cdots+x_n\mathbf{A}^{(n)}\\&=\begin{pmatrix}a_{11}x_1+\cdots+a_{1n}x_n\\ \vdots\\ a_{m1}x_1+\cdots+a_{mn}x_n\end{pmatrix}.\end{aligned}$$

□

注 2.3.2. 由上述命题有 $\ker(\varphi)=V_A$ 且 $\mathrm{im}(\varphi)=V_c(A)$。

例 2.3.7. 设

$$\begin{aligned}\varphi:&\mathbb{R}^5\longrightarrow\mathbb{R}^3\\&\begin{pmatrix}x_1\\ \vdots\\ x_5\end{pmatrix}\longmapsto\begin{pmatrix}x_1+x_2+x_3+x_4+x_5\\ x_1-x_2-x_3-x_4-x_5\\ 4x_1+2x_2+2x_3+2x_4+2x_5\end{pmatrix}.\end{aligned}$$

则 φ 在标准基下的矩阵为

$$A_\varphi=\begin{pmatrix}1&1&1&1&1\\1&-1&-1&-1&-1\\4&2&2&2&2\end{pmatrix}\xrightarrow{I,II\text{类初等行变换}}\begin{pmatrix}1&1&1&1&1\\0&-2&-2&-2&-2\\0&0&0&0&0\end{pmatrix}.$$

于是 $\mathrm{rank}(A_\varphi)=2$，$\dim(\mathrm{im}(\varphi))=2$。由对偶定理，$\dim(\ker(\varphi))=3$。下面解出 $\ker(\varphi)$。

$$\begin{cases}x_1+x_2+x_3+x_4+x_5=0\\ x_2+x_3+x_4+x_5=0\end{cases}\Longrightarrow\begin{cases}x_1=0\\ x_2+x_3+x_4+x_5=0\end{cases}.$$

于是 $\ker(\varphi)=<(0,-1,1,0,0)^t,(0,-1,0,1,0)^t,(0,-1,0,0,1)^t>$，$\mathrm{im}(\varphi)=<(1,1,4)^t,(1,-1,2)^t>$。

反过来，我们也可以从矩阵出发定义线性映射。

定义 2.3.4. 设 $A\in\mathbb{R}^{m\times n}$，则我们定义 $\varphi:\mathbb{R}^n\to\mathbb{R}^m$ 是满足 $\varphi(\mathbf{e}^{(j)})=\mathbf{A}^{(j)}$ 的线性映射，称为矩阵 A 对应的线性映射。由定理 2.3.1，这样的 φ 存在且唯一，我们将其记为 φ_A。显然 φ_A 在标准基下的矩阵是 A。

例 2.3.8. 证明对偶定理的方程版与映射版是一致的。

证明. 设 $A \in \mathbb{R}^{m\times n}$，则 $\ker(\varphi_A) = V_A$，$\mathrm{im}(\varphi_A) = V_c(A)$。于是

$$\dim(\ker(\varphi_A)) + \dim(\mathrm{im}(\varphi_A)) = n \Longleftrightarrow \dim(V_A) + \dim(V_c(A)) = n \Longleftrightarrow \dim(V_A) + \mathrm{rank}(A) = n.$$

□

2.4 矩阵的运算

这一节我们主要的任务是从线性映射的角度定义矩阵的运算，并考查其性质。

由 2.3.3 小节的内容，我们已经有了矩阵和线性映射之间的对应关系。

设 $\varphi:\mathbb{R}^n\to\mathbb{R}^m$ 是线性映射，矩阵

$$A_\varphi=(\varphi(\mathbf{e}^{(1)}),\dots,\varphi(\mathbf{e}^{(n)}))$$

为 φ 在标准基 $(\mathbf{e}^{(1)},\dots,\mathbf{e}^{(n)})$ 和 $(\mathbf{e}^{(1)},\dots,\mathbf{e}^{(m)})$ 下的矩阵.

给定矩阵 A，$\varphi_A:\mathbb{R}^n\to\mathbb{R}^m$ 是满足

$$\varphi(\mathbf{e}^{(j)})=\mathbf{A}^{(j)}$$

的线性映射。

我们记所有 $\mathbb{R}^n\to\mathbb{R}^m$ 的线性映射组成的集合为 $\mathrm{Hom}(\mathbb{R}^n,\mathbb{R}^m)$。

2.4.1 矩阵的加法和数乘

定理 2.4.1. 设 $\Phi:\mathrm{Hom}(\mathbb{R}^n,\mathbb{R}^m)\to\mathbb{R}^{m\times n}$, $\varphi\mapsto A_\varphi$，则 Φ 是双射，并且 Φ^{-1} 是

$$\Psi=:\mathbb{R}^{m\times n}\to\mathrm{Hom}(\mathbb{R}^n,\mathbb{R}^m),\ A\mapsto\varphi_A.$$

证明. 由于

$$\begin{aligned}\Phi\circ\Psi(A)&=\Phi(\varphi_A)&&(\Psi\text{的定义})\\&=A_{\varphi_A}&&(\Phi\text{的定义})\\&=(\varphi_A(\mathbf{e}^{(1)}),\dots,\varphi_A(\mathbf{e}^{(n)}))&&(A_{\varphi_A}\text{的定义})\\&=(\mathbf{A}^{(1)},\dots,\mathbf{A}^{(n)})&&(\varphi_A\text{的定义}).\end{aligned}$$

于是 $\Phi\circ\Psi=\mathrm{id}_{\mathbb{R}^{m\times n}}$。

反之有

$$\begin{aligned}\Psi\circ\Phi(\varphi)&=\Psi(A_\varphi)&&(\Phi\text{的定义})\\&=\varphi_{A_\varphi}&&(\Psi\text{的定义}).\end{aligned}$$

对任意的 $j\in\{1,\dots,n\}$，注意到 $\varphi_{A_\varphi}(\mathbf{e}^{(j)})=\mathbf{A}_\varphi^{(j)}=\varphi(\mathbf{e}^{(j)})$(由 φ_{A_φ} 的定义)，于是由线性映射基本定理 (唯一性)，有 $\varphi_{A_\varphi}=\varphi$，即对 $\forall\varphi\in\mathrm{Hom}(\mathbb{R}^n,\mathbb{R}^m)$, $\Psi\circ\Phi(\varphi)=\varphi$，即 $\Psi\circ\Phi=\mathrm{id}_{\mathrm{Hom}(\mathbb{R}^n,\mathbb{R}^m)}$。 □

例 2.4.1. (1) 设 $O_{m\times n}$ 是零矩阵，则 $\varphi_{O_{m\times n}}(\mathbf{e}^{(j)})=\mathbf{O}_{m\times n}^{(j)}=\mathbf{O}_m$, $j=1,\dots,n$. 这对应零映射，即 $\forall x_1,\dots,x_n\in\mathbb{R}$, $\varphi_{O_{m\times n}}(x_1\mathbf{e}^{(1)}+\cdots+x_n\mathbf{e}^{(n)})=\mathbf{O}_m$。

(2) 设 E_n 是 n 阶单位方阵，则 $\varphi_{E_n}(\mathbf{e}^{(j)})=\mathbf{E}_n^{(j)}=\mathbf{e}^{(j)}$, $j=1,\dots,n$. 则对 $\forall x_1,\dots,x_n\in\mathbb{R}$，有

$$\begin{aligned}\varphi_{E_n}(x_1\mathbf{e}^{(1)}+\cdots+x_n\mathbf{e}^{(n)})&=x_1\varphi_{E_n}(\mathbf{e}^{(1)})+\cdots+x_n\varphi_{E_n}(\mathbf{e}^{(n)})\\&=x_1\mathbf{e}^{(1)}+\cdots+x_n\mathbf{e}^{(n)}.\end{aligned}$$

即 φ_{E_n} 是恒同映射。

命题 2.4.1. 设 $\varphi,\psi\in \mathrm{Hom}(\mathbb{R}^n,\mathbb{R}^m)$, $\alpha\in\mathbb{R}$, 则我们有如下定义:

$$\varphi+\psi:\mathbb{R}^n\to\mathbb{R}^m,\ \mathbf{x}\mapsto\varphi(\mathbf{x})+\psi(\mathbf{x});$$
$$\alpha\varphi:\mathbb{R}^n\to\mathbb{R}^m,\ \mathbf{x}\mapsto\alpha\varphi(\mathbf{x}).$$

则 $\varphi+\psi$ 和 $\alpha\varphi$ 都是线性映射 (留作练习)。

设 φ 和 ψ 在标准基下的矩阵分别是 A,B, 那么 $\varphi+\psi$ 在标准基下的矩阵

$$A_{\varphi+\psi}=(\mathbf{A}^{(1)}+\mathbf{B}^{(1)},\dots,\mathbf{A}^{(n)}+\mathbf{B}^{(n)});$$
$$A_{\alpha\varphi}=(\alpha\mathbf{A}^{(1)},\dots,\alpha\mathbf{A}^{(n)}).$$

证明留作练习。

定义 2.4.1. 设 A,B 是 $\mathbb{R}$ 上的 $m\times n$ 矩阵, $\alpha\in\mathbb{R}$。则定义矩阵 $A+B=(\mathbf{A}^{(1)}+\mathbf{B}^{(1)},\dots,\mathbf{A}^{(n)}+\mathbf{B}^{(n)})$ 及 $\alpha A=(\alpha\mathbf{A}^{(1)},\dots,\alpha\mathbf{A}^{(n)})$, 即矩阵的加法和数乘。若 $A=(a_{ij})$, $B=(b_{ij})$, 则 $A+B=(a_{ij}+b_{ij})$, $\alpha A=(\alpha a_{ij})$。我们还可以看到, $A=(\mathbf{A}_1+\mathbf{B}_1,\cdots,\mathbf{A}_m+\mathbf{B}_m)^t$, $\alpha A=(\alpha\mathbf{A}_1,\cdots,\alpha\mathbf{A}_m)^t$。此外, 自然地可以定义 $A-B=A+(-1)B$。

例 2.4.2. 设 $A=\begin{pmatrix}1&2\\3&4\end{pmatrix},B=\begin{pmatrix}1&0\\2&1\end{pmatrix}$, 则 $A-B=\begin{pmatrix}0&2\\1&3\end{pmatrix}$。

有了线性映射和矩阵的加法和数乘的定义以后, 我们很容易得到以下推论:

推论 2.4.1. 定理2.4.1中的 Φ 是线性双射。

证明. 记号与前面相同。双射已经在定理2.4.1中证明, 下面证明线性性。注意到

$$\begin{aligned}\Phi(\alpha\varphi+\beta\psi)&=A_{\alpha\varphi+\beta\psi}\\&=A_{\alpha\varphi}+A_{\beta\psi}&&\text{(矩阵加法定义)}\\&=\alpha A_{\varphi}+\beta A_{\psi}&&\text{(矩阵数乘定义)}\\&=\alpha\Phi(\varphi)+\beta\Phi(\psi)&&\text{(Φ的定义).}\end{aligned}$$

即得结论。 □

例 2.4.3. 设 $A,B\in\mathbb{R}^{m\times n}$, 则 $\mathrm{rank}(A+B)\leqslant\mathrm{rank}(A)+\mathrm{rank}(B)$。

证明. 由矩阵加法的定义, 显然有:

$$V_c(A+B)=<\mathbf{A}^{(1)}+\mathbf{B}^{(1)},\dots,\mathbf{A}^{(n)}+\mathbf{B}^{(n)}>.$$

于是 $\forall j\in\{1,2,\dots,n\}$, $\mathbf{A}^{(j)}+\mathbf{B}^{(j)}\in V_c(A)+V_c(B)$, 即 $V_c(A+B)\subset V_c(A)+V_c(B)$。那么, 由秩的定义即得:

$$\begin{aligned}\mathrm{rank}(A+B)&=\dim V_c(A+B)\\&\leqslant\dim(V_c(A)+V_c(B))\\&\leqslant\dim(V_c(A))+\dim(V_c(B))\\&\leqslant\mathrm{rank}(A)+\mathrm{rank}(B).\end{aligned}$$

即得结论。 □

2.4.2 矩阵的转置

定义 2.4.2. 设 $A \in \mathbb{R}^{m\times n}$, $A = (a_{ij})_{m\times n}$，则 A 的转置 (transpose) 是 $n\times m$ 阶矩阵，记为 A^t。即

$$A^t = \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{m1} \\ a_{12} & a_{22} & \cdots & a_{m2} \\ \vdots & \vdots & & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{mn} \end{pmatrix}_{n\times m}.$$

以下两个性质是显然的。

命题 2.4.2. 设 $A \in \mathbb{R}^{m\times n}$，则 $(A^t)^t = A$, $\operatorname{rank}(A) = \operatorname{rank}(A^t)$。

证明. 由定义即有 $(A^t)^t = A$。因为 $\dim(V_r(A^t)) = \dim(V_c(A))$，所以 $\operatorname{rank}(A) = \operatorname{rank}(A^t)$。 □

命题 2.4.3. 设 $A, B \in \mathbb{R}^{m\times n}$, $\alpha \in \mathbb{R}$，则 $(A+B)^t = A^t + B^t$, $(\alpha A)^t = \alpha A^t$。

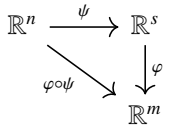
证明留作练习。

2.4.3 矩阵的乘法

首先我们考虑线性映射的复合。

命题 2.4.4. 设 $\psi \in \operatorname{Hom}(\mathbb{R}^n, \mathbb{R}^s)$, $\varphi \in \operatorname{Hom}(\mathbb{R}^s, \mathbb{R}^m)$，则 $\varphi\circ\psi \in \operatorname{Hom}(\mathbb{R}^n, \mathbb{R}^m)$。

证明. 即下面的交换图。



下面验证 $\varphi\circ\psi$ 的线性性。

设 $\alpha, \beta \in \mathbb{R}$, $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$，则

$$\varphi\circ\psi(\alpha\mathbf{x} + \beta\mathbf{y}) = \varphi(\alpha\psi(\mathbf{x}) + \beta\psi(\mathbf{y})) = \alpha\varphi\circ\psi(\mathbf{x}) + \beta\varphi\circ\psi(\mathbf{y}).$$

即得结论。 □

下面我们把线性映射的复合用矩阵表示出来。设 ψ, φ, $\varphi\circ\psi$ 在标准基下的矩阵分别是 B, A, C，则

$$C = (\varphi\circ\psi(\mathbf{e}^{(1)}), \ldots, \varphi\circ\psi(\mathbf{e}^{(n)})) = (\varphi(\mathbf{B}^{(1)}), \ldots, \varphi(\mathbf{B}^{(n)})).$$

设 $B = (b_{kj})_{s\times n}$，即

$$\mathbf{B}^{(j)} = (b_{ij}, \ldots, b_{sj})^t = b_{ij}\boldsymbol{\delta}_1 + \cdots + b_{sj}\boldsymbol{\delta}_s$$

其中 $\boldsymbol{\delta}_1, \ldots, \boldsymbol{\delta}_s$ 是 $\mathbb{R}^s$ 的标准基。则

$$\varphi(\mathbf{B}^{(j)}) = b_{1j}\varphi(\boldsymbol{\delta}_1) + \cdots + b_{sj}\varphi(\boldsymbol{\delta}_s) = b_{1j}\mathbf{A}^{(1)} + \cdots + b_{sj}\mathbf{A}^{(s)}.$$

于是 $\mathbf{C}^{(j)} = b_{1j}\mathbf{A}^{(1)} + \cdots + b_{sj}\mathbf{A}^{(s)}$。令 $C = (c_{ij})_{m\times n}$, $A = (a_{ik})_{m\times s}$，则

$$\begin{aligned} c_{ij} &= b_{1j}a_{i1} + \cdots + b_{sj}a_{is} \\ &= a_{i1}b_{1j} + \cdots + a_{is}b_{sj} \\ &= \sum_{k=1}^{s} a_{ik}b_{kj}. \end{aligned}$$

此即矩阵的乘法。

定义 2.4.3. 设 $A \in \mathbb{R}^{m\times s}$, $B \in \mathbb{R}^{s\times n}$，则定义 A 与 B 的乘积是 $m\times n$ 阶矩阵 $C = (c_{ij})_{m\times n}$，其中 $c_{ij} = \sum_{k=1}^{s} a_{ik}b_{kj}$。记作 $C = AB$。

由上面的讨论可知，$\varphi\circ\psi$ 在标准基下的矩阵就是 $C = AB$，即 $\varphi_A \circ \varphi_B = \varphi_{AB}$。

例 2.4.4. 设 $(\alpha_1,\dots,\alpha_s) \in \mathbb{R}^{1\times s}$, $(\beta_1,\dots,\beta_s)^t \in \mathbb{R}^{s\times 1}$，则

$$(\alpha_1,\dots,\alpha_s)\begin{pmatrix}\beta_1\\ \vdots\\ \beta_s\end{pmatrix} = \alpha_1\beta_1 + \cdots + \alpha_s\beta_s.$$

于是我们看到，对于 $C = AB = (c_{ij})$，由于

$$c_{ij} = \sum_{k=1}^{s} a_{ik}b_{kj} = (a_{i1},\dots,a_{is})\begin{pmatrix}b_{ij}\\ \vdots\\ b_{sj}\end{pmatrix} = \mathbf{A}_i\mathbf{B}^{(j)}.$$

因此

$$AB = \begin{pmatrix}\mathbf{A}_1\mathbf{B}^{(1)} & \cdots & \mathbf{A}_1\mathbf{B}^{(n)}\\ \vdots & & \vdots\\ \mathbf{A}_m\mathbf{B}^{(1)} & \cdots & \mathbf{A}_m\mathbf{B}^{(n)}\end{pmatrix}$$

例 2.4.5. (1) 设 $A = \begin{pmatrix}1 & 2\\ 3 & 4\end{pmatrix}$, $B = \begin{pmatrix}2 & 1 & 0\\ 3 & 1 & 3\end{pmatrix}$，则 $AB = \begin{pmatrix}8 & 3 & 6\\ 18 & 7 & 12\end{pmatrix}$，而 BA 没有定义。
(2) 即使 AB 和 BA 都有定义 (此时 A, B 必须都是方阵)，一般地也有 $AB \neq BA$。例如，若 $A = \begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}$, $B = \begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}$，则 $AB = \begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}$, $BA = \begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}$。

例 2.4.6. 设 $A \in \mathbb{R}^{m\times n}$, $\operatorname{rank}(A) = 1$, 则 $\exists \alpha_1,\dots,\alpha_m$ 及 $\beta_1,\dots,\beta_n \in \mathbb{R}$ 使得 $A = (\alpha_1,\dots,\alpha_m)^t(\beta_1,\dots,\beta_n)$。

证明. 由于 $\operatorname{rank}(A) = 1$，即 $\dim V_c(A) = 1$，设 $\boldsymbol{\alpha} = (\alpha_1,\dots,\alpha_m)^t$ 是 $V_c(A)$ 的一组基，则对 $\forall j = 1,\dots,n$, $\exists \beta_j \in \mathbb{R}$ 使得 $\mathbf{A}^{(j)} = \beta_j\boldsymbol{\alpha}$，即 $A = (\alpha_1,\dots,\alpha_m)^t(\beta_1,\dots,\beta_n)$。 □

2.4.4 矩阵加法、数乘和乘法的运算律

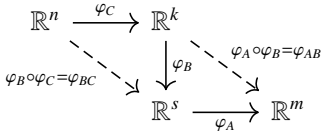
我们首先陈述矩阵关于加法和数乘的运算律，它们的证明都十分容易，留作练习。

设 $A, B, C \in \mathbb{R}^{m\times n}$, $\alpha, \beta \in \mathbb{R}$，则有：

$A + B = B + A$	加法交换
$(A + B) + C = A + (B + C)$	加法结合
$A + O_{m\times n} = A$	加法单位
$A + (-A) = O_{m\times n}$	加法逆
$\alpha(\beta A) = (\alpha\beta)A$	数乘结合
$1\cdot A = A$	数乘单位
$\alpha(A + B) = \alpha A + \alpha B$	分配律
$(\alpha + \beta)A = \alpha A + \beta A$	分配律

以后我们会看到，$\mathbb{R}^{m\times n}$ 在加法和数乘下构成了一个**向量空间**。

接下来我们考虑矩阵的乘法。首先，矩阵的乘法满足结合律，这可以由映射复合的结合律以及矩阵与线性映射之间的一一对应 (确切地说，是线性同构) 证得。设 $A \in \mathbb{R}^{m\times s}$，$B \in \mathbb{R}^{s\times k}$，$C \in \mathbb{R}^{k\times n}$，我们欲证明 $(AB)C = A(BC)$。证明可以用下面两个图表示，其中用到了定理1.3.2和定理2.4.1。



$$\begin{array}{ccc} \varphi_A \circ (\varphi_B \circ \varphi_C) & = & (\varphi_A \circ \varphi_B) \circ \varphi_C \\ \| & & \| \\ \varphi_A \circ \varphi_{BC} & & \varphi_{AB} \circ \varphi_C \\ \| & & \| \\ \varphi_{A(BC)} & = & \varphi_{(AB)C} \end{array}$$

矩阵乘法与加法之间的左右分配律如下：设 $A \in \mathbb{R}^{m\times s}$，$B, C \in \mathbb{R}^{s\times n}$，则 $A(B+C) = AB+AC$；设 $A \in \mathbb{R}^{n\times k}$，$B, C \in \mathbb{R}^{s\times n}$，则 $(B + C)A = BA + CA$。

矩阵乘法和数乘之间也有结合律：设 $A \in \mathbb{R}^{m\times s}$，$B \in \mathbb{R}^{s\times n}$，$\alpha \in \mathbb{R}$，则 $(\alpha A)B = A(\alpha B) = \alpha(AB)$。

下面考虑矩阵乘法和转置的关系。

命题 2.4.5. 设 $A \in \mathbb{R}^{m\times s}$，$B \in \mathbb{R}^{s\times n}$，则 $(AB)^t = B^tA^t$。

证明. 设 $A = (a_{ik})_{m\times s}$，$B = (b_{kj})_{s\times n}$，则 $A^t = (a'_{kj})_{s\times m}$，$B^t = (b'_{jk})_{n\times s}$，其中 $a_{ik} = a'_{ki}$，$b_{kj} = b'_{jk}$。令 $C = AB = (c_{ij})_{m\times n}$，$D = B^tA^t = (d_{ji})_{n\times m}$，则

$$d_{ji} = \sum_{k=1}^{s} b'_{jk}a'_{ki} = \sum_{k=1}^{s} a_{ik}b_{kj} = c_{ij}.$$

即 $D^t = C$。 □

2.4.5 对角矩阵

下面我们考虑一类特殊的矩阵：对角矩阵。由于对角矩阵具有比较简单的形式和运算性质，因此线性代数课程的主线之一就是如何将矩阵化成对角矩阵。

定义 2.4.4. 形如 $\begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{pmatrix}_{n\times n}$ 的方阵称为对角矩阵。

对角矩阵与其它矩阵的乘法是简单的。

命题 2.4.6. 设 $A \in \mathbb{R}^{m\times n}$，则

(i) $\begin{pmatrix} \lambda_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda_m \end{pmatrix} A = \begin{pmatrix} \lambda_1\mathbf{A}_1 \\ \vdots \\ \lambda_m\mathbf{A}_m \end{pmatrix}$;

(ii) $A \begin{pmatrix} \lambda_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda_n \end{pmatrix} = \left(\lambda_1\mathbf{A}^{(1)}, \ldots, \lambda_n\mathbf{A}^{(n)}\right)$.

推论 2.4.2. 设 $A \in \mathbb{R}^{m\times n}$，则 $(\lambda E_m)A = A(\lambda E_n) = \lambda A$。特别地，$n$ 阶单位矩阵的倍数与任何 n 阶方阵都可交换。

实际上，与任何 n 阶方阵都可交换的矩阵只能是 n 阶单位矩阵的倍数，证明见下节。

例 2.4.7. $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$，$B = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$，则 $AB = \begin{pmatrix} 1 & 4 \\ 3 & 8 \end{pmatrix}$，$BA = \begin{pmatrix} 1 & 2 \\ 6 & 8 \end{pmatrix}$，仍然有 $AB \neq BA$。

2.4.6 秩不等式

最后我们从线性映射的角度证明一些关于矩阵的秩的不等式。更多有关秩不等式的内容可以参考习题课讲义。

定理 2.4.2. 设 $A \in \mathbb{R}^{m\times s}$，$B \in \mathbb{R}^{s\times n}$，则 $\operatorname{rank}(AB) \leqslant \min(\operatorname{rank}(A), \operatorname{rank}(B))$。

证明. 只需证 $\operatorname{rank}(AB) \leqslant \operatorname{rank}(A)$，$\operatorname{rank}(AB) \leqslant \operatorname{rank}(B)$ 即可。对于 $\operatorname{rank}(AB) \leqslant \operatorname{rank}(A)$，只需注意到下面的交换图：

$$\begin{array}{ccc} \mathbb{R}^n & \xrightarrow{\varphi_B} & \mathbb{R}^s \\ & \searrow^{\varphi_{AB}} & \downarrow{\scriptstyle \varphi_A} \\ & & \mathbb{R}^m \end{array}$$

，于是

$$\begin{array}{ccccc} \operatorname{im}(\varphi_B) & \subset & \mathbb{R}^s & & \\ \Downarrow & & & & \\ \varphi_A(\operatorname{im}(\varphi_B)) & \subset & \varphi_A(\mathbb{R}^s) & \text{，因此} & \begin{array}{ccc} \dim(\operatorname{im}(\varphi_{AB})) & \leqslant & \dim(\operatorname{im}(\varphi_A)) \\ \| & & \| \\ \operatorname{rank}(AB) & \leqslant & \operatorname{rank}(A) \end{array} \\ \| & & \| & & \\ \operatorname{im}(\varphi_{AB}) & \subset & \operatorname{im}(\varphi_A) & & \end{array}.$$

下面证明 $\operatorname{rank}(AB) \leqslant \operatorname{rank}(B)$。设 $\mathbf{x} \in \ker(\varphi_B)$，即 $\varphi_B(\mathbf{x}) = \mathbf{0}$，则

$$\varphi_{AB}(\mathbf{x}) = \varphi_A \circ \varphi_B(\mathbf{x}) = \varphi_A(\varphi_B(\mathbf{x})) = \varphi_A(\mathbf{0}) = \mathbf{0},$$

即 $\mathbf{x} \in \ker(\varphi_{AB})$。由 $\mathbf{x}$ 的任意性知 $\ker(\varphi_B) \subset \ker(\varphi_{AB})$，因此 $\dim(\ker(\varphi_B)) \leqslant \dim(\ker(\varphi_{AB}))$。再利用对偶定理可得 $n - \dim(\operatorname{im}(\varphi_B)) \leqslant n - \dim(\operatorname{im}(\varphi_{AB}))$，所以 $\dim(\operatorname{im}(\varphi_{AB})) \leqslant \dim(\operatorname{im}(\varphi_B))$，即 $\operatorname{rank}(AB) \leqslant \operatorname{rank}(B)$。 □

定理 2.4.3 (Sylvester 不等式). 设 $A \in \mathbb{R}^{m\times s}$，$B \in \mathbb{R}^{s\times n}$，则 $\operatorname{rank}(AB) \geqslant \operatorname{rank}(A) + \operatorname{rank}(B) - s$。

证明. 设 $\mathbf{u}_1, \ldots, \mathbf{u}_d$ 是 $\ker(\varphi_A) \cap \operatorname{im}(\varphi_B)$ 的一组基，则由定理2.1.1(基扩充定理)，存在 $\mathbf{u}_{d+1}, \ldots, \mathbf{u}_k \in \operatorname{im}(\varphi_B)$ 使得 $\mathbf{u}_1, \ldots, \mathbf{u}_d, \mathbf{u}_{d+1}, \ldots, \mathbf{u}_k$ 是 $\operatorname{im}(\varphi_B)$ 的一组基。下面证明 $\varphi_A(\mathbf{u}_{d+1}), \ldots, \varphi_A(\mathbf{u}_k)$ 线性无关。

假设 $\exists \alpha_{d+1}, \ldots, \alpha_k \in \mathbb{R}$ 使得

$$\alpha_{d+1}\varphi_A(\mathbf{u}_{d+1}) + \cdots + \alpha_k\varphi_A(\mathbf{u}_k) = \mathbf{0}. \tag{$*$}$$

我们的证明目标是 $\alpha_{d+1} = \cdots = \alpha_k = 0$。利用 $(*)$ 式及 φ_A 的线性性知 $\varphi_A(\sum_{i=d+1}^k \alpha_i\mathbf{u}_i) = \mathbf{0}$，则 $\sum_{i=d+1}^k \alpha_i\mathbf{u}_i \in \ker(\varphi_A)$。于是 $\sum_{i=d+1}^k \alpha_i\mathbf{u}_i \in \ker(\varphi_A) \cap \operatorname{im}(\varphi_B)$。那么，由 $\mathbf{u}_1, \ldots, \mathbf{u}_d$ 是 $\ker(\varphi_A) \cap \operatorname{im}(\varphi_B)$ 的一组基可知：$\exists \alpha_1, \ldots, \alpha_d \in \mathbb{R}$ 使得 $\alpha_1\mathbf{u}_1 + \cdots + \alpha_d\mathbf{u}_d - \sum_{i=d+1}^k \alpha_i\mathbf{u}_i = \mathbf{0}$。再利用 $\mathbf{u}_1, \ldots, \mathbf{u}_k$ 是 $\operatorname{im}(\varphi_B)$ 的一组基就有：$\alpha_1 = \cdots = \alpha_k = 0$，特别地，$\alpha_{d+1} = \cdots = \alpha_k = 0$，即 $\varphi_A(\mathbf{u}_{d+1}), \ldots, \varphi_A(\mathbf{u}_k)$ 线性无关成立。

另一方面，任取 $\varphi_A(\mathbf{u}) \in \operatorname{im}(\varphi_{AB})$ (其中 $\mathbf{u} \in \varphi_B$)，我们知道存在唯一一组 $\alpha_1, \ldots, \alpha_k \in \mathbb{R}$ 使得

$$\mathbf{u} = \sum_{i=1}^k \alpha_i\mathbf{u}_i,$$

由于 $\varphi_A(\mathbf{u}_1) = \cdots = \varphi_B(\mathbf{u}_d) = \mathbf{0}$，因此用 φ_B 作用到上式两边得到

$$\varphi_A(\mathbf{u}) = \sum_{i=d+1}^{k} \alpha_i \varphi_A(\mathbf{u}_i),$$

因此 $\varphi_A(\mathbf{u}_{d+1}), \ldots, \varphi_A(\mathbf{u}_k)$ 是 $\mathrm{im}(\varphi_{AB})$ 的一组基。

之后，我们只需注意到 $k = \dim(\mathrm{im}(\varphi_B)) = \mathrm{rank}(B)$，于是

$$\mathrm{rank}(AB) = \dim(\mathrm{im}(\varphi_{AB})) = k - d = \mathrm{rank}(B) - d.$$

又因为

$$\begin{aligned} d &= \dim(\ker(\varphi_A) \cap \mathrm{im}(\varphi_B)) \\ &\leqslant \dim(\ker(\varphi_A)) = s - \dim(\mathrm{im}(\varphi_A)) = s - \mathrm{rank}(A). \end{aligned}$$

结合上面两个不等式即有：$\mathrm{rank}(AB) = \mathrm{rank}(B) - d \geqslant \mathrm{rank}(B) + \mathrm{rank}(A) - s$。 □

这个证明的方法我们在下册还会再次用到。

推论 2.4.3. 设 $P \in \mathbb{R}^{m\times m}$，$Q \in \mathbb{R}^{n\times n}$，$A \in \mathbb{R}^{m\times n}$，则
(i) 如果 $\mathrm{rank}(P) = m$，则 $\mathrm{rank}(PA) = \mathrm{rank}(A)$；
(ii) 如果 $\mathrm{rank}(Q) = n$，则 $\mathrm{rank}(AQ) = \mathrm{rank}(A)$。

证明. 只证明 (i)，(ii) 同理。利用定理2.4.1和定理2.4.2立刻可得：$\mathrm{rank}(P) + \mathrm{rank}(A) - m \leqslant \mathrm{rank}(PA) \leqslant \min(\mathrm{rank}(P), \mathrm{rank}(A))$，即 $m + \mathrm{rank}(A) - m \leqslant \mathrm{rank}(PA) \leqslant \mathrm{rank}(A)$，即 $\mathrm{rank}(PA) = \mathrm{rank}(A)$。 □

2.5 方阵

这一节我们专门讨论行数和列数相等的矩阵，即方阵。我们将所有方阵的集合 $\mathbb{R}^{n\times n}$ 也记为 $M_n(\mathbb{R})$。$M_n(\mathbb{R})$ 上的加法和数乘显然满足上一节关于一般矩阵的运算律，并且对于矩阵乘法而言，满足乘法的封闭性、结合律、单位元 E_n(无歧义时也记作 E 或 I)，并且乘法对加法满足左右分配律，即满足环的公理，$M_n(\mathbb{R})$ 是环。又因为纯量乘法满足

$$\lambda(AB) = (\lambda A)B = A(\lambda B)$$

集合 $M_n(\mathbb{R})$ 也称为 $\mathbb{R}$ 上的 n 阶矩阵代数。本节中的矩阵如无特殊说明的都是 n 阶方阵。

定义 2.5.1. 我们定义方阵的幂如下：$A^k = \underbrace{A\cdots A}_{k个}$。特别地，定义 $A^0 = E$。显然，对 $\forall k,l\in\mathbb{N}$ 都有 $A^{k+l} = A^kA^l$。

注 2.5.1. 对 $A,B\in M_n(\mathbb{R})$，我们已经通过反例说明了 $AB\neq BA$；并且，例 2.4.5(2) 还表明，$AB = O$ 不能推出 $A = O$ 或 $B = O$。

例 2.5.1. (1) 设 $D = \begin{pmatrix}\lambda_1 & & \\ & \ddots & \\ & & \lambda_n\end{pmatrix}$，则 $D^m = \begin{pmatrix}\lambda_1^m & & \\ & \ddots & \\ & & \lambda_n^m\end{pmatrix}$；

(2) 设 $A = \begin{pmatrix}a & c\\ 0 & b\end{pmatrix}$ $(a\neq b)$，则 $A^m = \begin{pmatrix}a^m & c\frac{a^m-b^m}{a-b}\\ 0 & b^m\end{pmatrix}$。

一般的，我们把第 i 行第 j 列 (以后简称 (i,j) 位置) 的元素为 1，其余位置的元素都为 0 的矩阵记作 E_{ij}，则显然有

$$AE_{ij} = (\mathbf{0},\dots,\mathbf{0},\mathbf{A}^{(i)},\mathbf{0},\dots,\mathbf{0}) = \begin{pmatrix}0 & \cdots & a_{1i} & \cdots & 0\\ \vdots & & \vdots & & \vdots\\ 0 & \cdots & a_{ni} & \cdots & 0\end{pmatrix}(\text{第 j 列是 } \mathbf{A}^{(i)}); \tag{2.5.1}$$

$$E_{ij}A = (\mathbf{0},\dots,\mathbf{0},\mathbf{A}_j^t,\mathbf{0},\dots,\mathbf{0})^t = \begin{pmatrix}0 & \cdots & 0\\ & \cdots & \\ a_{j1} & \cdots & a_{jn}\\ & \cdots & \\ 0 & \cdots & 0\end{pmatrix}(\text{第 i 行是 } \mathbf{A}_j). \tag{2.5.2}$$

定义 2.5.2. 设 $A\in M_n(\mathbb{R})$，如果对 $\forall B\in M_n(\mathbb{R})$，有 $AB = BA$，则称 A 是 $M_n(\mathbb{R})$ 中的中心元。

显然对 $\forall\lambda\in\mathbb{R}$，$\lambda E$ 是中心元。

定理 2.5.1. $M_n(\mathbb{R})$ 中的中心元都是数乘矩阵 λE，$\lambda\in\mathbb{R}$。

证明. 设 $A = (a_{ij})_{n\times n}$ 是中心元，我们解出 A 的形式即可。首先，对 $\forall B = (b_{ij})_{n\times n}$，有 $B = \sum_{i,j=1}^n b_{ij}E_{ij}$。于是，要使 $AB = BA$ 对任意 B 成立，只需 $\forall i,j = 1,\dots,n$，有 $AE_{ij} = E_{ij}A$ 即可。于是由 (2.5.1) 及 (2.5.2) 式，有 $\forall i\neq j$，$a_{ij} = 0$；而对所有 $i = j$ 则有 $a_{ii} = a_{jj}$。此即 A 是数乘矩阵。 □

例 2.5.2. 设 $A\in M_n(\mathbb{R})$，求 $(A+\lambda E)^k$。

解. 利用 $A(\lambda E)=(\lambda E)A=\lambda A$ 即可得到：

$$\begin{aligned}(A+\lambda E)^k &= A^k+\binom{k}{1}A^{k-1}(\lambda E)+\cdots+\binom{k}{k-1}A(\lambda E)^{k-1}+\lambda^k E\\ &= A^k+\binom{k}{1}\lambda A^{k-1}+\cdots+\binom{k}{k-1}\lambda^{k-1}A+\lambda^k E\end{aligned}$$

□

接下来我们引入一类重要的方阵：可逆矩阵。

定义 2.5.3. 设 $A\in M_n(\mathbb{R})$，如果 $\exists B\in M_n(\mathbb{R})$ 使得 $AB=BA=E$，则称 A 是可逆矩阵，且称 B 是 A 的逆矩阵，记为 $B=A^{-1}$。

下面的命题表明逆矩阵如果存在则必唯一。

命题 2.5.1. 设 $A,B,C\in M_n(\mathbb{R})$, $AB=BA=E$，若 $CA=E$ 或 $AC=E$ 有一个成立，则必有 $B=C$。

证明. 只证明 $CA=E$ 的情形，另一个同理。由 $B=EB=(CA)B=C(AB)=CE=C$ 即得结论。 □

定理 2.5.2. 设 $A\in M_n(\mathbb{R})$，则 A 可逆 $\Longleftrightarrow A$ 满秩。

证明. ($\Longrightarrow$) 设 $B\in M_n(\mathbb{R})$ 且 $AB=E$，则 $n=\operatorname{rank}(AB)\leqslant\min(\operatorname{rank}(A),\operatorname{rank}(B))\leqslant\operatorname{rank}(A)\leqslant n$，即 $\operatorname{rank}(A)=n$ 成立。
($\Longleftarrow$) 设 $\varphi_A:\mathbb{R}^n\to\mathbb{R}^n$, $\mathbf{x}\mapsto A\mathbf{x}$ 是 A 对应的线性映射，由于 $\operatorname{rank}(A)=\dim(\operatorname{im}(\varphi_A))=n$，由推论2.3.1知 φ_A 是双射，于是存在 φ_A 的逆映射 φ_A^{-1}(也是双射)。我们验证 φ_A^{-1} 是线性映射。设 $\mathbf{x},\mathbf{y}\in\mathbb{R}^n$，由 φ_A 是满射可得 $\exists\mathbf{u},\mathbf{v}\in\mathbb{R}^n$ 使得 $\varphi_A(\mathbf{u})=\mathbf{x}$，$\varphi_A(\mathbf{v})=\mathbf{y}$。于是由 φ_A 的线性性可得 $\forall\alpha,\beta\in\mathbb{R}$, $\varphi_A(\alpha\mathbf{u}+\beta\mathbf{v})=\alpha\mathbf{x}+\beta\mathbf{y}$，那么，按照 φ_A^{-1} 的定义就分别有：

$$\alpha\mathbf{u}+\beta\mathbf{v}=\varphi_A^{-1}(\alpha\mathbf{x}+\beta\mathbf{y}),\ \alpha\mathbf{u}+\beta\mathbf{v}=\alpha\varphi_A^{-1}(\mathbf{x})+\beta\varphi_A^{-1}(\mathbf{y})$$

此即 φ_A^{-1} 是线性映射。于是，可设 φ_A^{-1} 对应的矩阵是 B，即 $\varphi_A^{-1}=\varphi_B$。那么就有

$$\begin{aligned}\varphi_{AB}=\varphi_A\circ\varphi_B=\varphi_A\circ\varphi_A^{-1}=\mathrm{id}_{\mathbb{R}^n}\Longrightarrow AB=E;\\ \varphi_{BA}=\varphi_B\circ\varphi_A=\varphi_A^{-1}\circ\varphi_A=\mathrm{id}_{\mathbb{R}^n}\Longrightarrow BA=E.\end{aligned}$$

即 A 可逆且逆矩阵是 B。 □

推论 2.5.1. 设 $A,B,C\in M_n(\mathbb{R})$，如果 $AB=E$ 或 $CA=E$，则 $B=A^{-1}$ 或 $C=A^{-1}$。

证明. 只证明 $AB=E$ 的情形，另一个同理。由 $AB=E$ 易证 $\operatorname{rank}(A)=n$(见上面的定理2.5.2($\Longrightarrow$)")，于是 A 可逆，记 A 的逆为 A^{-1}，则 $AB=E\Longrightarrow A^{-1}AB=A^{-1}$，即 $B=A^{-1}$。 □

推论 2.5.2. 设 $A,B\in M_n(\mathbb{R})$，如果 A,B 都可逆，则 AB 可逆且 $(AB)^{-1}=B^{-1}A^{-1}$。

证明. 由 $(AB)(B^{-1}A^{-1})=A(BB^{-1})A^{-1}=AA^{-1}=E$ 即得结论。 □

推论 2.5.3. 设 $A\in M_n(\mathbb{R})$ 是可逆矩阵，则 A^t 也可逆并且 $(A^t)^{-1}=(A^{-1})^t$。

证明. 注意到 $A^t(A^{-1})^t=(A^{-1}A)^t=E^t=E$ 即可。 □

下面我们定义一些其它类型的方阵，它们的性质我们会在后面慢慢学习。

定义 2.5.4. 设 $A \in M_n(\mathbb{R})$。如果 $A^t = A$，则称 A 是对称的；如果 $A^t = -A$，则称 A 是斜对称 (反对称) 的；如果存在 $k \in \mathbb{Z}^+$ 使得 $A^k = O$，则称 A 是幂零的；如果 $A^2 = E$，则称 A 是对合的；如果 $A^2 = A$，则称 A 是幂等的。

实际上，直接计算 AB，A^m 或 A^{-1} 在矩阵规模很大时不是一件很容易的事情。为此，我们往往要基于矩阵的特殊性质或者利用更高级的工具来简化计算。在本节的最后，我们给出下面的例子作为一个引子。

例 2.5.3. 设 $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$，计算 A^m，$m \geqslant 0$。

解. 简单的计算可以猜测：$A^m = \begin{pmatrix} f_{m-1} & f_m \\ f_m & f_{m+1} \end{pmatrix}$，其中 $f_0 = f_1 = 1$，$f_{m+1} = f_m + f_{m-1}$，即 $\{f_m\}, m = 0, 1, \cdots$ 是斐波那契数列。我们可以用数学归纳法证明这个结论，但我们下面给出一个更直接的计算方法。

引入 $B = \begin{pmatrix} -\dfrac{\lambda_2}{5} & \dfrac{1}{5} \\ -\sqrt{5}\lambda_1 & \sqrt{5} \end{pmatrix}$，其中 $\lambda_1 = \dfrac{1 + \sqrt{5}}{2}$，$\lambda_2 = \dfrac{1 - \sqrt{5}}{2}$。不难计算出

$$B^{-1} = \begin{pmatrix} \sqrt{5} & -\dfrac{1}{5} \\ \sqrt{5}\lambda_1 & -\dfrac{\lambda_2}{5} \end{pmatrix}, \ A = B^{-1} \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} B.$$

则 $A^m = B^{-1} \begin{pmatrix} \lambda_1^m & 0 \\ 0 & \lambda_2^m \end{pmatrix} B$，代入数值后即可得到 A^m 的通项公式。此外，通过对比元素也可以得到 f_m 的通项公式：

$$f_m = \frac{\sqrt{5}}{5}(\lambda_1^m - \lambda_2^m).$$

另外，由这个通项公式可知，$\lim_{m \to \infty} \dfrac{f_m}{\lambda_1^m} = \dfrac{\sqrt{5}}{5}$，即当 m 充分大时斐波那契数列与等比数列的增长速度相同。 □

2.6 矩阵的等价

这一节我们来更深入地讨论矩阵的初等变换。

定义 2.6.1. 设 $A, B \in \mathbb{R}^{m\times n}$，如果存在 $P \in M_m(\mathbb{R})$, $Q \in M_n(\mathbb{R})$ 且 P, Q 都可逆，使得 $A = PBQ$，则称 A 和 B 初等等价，记为 $A \sim_e B$。

下面我们先验证 $\sim_e$ 是等价关系。

(1)$\forall A \in \mathbb{R}^{m\times n}$，显然 $A = E_m A E_n$，即 $A \sim_e A$；

(2) 若 $A \sim_e B$，即存在可逆矩阵 P, Q 使得 $A = PBQ$，那么 $B = P^{-1}AQ^{-1}$，即 $B \sim_e A$；

(3) 若 $A \sim_e B$, $B \sim_e C$，即存在可逆矩阵 P, Q, S, T 使得 $A = PBQ$, $B = SCT$，则 $A = (PS)C(TQ)$，并且由推论2.5.2可知 PS, TQ 都可逆，所以 $A \sim_e C$。

命题 2.6.1. 设 $A, B \in \mathbb{R}^{m\times n}$，如果 $A \sim_e B$，则 $\operatorname{rank}(A) = \operatorname{rank}(B)$。

证明. $A \sim_e B \Longrightarrow$ 存在可逆矩阵 P, Q 使得 $A = PBQ$。由推论2.4.3即得结论。 □

下面我们定义三类初等矩阵，它们都是可逆矩阵，并且分别对应于三类初等变换。

定义 2.6.2. 将 E_n 中第 $i, j (i \neq j)$ 两行交换后得到的矩阵称为 (I) 型初等矩阵，记为 $F_{i,j}^{(n)}$(在不引起歧义时可以省略上角标 (n)，即 $F_{i,j}$，以下相同)。

显然 $F_{i,j} = E - E_{ii} - E_{jj} + E_{ij} + E_{ji}$ 并且 $F_{i,j}^2 = E$，即 $F_{i,j}$ 可逆。此外，设 $A \in \mathbb{R}^{m\times n}$，则有

$$F_{i,j}^{(m)} A = \begin{pmatrix} \mathbf{A}_1 \\ \vdots \\ \mathbf{A}_j \\ \vdots \\ \mathbf{A}_i \\ \vdots \\ \mathbf{A}_m \end{pmatrix} \qquad \text{(A 的第 i,j 行互换);}$$

$$AF_{i,j}^{(n)} = (\mathbf{A}^{(1)}, \ldots, \mathbf{A}^{(j)}, \ldots, \mathbf{A}^{(i)}, \ldots, \mathbf{A}^{(n)}) \qquad \text{(第 i,j 列互换).}$$

定义 2.6.3. 设 $\lambda \in \mathbb{R}$, $i, j \in \{1, \ldots, n\}$, $i \neq j$，将 E_n 中第 j 行乘以 λ 后加到第 i 行得到的矩阵称为 (II) 型初等矩阵，记为 $F_{i,j}^{(n)}(\lambda)$。

容易验证 $F_{i,j}(\lambda) = E + \lambda E_{ij}$，并且 $[F_{i,j}(\lambda)]^{-1} = F_{i,j}(-\lambda)$ (注意到 $E_{ij}^2 = O$, $(E + \lambda E_{ij})(E - \lambda E_{ij}) = E$)。设 $A \in \mathbb{R}^{m\times n}$，则有

$$F_{i,j}^{(m)}(\lambda) A = \begin{pmatrix} \mathbf{A}_1 \\ \vdots \\ \mathbf{A}_{i-1} \\ \mathbf{A}_i + \lambda \mathbf{A}_j \\ \mathbf{A}_{i+1} \\ \vdots \\ \mathbf{A}_m \end{pmatrix} \qquad \text{(A 的第 i 行加上第 j 行的 } \lambda \text{ 倍)}$$

$$AF_{i,j}^{(n)}(\lambda) = (\mathbf{A}^{(1)}, \ldots, \mathbf{A}^{(j)} + \lambda \mathbf{A}^{(i)}, \ldots, \mathbf{A}^{(n)}) \qquad \text{(A 的第 j 列加上第 i 列的 } \lambda \text{ 倍)}$$

定义 2.6.4. 设 $\lambda \in \mathbb{R}, \lambda \neq 0$, $i \in \{1, \ldots, n\}$，将 E_n 中第 i 行乘以 λ 得到的矩阵称为 (III) 型初等矩阵，记为 $F_i^{(n)}(\lambda)$。

显然 $F_i^{(n)}(\lambda) = E + (\lambda - 1)E_{ii}$ 并且 $[F_i^{(n)}(\lambda)]^{-1} = F_i^{(n)}(\frac{1}{\lambda})$。设 $A \in \mathbb{R}^{m \times n}$，则有

$$F_i^{(m)}(\lambda)A = \begin{pmatrix} \mathbf{A}_1 \\ \vdots \\ \lambda \mathbf{A}_i \\ \vdots \\ \mathbf{A}_m \end{pmatrix} \qquad \text{(A 的第 i 行乘以 } \lambda \text{ 倍)}$$

$$AF_{i,j}^{(n)}(\lambda) = (\mathbf{A}^{(1)}, \ldots, \lambda \mathbf{A}^{(i)}, \cdots, \mathbf{A}^{(n)}) \qquad \text{(A 的第 i 列乘以 } \lambda \text{ 倍)}$$

由以上讨论可以看到，矩阵的初等行变换就是左乘初等矩阵，矩阵的初等列变换就是右乘初等矩阵。

2.7 矩阵的求逆与秩标准型

之前我们定义了方阵的逆，但我们并没有给出具体计算逆矩阵的方法。这一节我们将会给出矩阵求逆的方法，并且定义矩阵的第一种标准型：秩标准型 (在下册我们还会学习矩阵的另外两种标准型：若尔当标准型和有理标准型)。

下面我们给出矩阵求逆的算法，并验证证明其正确性。

设 $A \in M_n(\mathbb{R})$，作 $B = (A \mid E_n)$，对 B 作初等行变换，若 $\operatorname{rank}(A) < n$，则 A 不可逆，算法结束；否则经过有限步后可将 B 中的子矩阵 A 化成 E，则此时 E 的部分就化成了 A^{-1}。这是因为对 B 作初等变换的过程等价于依次对 $(A \mid E)$ 左乘初等矩阵 $P_1, \dots, P_k$。由于 $P_k \cdots P_1 A = E$，故 $A^{-1} = P_k \cdots P_1$，而 $P_k \cdots P_1 B = (P_k \cdots P_1 A \mid P_k \cdots P_1) = (E \mid A^{-1})$。

下面我们计算一个简单的例子来加深对这个算法的理解。

例 2.7.1. 设 $A = \begin{pmatrix} 0 & 2 & 0 \\ 1 & 1 & -1 \\ 2 & 1 & -1 \end{pmatrix}$，求 A^{-1}。

解. 令 $B = \left(\begin{array}{ccc:ccc} 0 & 2 & 0 & 1 & 0 & 0 \\ 1 & 1 & -1 & 0 & 1 & 0 \\ 2 & 1 & -1 & 0 & 0 & 1 \end{array}\right)$，对 B 作以下初等行变换：

$$
\begin{aligned}
B = \left(\begin{array}{ccc:ccc} 0 & 2 & 0 & 1 & 0 & 0 \\ 1 & 1 & -1 & 0 & 1 & 0 \\ 2 & 1 & -1 & 0 & 0 & 1 \end{array}\right) &\xrightarrow{F_{1,2}} \left(\begin{array}{ccc:ccc} 1 & 1 & -1 & 0 & 1 & 0 \\ 0 & 2 & 0 & 1 & 0 & 0 \\ 2 & 1 & -1 & 0 & 0 & 1 \end{array}\right) \\
&\xrightarrow{F_{3,1}(-2)} \left(\begin{array}{ccc:ccc} 1 & 1 & -1 & 0 & 1 & 0 \\ 0 & 2 & 0 & 1 & 0 & 0 \\ 0 & -1 & 1 & 0 & -2 & 1 \end{array}\right) \xrightarrow{F_{1,3}(1)} \left(\begin{array}{ccc:ccc} 1 & 0 & 0 & 0 & -1 & 1 \\ 0 & 2 & 0 & 1 & 0 & 0 \\ 0 & -1 & 1 & 0 & -2 & 1 \end{array}\right) \\
&\xrightarrow{F_2(\frac{1}{2})} \left(\begin{array}{ccc:ccc} 1 & 0 & 0 & 0 & -1 & 1 \\ 0 & 1 & 0 & \frac{1}{2} & 0 & 0 \\ 0 & -1 & 1 & 0 & -2 & 1 \end{array}\right) \xrightarrow{F_{3,2}(1)} \left(\begin{array}{ccc:ccc} 1 & 0 & 0 & 0 & -1 & 1 \\ 0 & 1 & 0 & \frac{1}{2} & 0 & 0 \\ 0 & 0 & 1 & \frac{1}{2} & -2 & 1 \end{array}\right) \\
&= \left(\begin{array}{ccc:ccc} \multicolumn{3}{c:}{\multirow{2}{*}{$\underbrace{\qquad\qquad}_{E}$}} & \multicolumn{3}{c}{\multirow{2}{*}{$\underbrace{\qquad\qquad}_{A^{-1}}$}} \\ & & & & & \\ \end{array}\right)
\end{aligned}
$$

这样我们就计算出了 A^{-1} 并且知道 $A^{-1} = F_{3,2}(1)F_2(\frac{1}{2})F_{1,3}(1)F_{3,1}(-2)F_{1,2}$。 □

定理 2.7.1. 设 $A \in \mathbb{R}^{m\times n}$，$\operatorname{rank}(A) = r$，则存在 $P \in M_m(\mathbb{R})$，$Q \in M_n(\mathbb{R})$ 使得

(i)P, Q 都是有限个初等矩阵的乘积；

(ii)$PAQ = \begin{pmatrix} E_r & O \\ O & O \end{pmatrix}_{m\times n}$。我们把 A 对应的 $\begin{pmatrix} E_r & O \\ O & O \end{pmatrix}_{m\times n}$ 称为 A 的秩标准型。

证明. 利用定理2.2.1的证明过程，我们知道存在若干个 (I)、(II) 型初等矩阵 $P_1, \dots, P_s$ 和 $Q_1, \dots, Q_t$ 使得 $P_s \cdots P_1 A Q_1 \cdots Q_s = \begin{pmatrix} \Lambda & O \\ O & O \end{pmatrix}$，其中 Λ 是 $r \times r$ 阶的对角矩阵。于是存在 r 个 (III) 型初等矩阵 $P_{s+1}, \dots, P_{s+r}$ 使得 $P_{s+r} \cdots P_1 A Q_1 \cdots Q_s = \begin{pmatrix} E_r & O \\ O & O \end{pmatrix}$。 □

现在我们可以讲清楚定义2.6.1中等价关系的等价类是什么了。

推论 2.7.1. $\mathbb{R}^{m\times n}/\sim_e = \left\{ \begin{pmatrix} E_r & O \\ O & O \end{pmatrix} \;\middle|\; r = 0, \dots, \min(m, n) \right\}$。

定理2.7.1也告诉我们，可逆矩阵一定可以写成若干个初等矩阵的积。

2.8 矩阵的分块

引理 2.8.1. 设 $A \in \mathbb{R}^{m\times s}$, $B \in \mathbb{R}^{s\times n}$, 则

(i) 若 $A = \begin{pmatrix} A' \\ A'' \end{pmatrix}$, 则 $AB = \begin{pmatrix} A'B \\ A''B \end{pmatrix}$;

(ii) 若 $B = (B', B'')$, 则 $AB = (AB', AB'')$。

利用矩阵乘法的定义验证即可，留作练习。

引理 2.8.2. 设 $A \in \mathbb{R}^{m\times s}$, $B \in \mathbb{R}^{s\times n}$, 并且有如下分块：

$$A = \begin{pmatrix} A_1 \\ \vdots \\ A_p \end{pmatrix}, \quad B = (B_1, \ldots, B_q).$$

则

1. $AB = \begin{pmatrix} A_1B \\ \vdots \\ A_pB \end{pmatrix} = (AB_1, \ldots, AB_q)$;

2. $AB = \begin{pmatrix} A_1B_1 & \cdots & A_1B_q \\ \vdots & \vdots & \vdots \\ A_pB_1 & \cdots & A_pB_q \end{pmatrix}$。

这是引理2.8.1的自然推广，用矩阵乘法的定义即可验证它。

引理 2.8.3. 设 $A \in \mathbb{R}^{m\times s}$, $B \in \mathbb{R}^{s\times n}$, 令 $A = (A_1,\ A_2)$, $A_1 \in \mathbb{R}^{m\times s_1}$, $A_2 \in \mathbb{R}^{m\times s_2}$, $B = \begin{pmatrix} B_1 \\ B_2 \end{pmatrix}$, $B_1 \in \mathbb{R}^{s_1\times n}$, $B_2 \in \mathbb{R}^{s_2\times n}$, 则 $AB = (A_1,\ A_2)\begin{pmatrix} B_1 \\ B_2 \end{pmatrix} = A_1B_1 + A_2B_2$。

同样用矩阵乘法的定义即可验证。

引理 2.8.4. 设 $A \in \mathbb{R}^{m\times s}$, $B \in \mathbb{R}^{s\times n}$, 令 $A = (A_1, \ldots, A_p)$, $A_l \in \mathbb{R}^{m\times s_l}$, $B = \begin{pmatrix} B_1 \\ \vdots \\ B_p \end{pmatrix}$, $B_l \in \mathbb{R}^{s_l\times n}$, 则

$$AB = (A_1, \ldots, A_p)\begin{pmatrix} B_1 \\ \vdots \\ B_p \end{pmatrix} = A_1B_1 + \cdots + A_pB_p。$$

有了以上引理，我们很容易证明矩阵的分块 (只要是合适的，即分出的块可以做运算) 是保持运算的。

定理 2.8.1. 设 $A \in \mathbb{R}^{m\times s}$, $B \in \mathbb{R}^{s\times n}$, 令 $A = (A_{ik})$, $A_{ik} \in \mathbb{R}^{m_i\times s_k}$, $B = (B_{kj})$, $B_{kj} \in \mathbb{R}^{s_k\times n_j}$, 其中 $i = 1, \ldots, p$, $k = 1, \cdots l$, $j = 1, \ldots, q$。则 $AB = (C_{ij})$, 其中 $C_{ij} = A_{i1}B_{1j} + \cdots + A_{il}B_{lj}$。

例 2.8.1. 设 $D = \begin{pmatrix} D_1 & & \\ & \ddots & \\ & & D_k \end{pmatrix}$, 其中 $D_i \in M_{n_i}(\mathbb{R})$, 则 $D^m = \begin{pmatrix} D_1^m & & \\ & \ddots & \\ & & D_k^m \end{pmatrix}$。

例 2.8.2 (矩阵的乘法分解). 设 $A \in \mathbb{R}^{m\times n}$ 且 $\operatorname{rank}(A) = r > 0$，则存在 $B \in \mathbb{R}^{m\times r}$，$C \in \mathbb{R}^{r\times n}$ 使得 $A = BC$ 并且 $\operatorname{rank}(B) = \operatorname{rank}(C) = r$。

证明. 由定理2.7.1，存在可逆矩阵 $P \in M_m(\mathbb{R})$，$Q \in M_n(\mathbb{R})$ 使得

$$A = P\begin{pmatrix} E_r & O \\ O & O \end{pmatrix}Q = P\begin{pmatrix} E_r \\ O \end{pmatrix}(E_r,\ O)Q.$$

取 $B = P\begin{pmatrix} E_r \\ O \end{pmatrix}$，$C = (E_r,\ O)Q$，则 $A = BC$ 且 $\operatorname{rank}(B) = \operatorname{rank}(C) = r$，即可。 □

下面的引理常用来证明秩不等式。

引理 2.8.5. 设 $A \in \mathbb{R}^{m\times n}$，$B \in \mathbb{R}^{k\times l}$，$C \in \mathbb{R}^{k\times n}$，则 $\operatorname{rank}\begin{pmatrix} A & O \\ C & B \end{pmatrix} \geqslant \operatorname{rank}(A) + \operatorname{rank}(B)$，当 $C = O$ 时等号成立。

证明. 不妨设 $\mathbf{A}^{(1)}, \ldots, \mathbf{A}^{(p)}$ 是 $V_c(A)$ 的基，$\mathbf{B}^{(1)}, \cdots, \mathbf{B}^{(q)}$ 是 $V_c(B)$ 的基。则对 $M = \begin{pmatrix} A & O \\ C & B \end{pmatrix}$ 的相对应的 $p + q$ 列而言，若 $\sum_{i=1}^{p} \alpha_i \mathbf{M}^{(i)} + \sum_{j=1}^{q} \beta_j \mathbf{M}^{(j)} = \mathbf{0}$，即

$$\alpha_1\begin{pmatrix} \mathbf{A}^{(1)} \\ \mathbf{C}^{(1)} \end{pmatrix} + \cdots + \alpha_p\begin{pmatrix} \mathbf{A}^{(p)} \\ \mathbf{C}^{(p)} \end{pmatrix} + \beta_1\begin{pmatrix} \mathbf{0} \\ \mathbf{B}^{(1)} \end{pmatrix} + \cdots + \beta_q\begin{pmatrix} \mathbf{0} \\ \mathbf{B}^{(q)} \end{pmatrix} = \begin{pmatrix} \mathbf{0} \\ \mathbf{0} \end{pmatrix}. \tag{2.8.1}$$

所以 $\sum_{i=1}^{p} \alpha_i \mathbf{M}^{(i)} = \mathbf{0}$，由 $\mathbf{A}^{(1)}, \ldots, \mathbf{A}^{(p)}$ 是基即得 $\alpha_1 = \cdots = \alpha_p = 0$。再代回 (2.8.1) 式即得 $\sum_{j=1}^{q} \beta_j \mathbf{M}^{(j)} = \mathbf{0}$，于是 $\beta_1 = \cdots = \beta_q = 0$。所以 $\mathbf{M}^{(1)}, \ldots, \mathbf{M}^{(p)}, \mathbf{M}^{(n+1)}, \ldots, \mathbf{M}^{(n+q)}$ 线性无关。那么就有 $\operatorname{rank}(M) \geqslant p + q = \operatorname{rank}(A) + \operatorname{rank}(B)$。
特别地，当 $C = O$ 时，$\forall j \in \{1, 2, \ldots, n + l\}$，由于

$$\begin{aligned} \mathbf{M}^{(j)} \in &< \mathbf{M}^{(1)}, \ldots, \mathbf{M}^{(p)} > + < \mathbf{M}^{(n+1)}, \ldots, \mathbf{M}^{(n+q)} > \\ = &< \mathbf{M}^{(1)}, \ldots, \mathbf{M}^{(p)}, \mathbf{M}^{(n+1)}, \ldots, \mathbf{M}^{(n+q)} > . \end{aligned}$$

即 $\operatorname{rank}(M) \leqslant p + q$。于是此时只能有 $\operatorname{rank}(M) = \operatorname{rank}(A) + \operatorname{rank}(B)$。 □

例 2.8.3. 用上面的引理证明定理2.4.3(Sylvester 不等式)。

证明. 令 $M = \begin{pmatrix} AB & O \\ O & E_s \end{pmatrix}$，$R = \begin{pmatrix} O & A \\ -B & E_s \end{pmatrix}$，$P = \begin{pmatrix} E_m & A \\ O & E_s \end{pmatrix}$，$Q = \begin{pmatrix} E_n & O \\ -B & E_s \end{pmatrix}$，则 $R = PMQ$ 且 P, Q 满秩，注意到 $\operatorname{rank}(M) = \operatorname{rank}(AB) + s$，而由引理2.8.5有 $\operatorname{rank}(R) \geqslant \operatorname{rank}(A) + \operatorname{rank}(B)$，因此

$$\operatorname{rank}(AB) = \operatorname{rank}(M) - s = \operatorname{rank}(R) - s \geqslant \operatorname{rank}(A) + \operatorname{rank}(B) - s.$$

即得结论。 □

2.9 线性流形 (线性方程组解的结构)

在本章的最后，我们从线性映射的角度重新认识线性方程组。

引理 2.9.1. 设 $V \subset \mathbb{R}^n$ 是 d 维子空间，则 V 是某个 n 元齐次方程组的解空间。

证明. 若 $V = \{\mathbf{0}\}$，则 $V = V_E$(记号出自定义2.3.3)。否则，设 $\mathbf{v}_1, \dots, \mathbf{v}_d$ 是 V 的一组基，则由基扩充定理，它们可以扩充成 $\mathbb{R}^n$ 的一组基 $\mathbf{v}_1, \dots, \mathbf{v}_d, \mathbf{v}_{d+1}, \dots, \mathbf{v}_n$。那么，由线性映射基本定理，存在 $\varphi : \mathbb{R}^n \to \mathbb{R}^n$ 满足

$$\varphi(\mathbf{v}_i) = \mathbf{0},\ i = 1, \dots, d; \qquad \varphi(\mathbf{v}_j) = \mathbf{v}_j,\ j = d+1, \dots, n.$$

于是 $\dim(\mathrm{im}(\varphi)) = n - d$ ($\mathrm{im}(\varphi) =< \mathbf{v}_{d+1}, \dots, \mathbf{v}_n >$)，那么由对偶定理，$\dim(\ker(\varphi)) = d$，所以 $V = \ker(\varphi)$(由 φ 的构造显然有 $V \subset \ker(\varphi)$)。因此，设 A 是 φ 在 $\mathbb{R}^n$ 的标准基下的矩阵表示，则有 $V = V_A$。 □

定义 2.9.1. 设 $\mathbf{v} \in \mathbb{R}^n$，$V \subset \mathbb{R}^n$ 是子空间，则我们称 $\mathbf{v} + V = \{\mathbf{v} + \mathbf{x} \mid \mathbf{x} \in V\}$ 是一个线性流形。

定理 2.9.1. $S \subset \mathbb{R}^n$ 是线性流形 $\iff$ S 是 n 元线性方程组的解集。

证明. ($\Longleftarrow$) 只需注意到齐次线性方程组的解集是子空间，而由命题1.2.1，非齐次线性方程组的解是特解加上齐次方程组的解。于是线性方程组的解集符合线性流形的定义。
($\Longrightarrow$) 设 $S = \mathbf{v} + V$，则由上面的引理，存在列数为 n 的矩阵使得 $V = V_A$。记 $\mathbf{w} = A\mathbf{v}$，则对 $\forall \mathbf{x} = \mathbf{v} + \mathbf{y} \in S$，有 $A\mathbf{y} = 0$，从而 $A\mathbf{x} = A\mathbf{v} = \mathbf{w}$，即 S 中的元素都是方程组 $A\mathbf{x} = \mathbf{w}$ 的解。 □

定义 2.9.2. 设线性流形 $S = \mathbf{v} + V$ 是某个 n 元线性方程组的解集，则我们称 V 的一组基为该方程组的一个**基础解系**，称 $\mathbf{v}$ 为该方程组的一个**特解**。

定理2.9.1告诉我们，求解线性方程组只需要求出基础解系和一个特解即可。

例 2.9.1. 求解方程组 $\begin{cases} x_1 + x_2 - x_3 = 1 \\ x_1 - x_2 + x_3 = 2 \\ 2x_1 = 3 \end{cases}$.

解. 方程组的一个特解为 $\begin{cases} x_1 = \frac{3}{2} \\ x_2 = 1 \\ x_3 = \frac{3}{2} \end{cases}$，对应齐次方程组的解空间为 $< \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} >$。于是解流形为 $\left\{(\frac{3}{2}, 1, \frac{3}{2})^t + \lambda(0,1,1)^t \mid \lambda \in \mathbb{R}\right\}$。 □

定义 2.9.3. 设 $\mathbf{v} + V$ 是 $\mathbb{R}^n$ 中的线性流形，如果 $\dim V = n - 1$，则称 $\mathbf{v} + V$ 是超平面 (hyperplane)。

推论 2.9.1. $P \subset \mathbb{R}^n$ 是超平面 $\iff$ $\exists \alpha_1, \dots, \alpha_n \in \mathbb{R}$ 不全为 0 以及 $\beta \in \mathbb{R}$ 使得 P 是 $\alpha_1 x_1 + \cdots + \alpha_n x_n = \beta$ 在 $\mathbb{R}^n$ 中的解集。

证明. ($\Longleftarrow$) 因为 $\alpha_1, \dots, \alpha_n$ 不全为 0，故 $\mathrm{rank}(\alpha_1, \dots, \alpha_n) = 1$，并且 $\mathrm{rank}(\alpha_1, \dots, \alpha_n, \beta) = 1$，于是方程 $\alpha_1 x_1 + \cdots + \alpha_n x_n = \beta$ 的解为 $\mathbf{v} + V$，其中 $\dim V = n - 1$。
($\Longrightarrow$) 设 $P = \mathbf{v} + V$，$\dim V = n - 1$，则由引理2.9.1，存在列数为 n 的矩阵 A 使得 $V = V_A$，$\dim V_A = n - 1$，则由对偶定理，$\mathrm{rank}(A) = 1$。那么可设 $(\alpha_1, \dots, \alpha_n)$ 是 A 的非零行，即 $V = V_{(\alpha_1, \dots, \alpha_n)}$。则由定理2.9.1可得 P 是 $\alpha_1 x_1 + \cdots + \alpha_n x_n = \beta$ 的解，其中 $\beta = (\alpha_1, \dots, \alpha_n)\mathbf{v}$。 □

例 2.9.2. 求过点 $(1,0,0)^t$, $(0,1,0)^t$, $(0,0,1)^t$ 的平面方程。

解. 设方程为 $\alpha_1 x_1 + \alpha_2 x_2 + \alpha_n x_n = \beta$，代入点得到 $\alpha_1 = \alpha_2 = \alpha_3 = \beta$，取 $\beta = 1$ 即得到该平面的一个方程为 $x_1 + x_2 + x_3 = 1$。 □

2.10 习题

向量

1. 验证命题2.1.1.

2. 验证命题2.1.5中定义的线性包络确实是子空间，并证明推论2.1.4.

3. 验证推论2.1.5.

4. 解向量方程: $3(\mathbf{x}_1-\mathbf{x})+2(\mathbf{x}_2+\mathbf{x})=5(\mathbf{x}_3+\mathbf{x})$, 其中

$$\mathbf{x}_1=(2,5,1,3),\quad \mathbf{x}_2=(10,1,5,10),\quad \mathbf{x}_3=(4,1,-1,1).$$

5. 判断下列向量组是否线性无关, 并计算这些向量组的线性包络的维数.
   (1) $\mathbf{x}_1=(1,2,3),\mathbf{x}_2=(2,-1,3)$;
   (2) $\mathbf{x}_1=(2,3,-1),\mathbf{x}_2=(3,5,2),\mathbf{x}_3=(-2,4,1)$;
   (3) $\mathbf{x}_1=(4,-5,2,6),\mathbf{x}_2=(2,-2,1,3),\mathbf{x}_3=(6,-3,3,9)$;
   (4) $\mathbf{x}_1=(4,-5,2,6),\mathbf{x}_2=(2,-2,1,3),\mathbf{x}_3=(5,-3,3,9),\mathbf{x}_4=(4,-1,5,6)$.

6. 假设向量 $\mathbf{x}_1,\mathbf{x}_2,\ldots,\mathbf{x}_k$ 线性无关. 判断下列向量组是否线性相关, 并计算这些向量组的线性包络的维数.
   (1)

$$\begin{cases}\mathbf{y}_1=3\mathbf{x}_1+2\mathbf{x}_2+\mathbf{x}_3+\mathbf{x}_4,\\ \mathbf{y}_2=2\mathbf{x}_1+5\mathbf{x}_2+3\mathbf{x}_3+2\mathbf{x}_4,\\ \mathbf{y}_3=3\mathbf{x}_1+4\mathbf{x}_2-\mathbf{x}_3+2\mathbf{x}_4\end{cases};$$

   (2) $\mathbf{y}_1=\mathbf{x}_1+\mathbf{x}_2,\mathbf{y}_2=\mathbf{x}_2+\mathbf{x}_3,\mathbf{y}_3=\mathbf{x}_3+\mathbf{x}_4,\cdots,\mathbf{y}_{k-1}=\mathbf{x}_{k-1}+\mathbf{x}_k,\mathbf{y}_k=\mathbf{x}_k+\mathbf{x}_1$;
   (3) $\mathbf{y}_1=\mathbf{x}_1-\mathbf{x}_2,\mathbf{y}_2=\mathbf{x}_2-\mathbf{x}_3,\mathbf{y}_3=\mathbf{x}_3-\mathbf{x}_4,\cdots,\mathbf{y}_{k-1}=\mathbf{x}_{k-1}-\mathbf{x}_k,\mathbf{y}_k=\mathbf{x}_k-\mathbf{x}_1$.

7. 求 λ 使得向量 $(7,-2,\lambda)$ 是向量 $(2,3,5),(3,7,8),(1,-6,1)$ 的线性组合.

8. 证明, $\mathbb{R}^n$ 中的向量组 $\mathbf{x}_1,\ldots,\mathbf{x}_n$ 生成 $\mathbb{R}^n$, 当且仅当它们是线性无关的.

9. 设 $\mathbf{v}_1=(x_{11},\ldots,x_{m1})^t,\ldots,\mathbf{v}_n=(x_{1n},\ldots,x_{mn})^t$ 是 $\mathbb{R}^m$ 中的 n 个线性无关的向量, 试证明: 其任意一组延长向量 $\mathbf{u}_1=(x_{11},\ldots,x_{m1},y_{11},\ldots,y_{k1})^t,\ldots\ldots,\mathbf{u}_n=(x_{1n},\ldots,x_{mn},y_{1n},\ldots,y_{kn})^t$ 也在 $\mathbb{R}^{m+k}$ 中线性无关.

10. 设 U 和 V 都是 $\mathbb{R}^n$ 的子空间, 试证明:
    (1) $U+V$ 是同时包含 U 和 V 的最小的子空间;
    (2) $U\cup V$ 是子空间 $\iff U\subset V$ 或 $V\subset U$.

11. 设在 $\mathbb{R}^n$ 中 $\operatorname{span}\{\mathbf{u}_1,\ldots,\mathbf{u}_s\}$ 的维数是 r, 在 $\mathbf{u}_1,\ldots,\mathbf{u}_s$ 中任取 m 个向量 $\mathbf{u}_{i_1},\ldots,\mathbf{u}_{i_m}$, 试证明:

$$\dim(\operatorname{span}\{\mathbf{u}_{i_1},\ldots,\mathbf{u}_{i_m}\})\geqslant r+m-s.$$

12. 设 $\mathbf{u}_1,\ldots,\mathbf{u}_s$ 和 $\mathbf{v}_1,\ldots,\mathbf{v}_t$ 是 $\mathbb{R}^n$ 中的两个向量组，并且这两个向量组内部都线性无关. 此外，每个 $\mathbf{u}_i$ 都不能写成 $\mathbf{v}_1,\ldots,\mathbf{v}_t$ 的线性组合，每个 $\mathbf{v}_j$ 也不能写成 $\mathbf{u}_1,\ldots,\mathbf{u}_s$ 的线性组合。试举出反例：合并的向量组 $\mathbf{u}_1,\ldots,\mathbf{u}_s,\mathbf{v}_1,\ldots,\mathbf{v}_t$ 可以是线性相关的! 这说明验证线性无关性必须按照定义，不可以使用一些”想当然”的办法.

矩阵的秩

1. 证明定理2.2.3.

2. 计算下列矩阵的秩.

$$(1)\begin{pmatrix} 2 & 5 & 6 & -1 & 1 \\ -4 & 3 & 5 & 2 & 0 \\ 3 & 2 & 7 & 1 & 8 \end{pmatrix};\ (2)\begin{pmatrix} 8 & -4 & 5 & 5 & 9 \\ 1 & -3 & -5 & 0 & 7 \\ 7 & -5 & 1 & 4 & 1 \\ 3 & -1 & 3 & 2 & 5 \end{pmatrix};$$

$$(3)\begin{pmatrix} 1 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 1 \end{pmatrix};\ (4)\begin{pmatrix} 1 & x & -1 & 2 \\ 2 & -1 & x & 5 \\ 1 & 10 & -6 & 1 \end{pmatrix}(x \text{ 是变量 });$$

3. 证明若 $a_0 \neq 0$, 则方阵

$$\begin{pmatrix} a_0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ a_1 & 0 & 0 & \cdots & 0 & 0 & 1 \\ a_2 & 0 & 0 & \cdots & 0 & 1 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ a_{n-1} & 0 & 1 & \cdots & 0 & 0 & 0 \\ a_n & 1 & 0 & \cdots & 0 & 0 & 0 \end{pmatrix}$$

的秩为 $n+1$.

4. 本题给出矩阵行秩等于列秩的另一个证明, 不用初等变换. 设 $m \times n$ 矩阵 $A = \left(a_{ij}\right)$ 的行秩为 r, 列秩为 s. 取 A 的 r 个线性无关的行向量 $\mathbf{A}_{i_1}, \mathbf{A}_{i_2}, \cdots, \mathbf{A}_{i_r}$. 这 r 个行向量形成一个 $r \times n$ 矩阵 $\tilde{A}$ 设 $\tilde{A}$ 的列秩为 $t, \tilde{\mathbf{A}}^{(j_1)}, \tilde{\mathbf{A}}^{(j_2)}, \cdots, \tilde{\mathbf{A}}^{(j_t)}$ 是 $\tilde{A}$ 的列向量的极大线性无关组. 证明:

(1) $t \leqslant r$.

(2) 矩阵 A 的任何一个列向量 $\mathbf{A}^{(j)}$ 都是列向量 $\mathbf{A}^{(j_1)}, \mathbf{A}^{(j_2)}, \ldots, \mathbf{A}^{(j_t)}$ 的线性组合, 从而 $s \leqslant t \leqslant r$, 即列秩不超过行秩 (提示: 利用 A 的任一行向量都是 $\mathbf{A}_{i_1}, \mathbf{A}_{i_2}, \ldots, \mathbf{A}_{i_r}$ 的线性组合).

(3) 对 $n \times m$ 矩阵

$$A^t = \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{m1} \\ a_{12} & a_{22} & \cdots & a_{m2} \\ \vdots & \vdots & & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{mn} \end{pmatrix},$$

有 $\dim V_c(A^t) = \dim V_r(A), \dim V_r(A^t) = \dim V_c(A)$. 结合 (2) 与 (3) 便知 $s \leqslant r, r \leqslant s$, 所以 $r = s$.

5. 设 $A = (a_{ij})_{m\times n} \in \mathbb{R}^{m\times n}$ $(m \leqslant n)$ 满足: $|a_{jj}| > \sum_{i=1, i\neq j}^{m} |a_{ij}|$, $\forall j = 1, \ldots, m$. 求证: $\operatorname{rank}(A) = m$. 这种矩阵被称为严格对角占优矩阵.

线性映射, 矩阵的运算, 方阵

1. 在下述映射中, 哪些是线性映射:
   a) $(x_1, x_2, \cdots, x_n)^t \mapsto (x_n, \cdots, x_2, x_1)^t$;
   b) $(x_1, x_2, \cdots, x_n)^t \mapsto \left(x_1, x_2^2, \cdots, x_n^n\right)^t$;
   c) $(x_1, x_2, \cdots, x_n)^t \mapsto (x_1, x_1 + x_2, \cdots, x_1 + x_2 + \cdots + x_n)^t$.

2. 证明命题2.4.1和命题2.4.3.

3. 验证矩阵的加法、数乘和乘法所满足的运算律.

4. 证明
$$\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}^m = \begin{pmatrix} 1 & ma & \frac{m(m-1)}{2}ab + mc \\ 0 & 1 & mb \\ 0 & 0 & 1 \end{pmatrix}$$
   求矩阵
$$\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}$$
   的逆矩阵.

5. 验证 $\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}^3 = E$.

6. 马尔可夫 (或随机) 矩阵在应用中十分重要:
$$P = \left(p_{ij}\right), \quad p_{ij} \geqslant 0, \quad \sum_{i=1}^{n} p_{ij} = 1, \quad i = 1, 2, \cdots, n.$$
   由马尔可夫矩阵确定的线性变换 φ_P 通常作用于概率列向量:
$$X = (x_1, \cdots, x_n)^t, \quad x_i \geqslant 0, \quad \sum_{i=1}^{n} x_i = 1.$$
   求证:
   a) 矩阵 $P \in M_n(\mathbb{R})$ 是马尔可夫的, 当且仅当对任意概率向量 X, PX 仍然是概率向量 (此处 $PX = \varphi_P(X)$).
   b) 如果 P 是正的马尔可夫矩阵 (即 $\forall i, j, \quad p_{ij} > 0$), 那么任意概率向量 X 对应到正的概率向量 PX (所有的分量严格大于 0).
   c) 如果 P 和 Q 都是马尔可夫矩阵, 那么矩阵 PQ 也是马尔可夫矩阵. 特别地, 马尔可夫矩阵的任意次方幂 P^k 是马尔可夫矩阵.

7. 若
$$H = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix},$$
   求 $H^t \cdot H$.

8. 由 S_n 中的 n 阶循环确定的置换矩阵 (行单位阵 E_n) 为

$$P=\begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix},$$

验证 $P^n = E$.

9. 对于任意两个 $m \times n$ 矩阵 A 和 B, 证明

$$\operatorname{rank}(A+B) \leqslant \operatorname{rank} A + \operatorname{rank} B.$$

10. 对于任意的 $m \times s$ 矩阵 A 和 $s \times n$ 矩阵 B, 证明

$$\operatorname{rank} A + \operatorname{rank} B - s \leqslant \operatorname{rank} AB.$$

11. 设 A, B, C 是 n 阶方阵, 若 $ABC = 0$, 则

$$\operatorname{rank} A + \operatorname{rank} B + \operatorname{rank} C \leqslant 2n.$$

12. 设 A, B, C 是 n 阶方阵, 证明

$$\operatorname{rank}(AB) + \operatorname{rank}(BC) \leqslant \operatorname{rank}(ABC) + \operatorname{rank}(B).$$

13. 设 A, B 是 n 阶方阵且 $AB = BA$, 证明

$$\operatorname{rank}(A) + \operatorname{rank}(B) \geqslant \operatorname{rank}(A+B) + \operatorname{rank}(AB).$$

14. 求矩阵

$$A=\begin{pmatrix} x_1y_1 & x_1y_2 & \cdots & x_1y_n \\ x_2y_1 & x_2y_2 & \cdots & x_2y_n \\ \cdots\cdots & \cdots & \cdots & \cdots \\ x_ny_1 & x_ny_2 & \cdots & x_ny_n \end{pmatrix}$$

的秩。(提示: $A = (x_1, \cdots, x_n)^t \cdot (y_1, \cdots, y_n)$.)

矩阵的等价, 求逆, 分块, 线性方程组解的结构

1. 称 $A = \left(a_{ij}\right)$ 是对称矩阵 (symmetric matrix)(或斜对称矩阵, anti-symmetric matrix), 若 $a_{ij} = a_{ji}$ (相对应地, $a_{ij} = -a_{ji}$). 证明: 若对称矩阵 (或斜对称矩阵)A 可逆, 则 A^{-1} 也是对称矩阵 (或斜对称矩阵).

2. 设

$$A=\begin{pmatrix}5&4&3&2&1\\4&8&6&4&2\\3&6&9&6&3\\2&4&6&8&4\\1&2&3&4&5\end{pmatrix},\quad F=\begin{pmatrix}2&3&2&1\\3&6&4&2\\4&8&6&3\\2&4&3&2\end{pmatrix}$$

求 A^{-1} 和 F^{-1}.

3. 设 n 阶方阵 A 满足 $A^n=O$, n 阶方阵 X 满足 $AX-X+A=O$. 试将 X 写成关于 A 的表达式.

4. 验证

$$A=\begin{pmatrix}a&b\\c&d\end{pmatrix}, ad-bc\neq 0\Longrightarrow A^{-1}=\frac{1}{ad-bc}\begin{pmatrix}d&-b\\-c&a\end{pmatrix}.$$

特别地,

$$ad-bc=1\Rightarrow A^{-1}=\begin{pmatrix}d&-b\\-c&a\end{pmatrix}.$$

如果 $ad-bc=0, A^{-1}$ 存在吗?

5. 证明任意二阶矩阵

$$A=\begin{pmatrix}a&b\\c&d\end{pmatrix}$$

满足关系式

$$A^2=(a+d)A-(ad-bc)E$$

(换言之, A 是二次方程 $x^2-(a+d)x+(ad-bc)=0$ 的一个“根”).

6. 如果 $ad-bc\neq 0$, 运用上题求逆矩阵 A^{-1}.

7. 证明若 $\begin{pmatrix}a&b\\c&d\end{pmatrix}^m=0$, 则 $\begin{pmatrix}a&b\\c&d\end{pmatrix}^2=0$.

8. 证明秩 r 的每个矩阵能表示成 r 个秩 1 的矩阵的和, 但是不能表示成小于 r 个的和.

9. 验证引理2.8.1至引理2.8.4, 即证明分块矩阵的运算规则与普通矩阵是相同的.

10. 设 A,B 是 n 阶方阵, 证明

$$\operatorname{rank}(A-ABA)=\operatorname{rank}(A)+\operatorname{rank}(E-BA)-n.$$

11. 设 A 和 B 是 n 阶方阵. 证明:

$$\operatorname{rank}\begin{pmatrix}A&AB\\B&B+B^2\end{pmatrix}=\operatorname{rank}(A)+\operatorname{rank}(B)$$

12. 求下列方阵的逆矩阵:

$$\begin{pmatrix} A & C \\ O & D \end{pmatrix}, \quad \begin{pmatrix} A & B & C \\ O & D & G \\ O & O & F \end{pmatrix}, \quad \begin{pmatrix} O & O & A \\ O & D & B \\ F & G & C \end{pmatrix},$$

其中 A, D, F 是可逆方阵.

13. 设 A 和 B 是方阵. 证明: 如果 $E + AB$ 可逆, 那么 $E + BA$ 可逆.

14. 对同阶方阵 A 和 B, 其交换子定义为 $[A, B] = AB - BA$. 现设 C 也是同阶方阵. 证明:
(1) $[A, BC] = [A, B]C + B[A, C]$;
(2) $[[A, B], C] + [[B, C], A] + [[C, A], B] = O$.

15. 求解线性方程组:

$$\begin{cases} x_1 + x_2 + x_3 + x_4 + x_5 = 0 \\ 3x_1 + 2x_2 + x_3 + x_4 - 3x_5 = 0 \\ x_2 + 2x_3 + 2x_4 + 6x_5 = 0 \\ 5x_1 + 4x_2 + 3x_3 + 3x_4 - x_5 = 0. \end{cases}$$

第三章　行列式

行列式的定义

在第一章中我们已经定义了二阶和三阶的行列式 (determinant)，现在我们来定义一般的行列式并探讨其性质。

定义 3.0.1. 设

$$\begin{aligned} f : \underbrace{\mathbb{R}^n \times \cdots \times \mathbb{R}^n}_{\text{m 个}} &\longrightarrow \mathbb{R} \\ (\mathbf{x}_1, \ldots, \mathbf{x}_m) &\longmapsto f(\mathbf{x}_1, \ldots, \mathbf{x}_m) \end{aligned}.$$

称 f 是 m 重线性函数，如果对 $\forall \alpha, \beta \in \mathbb{R}$, $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$, $k \in \{1, \ldots, m\}$，固定除 $\mathbf{x}_k$ 之外的变元，有：

$$f(\mathbf{x}_1, \ldots, \mathbf{x}_{k-1}, \alpha\mathbf{u}+\beta\mathbf{v}, \mathbf{x}_{k+1}, \ldots, \mathbf{x}_m) = \alpha f(\mathbf{x}_1, \ldots, \mathbf{x}_{k-1}, \mathbf{u}, \mathbf{x}_{k+1}, \ldots, \mathbf{x}_m)+\beta f(\mathbf{x}_1, \ldots, \mathbf{x}_{k-1}, \mathbf{v}, \mathbf{x}_{k+1}, \ldots, \mathbf{x}_m).$$

即若任意地固定 $m-1$ 个变元后 f 是线性函数，则 f 是多重线性函数。

例 3.0.1. (1) 设 $\mathbf{x} = (x_1, \ldots, x_n)^t \in \mathbb{R}^n$，$m = 1$ 时 $f(\mathbf{x}) = \alpha_1 x_1 + \cdots + \alpha_n x_n$ 回到了线性函数的情形。
(2)$m = 2$ 时考虑下面的多元函数：

$$\begin{aligned} f : \mathbb{R}^2 \times \mathbb{R}^2 &\longrightarrow \mathbb{R} \\ \left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}\right) &\longmapsto \begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix} = x_1 y_2 - x_2 y_1. \end{aligned}$$

容易验证这是一个二重线性函数。

设 $\mathbf{e}^{(1)}, \ldots, \mathbf{e}^{(n)}$ 是 $\mathbb{R}^n$ 的标准基。则每个变元 (向量)

$$\mathbf{x}_k = x_{1k}\mathbf{e}^{(1)} + \ldots + x_{nk}\mathbf{e}^{(n)} = \sum_{i=1}^{n} x_{ik}\mathbf{e}^{(i)}.$$

由 f 的多重线性性质，我们可以对 f 作如下展开 (建议初学者耐心推导)：

$$\begin{aligned} f(\mathbf{x}_1, \ldots, \mathbf{x}_m) &= f(\sum_{i_1=1}^{n} x_{i_1 1}\mathbf{e}^{(i_1)}, \mathbf{x}_2, \ldots, \mathbf{x}_m) \\ &= \sum_{i_1=1}^{n} x_{i_1 1} f(\mathbf{e}^{(i_1)}, \sum_{i_2=1}^{n} x_{i_2 2}\mathbf{e}^{(i_2)}, \ldots, \mathbf{x}_m) \\ &= \sum_{i_1=1}^{n} x_{i_1 1} \sum_{i_2=1}^{n} x_{i_2 2} f(\mathbf{e}^{(i_1)}, \mathbf{e}^{(i_2)}, \sum_{i_3=1}^{n} x_{i_3 3}\mathbf{e}^{(i_3)}, \cdots, \mathbf{x}_m) \\ &\quad \vdots \\ &= \sum_{i_1=1}^{n} \sum_{i_2=1}^{n} \cdots \sum_{i_m=1}^{n} x_{i_1 1} x_{i_2 2} \cdots x_{i_m m} f(\mathbf{e}^{(i_1)}, \ldots, \mathbf{e}^{(i_m)}). \end{aligned} \tag{3.0.1}$$

实际上，我们刚刚的推导是在取定一组基后，将张量展开成坐标形式。张量的内容我们会在下册简单介绍。

定义 3.0.2. 设 $f(\mathbf{x}_1,\dots,\mathbf{x}_m)$ 是 m 重线性函数，如果 $\forall i,j\in\{1,\dots,m\},i\neq j$，有 $f(\mathbf{x}_1,\dots,\mathbf{x}_j,\dots,\mathbf{x}_i,\dots,\mathbf{x}_m)=f(\mathbf{x}_1,\dots,\mathbf{x}_i,\dots,\mathbf{x}_j,\dots,\mathbf{x}_m)$，则称 f 是对称的。如果 $\forall i,j\in\{1,\dots,m\},i\neq j$，有 $f(\mathbf{x}_1,\dots,\mathbf{x}_j,\dots,\mathbf{x}_i,\dots,\mathbf{x}_m)=-f(\mathbf{x}_1,\dots,\mathbf{x}_i,\dots,\mathbf{x}_j,\dots,\mathbf{x}_m)$，则称 f 是斜对称的。

容易看到，这个定义与定义1.5.6是一致的。

引理 3.0.1. 设 f 是 m 重斜对称线性函数，则 $f(\mathbf{x}_1,\dots,\mathbf{v},\dots,\mathbf{v},\dots,\mathbf{x}_m)=0$。

证明. 由 $f(\mathbf{x}_1,\dots,\mathbf{v},\dots,\mathbf{v},\dots,\mathbf{x}_m)=-f(\mathbf{x}_1,\dots,\mathbf{v},\dots,\mathbf{v},\dots,\mathbf{x}_m)$ 即得结论。 □

当结论推广到一般的域上时要求域的特征不为 2。

记 $a_{i_1\dots i_m}=f(\mathbf{e}^{(i_1)},\dots,\mathbf{e}^{(i_m)})$。于是，$f(\mathbf{x}_1,\dots,\mathbf{x}_m)=\sum_{i_1=1}^n\cdots\sum_{i_m=1}^n a_{i_1\dots i_m}x_{i_1 1}\cdots x_{i_m m}$，并且其中的 $i_1,\dots,i_m$ 两两不同。下面我们考虑 $m=n$ 的情形。由于 $i_1,\dots,i_n$ 两两不同，即 $\sigma=\begin{pmatrix}1&2&\cdots&n\\ i_1&i_2&\cdots&i_n\end{pmatrix}$ 是一个置换，那么

$$f(\mathbf{x}_1,\dots,\mathbf{x}_n)=\sum_{\sigma\in S_n}a_{\sigma(1)\dots\sigma(n)}x_{\sigma(1)1}\cdots x_{\sigma(n)n}$$

引理 3.0.2. 设 $f(\mathbf{x}_1,\dots,\mathbf{x}_n)=\sum_{\sigma\in S_n}a_{\sigma(1)\dots\sigma(n)}x_{\sigma(1)1}\cdots x_{\sigma(n)n}$ 是 n 重斜对称线性函数，则 $\forall\sigma\in S_n$，$a_{\sigma(1)\sigma(2)\dots\sigma(n)}=\varepsilon_\sigma a_{12\dots n}$。

证明. 这实际上是定义1.5.6的直接推论。

设 $\sigma=\tau_1\cdots\tau_k$，其中 $\tau_1,\dots,\tau_k$ 是对换。我们对 k 进行归纳。$k=0$ 时 $\sigma=\mathrm{id}$，命题显然成立，$k=1$ 时由引理3.0.1, 利用 $f(\mathbf{e}^{(1)},\dots,(\mathbf{e}^{(i)}+\mathbf{e}^{(j)}),\dots,(\mathbf{e}^{(i)}+\mathbf{e}^{(j)}),\dots,\mathbf{e}^{(n)})=0$ 即得命题成立. 下设 $k>1$ 且 $k-1$ 时命题成立那么，令 $\pi=\tau_2\cdots\tau_k$，则 $\sigma=\tau_1\pi$。于是有

$$\begin{aligned}a_{\sigma(1)\dots\sigma(n)}&=f(\mathbf{e}^{(\sigma(1))},\dots,\mathbf{e}^{(\sigma(n))})\\&=f(\mathbf{e}^{(\tau_1\pi(1))},\dots,\mathbf{e}^{(\tau_1\pi(n))})\\&=-f(\mathbf{e}^{(\pi(1))},\dots,\mathbf{e}^{(\pi(n))})\\&=-\varepsilon_\pi a_{1\dots n}\\&=\varepsilon_\sigma a_{1\dots n}\end{aligned}$$

这样我们就完成了证明。 □

有了这个引理，在 f 斜对称且 $n=m$ 时，我们可以继续 (3.0.1) 式的推导如下：

$$\begin{aligned}f(\mathbf{x}_1,\dots,\mathbf{x}_n)&=\sum_{\sigma\in S_n}a_{\sigma(1)\dots\sigma(n)}x_{\sigma(1)1}\cdots x_{\sigma(n)n}\\&=\sum_{\sigma\in S_n}\varepsilon_\sigma a_{1\dots n}x_{\sigma(1)1}\cdots x_{\sigma(n)n}\\&=a_{1\dots n}\sum_{\sigma\in S_n}\varepsilon_\sigma x_{\sigma(1)1}\cdots x_{\sigma(n)n}\\&=\lambda\sum_{\sigma\in S_n}\varepsilon_\sigma x_{\sigma(1)1}\cdots x_{\sigma(n)n}\end{aligned}\tag{3.0.2}$$

其中 $\lambda=f(\mathbf{e}^{(1)},\dots,\mathbf{e}^{(n)})=a_{1\dots n}$ 是给定的常数。这样我们就已经做完了定义行列式的准备了。

定义 3.0.3. 行列式函数 $\det : \underbrace{\mathbb{R}^n \times \cdots \times \mathbb{R}^n}_{\text{n 个}} \longrightarrow \mathbb{R}$ 是 n 重线性斜对称函数，且满足

$$\det(\mathbf{e}^{(1)}, \ldots, \mathbf{e}^{(n)}) = 1.$$

例 3.0.2. 当 $n = 2$ 时，$S_2 = \{e,\ \sigma = (12)\}$，则 $\det : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}$ 为：

$$\begin{aligned}\det(\mathbf{x}_1, \mathbf{x}_2) &= \varepsilon_e x_{e(1)1} x_{e(2)2} + \varepsilon_\sigma x_{\sigma(1)1} x_{\sigma(2)2} \\ &= x_{11}x_{22} - x_{21}x_{12} \\ &= \begin{vmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{vmatrix}\end{aligned}$$

即这里我们定义的行列式与第一章中定义的行列式是一致的。

定义 3.0.4 (方阵的行列式). 设 $A = (a_{ij})_{n\times n} \in M_n(\mathbb{R})$，则定义 A 的行列式为 A 的列向量的行列式函数，即 $\det(A) = \det(\mathbf{A}^{(1)}, \ldots, \mathbf{A}^{(n)}) = \sum_{\sigma\in S_n} \varepsilon_\sigma a_{\sigma(1)1} \cdots a_{\sigma(n)n}$，也记为 $|A| = \det(A)$。

于是我们也可以直接将行列式用矩阵元素的组合描述：行列式是方阵中所有不同行不同列元素的乘积的交错和 (完全展开)。

3.1 行列式的基本性质

利用行列式的定义，容易证明行列式 $\det : M_n(\mathbb{R}) \to \mathbb{R}$ 有以下性质：

(1) 正规性：$\det(E_n) = 1$；

(2) 多重线性性质：即固定 $n-1$ 列后 det 是剩下那一列的线性函数，于是特别地，$\det(\alpha A) = \alpha^n \det(A)$；

(3) 斜对称性：即交换矩阵的两列后行列式的值变成相反数；

(4) 列等性：若矩阵的两列相等，则行列式的值为 0(可由斜对称性推出)。

引理 3.1.1. 设 $A \in M_n(\mathbb{R})$，如果 $\operatorname{rank}(A) < n$，则 $\det(A) = 0$。

证明. 由于 $\operatorname{rank}(A) < n$，即存在某一列可以由其它列线性表出，不妨设

$$\mathbf{A}^{(j)} = \sum_{i=1, i\neq j}^{n} \alpha_i \mathbf{A}^{(i)}$$

那么由多重线性性及列等性有：

$$\begin{aligned}
\det(A) &= \det(\mathbf{A}^{(1)}, \ldots, \mathbf{A}^{(j-1)}, \sum_{i=1, i\neq j}^{n} \alpha_i \mathbf{A}^{(i)}, \ldots, \mathbf{A}^{(n)}) \\
&= \sum_{i=1, i\neq j}^{n} \alpha_i \det(\mathbf{A}^{(1)}, \ldots, \mathbf{A}^{(j-1)}, \mathbf{A}^{(i)}, \mathbf{A}^{(j+1)}, \ldots, \mathbf{A}^{(n)}) \\
&= 0
\end{aligned}$$

即得结论。 □

(5) 列变换不变性：设 $\mathbf{v} \in \left\langle \mathbf{A}^{(1)}, \ldots, \mathbf{A}^{(j-1)}, \mathbf{A}^{(j+1)}, \ldots, \mathbf{A}^{(n)} \right\rangle$，则

$$\det(\mathbf{A}^{(1)}, \ldots, \mathbf{A}^{(j-1)}, \mathbf{A}^{(j)} + \mathbf{v}, \mathbf{A}^{(j+1)}, \ldots, \mathbf{A}^{(n)}) = \det(A)$$

这可以由多重线性性及列等性直接推出。

命题 3.1.1. 设 $A \in M_n(\mathbb{R})$，则 $\det(A) = \det(A^t)$。

证明. 我们利用行列式的完全展开来证明命题。设 $A = (a_{ij})_{n\times n}$，$A^t = (a'_{ij})_{n\times n}$，其中 $a'_{ij} = a_{ji}$，$i, j \in \{1, 2, \ldots, n\}$，则

$$\begin{aligned}
\det(A^t) &= \sum_{\sigma\in S_n} \varepsilon_\sigma a'_{\sigma(1)1} \cdots a'_{\sigma(n)n} \\
&= \sum_{\sigma\in S_n} \varepsilon_\sigma a_{1\sigma(1)} \cdots a_{n\sigma(n)} \\
&= \sum_{\sigma\in S_n} \varepsilon_\sigma a_{\sigma^{-1}(\sigma(1)),\sigma(1)} \cdots a_{\sigma^{-1}(\sigma(n)),\sigma(n)} \\
&= \sum_{\sigma^{-1}\in S_n} \varepsilon_{\sigma^{-1}} a_{\sigma^{-1}(1),1} \cdots a_{\sigma^{-1}(n),n} \quad \text{(注意到 } \varepsilon_{\sigma^{-1}} = \varepsilon_\sigma\text{)} \\
&= \det(A).
\end{aligned}$$

即得结论。 □

注 3.1.1. (i) 由命题3.1.1可知，以上对矩阵列叙述的性质中，把列换成行，性质依然成立；(ii) 由以上性质容易推出，设 $A \in M_n(\mathbb{R})$，对 A 作一次初等行 (列) 变换得到 B，若变换是 (I) 类，则 $\det(B) = -\det(A)$；若变换是 (II) 类，则 $\det(B) = \det(A)$；若变换是 (III) 类，则 $\det(B) = \lambda \det(A)$。

(6) 上 (下) 三角矩阵的行列式等于对角线上元素的乘积。称 $A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ & a_{22} & \cdots & a_{2n} \\ & & \ddots & \vdots \\ & & & a_{nn} \end{pmatrix}$ 为上三角矩阵，则 $\det(A) = a_{11}a_{22}\cdots a_{nn}$(下三角矩阵可类似定义)。利用完全展开或初等变换都可以证明这一结论。

例 3.1.1. 设 $A = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$，求 $\det(A)$。

解. $\det(A) = \begin{vmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{vmatrix} = -\begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{vmatrix} = -1.$ □

定理 3.1.1. 设 $A \in M_n(\mathbb{R})$，则 $\det(A) = 0 \Longleftrightarrow \mathrm{rank}(A) < n$。

证明. ($\Longleftarrow$) 即引理3.1.1。
($\Longrightarrow$) 通过 (I)、(II) 类初等变换，我们可以将 A 化成行阶梯型的矩阵 B，而 $\det(A)$ 与 $\det(B)$ 只差一个正负号，于是 $\det(A) = 0$ 表明 B 的对角线上有 0，于是 B 有全是 0 的行，即 $\mathrm{rank}(A) < n$。 □

3.2 行列式的进阶性质

在这一节中，我们将讨论行列式按照一行 (或一列) 的展开，并由此介绍行列式的更多性质。有关行列式按多行 (列) 展开 (Laplace 定理)，我们将在习题课讲义中进行介绍。

设 $A \in M_n(\mathbb{R})$, $i, j \in \{1, \dots, n\}$，记 M_{ij} 是 A 去掉第 i 行第 j 列后得到的 $n-1$ 阶方阵的行列式，称为 A 关于位置 (i, j) 的余子式 (minor)；定义 $A_{ij} = (-1)^{i+j} M_{ij}$ 为 a_{ij} 的代数余子式 (cofactor)。

例 3.2.1. 设 $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$，则 $M_{11} = \begin{vmatrix} 5 & 6 \\ 8 & 9 \end{vmatrix} = -3$, $A_{23} = (-1)^{2+3} \begin{vmatrix} 1 & 2 \\ 7 & 8 \end{vmatrix} = 6$。

命题 3.2.1. 若 $A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{n2} & \cdots & a_{nn} \end{pmatrix}$，则 $\det(A) = a_{11} M_{11} = a_{11} A_{11}$。

证明. 注意到 A 的第一列只有 a_{11} 非零，于是由 $\det(A^t) = \det(A)$ 及行列式的完全展开有：

$$\det(A) = \sum_{\sigma \in S_n} \varepsilon_\sigma a_{\sigma(1)1} a_{\sigma(2)2} \cdots a_{\sigma(n)n} = \sum_{\sigma \in S_n, \sigma(1)=1} \varepsilon_\sigma a_{11} a_{\sigma(2)2} \cdots a_{\sigma(n)n}.$$

由于 $\{\sigma \in S_n \mid \sigma(1) = 1\}$ 与 $\{2, 3, \dots, n\}$ 上的置换集合 S_{n-1} 相同，因此

$$\det(A) = a_{11} \sum_{\pi \in S_{n-1}} \varepsilon_\pi a_{\pi(2)2} \cdots a_{\pi(n)n} = a_{11} \begin{vmatrix} a_{22} & \cdots & a_{2n} \\ \vdots & \ddots & \vdots \\ a_{n2} & \cdots & a_{nn} \end{vmatrix} = a_{11} M_{11}.$$

即得结论。 □

定理 3.2.1. 设 $A \in M_n(\mathbb{R})$，则 $\forall i, j \in \{1, \dots, n\}$，有

$$\det(A) = \sum_{k=1}^{n} a_{ik} A_{ik} = \sum_{k=1}^{n} a_{kj} A_{kj}$$

分别称之为行列式按第 i 行/第 j 列展开。

证明. 我们只证明按列展开，按行展开的情形可由取转置直接得到。

设 $A=(a_{ij})_{n\times n}$，则

$$
\begin{aligned}
&\det(A)\\
&=\begin{vmatrix} a_{11} & \cdots & a_{1j} & \cdots & a_{1n}\\ a_{21} & \cdots & 0 & \cdots & a_{2n}\\ \vdots & & \vdots & & \vdots\\ a_{n1} & \cdots & 0 & \cdots & a_{nn}\end{vmatrix}+\begin{vmatrix} a_{11} & \cdots & 0 & \cdots & a_{1n}\\ a_{21} & \cdots & a_{2j} & \cdots & a_{2n}\\ \vdots & & \vdots & & \vdots\\ a_{n1} & \cdots & 0 & \cdots & a_{nn}\end{vmatrix}+\cdots+\begin{vmatrix} a_{11} & \cdots & 0 & \cdots & a_{1n}\\ a_{21} & \cdots & 0 & \cdots & a_{2n}\\ \vdots & & \vdots & & \vdots\\ a_{n1} & \cdots & a_{nj} & \cdots & a_{nn}\end{vmatrix} && \text{(多重线性性质)}\\
&=\sum_{i=1}^{n}\begin{vmatrix} a_{11} & \cdots & a_{1,j-1} & 0 & a_{1,j+1} & \cdots & a_{1n}\\ \vdots & & \vdots & \vdots & \vdots & & \vdots\\ a_{i1} & \cdots & a_{i,j-1} & a_{ij} & a_{i,j+1} & \cdots & a_{in}\\ \vdots & & \vdots & \vdots & \vdots & & \vdots\\ a_{n1} & \cdots & a_{n,j-1} & 0 & a_{n,j+1} & \cdots & a_{nn}\end{vmatrix}\\
&=\sum_{i=1}^{n}(-1)^{j-1}\begin{vmatrix} 0 & a_{11} & \cdots & a_{1,j-1} & a_{1,j+1} & \cdots & a_{1n}\\ \vdots & \vdots & & \vdots & \vdots & & \vdots\\ a_{ij} & a_{i1} & \cdots & a_{i,j-1} & a_{i,j+1} & \cdots & a_{in}\\ \vdots & \vdots & & \vdots & \vdots & & \vdots\\ 0 & a_{n1} & \cdots & a_{n,j-1} & a_{n,j+1} & \cdots & a_{nn}\end{vmatrix} && \text{(第 j 列换到第 1 列)}\\
&=\sum_{i=1}^{n}(-1)^{(j-1)+(i-1)}\begin{vmatrix} a_{ij} & a_{i1} & \cdots & a_{i,j-1} & a_{i,j+1} & \cdots & a_{in}\\ 0 & a_{11} & \cdots & a_{1,j-1} & a_{1,j+1} & \cdots & a_{1n}\\ \vdots & \vdots & & \vdots & \vdots & & \vdots\\ 0 & a_{i-1,1} & \cdots & a_{i-1,j-1} & a_{i-1,j+1} & \cdots & a_{i-1,n}\\ 0 & a_{i+1,1} & \cdots & a_{i+1,j-1} & a_{i+1,j+1} & \cdots & a_{i+1,n}\\ \vdots & \vdots & & \vdots & \vdots & & \vdots\\ 0 & a_{n1} & \cdots & a_{n,j-1} & a_{n,j+1} & \cdots & a_{nn}\end{vmatrix} && \text{(第 i 行换到第 1 行)}\\
&=\sum_{i=1}^{n}(-1)^{i+j}a_{ij}M_{ij}=\sum_{i=1}^{n}a_{ij}A_{ij} && \text{(命题3.2.1)}
\end{aligned}
$$

这样我们就完成了证明。 □

例 3.2.2. $\begin{vmatrix} a_{11} & a_{12} & a_{13}\\ a_{21} & a_{22} & a_{23}\\ a_{31} & a_{32} & a_{33}\end{vmatrix}=a_{11}\begin{vmatrix} a_{22} & a_{23}\\ a_{32} & a_{33}\end{vmatrix}-a_{21}\begin{vmatrix} a_{12} & a_{13}\\ a_{32} & a_{33}\end{vmatrix}+a_{31}\begin{vmatrix} a_{12} & a_{13}\\ a_{22} & a_{23}\end{vmatrix}$。

例 3.2.3 (Vandemonde 行列式). 设 $A_n=\begin{pmatrix} 1 & 1 & 1 & \cdots & 1\\ x_1 & x_2 & x_3 & \cdots & x_n\\ x_1^2 & x_2^2 & x_3^2 & \cdots & x_n^2\\ \vdots & \vdots & \vdots & & \vdots\\ x_1^{n-1} & x_2^{n-1} & x_3^{n-1} & \cdots & x_n^{n-1}\end{pmatrix}$，则 $\det(A_n)=\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)$，记作 $\Delta(x_1,\ldots,x_n)$。

证明. 用数学归纳法。$n=2$ 时 $A_2=x_2-x_1$ 显然成立；下面假设 $n-1$ 时结论成立，则对 n

有：

$$\Delta(x_1,\dots,x_n)=\begin{vmatrix}1 & 1 & 1 & \cdots & 1\\ 0 & x_2-x_1 & x_3-x_1 & \cdots & x_n-x_1\\ 0 & x_2^2-x_2x_1 & x_3^2-x_3x_1 & \cdots & x_n^2-x_nx_1\\ \vdots & \vdots & \vdots & & \vdots\\ 0 & x_2^{n-1}-x_2^{n-2}x_1 & x_3^{n-1}-x_3^{n-2}x_1 & \cdots & x_n^{n-1}-x_n^{n-2}x_1\end{vmatrix} \quad \text{(各行减去上一行的 } x_1 \text{ 倍)}$$

$$=(x_2-x_1)(x_3-x_1)\cdots(x_n-x_1)\begin{vmatrix}1 & 1 & \cdots & 1\\ x_2 & x_3 & \cdots & x_n\\ \vdots & \vdots & & \vdots\\ x_2^{n-2} & x_3^{n-2} & \cdots & x_n^{n-2}\end{vmatrix} \quad \text{(按第一列展开后提出公因子)}$$

$$=(x_2-x_1)(x_3-x_1)\cdots(x_n-x_1)\Delta(x_2,x_3,\dots,x_n) \quad \text{(定义)}$$

$$=(x_2-x_1)(x_3-x_1)\cdots(x_n-x_1)\prod_{2\leqslant i<j\leqslant n}(x_j-x_i) \quad \text{(归纳假设)}$$

$$=\prod_{1\leqslant i<j\leqslant n}(x_j-x_i).$$

□

定理 3.2.2. 设 $A\in M_m(\mathbb{R})$, $B\in M_n(\mathbb{R})$, $C\in\mathbb{R}^{m\times n}$, 令 $D=\begin{pmatrix}A & C\\ O & B\end{pmatrix}$, 则 $\det(D)=\det(A)\cdot\det(B)$。

证明. 我们给出一个比较抽象的证明，它借助了我们一开始在 (3.0.1) 和 (3.0.2) 处的推导。如果不借助这个推导，我们也可以用 Laplace 定理证明这一结论，参见习题课讲义。

我们令

$$\begin{aligned}f:\ \mathbb{R}^m\times\cdots\times\mathbb{R}^m &\longrightarrow \mathbb{R}\\ (\mathbf{A}^{(1)},\dots,\mathbf{A}^{(m)}) &\longmapsto \det(D).\end{aligned}$$

那么容易验证：固定 B,C 后 f 是一个 m 重的斜对称线性函数 (按照定义，留作练习)，于是按照推导 (3.0.2) 的结果，固定 B,C 后 f 是行列式的一个常数倍，即

$$\det(D)=f(\mathbf{A}^{(1)},\dots,\mathbf{A}^{(m)})=\lambda\det(A),\ \lambda\in\mathbb{R}.$$

下面只需要证明 $\lambda=\det(B)$ 即可。为此，我们取 $A=E_m$，则此时

$$\begin{aligned}\det(D)&=f(\mathbf{e}^{(1)},\dots,\mathbf{e}^{(m)})\\ &=\begin{vmatrix}E_m & C\\ O & B\end{vmatrix} \quad \text{(依次按第 1,2...,m 列展开得)}\\ &=\det(B)=\lambda\end{aligned}$$

即 $\det(D)=\det(A)\cdot\det(B)$。 □

推论 3.2.1. 设 $A\in M_m(\mathbb{R})$, $B\in M_n(\mathbb{R}), C\in\mathbb{R}^{n\times m}$, 则

(i) $\begin{vmatrix}A & O\\ C & B\end{vmatrix}=|A|\cdot|B|$;

(ii) $\begin{vmatrix} C & B \\ A & O \end{vmatrix} = (-1)^{mn}|A|\cdot|B|$。

证明. (i) $\begin{vmatrix} A & O \\ C & B \end{vmatrix} = \begin{vmatrix} A^t & C^t \\ O & B^t \end{vmatrix} = |A^t|\cdot|B^t| = |A|\cdot|B|$;

(ii) $\begin{vmatrix} C & B \\ A & O \end{vmatrix}$ (交换行 mn 次) $= \begin{vmatrix} A & O \\ C & B \end{vmatrix} = (-1)^{mn}|A|\cdot|B|$。 □

下面的定理表明行列式保持矩阵的乘法。

定理 3.2.3. 设 $A, B \in M_n(\mathbb{R})$，则 $\det(AB) = \det(A)\det(B)$。

证明. 我们仍然采用类似定理3.2.2的证明方法，这个定理的另一种证法是直接将 $\begin{pmatrix} A & O \\ -E_n & B \end{pmatrix}$ 通过初等变换变成 $\begin{pmatrix} O & AB \\ -E_n & B \end{pmatrix}$，留给读者思考。[1]

我们令

$$\begin{aligned} f:\ & \mathbb{R}^n \times \cdots \times \mathbb{R}^n \longrightarrow \mathbb{R} \\ & (\mathbf{B}^{(1)}, \ldots, \mathbf{B}^{(n)}) \longmapsto \det(AB) = \det(A\mathbf{B}^{(1)}, \ldots, A\mathbf{B}^{(n)}). \end{aligned}$$

固定 A，则容易验证 f 关于 B 的列向量是斜对称的 n 重线性函数 (留作练习)，则由推导 (3.0.2) 有 $\det(AB) = f(\mathbf{B}^{(1)}, \ldots, \mathbf{B}^{(n)}) = \lambda\det(B)$，其中 $\lambda \in \mathbb{R}$ 与 B 无关。于是，取 $B = E_n$ 即得到 $f(\mathbf{e}^{(1)}, \ldots, \mathbf{e}^{(n)}) = \lambda = \det(A)$，从而 $\det(AB) = \det(A)\det(B)$。 □

例 3.2.4. 计算 $\begin{vmatrix} 1 & \cos\theta_1 & \cos 2\theta_1 \\ 1 & \cos\theta_2 & \cos 2\theta_2 \\ 1 & \cos\theta_3 & \cos 2\theta_3 \end{vmatrix}$。

解. 原式 $= \begin{vmatrix} 1 & \cos\theta_1 & \cos^2\theta_1 \\ 1 & \cos\theta_2 & \cos^2\theta_2 \\ 1 & \cos\theta_3 & \cos^2\theta_3 \end{vmatrix} \cdot \begin{vmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{vmatrix} = 2(\cos\theta_2 - \cos\theta_1)(\cos\theta_3 - \cos\theta_1)(\cos\theta_3 - \cos\theta_2)$。

□

注 3.2.1. 定理3.2.3表明 $\det(AB) = \det(BA)$。(但 $\operatorname{rank}(AB) \neq \operatorname{rank}(BA)$，反例取例2.4.5(2) 即可)。

定义 3.2.1 (Kronecker 符号). 设 $i, j \in \{1, 2, \ldots, n\}$，我们记 $\delta_{ij} = \begin{cases} 1, & i = j; \\ 0, & i \neq j. \end{cases}$.

引理 3.2.1. 设 $A = (a_{ij})_{n\times n}$，则对 $\forall i, j \in \{1, \ldots, n\}$，有：

(i) $\sum_{k=1}^n a_{ik}A_{jk} = \delta_{ij}|A|$;

(ii) $\sum_{k=1}^n a_{ki}A_{kj} = \delta_{ij}|A|$。

[1] 可以参考《高等代数 (上册)》§4.3.1，丘维声，清华大学出版社。

证明. 我们只证明 (i), (ii) 同理, 留作练习。设 $\mathbf{b}=(b_1,\dots,b_n)$, $B=\begin{pmatrix}\mathbf{A}_1\\ \vdots\\ \mathbf{A}_{j-1}\\ \mathbf{b}\\ \mathbf{A}_{j+1}\\ \vdots\\ \mathbf{A}_n\end{pmatrix}$, 则由定理3.2.1有:

$$\det(B)=b_1A_{j1}+\cdots+b_nA_{jn}$$

(1)$\exists i\in\{1,\dots,j-1,j+1,\dots,n\}$, 使得$\mathbf{b}=\mathbf{A}_i$, 则 $\det(B)=0$(列等性), 即 $a_{i1}A_{j1}+\cdots+a_{in}A_{jn}=0$。
(2) 当 $i=j$ 时显然有 $B=A$, 按第 i 行展开即有 $\sum_{k=1}^n a_{ik}A_{ik}=\delta_{ii}|A|$。 □

定义 3.2.2. 设 $A=(a_{ij})_{n\times n}$, 我们定义 A 的伴随矩阵 (classical adjoint)$A^\vee$ 如下:

$$A^\vee=\begin{pmatrix}A_{11}&A_{21}&\cdots&A_{n1}\\ A_{12}&A_{22}&\cdots&A_{n2}\\ \vdots&\vdots&&\vdots\\ A_{1n}&A_{2n}&\cdots&A_{nn}\end{pmatrix}$$

其中 A_{ij} 是 a_{ij} 的代数余子式。

定理 3.2.4. 设 $A\in M_n(\mathbb{R})$, 则 $AA^\vee=A^\vee A=|A|E_n$。

证明. 设 $A^\vee=(a'_{ij})_{n\times n}$, $AA^\vee=(b_{ij})_{n\times n}$, 则 $a'_{ij}=A_{ji}$, $b_{ij}=\sum_{k=1}^n a_{ik}a'_{kj}=\sum_{k=1}^n a_{ik}A_{jk}=\delta_{ij}|A|$, 即 $AA^\vee=(|A|\delta_{ij})_{n\times n}=|A|E_n$。同理可证 $A^\vee A=|A|E_n$。 □

例 3.2.5. 设 $A\in M_n(\mathbb{R})$, 求证 $\det(A^\vee)=|A|^{n-1}$。

证明. 当 $|A|=0$ 时, 由 $AA^\vee=O$ 知 $\operatorname{rank}(A^\vee)<n$(这是因为若 $A=O$ 则 $A^\vee=O$, 否则设 $0<r=\operatorname{rank}(A)<n$, 则由 Sylvester 不等式有 $r+\operatorname{rank}(A^\vee)-n\leqslant 0$), 于是 $\det(A^\vee)=0$。
当 $|A|\neq 0$ 时, 对 $AA^\vee=|A|E_n$ 两边取行列式即得 $|A|\det(A^\vee)=|A|^n$, 即 $\det(A^\vee)=|A|^{n-1}$。 □

3.3 行列式的应用

这一节我们简单讨论一下行列式与线性方程组及矩阵的秩之间的联系。

定理 3.3.1. 设 $A \in M_n(\mathbb{R})$，则 A 可逆 $\Longleftrightarrow A^\vee$ 满秩，并且此时 $A^{-1} = \dfrac{1}{\det(A)}A^\vee$。

证明. ($\Longrightarrow$) 由于 A 可逆，即 $\det(A) \neq 0$，于是由定理3.2.4知 $A(\dfrac{1}{\det(A)}A^\vee) = E$，即 $A^{-1} = \dfrac{1}{\det(A)}A^\vee$。
($\Longleftarrow$) 由 $A^\vee$ 满秩知 $\det(A^\vee) \neq 0$，于是由例3.2.5得 $|A| \neq 0$，即 A 满秩 (可逆)。 □

下面我们考虑行列式与线性方程组的关系。

定理 3.3.2 (Cramer 法则). 设 $A = (a_{ij})_{n\times n} \in M_n(\mathbb{R})$，$\mathbf{x} = (x_1, \ldots, x_n)^t \in \mathbb{R}^n$，$b = (b_1, \ldots, b_n)^t$，则方程组 $A\mathbf{x} = \mathbf{b}$ 有唯一解 $\Longleftrightarrow A$ 可逆，并且此时解为

$$x_1 = \frac{\det(\mathbf{b}, \mathbf{A}^{(2)}, \ldots, \mathbf{A}^{(n)})}{\det(A)},\ x_2 = \frac{\det(\mathbf{A}^{(1)}, \mathbf{b}, \ldots, \mathbf{A}^{(n)})}{\det(A)}, \ldots\ldots, x_n = \frac{\det(\mathbf{A}^{(1)}, \ldots, \mathbf{A}^{(n-1)}, \mathbf{b})}{\det(A)}.$$

证明. ($\Longrightarrow$) 由命题1.2.1易证方程组 $A\mathbf{x} = \mathbf{b}$ 有唯一解 $\Longleftrightarrow A\mathbf{x} = \mathbf{0}$ 只有 0 解，即 $V_A = \{\mathbf{0}\}$，所以 $\operatorname{rank}(A) = n$，即 A 可逆。
($\Longleftarrow$) 若 A 可逆，则 $A(A^{-1}\mathbf{b}) = \mathbf{b}$，即 $\mathbf{x} = A^{-1}\mathbf{b}$ 是方程组的解，若另有解 $\mathbf{x}'$，则 $\mathbf{x} - \mathbf{x}'$ 是 $A\mathbf{x} = \mathbf{0}$ 的解，而 A 满秩推出 $A\mathbf{x} = \mathbf{0}$ 只有 0 解，即 $\mathbf{x} = \mathbf{x}' = \mathbf{0}$。故解唯一。

下面利用定理3.3.1给出解的形式。由 $\mathbf{x} = A^{-1}\mathbf{b} = \frac{1}{\det(A)}A^\vee\mathbf{b}$ 可得：对 $\forall i \in \{1, \ldots, n\}$，有

$$\begin{aligned} x_i &= \frac{1}{\det(A)}A_i^\vee\mathbf{b} \\ &= \frac{1}{\det(A)}(b_1A_{1i} + \cdots + b_nA_{ni}) \\ &= \frac{1}{\det(A)}\det\left(\mathbf{A}^{(1)}, \ldots, \mathbf{A}^{(i-1)}, \mathbf{b}, \mathbf{A}^{(i+1)}, \ldots, \mathbf{A}^{(n)}\right). \end{aligned}$$

此即我们所需要的解，具体写出来就是

$$x_i = \frac{\begin{vmatrix} a_{11} & \cdots & a_{1,i-1} & b_1 & a_{1,i+1} & \cdots & a_{1n} \\ a_{21} & \cdots & a_{2,i-1} & b_2 & a_{2,i+1} & \cdots & a_{2n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & \cdots & a_{n,i-1} & b_n & a_{n,i+1} & \cdots & a_{nn} \end{vmatrix}}{\det(A)}.$$

这样我们就完成了证明。 □

最后我们考虑行列式和矩阵的秩之间的联系。

定义 3.3.1. 设 $A = (a_{ij})_{m\times n}$，$k \leqslant \min(m, n)$，$i_1, \ldots, i_k \in \{1, \ldots, m\}$，$j_1, \ldots, j_k \in \{1, \ldots, n\}$，则

$$\begin{vmatrix} a_{i_1,j_1} & \cdots & a_{i_1,j_k} \\ \vdots & \ddots & \vdots \\ a_{i_k,j_1} & \cdots & a_{i_k,j_k} \end{vmatrix}$$

称为 A 的 k 阶子式，记为 $M_A\binom{i_1,\dots,i_k}{j_1,\dots,j_k}$。

引理 3.3.1. 设 $j_1,\dots,j_k\in\{1,\dots,n\}$，则 $\mathbf{A}^{(j_1)},\dots,\mathbf{A}^{(j_k)}$ 线性无关 $\Longleftrightarrow$ 存在子式 $M_A\binom{i_1,\dots,i_k}{j_1,\dots,j_k}\neq 0$。

证明. ($\Longrightarrow$) 令 $B=(\mathbf{A}^{(j_1)},\dots,\mathbf{A}^{(j_k)})_{m\times k}$，则 $\operatorname{rank}(B)=k$，于是存在 $i_1,\dots,i_k\in\{1,\dots,m\}$ 使得 $\mathbf{B}_{i_1},\dots,\mathbf{B}_{i_k}$ 线性无关，再令 $B'=\begin{pmatrix}\mathbf{B}_{i_1}\\ \vdots\\ \mathbf{B}_{i_k}\end{pmatrix}_{k\times k}$，则 B' 满秩，于是 $\det(B')\neq 0$。B' 即所需要的 $M_A\binom{i_1,\dots,i_k}{j_1,\dots,j_k}$。
($\Longleftarrow$) 由 $M_A\binom{i_1,\dots,i_k}{j_1,\dots,j_k}\neq 0$ 可得方程组

$$\alpha_1\begin{pmatrix}a_{i_1,j_1}\\ \vdots\\ a_{i_k,j_1}\end{pmatrix}+\cdots+\alpha_k\begin{pmatrix}a_{i_1,j_k}\\ \vdots\\ a_{i_k,j_k}\end{pmatrix}=\mathbf{0}$$

只有 0 解。于是添加一些方程后，有：

$$\alpha_1\begin{pmatrix}a_{1,j_1}\\ \vdots\\ a_{n,j_1}\end{pmatrix}+\cdots+\alpha_k\begin{pmatrix}a_{1,j_k}\\ \vdots\\ a_{n,j_k}\end{pmatrix}=\mathbf{0}$$

也只有 0 解。即 $\mathbf{A}^{(j_1)},\dots,\mathbf{A}^{(j_k)}$ 线性无关。 □

定理 3.3.3. 设 $A\in\mathbb{R}^{m\times n}$，则以下条件等价：

(i) $\operatorname{rank}(A)=r$;
(ii) A 中存在一个 r 阶子式非零，而其它任何大于 r 阶的子式都是 0;
(iii) A 中存在一个 r 阶子式非零，而其它任何 $r+1$ 阶的子式都是 0。

证明. (i)$\Longrightarrow$(ii)：设 $\mathbf{A}^{(j_1)},\dots,\mathbf{A}^{(j_r)}$ 线性无关，由引理 3.3.1，A 中存在一个 r 阶子式非零。若有 $s>r$ 使得一个 A 的 s 阶子式 $M_A\binom{i_1,\dots,i_s}{j_1,\dots,j_s}$ 非零，则由引理3.3.1，其对应的列向量 $\mathbf{A}^{(j_1)},\dots,\mathbf{A}^{(j_s)}$ 线性无关，这与 $\operatorname{rank}(A)=r$ 矛盾！
(ii)$\Longrightarrow$(iii)：显然。
(iii)$\Longrightarrow$(i)：由引理3.3.1，A 中有 r 列线性无关，而任何 $r+1$ 列都线性相关，故 $\operatorname{rank}(A)=r$。 □

设 $M_A,\widetilde{M}_A$ 都是 A 的子式，若 M_A 可以由 $\widetilde{M}_A$ 去掉一端的行和一端的列得到，则我们称 $\widetilde{M}_A$ 是 M_A 的加边子式。

定理 3.3.4. 设 $A\in\mathbb{R}^{m\times n}$，则 $\operatorname{rank}(A)=r\Longleftrightarrow A$ 有一个 r 阶的非零子式且这个子式的所有加边子式都是 0。

证明. ($\Longrightarrow$) 方向已经在定理3.3.3中证明。下面证明 ($\Longleftarrow$) 方向。
不妨设 $N=M\binom{1,2,\dots,r}{1,2,\dots,r}\neq 0$，则由引理3.3.1知 $\mathbf{A}^{(1)},\dots,\mathbf{A}^{(r)}$ 线性无关。不计正负号下，N 的所有加边子式为 $M\binom{1,2,\dots,r,i}{1,2,\dots,r,j}$，其中 $i\in\{1,\dots,m\}$，$j\in\{1,\dots,n\}$。用反证法，假设 $\operatorname{rank}(A)\neq r$，则

只可能是 $\mathrm{rank}(A) > r$，于是对任意的 i, j，有 $M\binom{1,2,\ldots,r,i}{1,2,\ldots,r,j} = 0$。即

$$\begin{vmatrix} a_{11} & \cdots & a_{1r} & a_{1j} \\ \vdots & & \vdots & \vdots \\ a_{r1} & \cdots & a_{rr} & a_{rj} \\ a_{i1} & \cdots & a_{ir} & a_{ij} \end{vmatrix} = 0$$

将上式按最后一行展开得 $a_{i1}c_1 + \cdots + a_{ir}c_r + a_{ij}N = 0$，其中 $c_1, \ldots, c_r$ 分别是子式 $M\binom{1,2,\ldots,r,i}{1,2,\ldots,r,j}$ 中 $a_{i1} \ldots, a_{ir}$ 的代数余子式。因为 $N \neq 0$，所以可以整理得到：

$$a_{ij} = (-\frac{c_1}{N})a_{i1} + \cdots + (-\frac{c_r}{N})a_{ir}$$

对任意 i, j 都成立。使 i 遍历 $\{1, \ldots, m\}$，即对任意的列指标 j，有

$$\mathbf{A}^{(j)} = (-\frac{c_1}{N})\mathbf{A}^{(1)} + \cdots + (-\frac{c_r}{N})\mathbf{A}^{(r)}.$$

即 $< \mathbf{A}^{(1)}, \ldots, \mathbf{A}^{(r)} >= V_c(A)$，于是 $\mathrm{rank}(A) \leqslant r$，与假设矛盾！这样我们就完成了证明。 □

有关行列式的计算技巧，我们不作过多介绍，读者可以参考习题课讲义及其他高等代数的标准教材。

3.4 习题

3.4.1 行列式的性质与计算

1. 证明引理3.2.1(ii).

2. 将下述三个变量的斜对称函数 $\Delta:\mathbb{R}^3\to\mathbb{R}$

$$\Delta(x,y,z)=(y-x)(z-x)(y-z)$$

写成三阶行列式的形式.

3. 设 $A=\left(a_{ij}\right),A'=\left(a'_{ij}\right)$ 是两个 $n\times n$ 矩阵, Δ,Δ' 是它们的行列式. 在下述情况下比较 Δ 和 Δ' :
   a) $a'_{ij}=2^{i-j}a_{ij}$;
   b) $a'_{ij}=a_{n+1-i,j}$;
   c) $a'_{ij}=a_{n+1-i,n+1-j}$.

4. 证明

$$\begin{vmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 2 & 1 & \cdots & 1 & 1 \\ 1 & 1 & 3 & \cdots & 1 & 1 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & 1 & 1 & \cdots & n & 1 \\ 1 & 1 & 1 & \cdots & 1 & n+1 \end{vmatrix}=n!.$$

5. 利用行列式的定义计算

$$\begin{vmatrix} 0 & \cdots & 0 & 0 & a_{1n} \\ 0 & \cdots & 0 & a_{2,n-1} & a_{2n} \\ 0 & \cdots & a_{3,n-2} & a_{3,n-1} & a_{3n} \\ \vdots & & \vdots & \vdots & \vdots \\ a_{n1} & \cdots & a_{n,n-2} & a_{n,n-1} & a_{nn} \end{vmatrix}.$$

6. 利用行列式的定义计算

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \\ a_{21} & a_{22} & a_{23} & a_{24} & a_{25} \\ a_{31} & a_{32} & 0 & 0 & 0 \\ a_{41} & a_{42} & 0 & 0 & 0 \\ a_{51} & a_{52} & 0 & 0 & 0 \end{vmatrix}.$$

7. 整数 $1798,2139,3255,4867$ 可以被 31 整除. 不必计算, 证明 4 阶行列式

$$\begin{vmatrix} 1 & 7 & 9 & 8 \\ 2 & 1 & 3 & 9 \\ 3 & 2 & 5 & 5 \\ 4 & 8 & 6 & 7 \end{vmatrix}$$

也可以被 31 整除.

8. 证明任意四阶斜对称行列式 $\left|a_{ij}\right|$, 其中 $a_{ij}\in\mathbb{Z}$, 是一个整数的平方. (实际上, 这对于任意阶的斜对称行列式都是对的.)

9. 用下述方法证明 $\det AB=\det A\cdot\det B$. 令 $2n\times 2n$ 阶辅助矩阵 $C=\begin{pmatrix} A & O\\ -E & B\end{pmatrix}$ 运用初等行变换将 C 化成
$$C'=\begin{pmatrix} O & AB\\ -E & B\end{pmatrix}.$$
(提示: 利用等式 $\det C=\det C'$ 和推论3.2.1.)

下面的题目是关于行列式计算技巧的典型题目.

10. 计算以下行列式:

(1) $\begin{vmatrix} 1 & 2 & 3 & \cdots & n\\ 2 & 3 & 4 & \cdots & 1\\ 3 & 4 & 5 & \cdots & 2\\ \vdots & \vdots & \vdots & & \vdots\\ n & 1 & 2 & \cdots & n-1\end{vmatrix}$; (2) $\begin{vmatrix} 1 & 1 & 1 & \cdots & 1\\ 1 & 1-x & 1 & \cdots & 1\\ 1 & 1 & 2-x & \cdots & 1\\ \vdots & \vdots & \vdots & & \vdots\\ 1 & 1 & 1 & \cdots & n-x\end{vmatrix}$;

(3) $\begin{vmatrix} a_1 & b_1 & 0 & \cdots & 0 & 0\\ 0 & a_2 & b_2 & \cdots & 0 & 0\\ 0 & 0 & a_3 & \cdots & 0 & 0\\ \vdots & \vdots & \vdots & & \vdots & \vdots\\ 0 & 0 & 0 & \cdots & a_{n-1} & b_{n-1}\\ b_n & 0 & 0 & \cdots & 0 & a_n\end{vmatrix}$; (4) $\begin{vmatrix} 1+a_1 & 1 & \cdots & 1\\ 2 & 2+a_2 & \cdots & 2\\ \vdots & \vdots & & \vdots\\ n & n & \cdots & n+a_n\end{vmatrix}$;

(5) $\begin{vmatrix} a & b & 0 & \cdots & 0 & 0 & 0\\ c & a & b & \cdots & 0 & 0 & 0\\ \cdots\cdots & \cdots & \cdots & \cdots & \cdots\cdots & \cdots\cdots & \\ 0 & 0 & 0 & \cdots & a & b & 0\\ 0 & 0 & 0 & \cdots & c & a & b\\ 0 & 0 & 0 & \cdots & 0 & c & a\end{vmatrix}$;

(6) $\begin{vmatrix} 1 & 1 & 1 & 1\\ a & b & c & d\\ a^2 & b^2 & c^2 & d^2\\ a^4 & b^4 & c^4 & d^4\end{vmatrix}$ (a,b,c,d 互不相等);

(7) $\begin{vmatrix} x_1 & a & \cdots & a & a\\ b & x_2 & \cdots & a & a\\ \vdots & \vdots & \ddots & \vdots & \vdots\\ b & b & \cdots & x_{n-1} & a\\ b & b & \cdots & b & x_n\end{vmatrix}$; (8) $\begin{vmatrix} \cos(\alpha_1-\beta_1) & \cos(\alpha_1-\beta_2) & \cdots & \cos(\alpha_1-\beta_n)\\ \cos(\alpha_2-\beta_1) & \cos(\alpha_2-\beta_2) & \cdots & \cos(\alpha_2-\beta_n)\\ \vdots & \vdots & & \vdots\\ \cos(\alpha_n-\beta_1) & \cos(\alpha_n-\beta_2) & \cdots & \cos(\alpha_n-\beta_n)\end{vmatrix}$;

11. 设 A,B 是任意 n 阶方阵. 证明
$$\det\begin{pmatrix} A & B\\ B & A\end{pmatrix}=\det(A+B)\cdot\det(A-B).$$

12. 设 X 是 $n\times k$ 矩阵而 Y 是 $k\times n$ 矩阵.

(1) 证明

$$\det(E_n+XY)=\det(E_k+YX).$$

提示: 利用关系式

$$\begin{pmatrix} E_k+YX & 0 \\ X & E_n \end{pmatrix}\begin{pmatrix} E_k & Y \\ 0 & E_n \end{pmatrix}=\begin{pmatrix} E_k & Y \\ 0 & E_n \end{pmatrix}\begin{pmatrix} E_k & 0 \\ X & E_n+XY \end{pmatrix}.$$

(2) 利用 (1) 的结论计算行列式

$$\begin{vmatrix} 1+a_1+b_1 & a_1+b_2 & \cdots & a_1+b_n \\ a_2+b_1 & 1+a_2+b_2 & \cdots & a_2+b_n \\ \vdots & \vdots & & \vdots \\ a_n+b_1 & a_n+b_2 & \cdots & 1+a_n+b_n \end{vmatrix}.$$

行列式的应用

1. 证明下述公式:

$$(AB)^\vee=B^\vee A^\vee;\quad (A^t)^\vee=(A^\vee)^t;$$
$$(\lambda A)^\vee=\lambda^{n-1}A^\vee;\quad (A^\vee)^\vee=(\det A)^{n-2}A.$$

2. 设 $A\in M_n(\mathbb{R})$. 证明

$$\operatorname{rank}(A^\vee)=\begin{cases} n, & \operatorname{rank}A=n; \\ 1, & \operatorname{rank}A=n-1; \\ 0, & \operatorname{rank}A\leqslant n-2. \end{cases}$$

3. 证明当未知量的个数与方程的个数相等时, 齐次线性方程组有非零解, 当且仅当系数矩阵的行列式等于零.

4. 设 $A=(a_{ij})$ 是 $(n-1)$ 行 n 列的矩阵, 当 $\operatorname{rank}A=n-1$ 时, 齐次线性方程组 $A\mathbf{x}=\mathbf{0}$ ($\mathbf{x}\in\mathbb{R}^n$) 的基础解系由一个列向量

$$\mathbf{x}_0=(D_1,-D_2,D_3,\ldots,(-1)^{n-1}D_n)^t$$

组成, 其中 D_i 是从 $A=\left(a_{ij}\right)$ 中去掉第 i 列所得矩阵的行列式. 任意解的形式为 $\mathbf{x}=\lambda\mathbf{x}_0,\ \forall\lambda\in\mathbb{R}$.

5. (1) 设 $A=\left(a_{ij}\right)\in M_n(\mathbb{R})$, 且 $\forall j\in\{1,\ldots,n\}$, 有 $\sum_{i=1,i\neq j}^n\left|a_{ij}\right|<\left|a_{jj}\right|$. 证明 $\det(A)\neq 0$.
(2) 设 $A=\left(a_{ij}\right)\in M_n(\mathbb{R})$, 且 $\forall j\in\{1,\ldots,n\}$, 有 $\sum_{i=1,i\neq j}^n\left|a_{ij}\right|<a_{jj}$. 证明 $\det(A)>0$.

6. (Binet-Cauchy 公式) 设 $A=\left(a_{ij}\right),B=\left(b_{ij}\right)$ 是 $m\times n$ 矩阵, $A_{i_1,\cdots,i_m}$ 和 $B_{i_1,\cdots,i_m}$ 分别是 A 和 B 的由指标为 $i_1,\cdots,i_m$ 的列合成的 m 阶子式, 并且

$$c_{ij}=\sum_{k=1}^n a_{ik}b_{jk},\quad C=\left(c_{ij}\right)\quad i=1,\cdots,m;\quad j=1,\cdots,m.$$

证明当 $m \leqslant n$ 时有

$$\det C = \sum_{1 \leqslant i_1 < i_2 < \cdots < i_m \leqslant n} A_{i_1, \cdots, i_m} B_{i_1, \cdots, i_m},$$

当 $m > n$ 时, $\det C = 0$.

7. (Laplace 定理) 设 $A = \left(a_{ij}\right)$ 是 n 阶方阵. 其 k 阶子式 $M\begin{pmatrix} i_1 & \cdots & i_k \\ j_1 & \cdots & j_k \end{pmatrix}$ (定义见于定义3.3.1) 的余子式 $\overline{M}\begin{pmatrix} i_1 & \cdots & i_k \\ j_1 & \cdots & j_k \end{pmatrix}$ 是 A 去掉第 $i_1, i_2, \cdots, i_k$ 行和第 $j_1, j_2, \cdots, j_k$ 列后得到的矩阵的行列式. 取定 $i_1, i_2, \cdots, i_k$, 则有

$$\det A = \sum_{1 \leqslant j_1 < j_2 < \cdots < j_k \leqslant n} (-1)^{i_1 + \cdots + i_k + j_1 + \cdots + j_k} M\begin{pmatrix} i_1 & \cdots & i_k \\ j_1 & \cdots & j_k \end{pmatrix} \overline{M}\begin{pmatrix} i_1 & \cdots & i_k \\ j_1 & \cdots & j_k \end{pmatrix}.$$

8. (1) 运用上题结论证明定理3.2.2;
   (2) 运用上题结论计算以下 $2n \times 2n$ 阶矩阵的行列式

$$\begin{vmatrix} a & & & & & b \\ & \ddots & & & \iddots & \\ & & a & b & & \\ & & b & a & & \\ & \iddots & & & \ddots & \\ b & & & & & a \end{vmatrix}.$$

9. 设

$$D = \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix}.$$

   证明:

$$\begin{vmatrix} a_{11} & \cdots & a_{1n} & x_1 \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & \cdots & a_{nn} & x_n \\ x_1 & \cdots & x_n & z \end{vmatrix} = Dz - \sum_{i,j=1}^{n} A_{ij} x_i x_j.$$

   其中 A_{ij} 是矩阵 D 在 a_{ij} 处的代数余子式.

10. 设

$$A = \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix}, \quad B = \begin{vmatrix} b_{11} & \cdots & b_{1k} \\ \vdots & & \vdots \\ b_{k1} & \cdots & b_{kk} \end{vmatrix},$$

$$D=\begin{vmatrix} a_{11}b_{11} & \cdots & a_{1n}b_{11} & a_{11}b_{12} & \cdots & a_{1n}b_{12} & \cdots & \cdots & a_{11}b_{1k} & \cdots & a_{1n}b_{1k} \\ \vdots & & \vdots & \vdots & & \vdots & \cdots & \cdots & \vdots & & \vdots \\ a_{n1}b_{11} & \cdots & a_{nn}b_{11} & a_{n1}b_{12} & \cdots & a_{nn}b_{12} & \cdots & \cdots & a_{n1}b_{1k} & \cdots & a_{nn}b_{1k} \\ \vdots & & \vdots & \vdots & & \vdots & \ddots & & \vdots & & \vdots \\ a_{11}b_{k1} & \cdots & a_{1n}b_{k1} & a_{11}b_{k2} & \cdots & a_{1n}b_{k2} & \cdots & \cdots & a_{11}b_{kk} & \cdots & a_{1n}b_{kk} \\ \vdots & & \vdots & \vdots & & \vdots & \cdots & \cdots & \vdots & & \vdots \\ a_{n1}b_{k1} & \cdots & a_{nn}b_{k1} & a_{n1}b_{k2} & \cdots & a_{nn}b_{k2} & \cdots & \cdots & a_{n1}b_{kk} & \cdots & a_{nn}b_{kk} \end{vmatrix}$$

D 是 nk 阶矩阵的行列式, 它是 A 与 B 的 Kroneker 积. 求证 $D=A^kB^n$.

11. 证明: 若 $A,B,C,D\in M_n(\mathbb{R})$, $\det A\neq 0$ 则

$$\begin{aligned}\det\begin{pmatrix} A & B \\ C & D \end{pmatrix} &= \det\left(AD-ACA^{-1}B\right) \\ &= (\det A)\cdot\det\left(D-CA^{-1}B\right).\end{aligned}$$

此外, 验证

$$\det\begin{pmatrix} A & B \\ C & D \end{pmatrix}=\begin{cases}\det(AD-CB), & \text{若}AC=CA,\\ \det(DA-CB), & \text{若}AB=BA.\end{cases}$$

第四章　群、环、域简介

这一章我们介绍抽象代数的基本概念：群、环和域。它们都是带有特定运算结构的集合，我们的目的是研究这些结构的性质，并将其应用到具体的数学对象上。这种思路也是代数学的基本想法之一。初学者面对这一章的内容或许会感到难以理解，但实际上这一章的内容大部分是很具体的 (甚至是可以“计算”的)，读者可以结合例子来慢慢理解这些代数学对象的“实在性”。

4.1　二元运算

定义 4.1.1. 设 S 是非空集合，我们称映射 $S\times S\to S$ 是一个二元运算，简称运算。对任意 $x,y\in S$，我们也把 $f(x,y)$ 简记为 xfy。

例 4.1.1.　(i) $+:\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z},\ (a,b)\mapsto a+b$ 是 $\mathbb{Z}$ 上的二元运算。

(ii) $\cdot:M_n(\mathbb{R})\times M_n(\mathbb{R}),\ (A,B)\mapsto AB$ 是 $M_n(\mathbb{R})$ 上的二元运算。

(iii) 记 $*:\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z},\ (x,y)\mapsto|x-y|$，则 $*$ 也是 $\mathbb{Z}$ 上的二元运算。

定义 4.1.2. 若二元运算 f 满足 $\forall x,y\in S,\ f(x,y)=f(y,x)$，则我们称 f 满足交换律；若二元运算 f 满足 $\forall x,y,z\in S,\ f(f(x,y),z)=f(x,f(y,z))$，则我们称 f 满足结合律。

当然，一个运算满足交换律和满足结合律之间没有必然关系，例如很容易看出例4.1.1中 (ii) 是结合但不交换的，(iii) 是交换但不结合的。

定理 4.1.1 (广义结合律). 设 $*$ 是集合 S 上的一个满足结合律的二元运算，$x_1,\dots,x_n\in S$，$n\geqslant 2$，归纳定义

$$x_1*x_2*\cdots*x_n=(x_1*\cdots*x_{n-1})*x_n\quad\text{(左正规化)}$$

则对任意 $\forall k\in\{1,\dots,n-1\}$，有

$$x_1*x_2*\cdots*x_n=(x_1*\cdots*x_i)*(x_{i+1}*\cdots*x_n).$$

证明. $n=1,2$ 时定理显然成立。当 $n=3$，由结合律，我们有

$$x_1*x_2*x_3=(x_1*x_2)*x_3=x_1*(x_2*x_3).$$

对 n 用数学归纳法。假设定理对 ”$<n$” 的所有正整数都成立，即括号的位置与二元运算无关。则对 n 个元素的二元运算，当 $i=n-1$ 时，即是定义。不妨设 $1\leqslant i<n-1$, 我们有：

$$\begin{aligned}
&x_1*\cdots*x_i*x_{i+1}*\cdots*x_n\\
=\ &(x_1*\cdots*x_{n-1})*x_n && \text{(定义)}\\
=\ &[(x_1*\cdots*x_i)*(x_{i+1}*\cdots*x_{n-1})]*x_n) && \text{(归纳假设)}\\
=\ &(x_1*\cdots*x_i)*[(x_{i+1}*\cdots*x_{n-1})*x_n)] && \text{(结合律)}\\
=\ &(x_1*\cdots*x_i)*(x_{i+1}*\cdots*x_n) && \text{(定义)}
\end{aligned}$$

即定理对 n 的情形也对，这样我们就完成了证明。 □

有了广义结合律，我们就可以对一个结合的二元运算 $*$ 定义**方幂**：设 $n \in \mathbb{Z}^+$，记 $\underbrace{x * \cdots * x}_{\text{n 个}} = x^n$，则对 $\forall m, n \in \mathbb{Z}^+$，方幂满足性质：$(x^n) * (x^m) = x^{n+m}$，$(x^n)^m = x^{mn}$。

定义 4.1.3. 设 $*$ 是集合 S 上的一个二元运算，$e \in S$，如果 $\forall x \in S, x * e = e * x = x$，则称 e 是 S 上关于 $*$ 的单位元或幺元 (identity)。

例 4.1.2. 显然 0 是 $\mathbb{Z}$ 上关于加法"+" 的单位元；E_n 是 $M_n(\mathbb{R})$ 上关于矩阵乘法的单位元。

命题 4.1.1. 设 $*$ 是集合 S 上的二元运算，若 e, e' 都是 S 上关于 $*$ 的单位元，则 $e = e'$。即单位元若存在则必唯一。

由 $e = ee' = e'$ 立刻得证。

定义 4.1.4. 设 $*$ 是 S 上的二元运算，e 是 S 中关于 $*$ 的单位元，$x \in S$。如果存在 $y \in S$ 使得 $x * y = y * x = e$，则我们称 x 是 S 中关于 $*$ 的可逆元，并称 y 是 x 的逆。

例 4.1.3. 显然 $\mathbb{Z}$ 中任意元素都关于 "$+$" 可逆，且 x 的逆就是 $-x$；在 $M_n(\mathbb{R})$ 中，关于矩阵乘法可逆的元素是所有满秩矩阵，并且逆是逆矩阵。

下面我们正式引入一个在代数和数论中都十分重要的研究对象：剩余类。在第一章中，我们定义了 $\mathbb{Z}$ 上的同余关系，

$$\forall a, b \in \mathbb{Z}, n \in \mathbb{Z}^+, a \equiv_n b \iff n | (a - b)$$

同余关系是一个等价关系。有时也记作 $a \equiv b \mod n$. 下面我们考虑 $\mathbb{Z}$ 在 $\equiv_n$ 关系下的分割. $\forall a \in \mathbb{Z}$，作带余除法 $a = qn + r$，$r \in \{0, 1, \ldots, n-1\}$，则 $a \equiv_n r$。于是 $\equiv_n$ 关系下有且只有 n 个等价类 $\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$，其中 $\overline{i} = \{i + kn \mid k \in \mathbb{Z}\}$，$i = 0, \ldots, n-1$。于是，我们有 $\mathbb{Z}/\equiv_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$。我们以后将 $\mathbb{Z}/\equiv_n$ 也记作 $\mathbb{Z}_n$ 或 $\mathbb{Z}/n\mathbb{Z}$，称之为 $\mathbb{Z}$ 模 n 的剩余类。我们在剩余类集合上可以定义运算加法 "$+$" 和乘法 "$\cdot$"[1] 如下：

$$\begin{aligned} + : \mathbb{Z} \times \mathbb{Z} &\longrightarrow \mathbb{Z} & \qquad \cdot : \mathbb{Z} \times \mathbb{Z} &\longrightarrow \mathbb{Z} \\ (\overline{a}, \overline{b}) &\longmapsto \overline{a + b} & (\overline{a}, \overline{b}) &\longmapsto \overline{ab} \end{aligned}$$

首先，这两个运算都是良定义的。我们只验证乘法 "$\cdot$" 的良定义性，加法 "$+$" 的验证留作练习。设 $\overline{a} = \overline{a'}$，$\overline{b} = \overline{b'}$，则 $n \mid a - a'$，$n \mid b - b'$，于是 $n \mid (a-a')(b-b') + a'(b-b') + b'(a-a')$，即 $n \mid ab - a'b'$，所以 $\overline{ab} = \overline{a'b'}$。此即 "$\cdot$" 良定义。

下面考察剩余类上加法和乘法满足的运算律。$\mathbb{Z}_n$ 上的加法满足：

(1) 交换律 $\overline{a} + \overline{b} = \overline{b} + \overline{a}$;

(2) 结合律 $(\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c})$;

(3) 加法单位元 $\overline{0}$：$\overline{0} + \overline{a} = \overline{a} + \overline{0} = \overline{a}$;

(4) 每个元素加法可逆：$\overline{a} + \overline{-a} = \overline{-a} + \overline{a} = \overline{0}$。

$\mathbb{Z}_n$ 上的乘法满足：

[1] 以后我们经常将 "$\cdot$" 省略。

(1) 交换律 $\overline{a}\overline{b} = \overline{b}\overline{a}$;

(2) 结合律 $(\overline{a}\overline{b})\overline{c} = \overline{a}(\overline{b}\overline{c})$;

(3) 单位元 $\overline{1}$: $\overline{1}\cdot\overline{a} = \overline{a}\cdot\overline{1} = \overline{a}$。

下面考虑 $\mathbb{Z}_n \setminus \{\overline{0}\}$ 上关于乘法可逆的元素 (显然 $\overline{0}$ 关于乘法不可逆)，我们有以下的命题：

命题 4.1.2. 设 $\overline{m} \in \mathbb{Z}_n$，则 $\overline{m}$ 在 $\mathbb{Z}_n$ 中关于乘法可逆 $\Longleftrightarrow \gcd(m,n) = 1$。

证明. ($\Longleftarrow$) 由 Bezout 关系，$\gcd(m,n) = 1 \Longrightarrow \exists a, b \in \mathbb{Z}$ 使得 $am+bn = 1$，则 $am \equiv 1 \mod n$，即 $\overline{a}\cdot\overline{m} = \overline{1}$，于是 $\overline{m}$ 乘法可逆 $\overline{a}$ 是 $\overline{m}$ 的乘法逆。
($\Longrightarrow$) 由 $\overline{m}$ 乘法可逆得存在 $\overline{a} \in \mathbb{Z}_n$ 使得 $\overline{a}\cdot\overline{m} = \overline{1}$，即 $am \equiv 1 \mod n$，所以存在 $b \in \mathbb{Z}$ 使得 $am + bn = 1$，即 $\gcd(m,n) = 1$。 □

马上我们就会知道，$\mathbb{Z}_n$ 是一个交换环，我们把 $\mathbb{Z}_n$ 中关于乘法可逆的元素放在一起做成一个集合，记作 $\mathbb{Z}_n^\times$。$\mathbb{Z}_n^\times$ 中的元素称为 (乘法) 可逆元或者单位 (unit)。

4.2 群

定义 4.2.1 (半群). 设 $*$ 是集合 S 上的一个二元运算，若 $*$ 满足结合律，则称 $(S,*)$ 是半群 (semigroup)(当运算已经明确时常常省略，即称 S 是半群)。特别地，若半群 $(S,*)$ 中有单位元 e，则称 $(S,*,e)$ 是幺半群 (monoid)；若半群 $(S,*)$ 中 $*$ 还满足交换律，则称 $(S,*)$ 是交换 (commutative or abeliean) 半群。

例 4.2.1. $(\mathbb{Z}_n,\cdot,\overline{1})$ 是幺半群；$(M_n(\mathbb{R}),\cdot,E_n)$ 也是幺半群。

下面的命题表明，幺半群中一个元素若可逆，则逆必然唯一。

命题 4.2.1. 设 $(S,*,e)$ 是幺半群，$x\in S$ 可逆，则 $\exists! y\in S$ 使得 $xy=yx=e$。

证明. 由于 $xy=yx=e$, $xz=zx=e$，因此 $y=ey=(zx)y=z(xy)=ze=z$。 □

于是我们可以定义群了。

定义 4.2.2. 设 $(G,*,e)$ 是幺半群，如果 $\forall g\in G$，g 都可逆，则称 $(G,*,e)$ 是群 (group)。

当一个群的运算明确时，我们常常省略群运算和单位元，而直接称 G 是群。以后，我们经常称群上的二元运算为乘法 (注意这只是一个称号！)。按这个定义，证明一个带有运算 (乘法) 的集合是群只需验证四点：乘法封闭，乘法结合律，存在单位元，求逆封闭。下面是一些常见的群的例子。

例 4.2.2. (1)$(\mathbb{Z},+,0)$ 和 $(\mathbb{Z}_n,+,\overline{0})$ 都是群，$(\mathbb{Q},+,0)$, $(\mathbb{R},+,0)$, $(\mathbb{C},+,0)$ 也都是群；
(2)$(M_n(\mathbb{R}),+,O_{n\times n})$ 是群；记 $\mathrm{GL}_n(\mathbb{R})=\{A\in M_n(\mathbb{R})\mid \mathrm{rank}(A)=n\}$，则 $(\mathrm{GL}_n(\mathbb{R}),\cdot,E_n)$ 是群，称为一般 (实) 线性群 (general linear group)；记 $\mathrm{SL}_n(\mathbb{R})=\{A\in M_n(\mathbb{R})\mid \det(A)=1\}$，则 $(\mathrm{SL}_n(\mathbb{R}),\cdot,E_n)$ 是群，称为特殊 (实) 线性群 (special linear group)；
(3) 设 X 是非空集合，记 $T_X=\{f:X\to X\mid f\text{是双射}\}$，则 $(T_X,\circ,\mathrm{id}_X)$ 是群，称为 X 的变换群。特别地，当 $X=\{1,2,\dots,n\}$ 时，即 $T_X=S_n$，我们称 $(S_n,\circ,e)$ 是 n 元置换群。

命题 4.2.2. 记 $\mathbb{Z}_n^*=\mathbb{Z}_n\setminus\{\overline{0}\}$，则 $(\mathbb{Z}_n^*,\cdot,\overline{1})$ 是群 $\Longleftrightarrow$ n 是素数。

证明. 由命题4.1.2立刻可证。 □

定义 4.2.3. 设 $(G,*,e)$ 是群，如果 $*$ 满足交换律，则称 G 是交换群或阿贝尔群 (abeliean group)，否则称为非交换群。

例 4.2.3. 在例4.2.2中，(1) 中的群和 (2) 中的 $(M_n(\mathbb{R}),+,O_{n\times n})$ 是交换群，其余例子都是非交换群。例如，S_3 中 $(1\ 2)(2\ 3)=(3\ 1\ 2)$, $(2\ 3)(1\ 2)=(1\ 3\ 2)$ 不相等。

当 G 是交换群时，我们经常称群 G 的运算为加法。

定义 4.2.4. 如果群 G 中只有有限个元素，则称 G 为有限群 (finite group)，否则称为无限群 (infinite group)。当 G 是有限群时，我们把 G 中元素的个数称为群 G 的阶 (order)，记为 $|G|$。

例 4.2.4. $(\mathbb{Z}_n,+,\overline{0}),(S_n,\circ,e)$ 都是有限群，而 $(\mathrm{GL}_n(\mathbb{R}),\cdot,E_n),(\mathrm{SL}_n(\mathbb{R}),\cdot,E_n)$ 都是无限群。

我们引入群的平移变换的概念，并证明一个引理。

引理 4.2.1. 设 G 是群，$a\in G$，则映射 $L_a:G\to G$, $g\mapsto ag$ 和 $R_a:G\to G$, $g\mapsto ga$ 都是双射，分别称为 G 关于 a 的左 (右) 平移变换。

证明. 由于 a 可逆，故可构造映射 $L_{a^{-1}}: G \to G,\ g \mapsto a^{-1}g$，则对 $\forall g \in G$，有

$$L_a \circ L_{a^{-1}}(g) = L_a(a^{-1}g) = aa^{-1}g = g$$

即 $L_a \circ L_{a^{-1}} = \mathrm{id}_G$。同理可以验证 $L_{a^{-1}} \circ L_a = \mathrm{id}_G$。于是 L_a 是双射。R_a 是双射可以用同样的方法证明。 □

有限群的构造可以用乘法表 (Cayley 表) 来表示。设群 $G = \{g_1, \ldots, g_n\}$，运算为乘法 $*$，则下表完全给出了 G 的结构：

$*$	g_1	g_2	$\cdots$	g_j	$\cdots$	g_n
g_1	g_1^2	g_1g_2	$\cdots$	g_1g_j	$\cdots$	g_1g_n
$\vdots$	$\vdots$					$\vdots$
g_i	g_ig_1	g_ig_2	$\cdots$	g_ig_j	$\cdots$	g_ig_n
$\vdots$	$\vdots$					$\vdots$
g_n	g_ng_1	g_ng_2	$\cdots$	g_ng_j	$\cdots$	g_n^2

由引理4.2.1知，Caylay 表的每一行，每一列的元素都互不相同，是 $g_1, \ldots, g_n$ 的一个重新排列。下面我们考虑一些低阶群的结构。

例 4.2.5. 1. $|G| = 1$: 即群 G 中只有一个单位元，记为 e；

2. $|G| = 2$: 即群 G 中只有单位元 e 和一个非单位元 a，此时乘法表为：

$*$	e	a
e	e	a
a	a	e

   $G = \{e, a\}$ 满足 $a^2 = e$。例如群 $(\mathbb{Z}_2, +, 0)$, $(S_2, \circ, e)$.

3. $|G| = 3$: 即群 G 中只有单位元 e 和两个非单位元 a, b，此时乘法表为：

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

   $G = \{e, a, b\}$ 满足 $b = a^2, b^2 = a, ab = ba = e$。例如群 $(\mathbb{Z}_3, +, 0)$,

$$\left\{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}\cos(2\pi/3) & -\sin(2\pi/3)\\ \sin(2\pi/3) & \cos(2\pi/3)\end{pmatrix}, \begin{pmatrix}\cos(4\pi/3) & -\sin(4\pi/3)\\ \sin(4\pi/3) & \cos(4\pi/3)\end{pmatrix}\right\}$$

4. $|G| = 4$，此时群 G 有两种结构，一是 $G = \{e, a, a^2, a^3\}$，满足 $a^4 = e$；另一种是 $G = \{e, a, b, ab\}$，满足 $a^2 = b^2 = (ab)^2 = e$，可以证明 4 阶群只有这两种结构，并且这两种结构是“不同”的！我们很快就会证明这一点。

有了群的概念以后，一个必然的问题是考虑不同的群之间的关系，这就是我们下面讨论的群的同态与同构。

定义 4.2.5. 设 $(G,*,e)$, $(H,\cdot,\varepsilon)$ 是两个群，我们称 $\varphi: G\to H$ 是 G 到 H 的同态映射 (homomorphism)，如果 φ 满足：$\forall g_1,g_2\in G$，有 $\varphi(g_1*g_2)=\varphi(g_1)\cdot\varphi(g_2)$。特别地，若 φ 是单射，则称 φ 是单同态 (injective homomorphism)；若 φ 是满射，则称 φ 是满同态 (surjective homomorphism)；若 φ 是双射，则称 φ 是同构 (isomorphism)。如果两个群 G,H 之间存在同构映射，则称 G 与 H 同构，记作 $G\simeq H$。

引理 4.2.2. 设 φ 是群 $(G,*,e)\to(H,\cdot,\varepsilon)$ 的同态，则：
(1)$\varphi(e)=\varepsilon$;
(2)$\forall g\in G$, $\varphi(g^{-1})=[\varphi(g)]^{-1}$;
(3) 若 φ 是同构，则逆映射 φ^{-1} 也是同构;
(4) 若 G 是交换群，H 是非交换群，则 φ 不是同构。

证明. (1) 首先我们有

$$\varphi(e)=\varphi(e*e)=\varphi(e)\cdot\varphi(e).$$

于是

$$\begin{aligned}\varepsilon&=\varphi(e)\cdot[\varphi(e)]^{-1}\\&=\varphi(e)\cdot\varphi(e)\cdot[\varphi(e)]^{-1}\\&=\varphi(e)\cdot\varepsilon\\&=\varphi(e).\end{aligned}$$

(2) 对 $\forall g\in G$，注意到 $\varepsilon=\varphi(e)=\varphi(g*g^{-1})=\varphi(g)\cdot\varphi(g^{-1})$，即 $\varphi(g^{-1})=[\varphi(g)]^{-1}$。
(3)φ 是双射推出 φ^{-1} 也是双射，于是我们只需证明 φ^{-1} 也是同态。对 $\forall h_1,h_2\in H$, $\exists!\, g_1,g_2\in G$ 使得 $\varphi(g_1)=h_1$, $\varphi(g_2)=h_2$，又因为 $\varphi(g_1*g_2)=\varphi(g_1)\cdot\varphi(g_2)=h_1\cdot h_2$，于是 $\varphi^{-1}(h_1\cdot h_2)=g_1*g_2=\varphi^{-1}(h_1)*\varphi^{-1}(h_2)$，即 φ^{-1} 是同态。
(4) 用反证法，设 φ 是同构。由于 G 是交换群，即任意 $a,b\in G$ 都有 $a*b=b*a$，用 φ 作用上去以后得到 $\varphi(a)\cdot\varphi(b)=\varphi(b)\cdot\varphi(a)$，又因为 φ 是双射，所以 $\varphi(a),\varphi(b)$ 可以取遍 H 中的所有元素，故 H 是交换群，这与 H 是非交换群矛盾！这样我们就完成了证明。 □

下面是一些同态的例子。

例 4.2.6. $\Pi_n:\mathbb{Z}\to\mathbb{Z}_n$, $a\mapsto\overline{a}$ 是群 $(\mathbb{Z},+,0)$ 到 $(\mathbb{Z}_n,+,\overline{0})$ 的同态；$\det:\mathrm{GL}_n(\mathbb{R})\to\mathbb{R}^*$, $A\to\det(A)$ 是群 $(\mathrm{GL}_n(\mathbb{R}),\cdot,E)$ 到 $(\mathbb{R}^*,\cdot,1)$ [1]的同态。验证留作练习。

引理 4.2.3. 设 G,H,K 是三个群，$\varphi:G\to H$, $\psi:H\to K$ 是群同态，则 $\psi\circ\varphi:G\to K$ 也是群同态。

证明可以由交换图 $\begin{array}{ccc}G&\xrightarrow{\varphi}&H\\&\searrow^{\psi\circ\varphi}&\downarrow\psi\\&&K\end{array}$ 表示，细节留作练习。

用上面的引理我们很容易证明群的同构是一个等价关系，细节留作练习。

例 4.2.7. 求证群 $(\mathbb{Z}_4,+,\overline{0})$ 与群 $(\mathbb{Z}_2\times\mathbb{Z}_2,+,(\overline{0},\overline{0}))$ 不同构。[2]

[1] $\mathbb{R}^*=\mathbb{R}\setminus\{0\}$
[2] 这里 $+$ 是指坐标分量对应相加。

证明. 用反证法，假设存在 $\varphi : \mathbb{Z}_4 \to \mathbb{Z}_2\times\mathbb{Z}_2$ 是同构，则 $\varphi(\bar{0}) = (\bar{0},\bar{0})$，注意到 $\forall y \in \mathbb{Z}_2\times\mathbb{Z}_2$, $y+y = (\bar{0},\bar{0})$，于是不管 $\varphi(\bar{1})$ 是 $\mathbb{Z}_2 \times \mathbb{Z}_2$ 中的哪个元素，都有 $\varphi(\bar{2}) = \varphi(\bar{1}) + \varphi(\bar{1}) = (\bar{0},\bar{0})$，这与 φ 是双射矛盾！ □

群论的一个基本问题就是给定一类群，寻找同构关系下的等价类，即对一类群按照同构进行分类。其中，一个基本的类型是对有限单群 [1] 进行分类。有限单群分类是 20 世纪最伟大的数学成就之一，相关的结果有上万页之多，即使简化后仍有数千页的证明，至今简化整理的工作尚未完成。

下面是一些小阶数群的分类。

表：阶数 $\leqslant 15$ 的群[2]

$\lvert G\rvert$	G	
	交换群	非交换群
1	$\{e\}$	
2	$\mathbb{Z}_2$	
3	$\mathbb{Z}_3$	
4	$\mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2$	
5	$\mathbb{Z}_5$	
6	$\mathbb{Z}_6$	$S_3 \simeq D_3$
7	$\mathbb{Z}_7$	
8	$\mathbb{Z}_8, \mathbb{Z}_2 \times \mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	D_4, Q_8
9	$\mathbb{Z}_9, \mathbb{Z}_3 \times \mathbb{Z}_3$	
10	$\mathbb{Z}_{10}$	D_5
11	$\mathbb{Z}_{11}$	
12	$\mathbb{Z}_{12}, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$	D_6, A_4, T
13	$\mathbb{Z}_{13}$	
14	$\mathbb{Z}_{14}$	D_7
15	$\mathbb{Z}_{15}$	

其中，$D_n = \{\sigma^i\tau^j \mid \sigma^n = \tau^2 = e,\ (\tau\sigma)^2 = e;\ i = 0,1,\ldots n-1;\ j = 0,1\}$ 是 $2n$ 阶群，被称为二面体群；S_n 是 n 元置换群；A_n 是全体 n 元偶置换在映射复合下形成的群；$Q_8 = \{\sigma^i\tau^j \mid \sigma^4 = e, \tau^2 = \sigma^2, \tau\sigma = \sigma^3\tau;\ i = 0,1,2,3;\ j = 0,1\}$；$T = \{\sigma^i\tau^j \mid \sigma^6 = 1, \tau^2 = \sigma^3, \tau\sigma = \sigma^5\tau;\ i = 0,1,\ldots,5;\ j = 0,1\}$。其中素数阶群和 $\leqslant 6$ 阶群的结构要求大家掌握，其余内容会在后续抽象代数课程中学习。

特别地，我们注意 D_3 的几何意义。考虑平面上的一个正三角形，对它进行变换，则保持这个三角形与原来重合的变换有且只有 6 个 (旋转 $0, \frac{2\pi}{3}, \frac{4\pi}{3}$ 角以及分别沿三条对称轴翻转)，它们在映射复合下构成的群称为 D_3。这样我们很容易看到 $D_3 \simeq S_3$。我们可以类似地定义 D_n 是保持正 n 边形与原来重合的变换构成的群。

下面我们开始介绍子群的概念。

定义 4.2.6. 设 $(G,*,e)$ 是群，$H \subset G$ 且 $e \in H$，如果 $(H,*,e)$ 也是群，则称 H 是 G 的子群 (subgroup)，记作 $H < G$。特别地，$\{e\}$ 和 G 本身都是 G 的子群，称为 G 的平凡子群 (trivial subgroup)；其余的 G 的子群称为 G 的真子群 (proper subgroup)。

[1] 我们会在抽象代数中介绍单群的概念，不过本讲义中不会出现了。

[2] 引自《近世代数引论》，冯克勤、李尚志、章璞著，中国科学技术大学出版社

引理 4.2.4. 设 $(G,*,e)$ 是群，H 是 G 的非空子集，则 H 是 G 的子群 $\Longleftrightarrow \forall h_1,h_2\in H,\ h_1h_2^{-1}\in H$。

证明. ($\Longrightarrow$) 由 H 是群，$h_2\in H$ 可知 $h_2^{-1}\in H$，又 $h_1\in H$，所以由群对乘法封闭可得 $h_1h_2^{-1}\in H$。($\Longleftarrow$) 首先，任取 $h\in H$ 则 $e=hh^{-1}\in H$，于是 $h^{-1}=eh^{-1}\in H$，即 H 对求逆封闭。下证 H 对乘法封闭。$\forall h_1,h_2\in H$，由上面的证明知 $h_2^{-1}\in H$，于是 $h_1h_2=h_1(h_2^{-1})^{-1}\in H$。即得结论。 □

引理 4.2.5. 设 $H_i,\ i\in I$ 是 G 的一族子群，则 $\bigcap\limits_{i\in I}H_i$ 也是 G 的子群。

证明. $\forall h_1,h_2\in\bigcap\limits_{i\in I}H_i$，我们知道对每个 $i\in I$，有 $h_1,h_2\in H_i$，由 H_i 是 G 的子群可知 $h_1h_2^{-1}\in H_i$。于是由交集的定义，$h_1h_2^{-1}\in\bigcap\limits_{i\in I}H_i$，再由引理4.2.4可知 $\bigcap\limits_{i\in I}H_i$ 也是 G 的子群。 □

需要注意的是，子群的积不一定是子群，即 $H<G,\ K<G$ 不能推出 $HK=\{hk\mid h\in H,\ k\in K\}<G$。反例取 S_3 的两个子群 $H=\{e,\ (1\ 2)\},\ K=\{e,\ (1\ 3)\}$ 即可验证。

例 4.2.8. 所有 n 元偶置换的集合 A_n 是 S_n 的子群，称为 n 元交错群。这是因为偶置换的积显然是偶置换，由引理1.5.6可知偶置换的逆也是偶置换，即 A_n 对乘法和求逆封闭，所以 $A_n<S_n$。

定义 4.2.7. 设 G 是群，$H<G$，任取 $g\in G$，称集合 $gH=\{gh\mid h\in H\}$ 为 H 的一个左陪集 (coset)。

类似地我们也可以定义右陪集的概念，事实上，H 的所有左陪集 (或右陪集) 构成了 G 的一个分割 [1](1.4.5 小节)，我们会在下面 Lagrange 定理的证明中顺便证明这一点。此外，注意到 $gH=L_g(H)$，而 L_g 是双射，因此 $\forall g\in G,\ |gH|=|H|$。

定理 4.2.1 (Lagrange 定理). 设 G 是有限群，$H<G$，则 $|H|\ \big|\ |G|$。

证明. 我们先证明如下的结论：如果子群 H 的两个左陪集 g_1H,g_2H 不相等，则 $g_1H\cap g_2H=\emptyset$。用反证法，假设存在 $a\in g_1H\cap g_2H$，则存在 $h_1,h_2\in H$ 使得 $a=g_1h_1=g_2h_2$，于是 $g_2=g_1(h_1h_2^{-1})\in g_1H$，那么 $\forall x\in g_2H$，都存在 $h\in H$ 使得 $x=g_2h=g_1(h_1h_2^{-1})h$，即 $x\in g_1H$，所以 $g_2H\subset g_1H$。同理可证 $g_1H\subset g_2H$，于是 $g_1H=g_2H$，这与 g_1H,g_2H 不相等矛盾！

下面我们证明原命题。H 是平凡子群时结论显然成立。下面考虑 H 是 G 的真子群的情形。令 $g_1=e$，取 $g_2\in G\setminus H$，如果 $g_1H\cup g_2H=G$，则由 $|gH|=|H|$ 可知 $2|H|=|G|$，命题成立；否则可取

$g_3\in G\setminus(g_1H\cup g_2H)$，如果 $G=g_1H\cup g_2H\cup g_3H$ 则命题成立；否则可以继续取 g_4 重复上述操作 $\cdots\cdots$。这一过程必然在有限步内终止，否则 $|G|=\infty$ 与 $|G|$ 是有限群矛盾！即 $\exists k\in\mathbb{N}^+$ 使得 $G=g_1H\cup\cdots\cup g_kH$ 是不交并，并且每个左陪集的元素个数都等于 $|H|$，所以 $|H|\ \big|\ |G|$。

□

实际上，G 的全体左陪集只有上面的 $g_1H,\ldots,g_kH$。这是因为 $\forall g\in G$，一定存在 $i\in\{1,\ldots,k\}$ 使得 $g\in g_iH$，即 $g=g_ih,\ h\in H$。于是 $g\in gH\cap g_iH\neq\emptyset$，故由上面的证明过程可知 $gH=g_iH$。

此外，若 $H<G$，则我们称 $|G|/|H|$ 为子群 H 在 G 中的指数，记作 $[G:H]$。

例 4.2.9. 由 Lagrange 定理立刻可以得到：如果 $|G|$ 是素数，则群 G 没有非平凡的子群。

[1]从而我们可以定义商群了，这会在抽象代数中学习。

下面我们考虑一类最简单的群：循环群。首先，在群 G 中我们可以将元素 x 的方幂推广到整数次方：记 $x^0 = e$, $x^{-n} = (x^{-1})^n$, $n \in \mathbb{Z}^+$。容易验证推广后的方幂仍然满足：$(x^n)(x^m) = x^{n+m}$, $(x^n)^m = x^{mn}$(留作练习)。

定义 4.2.8. 设 G 是群，若存在 $a \in G$ 使得 $\forall g \in G$，存在 $n \in \mathbb{Z}$ 使得 $g = a^n$，则称 G 是由元素 a 生成的循环群，记为 $G =< a >$；a 称为 G 的生成元。

显然 $< a >= \{a^m \mid m \in \mathbb{Z}\}$(重复的只保留一个代表)。注意循环群的生成元不一定是唯一的，因为 a 是生成元 $\iff$ a^{-1} 也是生成元。

例 4.2.10. 容易验证 $(\mathbb{Z}, +, 0)$, $(S_2, \circ, e)$ 都是循环群，它们的生成元分别是 1(或-1) 和 (1 2) (注意 $(1\ 2)^{-1} = (1\ 2)$)。

我们引入群元素的阶的概念。

定义 4.2.9. 设 G 是群，$a \in G$，如果不存在 $n \in \mathbb{Z}^+$ 使得 $z^n = e$，则称 a 是无穷阶元素，记为 $\mathrm{ord}(a) = \infty$；否则，一定存在一个最小的**正整数** k 使得 $a^k = e$，此时称 a 的阶是 k，记作 $\mathrm{ord}(a) = k$。

例 4.2.11. (1) S_3 中 (1 2) 的阶是 2，(1 2 3) 的阶是 3；

(2) $\mathbb{Z}$ 中任意元素的阶都是 ∞；

(3) $\mathbb{Z}_{10}$ 中 $\mathrm{ord}(\bar{2}) = 5$。

我们先证明下面两个引理。

引理 4.2.6. 设 G 是群，$g \in G$ 并且 $\mathrm{ord}(g) = k < \infty$，则 $g^n = e \iff k \mid n$。

证明. ($\Longrightarrow$) 作带余除法 $n = qk + r$，其中 $r \in \{0, 1, \ldots, k-1\}$，则 $g^{qk} = e^q = e$，于是 $g^n = g^{qk}g^r = g^r$，于是由 k 的最小性得 $r = 0$。
($\Longleftarrow$) $n = kq \Longrightarrow g^n = (g^k)^q = e^q = e$。 □

引理 4.2.7. 设 G 是群，$g \in G$。
(1) 若 $\mathrm{ord}(g) = \infty$，则 $\forall i, j \in \mathbb{Z}$，都有 $g^i \neq g^j$；
(2) 若 $\mathrm{ord}(g) = k \in \mathbb{Z}^+$，则 $k = |< g >|$ 并且 $< g >= \{e, g, \ldots, g^{k-1}\}$。

证明. (1) 用反证法。如果 $\exists i, j$ 使得 $g^i = g^j$，不妨设 $i > j$，则 $g^{i-j} = e$，与 $\mathrm{ord}(g) = \infty$ 矛盾！
(2)$< g >= \{g^n \mid n \in \mathbb{Z}\}$。而对每个 $n \in \mathbb{Z}$，都可以作带余除法 $n = qk + r$, $r \in \{0, \ldots, k-1\}$，此时 $g^n = g^{qk}g^r = g^r \in \{e, g, \ldots, g^{k-1}\}$。而 $\forall i, j \in \{0, 1, \ldots, k-1\}, i \neq j$，有 $g^i \neq g^j$(否则不妨设 $i > j$，则 $g^{i-j} = e$，而 $i - j < k$，这与 k 的最小性矛盾！)。此即我们所需要的结论。 □

推论 4.2.1. 设 G 是有限群，$g \in G$，则 $\mathrm{ord}(g) \mid |G|$。

这是 Lagrange 定理的直接推论。
下面我们可以对循环群的结构进行讨论了。

定理 4.2.2. 设 G 是循环群，若 $|G| = \infty$，则 $G \simeq (\mathbb{Z}, +, 0)$；若 $|G| = n$, $n \in \mathbb{Z}^+$，则 $G \simeq (\mathbb{Z}_n, +, \bar{0})$。

证明. (1) 设 $G =< g >$，如果 $\mathrm{ord}(g) = \infty$，则可以作映射：

$$\begin{aligned} \varphi : G &\longrightarrow \mathbb{Z} \\ g^n &\longmapsto n. \end{aligned}$$

由引理4.2.7(1) 易证 φ 是双射，并且 $\varphi(g^m g^n) = \varphi(g^{m+n}) = m+n = \varphi(g^m)+\varphi(g^n)$，即 φ 是同构。
(2)G 是循环群且 $|G| = n$，那么 G 的生成元 (不妨记作 a) 一定是 n 阶元。由引理4.2.7(2) 知 $G =< a >= \{e, a, \ldots, a^{n-1}\}$，于是可以作映射：

$$\begin{aligned} \varphi : G &\longrightarrow \mathbb{Z}_n \\ a^j &\longmapsto \bar{j}. \end{aligned}$$

容易验证 φ 是良定义的双射并且是同态，于是 φ 是同构。 □

例 4.2.12. *G 是群且 $|G| = 4$，则必有 $G \simeq \mathbb{Z}_4$ 或 $G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$。*

证明. 由 Lagrange 定理，G 中元素的阶只可能是 1，2，4。(1) 如果 G 中有一个 4 阶元 g，则容易作同构 $G \to \mathbb{Z}_4$，$g \mapsto \bar{1}$(验证同构是显然的)。
(2) 若 G 中只有单位元 e 和三个二阶元 a, b, c，则作映射

$$\begin{aligned} \varphi : G &\longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2 \\ e &\longmapsto (\bar{0}, \bar{0}) \\ a &\longmapsto (\bar{1}, \bar{0}) \\ b &\longmapsto (\bar{0}, \bar{1}) \\ c &\longmapsto (\bar{1}, \bar{1}). \end{aligned}$$

容易验证这是一个同构。 □

命题 4.2.3. *(1) 循环群都是交换群，并且其任何子群都是循环群；*
(2) 无限循环群 G 的子群必然同构于 $(m\mathbb{Z} = \{mn \mid n \in \mathbb{Z}\}, +, 0)$；
(3)G 是 n 阶循环群，则对每个 $m \mid n$，存在 G 的唯一 m 阶子群。[1]

证明. (1) 显然循环群是交换群。设 $G =< g >$ 是循环群，下面我们证明 G 的子群都形如 $< g^l >$，其中 l 是非负整数。设 H 是 G 的某个子群，平凡子群的情形显然取 $l = 0$ 即可，因此我们只需考虑非平凡情形。取 $l = \min\{i \in \mathbb{Z}^+ \mid g^i \in H\}$，则 $g^l \in H$，于是 $< g^l > \subset H$; 反过来，如果 $a = g^k \in H$，作带余除法 $k = lm + r$, $0 \leqslant r < l$，则 $g^r = \underbrace{(g^l)^{-m}}_{\in H} \underbrace{g^k}_{\in H} \in H$，由 l 的最小性可知 r 只能是 0，即 $a = (g^l)^m \in < g^l >$, $H \subset < g^l >$，所以 $H =< g^l >$。综上所述循环群的任何子群都是循环群。
(2) 这是 (1) 和定理4.2.2的直接推论。
(3) 设 $G =< g >$，由于 $m \mid n$，则按照子群的定义容易验证 $H =< g^{\frac{n}{m}} >= \{e, g^{\frac{n}{m}}, \ldots, (g^{\frac{n}{m}})^{m-1}\}$ 是 G 的 m 阶子群。而如果另有 H' 也是 G 的 m 阶子群，仿照 (1) 的过程取 $l = \min\{i \in \mathbb{Z}^+ \mid g^i \in H\}$，则 $H' =< g^l >= \{e, g^l, \ldots, (g^l)^{m-1}\}$，其中 m 应该满足 $g^{lm} = e = g^n$，且 $e, g^l, \ldots, (g^l)^{m-1}$ 互不相同。于是 $n \mid lm$，即 l 是满足 $\frac{n}{m} \mid l$ 的最小正整数，即 $l = \frac{n}{m}$, $H' = H$。 □

由一个元素生成的群是循环群，我们已经讲的比较清楚了。我们可以进一步考虑由一些元素生成的群，这就需要生成组的概念。

定义 4.2.10 (生成组). *设 G 是群，$S \subset G$ 是非空子集，如果包含 S 的 G 的子群只有 G 本身，则称 S 是 G 的生成组。*

[1] 这个结论可以推广到：G 是 n 阶群，则 G 是循环群 $\iff$ 对每个 $m \mid n$，存在唯一 G 的 m 阶子群。证明较难，可以参考《抽象代数学习辅导》孟道骥等著，科学出版社 P47。

我们也可以这样来看待这个定义：将所有包含 S 的 G 的子群作交集，得到的还是一个子群 (引理4.2.5)，记其为 $< S >$。即 $< S >$ 是 G 中包含 S 的最小的子群。如果 $< S >= G$，则 S 是 G 的生成组。此外，我们还可以从元素运算的角度定义生成组：记 $S^{-1} = \{a^{-1} \mid a \in S\}$，则

$$< S >= \{x_1 \cdots x_m \mid m \in \mathbb{Z}^+,\ x_i \in S \cup S^{-1}, i = 1,\ \ldots, m\} \tag{4.2.1}$$

可以证明这两个定义是一致的 (留作习题)。

例 4.2.13. $\mathrm{GL}_n(\mathbb{R})$ 的生成组是 $\mathbb{R}$ 上所有 n 阶初等矩阵的集合；S_n 的生成组是全体对换或全体循环。

当生成组 S 是有限集时我们称群 G 是**有限生成**的，显然有限群必然是有限生成的，但有限生成的群可以是无限群，例如 $(\mathbb{Z}, +, 0) =< 1 >$ 就是有限生成的。

接下来我们更深入地讨论群同态和同构的一些性质。

定义 4.2.11. 设 $f : (G, *, e) \to (H, \cdot, \varepsilon)$ 是群同态，我们定义同态核 $\ker(f) = \{x \in G \mid f(x) = \varepsilon\}$，同态像 $\mathrm{im}(f) = \{y \in H \mid \exists x \in G 使得 y = f(x)\}$。

容易验证 $\ker(f)$ 和 $\mathrm{im}(f)$ 分别是 G 和 H 的子群。我们验证 $\ker(f)$ 是 G 的子群，另一个验证留作练习。设 $a, b \in \ker(f)$，即 $f(a) = f(b) = \varepsilon$ 则 $f(ab^{-1}) = f(a)[f(b)]^{-1} = \varepsilon$，所以 $ab^{-1} \in \ker(f)$。由引理4.2.4即得结论。

我们有更进一步的结论：$\ker(f)$ 是 G 的正规子群[1] ，并且 G 的每个正规子群都是 G 到某个群的同态核。我们会在抽象代数课程中证明这一点。

例 4.2.14. (1) 令 $\varphi : S_n \to (\{\pm 1, \times, 1\})$, $\sigma \mapsto \varepsilon_\sigma$，则 $\ker(f) = A_n$。

(2) 令 $\varphi : S_n \to \mathrm{GL}_n(\mathbb{R})$, $\sigma \mapsto A = (a_{ij})_{n\times n}$，其中 $a_{ij} = \begin{cases} 1, & i = \sigma(j); \\ 0, & i \neq \sigma(j). \end{cases}$ 则 $\ker(\varphi) = \{e\}$。

引理 4.2.8. 设 $f : (G, *, e) \to (H, \cdot, \varepsilon)$ 是群同态，则 f 是单同态 $\iff \ker(f) = \{e\}$；f 是满同态 $\iff \mathrm{im}(f) = H$。

直接按照单同态和满同态的定义即可证明。

下面的定理表明了变换群在群论中的重要作用。

定理 4.2.3 (Cayley 定理). 任何一个群 G 都同构于 G 到自身的变换群 T_G(定义于例4.2.2(3)) 的某一个子群。

证明. 作映射 $\varphi : G \to T_G$, $g \mapsto L_g$，其中 L_g 是引理 4.2.1 中定义的左平移变换 (显然 $L_g \in T_G$)。

首先，φ 是同态，这是因为任取 $g_1, g_2 \in G$ 及 $x \in G$，有 $L_{g_1g_2}(x) = g_1g_2x = L_{g_1} \circ L_{g_2}(x)$，从而

$$\varphi(g_1g_2) = L_{g_1g_2} = L_{g_1} \circ L_{g_2} = \varphi(g_1) \circ \varphi(g_2).$$

其次 φ 是单射，这是因为：如果 $\varphi(g_1) = \varphi(g_2)$，即 $L_{g_1} = L_{g_2}$，则 $L_{g_1}(e) = L_{g_2}(e)$，即 $g_1e = g_2e$，$g_1 = g_2$。于是 $\mathrm{im}(\varphi)$ 作为 T_G 的子群与 G 同构。 □

推论 4.2.2. 设 G 是 n 阶群，则 G 同构于 S_n 的某一个子群。

[1] 即 $\forall g \in G$, $a \in \ker(f)$，有 $gag^{-1} \in \ker(f)$。

这是 Cayley 定理的直接推论。

需要注意的是，无限群可以同构于自身的一个真子群，例如 $m\mathbb{Z} < \mathbb{Z}$，但 $\mathbb{Z} \to m\mathbb{Z} : n \mapsto mn$ 就是一个同构。

最后，我们考虑群到自身的同态 (或同构) 映射，称为群的**自同态 (或自同构)**。

命题 4.2.4. *群 G 到自身的所有同态的集合 (记作 $\mathrm{Hom}(G)$) 在映射复合下构成了一个幺半群；G 到自身的所有同构的集合 (记作 $\mathrm{Aut}(G)$) 在映射复合下构成群。*

证明留作练习。

定义 4.2.12. *我们称形容：$I_a : G \to G,\ g \mapsto aga^{-1}$ 的 G 的自同构 (验证这是同构留作练习) 为群 G 的内自同构映射。容易验证 G 的所有内自同构映射构成一个群 (练习)，称为 G 的内自同构群，记作 $\mathrm{Inn}(G)$。*

可以证明 $\mathrm{Inn}(G)$ 是 $\mathrm{Aut}(G)$ 的一个正规子群，并且 G 是交换群 $\iff \mathrm{Inn}(G)$ 是平凡群 $\{\mathrm{id}\}$。

例 4.2.15. *设 G 是有限群，设 $\varphi \in \mathrm{Aut}(G), \varphi^2 = \mathrm{id}_G$，并且若 $a \neq e$ 则一定有 $\varphi(a) \neq a$，则：*
(1)G 是交换群；
(2)$|G|$ 是奇数。

证明. 首先，任取 $a \in G$，令 $g = \varphi(a)a^{-1}$，则

$$\varphi(g) = \varphi^2(a)[\varphi(a)]^{-1} = a[\varphi(a)]^{-1} = [\varphi(a)a^{-1}]^{-1} = g^{-1}.$$

下面说明 g 能取遍 G。注意到如果 $\varphi(a)a^{-1} = \varphi(b)b^{-1}$，则

$$\varphi(b^{-1}a) = \varphi^{-1}(b)\varphi(a) = b^{-1}a.$$

于是 $b^{-1}a = e$，即 $a = b$。这说明 $\psi : a \to \varphi(a)a^{-1}$ 是单射。由定理 1.3.3 知 ψ 是双射，即当 a 取遍 G 时 g 可以取遍 G。

那么 φ 就是映射 $G \to G,\ g \mapsto g^{-1}$。于是：
(1)$\forall a, b \in G,\ ab = \varphi(a^{-1})\varphi(b^{-1}) = \varphi((ba)^{-1}) = ba$。即 G 是交换群。
(2) 先证明：如果 $g_i \neq g_j$且$g_i \neq g_j^{-1}$，则 $\{g_i, g_i^{-1}\} \cap \{g_j, g_j^{-1}\} = \emptyset$。

用反证法。如果 $\{g_i, g_i^{-1}\} \cap \{g_j, g_j^{-1}\} \neq \emptyset$，则由条件可知 $g_i \notin \{g_j, g_j^{-1}\}$，那么只能是 $g_i^{-1} \in \{g_j, g_j^{-1}\}$。如果 $g_i^{-1} = g_j$，那么 $g_i = g_j^{-1} \in \{g_j, g_j^{-1}\}$，矛盾；如果 $g_i^{-1} = g_j^{-1}$，那么 $g_i = g_j \in \{g_j, g_j^{-1}\}$，也矛盾！于是 $g_i \neq g_j$且$g_i \neq g_j^{-1} \Longrightarrow \{g_i, g_i^{-1}\} \cap \{g_j, g_j^{-1}\} = \emptyset$。

因此，G 由 e 与成对的 $\{g_i, g_i^{-1}\},\ i = 1, \ldots, k$ 组成，不同的 i 对应的对交为空集。所以 $|G|$ 是奇数。 □

4.3 环

上一节我们介绍了群的概念和简单性质。然而，群中只有一种运算，而我们常见的数学结构中往往有两种或更多的运算，并且运算之间有联系。这时，我们就需要更多的工具来研究问题，例如本节的环。

定义 4.3.1. 设 $(R,'+','0')$ 是一个交换群，如果 R 上还有另一种运算“乘法” $'\cdot'$，并且 $(R,'\cdot')$ 构成乘法半群 (即 $'\cdot'$ 满足结合律)，如果乘法对加法“+”还满足左右分配律，即 $\forall x,y,z\in R$:

$$(x+y)\cdot z = x\cdot z + y\cdot z;\ x\cdot(y+z) = x\cdot z + y\cdot z.$$

则称 $(R,'+','\cdot')$ 是一个环。

注 4.3.1. (1) 一般地，我们研究的环都要求乘法构成一个幺半群，即乘法有单位元 $'1'$，称为幺环。以后，如果我们不作特别说明的话，我们所说的环都是幺环，同时标明乘法单位元。
(2) 以后，在不引起歧义的情况下，我们经常将乘法的“$\cdot$”省略。

例 4.3.1. (1)$(\mathbb{Z},+,0,\cdot,1)$, $(\mathbb{Q},+,0,\cdot,1)$, $(\mathbb{R},+,0,\cdot,1)$, $(\mathbb{C},+,0,\cdot,1)$ 都是环。
(2) 由 4.1 节最后的大段论述可知，$(\mathbb{Z}_n,+,\overline{0},\cdot,\overline{1})$ 是环，称为模 n 的剩余类环。
(3) 所有 n 阶方阵的集合在矩阵的加法和乘法下构成环，称 $(M_n(\mathbb{R}),+,O_{n\times n},\cdot,E_n)$ 为 n 阶矩阵环。
(4) 设 X 是集合，R 是环，我们将所有 $X\to R$ 的函数放在一起做成一个集合，记为 R^X，在 R^X 上定义加法和乘法如下：$\forall f,g: X\to R$，定义：

$$\begin{aligned} f+g: X &\longrightarrow R & \qquad f\cdot g: X &\longrightarrow R \\ x &\longmapsto f(x)+g(x) & x &\longmapsto f(x)\cdot g(x) \end{aligned}$$

容易验证 (验证留作练习) 这是一个环，0 函数和 1 函数分别是其加法单位元和乘法单位元，称为 X 到 R 的函数环。
(5) 设 $(A,+,0)$ 是一个加法交换群，在 A 上定义乘法：$\forall x,y\in A$，定义 $x\cdot y=0$，则 A 关于这个乘法是一个半群 (但不是幺半群！)，我们称 $(A,+,0,'\cdot')$ 是 A 的零乘法环 (不是幺环)。

以后，我们将 R 对于加法做成的群的单位元 0 为 R 的零元，乘法幺半群的的单位元 1 称为幺元。设 $a\in R$，我们将 a 在加法运算下的逆记为 $-a$，称为 a 的负元。将 $m(\in\mathbb{Z}^+)$ 个 a 连加得到的结果记为 ma，并规定 $0a=0$, $(-n)a=-(na)$。此外，将 m 个 a 连乘得到的结果记为 a^m。此外，将 $a+(-b)$ 简记为 $a-b$。

命题 4.3.1. (1) 对 $\forall a,b\in R$ 和 $m,n\in\mathbb{Z}$，我们有 $(m+n)a=ma+na$, $m(-a)=-(ma)$, $(mn)a=m(na)$, $m(a+b)=ma+mb$[1];

(2) 对 $\forall a\in R$, $m,n\in\mathbb{Z}^+$，有 $a^{m+n}=a^ma^n$, $a^{mn}=(a^m)^n$;

(3) 广义分配律：$a_1,\dots,a_n,b_1,\dots,b_m\in R$，则 $(\sum_{i=1}^n a_i)(\sum_{j=1}^m b_j)=\sum_{i=1}^n\sum_{j=1}^m a_ib_j$;

(4) $\forall a,b\in R$, 有 $a0=0a=0$(这里 0 是 R 的零元) 以及 $(-a)b=a(-b)=-(ab)$, $(-a)(-b)=ab$。

[1] 即任何一个环的加法结构可以视作整数环 $\mathbb{Z}$ 上的左模。实际上交换群即可满足这些性质，为此，我们可以使用主理想整环上的有限生成模结构定理来给出有限生成交换群的分类，我们会在抽象代数中学习。

证明. (1)(2) 的证明比较简单，留作练习。(3) 只需对 m,n 分别做数学归纳法即可。
对于 (4)，首先 $a0 = a(0+0) = a0+a0$，于是 $0 = a0$(加法成群，因此有消去律)。$0a = 0$ 同理可证。其次，注意到 $a(b+(-b)) = a0 = 0$，用分配律展开得 $ab + a(-b) = 0$，而 ab 的负元为 $-(ab)$，所以 $a(-b) = -ab$。$(-a)b = -(ab)$ 同理。最后，$(-a)(-b) = -(a(-b)) = -(-ab) = ab$。 □

推论 4.3.1 (二项式定理). 设 R 是环，$a,b \in R$ 且 $ab = ba$，$n \in \mathbb{Z}$，则

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

证明是简单的，留作练习。

一个平凡的情形是，如果一个环 R 中 $0 = 1$，那么 R 中只有一个元素 0。这是因为 $\forall a \in \mathbb{R}$，有 $a = a\cdot 1 = a\cdot 0 = 0$。零环的结构简单，没有研究价值，因此下面我们只要不特别声明，均要求环 R 中 $0 \neq 1$。

定义 4.3.2. 设 R 是环，$a \in R \setminus \{0\}$，如果 $\exists b \in R \setminus \{0\}$ 使得 $ab = 0$，则称 a 为 R 中的左零因子；反过来，$b \in R \setminus \{0\}$，如果 $\exists a \in R \setminus \{0\}$ 使得 $ab = 0$，则称 b 为 R 中的右零因子。左零因子和右零因子统称为零因子。如果 R 中乘法是交换的，则不区分左零因子和右零因子。

例 4.3.2. (1)$(\mathbb{Z},+,0,\cdot,1)$ 中没有零因子。
(2)$(M_n(\mathbb{R}),+,O_{n\times n},\cdot,E_n)$ 中，矩阵 A 是零因子 $\iff \operatorname{rank}(A) < n$。
这是因为：如果存在非零矩阵 B 使得 $AB = O_{n\times n}$ 或 $BA = O_{n\times n}$，则由 Sylvester 不等式易得 $\operatorname{rank}(A) < n$；反之，$\operatorname{rank}(A) < n$ 可知 $A\mathbf{x} = \mathbf{0}$ 的解空间 V_A 不是零子空间，设 $\mathbf{v} \in V_A$，令 $B = (\mathbf{v},\mathbf{0},\ldots,\mathbf{0})$ 即有 $AB = O_{n\times n}$。

命题 4.3.2. R 是无零因子环 $\iff$ R 满足左右消去律 (即 $x \neq 0$，则 $xy = xz$ 或 $yx = zx$ 都可以得到 $y = z$)。

这个命题在群当中是显然的，因为我们可以左乘 (或右乘)x^{-1} 直接得到结论。但在环中，由于元素关于乘法不一定可逆，因此我们需要借助加法。

证明. ($\Longrightarrow$) 由 R 中无零因子，故 $xy = xz \Rightarrow x(y-z) = 0 \Rightarrow y - z = 0$，即 $y = z$。右消去律同理。
($\Longleftarrow$) 设环 R 满足左右消去律，则若 $ax = 0$，即 $ax = a0$，由左消去律得 $x = 0$，即 R 没有右零因子；同理可证 R 没有左零因子。 □

下面我们定义一些特殊的环。

交换环 (abeliean ring)	R 上的乘法满足交换律
整环 (integral domain)	无零因子交换幺环
除环 (体，斜域，division ring)	$R \setminus \{0\}$ 关于乘法成群，即非零元关于乘法都可逆
域 (field)	交换的除环，即可以进行“通常”的加减乘除的结构

定义 4.3.3. 设 R 是环，$a \in R$，如果存在 $b \in R$ 使得 $ab = 1$，则称 a 右可逆；同理可以定义左可逆。如果 a 既是左可逆的又是右可逆的，则称 a 是 R 中的 (乘法) 可逆元或者单位 (unit)。如果 a 可逆，则逆一定唯一，证明方法类似于逆矩阵的唯一性。显然 R 中的所有单位关于 R 上的乘法构成群 (验证留作练习)，称为 R 的单位群 (unit group)，记作 $R^\times$ 或 U_R。

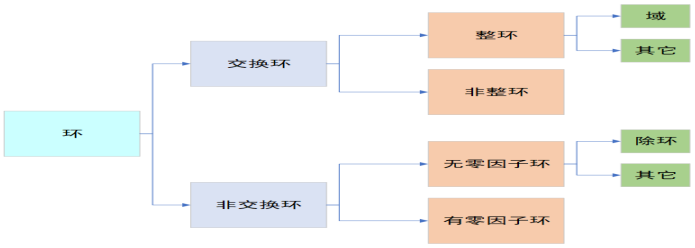


图 4.3-1 环

首先，零因子一定不会是单位，这是因为如果环 R 中 $ab = 0$，$a, b \neq 0$，那么如果 $ac = ca = 1$，就有 $a(c+b) = 1$，那么 $c + b = ca(c+b) = c$，即 $b = 0$，矛盾！但我们需要注意的是，乘法不可逆元不全是零因子，例如 $(\mathbb{Z}, +, 0, \cdot, 1)$ 中 2 是乘法不可逆元，但不是零因子。

例 4.3.3. 矩阵环 $M_n(\mathbb{R})$ 中的所有单位是 $\mathrm{GL}_n(\mathbb{R})$。

命题 4.3.3. 在剩余类环 $\mathbb{Z}_n$ 中：
(1)$\overline{m}$ 是单位 $\iff \gcd(m, n) = 1$；
(2)$\overline{m}$ 是零因子 $\iff \gcd(m, n) > 1$ 且 $n \nmid m$。

证明. 命题的前一部分已经在命题4.1.2中证明过了，下面证明后一部分。
($\Longrightarrow$) 由 $\overline{m}$ 是零因子，即 $\overline{m} \neq \overline{0}$ 且 $\overline{m}$ 不可逆，即 $n \nmid m$ 且 $\gcd(m, n) > 1$。
($\Longleftarrow$) 设 $g = \gcd(m, n)$，由 $g > 1$，$n \nmid m$ 可知 $\exists k, l \in \mathbb{Z}$ 使得 $m = kg$，$n = lg$ 并且 $\overline{l} \neq \overline{0}$，于是 $lm = lkg = kn$，即 $\overline{lm} = \overline{lm} = \overline{0}$。

□

于是 $\mathbb{Z}_n$ 的单位群 $\mathbb{Z}_n^\times$ 中有 $\varphi(n)$ 个元素 ($\varphi(n)$ 是欧拉函数，表示小于 n 并且与 n 互素的正整数个数)。特别地，当 p 是素数时，$|\mathbb{Z}_p^\times| = p - 1$。于是我们有下面的定理。

定理 4.3.1 (Euler 定理). 对 $\forall a \in \mathbb{Z}$，$n \in \mathbb{Z}^+$，假设 $\gcd(a, n) = 1$，则有 $a^{\varphi(n)} \equiv 1 \mod n$，其中 φ 是欧拉函数。特别地，若 p 是素数，则 $a^{p-1} \equiv 1 \mod p$(Fermat 小定理)。

证明. 由于 $\gcd(a, n) = 1$，故可以任取 $\overline{a} \in \mathbb{Z}_n^\times$，由于 $\mathbb{Z}_n^\times$ 关于剩余类的乘法是群，故可以考虑 $\overline{a}$ 在这个群中的阶 $\mathrm{ord}(\overline{a})$。由推论4.2.1，我们有 $\mathrm{ord}(\overline{a}) \mid |\mathbb{Z}_n^\times|$，又由上面的论证知 $|\mathbb{Z}_n^\times| = \varphi(n)$，即 $\overline{a}^{\varphi(n)} = \overline{1}$，也即 $a^{\varphi(n)} \equiv 1 \mod n$。特别地，当 p 是素数时，$\varphi(p) = p - 1$，即得到 Fermat 小定理。 □

类似于群的同态和同构，我们可以定义环的同态和同构。

定义 4.3.4. 设 $(R, +, 0_R, \cdot, 1_R)$ 和 $(S, +, 0_S, \cdot, 1_S)$ 是两个环，$\varphi : R \to S$。如果对 $\forall z, y \in R$，有 $\varphi(x + y) = \varphi(x) + \varphi(y)$，$\varphi(xy) = \varphi(x)\varphi(y)$ 成立，则我们称 φ 是环同态。类似地我们可以定义单同态、满同态和同构的概念。

例 4.3.4. $\pi_n : \mathbb{Z} \to \mathbb{Z}_n$，$a \mapsto \overline{a}$ 是环同态，验证留作练习。

定义 4.3.5. 设 $\varphi : R \to S$ 是环同态，我们同样可以定义同态核：$\ker(\varphi) = \{r \in R \mid \varphi(r) = 0_S\}$ 和同态像：$\mathrm{im}(\varphi) = \{s \in S \mid \exists r \in R \text{使得} \varphi(r) = s\}$。

命题 4.3.4. 设 $\varphi : R \to S$ 是环同态，则 φ 是单同态 $\iff \ker(\varphi) = \{0_R\}$。

直接利用定义即可证明。

一般的，我们以后提到环同态时默认满足 $\varphi(1_R) = 1_S$，这个条件在下面的情形中可以自然推出。

命题 4.3.5. (1) 设 R,S 是环，S 无零因子。如果环同态 $\varphi: R \to S$ 不是零同态 (即 $\forall x \in R,\ \varphi(r) = 0_S$)，那么 $\varphi(1_R) = \varphi(1_S)$。
(2) 设 R,S 是环，若 $\varphi: R \to S$ 是满同态，则 $\varphi(1_R) = \varphi(1_S)$。

证明. (1) 注意到 $\varphi(1_R)\varphi(1_R) = \varphi(1_R \cdot 1_R) = \varphi(1_R)$，即 $\varphi(1_R)(\varphi(1_R) - 1_S) = 0_S$，由 S 无零因子，故 $\varphi(1_R) = 0_S$ 或 $\varphi(1_R) = 1_S$。前者表明 $\forall r \in R,\ \varphi(r) = \varphi(1_R)\varphi(r) = 0_S$，即零同态；后者即我们所需要的结论。
(2) 任取 $y \in S$，则存在 $x \in R$ 使得 $\varphi(x) = y$，于是 $\varphi(1_R)y = \varphi(1_R)\varphi(x) = \varphi(1_R x) = \varphi(x) = y$；同理 $y\varphi(1_R) = y$，于是由乘法幺元的定义及唯一性知 $\varphi(1_R) = 1_S$。 □

然而，在一般情形下 $\varphi(1_R) = 1_S$ 可能不对，例如 $\mathbb{Z}_3 \to \mathbb{Z}_6,\ \overline{a} \mapsto \overline{4a}$。按照代数学引论的定义我们不把这样的映射称为环同态。

下面我们考虑一个重要的定义：环的**特征** (characteristic)，它反映了环的加法性质。

定义 4.3.6. 设 R 为环。如果 1 在加法群 $(R,+,0)$ 中是无穷阶的，则称 R 的特征为 0；反之，如果 1 在 $(R,+,0)$ 中是 $n(\in \mathbb{Z}^+)$ 阶的，则称 R 的特征为 n。我们将环 R 的特征记为 $\mathrm{char}(R)$。

例 4.3.5. $\mathrm{char}(\mathbb{Z}) = 0,\ \mathrm{char}(\mathbb{Z}_n) = n.$

命题 4.3.6. 如果环 R 的特征 $\mathrm{char}(R) = m > 0$，$n \in \mathbb{Z}$ 且 $m \mid n$，则任意 $r \in R$，有 $nr = 0$。

证明. 记 $0_R, 1_R$ 分别为环 R 中的加法零元和乘法幺元，首先 $\underbrace{1_R + \cdots + 1_R}_{\text{m 个}} = 0_R$。设 $n = km$，则由命题4.3.1及环中的分配律可得 $nr = km(1_R \cdot r) = k(m(1_R \cdot r)) = k\left(\underbrace{(1_R \cdot r + \cdots + 1_R \cdot r)}_{\text{m 个}}\right) =$
$k\left(\underbrace{(1_R + \cdots + 1_R)}_{\text{m 个}} \cdot r\right) = k(0_R \cdot r) = 0$。 □

命题 4.3.7. 设 R 为无零因子环，令 $R^* = R \setminus \{0\}$，则 R^* 中的元素对于 R 的加法具有相同的阶，且当这一共同的阶有限时，必为素数。

证明. 首先，如果 R^* 中的所有元素关于加法都是无穷阶的，那么命题显然成立。

其次，如果存在 $a \in R^*$ 使得 a 关于加法的阶是一个有限的正整数 n，那么，对任意的 $b \in R^*$，我们需要证明 b 的加法阶也是 n。由于 $na = 0$，注意到 $0 = 0b = (na)b = a(nb)$，而 R 是无零因子环，且 $a \neq 0$，于是 $nb = 0$，即 b 的加法阶整除 n。设 b 的加法阶为 m，反过来对 a 进行上述讨论可得 $n \mid m$，所以 $n = m$，由 b 的任意性可知 R^* 中所有元素的加法阶都相同。

最后，如果 R^* 中元素的加法阶是 $n \in \mathbb{Z}^+$，我们需要证明 n 是素数。用反证法，如果存在 $k,l \in \{2,3,\ldots,n-1\}$ 使得 $n = kl$，则对 $a \in R^*$，有 $(ka)(la) = na^2 = (na)a = 0$，但由加法阶的定义可知 $ka \neq 0,\ la \neq 0$，于是 $ka,\ la$ 是零因子，这与 R 是无零因子环矛盾！这样我们完成了证明。 □

上面的命题告诉我们无零因子环的特征必定为素数。反过来，如果环的特征是合数，则必有零因子 (证明留作练习)。

命题 4.3.8. 设 R 为整环，其特征为素数 p，则对任何 $a,b \in R$，有

$$(a+b)^p = a^p + b^p, \quad (a-b)^p = a^p - b^p.$$

利用二项式定理及 $p \mid \binom{p}{k}$ (例1.6.3) 即可证明。

类似于子群的概念，我们也可以定义子环：

定义 4.3.7. 设 $(R,+,0,\cdot,1)$ 是环，如果 $S \subset R$，且 $(S,+,0,\cdot)$ 也是环 (这里有时并不要求 S 里有 1)，则称 S 是 R 的子环 (subring)。

利用定义我们很容易得到判断子环的充要条件：

命题 4.3.9. S 是环 R 的子环 $\iff \forall a,b \in S$，有 $a-b \in S$，$ab \in S$。

由此容易证明，环 R 的子环的子环还是 R 的子环，留作练习。

例 4.3.6. (1)$\mathbb{Z}$ 是 $\mathbb{Q}$ 的子环，任意 $m \in \mathbb{Z}$，$m\mathbb{Z} = \{mn \mid n \in \mathbb{Z}\}$ 是 $\mathbb{Z}$ 的子环。实际上，$\mathbb{Z}$ 的子环一定是 $m\mathbb{Z}$ 的形式 (验证之)。

(2) 设 R 是环，我们记 $C_R = \{c \in R \mid \forall r \in R,\ rc = cr\}$，称 C_R 为环 R 的中心，容易验证 C_R 是 R 的子环 (留作练习)。

(3) 设 $\varphi : R \to S$ 是环同态，容易验证 $\ker(\varphi)$ 和 $\mathrm{im}(\varphi)$ 分别是 R 和 S 的子环。

(4) 我们考虑闭区间 $[0,1] \to \mathbb{R}$ 的函数环 $\mathbb{R}^{[0,1]}$。作嵌入映射 $\varphi : \mathbb{R} \to \mathbb{R}^{[0,1]}$，$x \mapsto 1_x$(其中 1_x 表示常值映射，它把 $[0,1]$ 闭区间上的数都映到 x)，则容易验证 φ 是单同态，于是我们可以将 $\mathbb{R}$ 视作 $\mathbb{R}^{[0,1]}$ 的子环 (确切地说是 $\mathrm{im}(\varphi) = \{1_x \mid x \in \mathbb{R}\}$ 是 $\mathbb{R}^{[0,1]}$ 的子环)。此外，容易验证 $[0,1]$ 上的所有有界函数、连续函数、可微函数构成的环 (分别记作 $\mathbb{R}_b^{[0,1]}, \mathbb{R}_c^{[0,1]}, \mathbb{R}_d^{[0,1]}$) 都是 $\mathbb{R}^{[0,1]}$ 的子环。

子环的性质还不够好，我们以后经常研究满足以下条件 (乘法吸收性) 的子环，即理想。

定义 4.3.8. 设 I 为环 R 的子环，如果 $\forall a \in I, x \in R$，都有 $xa \in I$，则称 I 为 R 的左理想；如果 $\forall a \in I, x \in R$，都有 $ax \in I$，则称 I 为 R 的右理想。若子环 I 既是左理想，又是右理想，则称 I 为双边理想，简称理想 (ideal)。

显然 $\{0\}$ 和 R 本身是 R 的理想，称为平凡理想；再例如，$m\mathbb{Z}$ 是 $\mathbb{Z}$ 的理想。有了理想的概念，我们就可以作商环了。我们将在抽象代数课程中学习后续的内容。

下面我们讨论一个特殊的例子：四元数除环 (四元数体)。它是由英国数学家 Hamilton 发现的，在代数学和微分几何上都有重要的作用。

首先，中学时我们就知道，每个复数 $a + b\sqrt{-1}$ 都可以看成一个实数对 (a,b). 而将复数看成实数对后，加法和乘法可以表示为

$$(a_1,b_1)+(a_2,b_2) = (a_1+a_2, b_1+b_2)$$
$$(a_1,b_1)(a_2,b_2) = (a_1a_2 - b_1b_2, a_1b_2 + a_2b_1)$$

那么，按这个思路，我们可以将每个四元数可以看成一个实数四元组，然后再定义合理的加法和乘法，使得这个四元组能进行加减乘除运算 (只不过乘法不满足交换律)。不过这种做法似乎不够自然。下面我们利用矩阵将“虚”的部分实体化，这样就可以更加自然地定义四元数的概念。

相信大家中学时已经学过复数的相关定义，我们也会在下一章更严格地介绍复数。首先注意到，如果将复数 $a + b\sqrt{-1}$ 写成一个矩阵

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

则所有复数的集合对应于 $M_2(\mathbb{R})$ 的一个子集

$$\left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R}\right\}$$

而且复数的加法和乘法恰好对应矩阵的加法和乘法。按照这个思路，我们考虑 $M_2(\mathbb{C})$ 中的子集

$$\mathbb{H} = \left\{\begin{pmatrix} \alpha & \beta \\ -\beta & \overline{\alpha} \end{pmatrix} \mid \alpha, \beta \in \mathbb{C}\right\}$$

容易验证 $\mathbb{H}$ 是 $(M_2(\mathbb{C}), +, O_{2\times 2}, \cdot, E_2)$ 的一个子环。下面考虑 $\mathbb{H}$ 的性质。容易看出：

(1) $\mathbb{H}$ 中包含幺元 $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$。

(2) 令

$$\mathbf{i} = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}, \quad \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathbf{k} = \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}.$$

则 $\mathbf{jk} = \mathbf{i}$, $\mathbf{kj} = -\mathbf{i}$，即 $\mathbb{H}$ 不是交换环。

(3) 如果

$$A = \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} \in M_2(\mathbb{C}),\ A \neq O_{2\times 2}$$

则 A 是可逆矩阵，而且

$$A^{-1} = \frac{1}{|\alpha|^2 + |\beta|^2} \begin{pmatrix} \overline{\alpha} & -\beta \\ \overline{\beta} & \alpha \end{pmatrix}.$$

综上所述，$\mathbb{H}$ 是非交换的除环，这就是四元数除环。

现在我们回到最初的问题：将四元数写成实数四元组并定义加法和乘法。利用上面定义的 $\mathbf{i}, \mathbf{j}, \mathbf{k}$ 容易验证，对于 $\alpha = a + b\sqrt{-1}, \beta = c + d\sqrt{-1}$，其中 $a, b, c, d \in \mathbb{R}$，有

$$\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} = \begin{pmatrix} a + b\sqrt{-1} & c + d\sqrt{-1} \\ -c + d\sqrt{-1} & a - b\sqrt{-1} \end{pmatrix} = a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}.$$

其中 $\mathbf{1}$ 是单位矩阵. 这样我们就可以将四元数看成四元实数组了，而四元实数组的加法就是对应的分量相加。对于乘法，$\mathbf{1}$ 是幺元，而 $\mathbf{i}, \mathbf{j}, \mathbf{k}$ 满足

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -\mathbf{1},\ \mathbf{ij} = -\mathbf{ji} = \mathbf{k},\ \mathbf{jk} = -\mathbf{kj} = \mathbf{i},\ \mathbf{ki} = -\mathbf{ik} = \mathbf{j}.$$

将上述公式线性扩充到任何两个四元实数组, 即可得到乘法规则。

以后我们会知道，$\mathbb{R}, \mathbb{C}, \mathbb{H}$ 都可以视作 $\mathbb{R}$ 上的向量空间，并且这个向量空间中可以定义满足结合律的线性的乘法，而且非零元素对乘法都可逆。这种结构称为 $\mathbb{R}$ 上的可除代数 (division algebra)。Frobenius 证明了 $\mathbb{R}$ 上的可除代数必然同构于 $\mathbb{R}, \mathbb{C}$ 或 $\mathbb{H}$ 中的一种，感兴趣的读者可以参考 Algebra, Thomas.W.Hungerford,GTM73 的 §9.6。

4.4 域

上一节中我们已经定义了域，这一节我们来讨论域的更多性质。以下我们默认域中 $0 \neq 1$。

定义 4.4.1. 设 $(\mathbb{F}, +, 0, \cdot, 1)$ 是交换环，$0 \neq 1$，如果 $\mathbb{F} \setminus \{0\}$ 中的每个元素都是乘法可逆元，则称 $\mathbb{F}$ 是域。

显然 $\mathbb{F}$ 是域 $\iff \mathbb{F}^\times = \mathbb{F} \setminus \{0\}$ 是乘法群。域一定是整环。

例 4.4.1. $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p (p$ 是素数$)$ 都是域。

下面我们考虑如何从一个整环构造一个域，这个过程实际上是一个局部化 (localization) 的过程。关于一般的局部化，我们会在抽象代数中学习。

设 D 是整环，记 $D^* = D \setminus \{0\}$，则 D^* 满足：

(1)$1 \in D^*$;

(2) 若 $a, b \in D^*$，则 $ab \in D^*$. [1]

于是我们可以在 $D \times D^*$ 上定义如下的等价关系：设 $(a, b), (c, d) \in D \times D^*$，我们定义

$$(a, b) \sim (c, d) \iff ad = bc$$

下面我们验证 $\sim$ 确实是一个等价关系。

(1) 自反性：设 $(a, b) \in D \times D^*$，则由 $ab = ba$ 显然有 $(a, b) \sim (a, b)$;

(2) 对称性：设 $(a, b) \sim (c, d)$，即 $ad = bc$，所以 $bc = ad$，即 $(c, d) \sim (a, b)$;

(3) 传递性：如果 $(a_1, b_1) \sim (a_2, b_2)$，$(a_2, b_2) \sim (a_3, b_3)$，则 $a_1 b_2 = a_2 b_1$，$a_2 b_3 = a_3 b_2$，于是 $a_1 a_2 b_2 b_3 = a_2 a_3 b_1 b_2$，即 $(a_1 b_3 - a_3 b_1)(a_2 b_2) = 0$，由 $b_2 \neq 0$，于是 $a_1 b_3 - a_3 b_1 = 0$ 或 $a_2 = 0$，前者直接说明 $(a_1, b_1) \sim (a_3, b_3)$，后者表明 $a_1 b_2 = 0$，$a_3 b_2 = 0$ ，即 $a_1 = a_3 = 0$，所以 $a_1 b_3 = a_3 b_1 = 0$，即 $(a_1, b_1) \sim (a_3, b_3)$。

有了这个等价关系，我们可以定义商集 $F = D \times D^* / \sim$，为了书写简便，我们将 (a, b) 的等价类 $\overline{(a, b)} \in F$ 记作 $\dfrac{a}{b}$。下面我们在 F 上定义合适的加法和乘法运算使得 F 成为一个域。

令

$$\begin{aligned} +: F \times F &\longrightarrow F & \times : F \times F &\longrightarrow F \\ (\frac{a}{b}, \frac{c}{d}) &\longmapsto \frac{ad + bc}{bd} & (\frac{a}{b}, \frac{c}{d}) &\longmapsto \frac{ac}{bd} \end{aligned} \tag{4.4.1}$$

首先，我们定义的加法和乘法是良定义的，这只需用定义验证 (留作练习)：如果 $\dfrac{a}{b} = \dfrac{a'}{b'}$，$\dfrac{c}{d} = \dfrac{c'}{d'}$，则 $\dfrac{a}{b} + \dfrac{c}{d} = \dfrac{a'}{b'} + \dfrac{c'}{d'}$ 及 $\dfrac{a}{b} \times \dfrac{c}{d} = \dfrac{a'}{b'} \times \dfrac{c'}{d'}$。

其次，容易验证 F 在这样定义的加法和乘法之下仍然是整环 (验证环，乘法交换，无零因子，细节留作练习)，其中，F 关于加法的零元是 $\dfrac{0}{1}$，乘法的幺元是 $\dfrac{1}{1}$，$\dfrac{a}{b}$ 关于加法的负元是 $\dfrac{-a}{b}$。

最后，若 $\dfrac{a}{b} \in F^*$(即 $\dfrac{a}{b} \neq \dfrac{0}{1}$)，则 $\dfrac{a}{b}$ 关于乘法的逆元是 $\dfrac{b}{a}$。

综上所述，F 是域，称为整环 D 的**分式域**。

注 4.4.1. 我们可以将 D 嵌入到 F 中 $a \mapsto \dfrac{a}{1}$(这是一个单同态)，于是我们将 $\dfrac{a}{1}$ 也简记为 a。

[1] 以后我们会知道，满足这两条性质的环的非空子集称为乘性子集，我们可以在乘性子集上进行类似的操作，而不是仅限于 D^*。

由前面命题4.3.3的讨论立刻有下面的定理：

定理 4.4.1. 剩余类环 $\mathbb{Z}_n$ 是域 $\iff$ n 是素数。

下面我们考虑域的同态。

定义 4.4.2. 设 $\mathbb{F},\mathbb{K}$ 是两个域，如果 $\varphi:\mathbb{F}\to\mathbb{K}$ 是环同态，则称 φ 是域同态。如果 φ 是双射则称为域同构。

命题 4.4.1. 设 $\varphi:\mathbb{F}\to\mathbb{K}$ 是非零的域同态，则 φ 必是单射。

证明. 只需证明 $\ker(\varphi)=\{0_{\mathbb{F}}\}$。用反证法。如果 $\exists a\in\mathbb{F}\setminus\{0_{\mathbb{F}}\}$ 使得 $\varphi(a)=0_{\mathbb{K}}$，则由命题4.3.5有 $1_{\mathbb{K}}=\varphi(1_{\mathbb{F}})=\varphi(a^{-1}a)=\varphi(a^{-1})0_{\mathbb{K}}=0_{\mathbb{K}}$，即 $1_{\mathbb{K}}=0_{\mathbb{K}}$，矛盾！ □

于是，我们在考虑域的同态时，只需要考虑单同态的情形，即我们只需要考虑把一个域嵌入到一个更大的域中。等价地有如下定义：

定义 4.4.3. 设 P 是域，且 P 是域 $\mathbb{F}$ 的子环，则称 P 是 $\mathbb{F}$ 的子域，$\mathbb{F}$ 是 P 的扩域 (field extension)。

例 4.4.2. (1)$\mathbb{Q}\subset\mathbb{R}\subset\mathbb{C}$，前者是后者的子域；
(2) 固定一个 $p\in\mathbb{Z}^+$ 是非平方数，则 $\mathbb{Q}(\sqrt{p})=\{a+b\sqrt{p}\mid a,b\in\mathbb{Q}\}$ 是 $\mathbb{Q}$ 的扩域 (验证留作练习)。

用定义容易验证，域 $\mathbb{F}$ 的任意多个子域的交也是 $\mathbb{F}$ 的子域。

定义 4.4.4. 一个域如果不包含任何真子域，则称为素域。

为了研究素域的性质，我们需要将环的特征的概念应用到域上。设 $\mathbb{F}$ 是域，由于域是无零因子环，故 $\mathrm{char}(\mathbb{F})=0$ 或 $\mathrm{char}(\mathbb{F})=p$，$p$ 为素数。更进一步地，我们有

定理 4.4.2. (1) 有理数域 $\mathbb{Q}$ 和素数阶的剩余类域 $\mathbb{Z}_p$ 都是素域；
(2) 如果 $\mathbb{F}$ 是素域，则 $\mathbb{F}$ 必同构于 $\mathbb{Q}$ 或 $\mathbb{Z}_p$。

证明. (1) 设 P 是 $\mathbb{Q}$ 的子域，由于 $1\in P$，P 对加减法封闭，故 $\mathbb{Z}=<1>\subset P$，即 $\forall m,n\in\mathbb{Z}$，$m,n\in P$，又 P 中非零元都关于乘法可逆，即 $n\neq 0\Rightarrow n^{-1}\in P$，于是由乘法封闭知 $mn^{-1}\in P$，即 $\mathbb{Q}\subseteq P$。于是 $P=\mathbb{Q}$，即 $\mathbb{Q}$ 是素域。

同样地，设 p 是素数，L 是 $\mathbb{Z}_p$ 的子域，则 $\overline{1}\in L$，于是 L 包含 $\overline{1}$ 生成的加法子群 $<\overline{1}>$，但 $<\overline{1}>=\mathbb{Z}_p$，于是 $\mathbb{Z}_p\subseteq L\subseteq\mathbb{Z}_p$，所以 $L=\mathbb{Z}_p$，即 $\mathbb{Z}_p$ 是素域。

(2) 设 $\mathbb{F}$ 是素域，e 是其乘法幺元，$H=<e>$ 是 e 生成的加法子群。由于 $(me)(ne)=(mn)e$，$m,n\in\mathbb{Z}$，故 H 是 $\mathbb{F}$ 的子环，且 H 是整环 (域的子环一定是整环)。

(i) $\mathrm{char}(\mathbb{F})=0$，即 H 是无限阶循环群，则容易验证 $\varphi:H\to\mathbb{Z}$，$ne\mapsto n$ 是一个环同构 (双射显然，$\varphi((me)(ne))=\varphi((mn)e)=mn=\varphi(me)\varphi(ne)$)。作 H 的分式域 $\mathbb{K}$，我们可以将 φ 扩张成

$$\begin{aligned}\varphi':&\mathbb{K}\longrightarrow\mathbb{Q}\\&(me)(se)^{-1}\longmapsto ms^{-1}\end{aligned}$$

用定义容易验证 φ' 是域同构，注意到 $\mathbb{K}$ 是 $\mathbb{F}$ 的子域，而 $\mathbb{F}$ 是素域，故 $\mathbb{F}=\mathbb{K}$，即此时 $\mathbb{F}\simeq\mathbb{Q}$。

(ii) $\mathrm{char}(\mathbb{F}) = p$，即 H 是 p 阶循环群 (p 为素数)，即 $H = \{0, e, \ldots, (p-1)e\}$，满足 $pe = 0$。容易验证 H 是域 (对于 $me \in H,\ m \in \{0, \ldots, p-1\}$，由 m, p 互素可知存在 $s, t \in \mathbb{Z}$ 使得 $sm + tp = 1$，做带余除法 $s = up + r,\ r \in \{0, 1, \ldots, p-1\}$，则可以验证 $(me)^{-1} = re$)。作映射 $\varphi : H \to \mathbb{Z}_p,\ me \mapsto \overline{m}$，容易验证这是一个域同构。而由 $\mathbb{F}$ 是素域可知 $H = \mathbb{F}$，即此时 $\mathbb{F} \simeq \mathbb{Z}_p$。

□

域扩张和域的自同构群的理论是伽罗瓦理论的基础，我们会在抽象代数中进一步学习。

最后我们简单讨论一下一般域上的线性代数，更详细的讨论会在下册抽象向量空间中进行。

设 $\mathbb{F}$ 是域，我们考虑坐标空间 $\mathbb{F}^n = \{(x_1, \ldots, x_n)^t \mid x_i \in \mathbb{F}\}$，则仿照 $\mathbb{R}^n$，在 $\mathbb{F}^n$ 上可以自然地定义加法和 “数乘 (域上的元素乘以向量)”。容易验证 $\mathbb{F}^n$ 也满足 2.1.1 小节中的运算律。同理我们也可以定义 $\mathbb{F}$ 上的矩阵空间 $\mathbb{F}^{m\times n}$ 和 $M_n(\mathbb{F})$，它们和 $\mathbb{R}$ 上的矩阵满足相同的运算律和性质 (验证之)。

例 4.4.3. 设 $A = \begin{pmatrix} \overline{1} & \overline{2} & \overline{3} \\ \overline{0} & \overline{2} & \overline{4} \\ \overline{1} & \overline{4} & \overline{2} \end{pmatrix} \in M_3(\mathbb{Z}_5)$，试计算 V_A 的维数和一组基。

解. 对 A 作如下的初等行变换：

$$A \xrightarrow{r_3 - r_1} \begin{pmatrix} \overline{1} & \overline{2} & \overline{3} \\ \overline{0} & \overline{2} & \overline{4} \\ \overline{0} & \overline{2} & \overline{4} \end{pmatrix} \xrightarrow{r_3 - r_2} \begin{pmatrix} \overline{1} & \overline{2} & \overline{3} \\ \overline{0} & \overline{2} & \overline{4} \\ \overline{0} & \overline{0} & \overline{0} \end{pmatrix}$$

即 $\mathrm{rank}(A) = 2$，所以 $\dim(V_A) = 1$。在 $\mathbb{Z}_5$ 上解齐次线性方程组 $\begin{cases} x_1 + \overline{2}x_2 + \overline{3}x_3 = \overline{0} \\ \overline{2}x_2 + \overline{4}x_3 = \overline{0} \end{cases}$，可得 $\begin{cases} x_1 = \overline{1}x_3 \\ x_2 = \overline{3}x_3 \end{cases}$。取 $x_3 = \overline{1}$ 即有 $V_A = < (\overline{1}, \overline{3}, \overline{1})^t >$。 □

设 $\mathbb{F}$ 是域，我们同样可以定义 $M_n(\mathbb{F})$ 上的行列式，它满足如下性质：

命题 4.4.2. 设 $\mathbb{F}, \mathbb{K}$ 是域，R 是 $\mathbb{F}$ 的子环，$\varphi : R \to \mathbb{K}$ 是环同态，令 $A = (a_{ij})_{n\times n} \in M_n(R)$，将 φ 扩张到矩阵上：$\varphi : M_n(R) \to M_n(\mathbb{K}),\ A \mapsto \varphi(A) = (\varphi(a_{ij}))_{n\times n}$，则 $\varphi(\det(A)) = \det(\varphi(A))$。

证明. 利用行列式的完全展开定义有：

$$\det(A) = \sum_{\sigma \in S_n} \varepsilon_\sigma a_{\sigma(1)1} \cdots a_{\sigma(n)n}$$

由于 φ 是环同态，所以

$$\varphi(\det(A)) = \sum_{\sigma \in S_n} \varepsilon_\sigma \varphi(a_{\sigma(1)1}) \cdots \varphi(a_{\sigma(n)n}) = \det(\varphi(A))$$

即得结论。 □

推论 4.4.1. 条件同上面的命题。若 $\varphi(A)$ 满秩，则必有 A 满秩。

利用 $\det(\varphi(A)) \neq 0 \Rightarrow \varphi(\det(A)) \neq 0 \Rightarrow \det(A) \neq 0$ 即可证明。需要注意的是，推论的逆命题不一定成立，反例的构造留作思考。

例 4.4.4. 判断矩阵 $A = \begin{pmatrix} 2 & 7 & 6 & 4 \\ 5 & 8 & 11 & 9 \\ 3 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \in M_4(\mathbb{Z})$ 是否满秩。

解. 作同态 $\pi_2 : \mathbb{Z} \to \mathbb{Z}_2,\ a \mapsto \overline{a}$，则

$$\pi_2(A) = \begin{pmatrix} \overline{0} & \overline{1} & \overline{0} & \overline{0} \\ \overline{1} & \overline{0} & \overline{1} & \overline{1} \\ \overline{1} & \overline{1} & \overline{1} & \overline{0} \\ \overline{0} & \overline{1} & \overline{1} & \overline{1} \end{pmatrix}$$

计算得 $\det(\pi_2(A)) = \overline{1} \neq \overline{0}$，于是 $\mathrm{rank}(A) = 4$，即 A 满秩。 □

本章的内容只是对抽象代数的一个浅显的介绍，更加深入的内容读者可以参考抽象代数的标准教材。

4.5 习题

半群与群

1. 验证剩余类上的加法和乘法的良定义性, 并验证其上的运算律.

2. 设给出一个任意的代数结构 $(X,*)$, 使得任取 $x,y\in X,(x*y)*y=x,y*(y*x)=x$. 证明 $x*y=y*x$, 即运算 $*$ 是交换的.

3. 证明集合
$$M_n^0(\mathbb{R})=\left\{A=\left(a_{ij}\right)\in M_n(\mathbb{R})\mid \sum_{j=1}^{n}a_{ij}=0,\quad i=1,2,\cdots,n\right\}$$
在矩阵的通常乘法运算下构成一个半群. $\left(M_n^0(\mathbb{R}),\cdot\right)$ 是幺半群吗?

4. 在乘法幺半群 M 中选出任意一个元素 t, 并引入一个新的运算 $*:x*y=xty$. 证明 $(M,*)$ 是一个半群, 并且 $(M,*)$ 是一个幺半群当且仅当所选的元素 t 是可逆的, 此时它的单位元是 t^{-1}.

5. 证明集合 $\mathbb{Z}$ 关于运算 $\circ$ 构成一个交换幺半群, 其中 $\circ:n\circ m=n+m+nm=(1+n)\times(1+m)-1$. 什么是 $(\mathbb{Z},\circ)$ 的单位元? 找出 $(\mathbb{Z},\circ)$ 的全部可逆元.

6. 验证例4.2.6是群同态.

7. 验证引理4.2.3, 并验证群的同构是等价关系.

8. 验证群 G 中元素 x 的方幂满足 $(x^n)(x^m)=x^{n+m}$, $(x^n)^m=x^{mn}$, $\forall m,n\in\mathbb{Z}$.

9. 设 $f:G\to H$ 是群同态, 验证 $\mathrm{im}(f)$ 是 H 的子群.

10. 证明命题4.2.4.

11. 验证定义4.2.10和式 (4.2.1) 定义出的群的生成组是一致的.

12. 验证定义4.2.12中的内自同构映射确实是一个同构, 并证明所有内自同构映射在映射复合下构成一个群.

13. 证明群 G 中乘法可换的元素 a,b 若有互素的阶 s,t, 则在 G 中生成一个 st 阶的循环子群: $<a,b>=<ab>$.

    (提示: 包含关系 $<ab>\subset<a,b>=\left\{a^ib^j\mid 0\leqslant i\leqslant s-1,0\leqslant j\leqslant t-1\right\}$ 显然成立. 由 Bezout 关系 (定理1.6.1), 从 $\gcd(s,t)=1$ 可知, 存在 $k,l\in\mathbb{Z}$, 使 $tk+sl=1$. 考虑到定理 $1,a=a^{1-sl}=a^{tk}=a^{tk}b^{tk}=(ab)^{tk}\in<ab>$. 类似地, $b\in<ab>$, 故 $<a,b>\subset<ab>$.)

14. 设 $M=<S>$ 是由集合 S 生成的幺半群, 如果每个元素 $s\in S$ 在 M 中可逆, 证明 M 是一个群.

15. 证明下述论断: 设 G 是一个幺半群, 使得任取 $a,b\in G$, 方程 $ax=b,ya=b$ 有唯一解, 则 G 是一个群.

16. 令 $\varphi_{a,b}:x\mapsto ax+b(a,b\in\mathbb{R};a\neq 0)$ 是实直线上的一个仿射变换, 它们的集合记作 $\mathbb{A}_1(\mathbb{R})$, 在 $\mathbb{A}_1(\mathbb{R})$ 中定义乘法 $\varphi_{a,b}\varphi_{c,d}=\varphi_{ac,ad+b}$, 证明 $\mathbb{A}_1(\mathbb{R})$ 是一个群. $\mathbb{A}_1(\mathbb{R})$ 包含有一个子群 $\mathrm{GL}_1(\mathbb{R})$, 它使点 $x=0$ 保持不动, 也包含有一个由 “纯位移” $x\mapsto x+b$ 组成的子群.

17. 群 $\mathrm{SL}_2(\mathbb{Z})$ 包含有元素 $A=\begin{pmatrix}0&1\\-1&0\end{pmatrix}$ 和 $B=\begin{pmatrix}0&1\\-1&-1\end{pmatrix}$, 阶数分别为 4 和 3 . 证明 $<AB>$ 是 $\mathrm{SL}_2(\mathbb{Z})$ 中的无限循环子群. 这说明群 G 中两个有限阶元素的乘积不一定是有限阶元. 这件事在交换群中成立吗?

18. 证明若群 G 的阶 $|G|=2n$ 是一个偶数, 则 G 中包含有一个二阶元 $g\neq e$. 提示: 观察 G 用元素对 g,g^{-1} 的划分.

19. 证明 $S_n=<(12),(13),\cdots,(1n)>$.

20. 证明 $S_n=<(12),(123\cdots n)>$.

21. 证明交错群 $A_n, n\geqslant 3$, 是由长度为 3 的循环生成的, 并且事实上

$$A_n=<(123),(124),\cdots,(12n)>.$$

22. 证明循环 $\pi=(12\cdots n)\in S_n$ 的 k 次方幂 π^k 是 d 个互不相交的循环的乘积, 每一个的长度为 $q=n/d$, 其中 $d=\gcd(n,k)$ 是 n 和 k 的最大公因数.

23. 设置换 $\pi\in S_n$, 将 π 分解成互不相交的循环的乘积, 证明 π 的阶 (即循环子群 $<\pi>$ 的阶), 等于这些循环的阶的最小公倍数.

24. 设 $A,B\in M_n(\mathbb{R})$ 且 $(AB)^m=E$ 对某个整数 m 成立, 那么一定有 $(BA)^m=E$ 吗?

25. 设 G 是一个有限 (乘法) 群, H 是 G 的一个非空子集, 如果 H 关于 G 的乘法封闭, 证明 H 是一个子群. 事实上, 在这种情况下, 在 H 中存在单位元 e 和逆元 $h^{-1}, h\in H$ 的要求是多余的.

26. 正有理数的乘法群 $(\mathbb{Q}_+,\cdot)$ 可以有什么样的生成元集? 提示: 利用整数的素因子分解 (算术基本定理). 在 $(\mathbb{Q}_+,\cdot)$ 中是否存在有限生成元集?

27. 用 Cayley 定理证明: 对于给定的阶数 n, 在同构的意义下仅有有限多个 n 阶群.

28. 证明每个有限群都可以嵌入到具有两个生成元的有限群中 (即存在到这种群内的一个单同态).

29. 证明: 如果一个幺半群 (单位元记作 1) 中的元素 a 有右逆 b (即 $ab=1$) 和左逆 c (即 $ca=1$), 那么 $b=c, a$ 是可逆元, 逆为 $a^{-1}=b$. 证明 a 可逆且以 b 为逆元当且仅当 $aba=a$ 和 $ab^2a=1$ 成立.

30. 设 α 是平面上绕原点的旋转, ρ 是关于 x 轴的反射. 证明: $\rho\alpha\rho^{-1}=\alpha^{-1}$.

31. 设 G 是么半群 M 的子集. 证明 G 是子群当且仅当 G 中每个元素在 M 中可逆且对于任意 $g,h\in G$ 有 $gh^{-1}\in G$.

32. 设 G 是半群, 具有如下性质: (1) G 含有右单位元 1_r, 即 $a\cdot 1_r=a$ 对任意的 $a\in G$; (2) G 中的每个元素 a 有右逆, 即存在 $b\in G$ 使得 $ab=1_r$, 证明: G 是群.

33. 证明: (1) 在群中左右消去律都成立, 即 $ax=ay\Longrightarrow x=y, xa=ya\Longrightarrow x=y$;
(2) 左右消去律都成立的有限半群一定是群.

34. 证明: 一个群不会是两个真子群的并.

35. 设 H 是群 G 的有限非空子集. 如果 H 对乘法封闭, 那么 H 是 G 的子群.

36. 设 $\varphi : G \to G'$ 是满群同态. 证明: 如果 G 是循环群, 则 G' 是循环群; 如果 G 是交换群, 则 G' 是交换群.

37. 证明: 实数加法群到非零复数乘法群的映射 $f(x) = e^{ix}$ 是群同态. 确定 f 的核与像.

38. 证明: (1) 形如 $M = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$ 的 n 阶实方阵, 其中 $A \in \mathrm{GL}_r(\mathbb{R}), C \in \mathrm{GL}_{n-r}(\mathbb{R})$, 形成 $\mathrm{GL}_n(\mathbb{R})$ 的一个子群 H ;
(2) 映射 $H \to \mathrm{GL}_r(\mathbb{R}), M \to A$ 是群同态. 确定其核.

39. 确定整数加法群到自身的所有群同态. 确定它们中哪些是单射, 哪些是满射, 哪些是同构. 如果去掉" 到自身" 的限制, 那么同态像应该具有什么样的结构?

40. 证明映射 $A \to (A^t)^{-1}$ 是 $\mathrm{GL}_n(\mathbb{R})$ 的自同构.

41. 设 G 是群. 对 $a \in G$, 定义 G 的右平移 a_R 为映射 $G \to G, x \to xa$. 证明在映射合成下 G 的右平移全体 G_R 是群, 且映射 $a \to a_R^{-1}$ 是 G 到 G_R 的群同构.

42. 把函数的复合定义为函数间的乘法, 于是函数 $f = 1/x, g = (x-1)/x$ 生成一个群. 证明这个群与对称群 S_3 同构.

43. 在同构的意义下分类所有的 6 阶群 (提示: 分情况讨论: G 有 6 阶元, G 没有 6 阶元但有 3 阶元, G 只有 1 阶和 2 阶元).

44. 设 $G =< g >$ 是循环群, 求证:
(1) 若 $|G| = \infty$, 则 G 的生成元只有 g 和 g^{-1};
(2) 若 $|G| = n$, 则 g^k 是 G 的生成元 $\iff \gcd(k, n) = 1$.

45. 设 H, K 是 G 的子群, 定义集合 $HK = \{hk \mid \forall h \in H,\ k \in K\}$, $KH = \{kh \mid \forall h \in H,\ k \in K\}$. 求证:
(1)HK 是 G 的子群 $\iff HK = KH$;
(2) 集合 HK 的元素个数 $|HK| = \dfrac{|H| \cdot |K|}{|H \cap K|}$.

环, 域

1. 验证例4.3.1.

2. 补充命题4.3.1和推论4.3.1的证明.

3. 设 R 是幺环, 验证 R 中的所有单位 (乘法可逆元) 在 R 的乘法下是一个群.

4. 验证例4.3.4.

5. 证明: 如果环的特征是合数, 则必有零因子.

6. 验证子环的子环还是子环, 并验证4.3.6.

7. 验证分式域上用式 (4.4.1) 定义的加法和乘法是良定义的, 并验证其确实是一个域.

8. 验证例4.4.2.

9. 设 F 是域, 验证坐标空间 F^n 和矩阵空间 $M_n(F)$ 分别与 $\mathbb{R}^n$, $M_n(\mathbb{R})$ 满足相同的运算律 (见第二章).

10. 构造推论4.4.1逆命题的反例.

11. 设 C 是实数集上的 (实值) 连续函数全体. 定义其加法为 $(f+g)(x)=f(x)+g(x)$, 乘法为 $(f\cdot g)(x)=f(g(x))$. 证明: $(C,+)$ 是交换群, $(C,\cdot)$ 是幺半群. $(C,+,\cdot)$ 是否为环?

12. 命 $\mathbb{Q}[\sqrt{2},\sqrt{3}]$ 是 $\mathbb{C}$ 中含所有有理数和 $\sqrt{2},\sqrt{3}$ 的子环中的最小者. 是否有 $\mathbb{Q}[\sqrt{2},\sqrt{3}]=\mathbb{Q}[\sqrt{2}+\sqrt{3}]$? 是否有 $\mathbb{Z}[\sqrt{2},\sqrt{3}]=\mathbb{Z}[\sqrt{2}+\sqrt{3}]$?

13. 确定下面的集合 S 是否是环 R 的子环.
(1) $S=\{\frac{a}{b}\mid a,b\in\mathbb{Z},b\neq 0$ 且 $3\nmid b\},R=\mathbb{Q}$.
(2) S 是函数 $1,\cos nt,\sin nt,n\in\mathbb{Z}$ 的整系数线性组合全体 (注意线性组合都是有限和), R 是 t 的所有实值函数集.

14. 确定下列环中的可逆元: (1) $\mathbb{Z}_{12}$, (2) $\mathbb{Z}_8$, (3) $\mathbb{Z}_m$.

15. 假设集合 R 上有两个运算, 除加法的交换律外满足环的所有其他公理. 利用分配律证明加法是交换的, 从而 R 是环.

16. 设 X 是集合, $P(X)$ 是 X 的所有子集形成的集合. 定义 $P(X)$ 的加法和乘法如下: $A+B=A\cup B-A\cap B, A\cdot B=A\cap B$. 证明: 在这些运算下 $P(X)$ 是环, 且其加法群的非零元素的阶都是 2 .

17. 证明: 如果在环中 $1-ab$ 可逆, 那么 $1-ba$ 也可逆.

18. (华罗庚恒等式) 设幺环 R 中 a,b 都是单位, 并且 $ab-1$ 也是单位, 求证: $a-b^{-1}$ 和 $(a-b^{-1})^{-1}-a^{-1}$ 都可逆, 且 $(a-b^{-1})^{-1}-a^{-1}=(aba-a)^{-1}$.

19. 确定环同态 $\varphi:\mathbb{R}[x,y,z]\to\mathbb{R}[t], x\to t, y\to t^2, z\to t^3$ 的核.

20. 设 $\varphi:R\to R'$ 是环同态. 证明: $\ker\varphi$ 对加法和乘法封闭. 如果 $x\in\ker\varphi$, 则对 R 中的任意元素 a, 有 $ax\in\ker\varphi$ 和 $xa\in\ker\varphi$.

21. 如果环中的任意元素 x 的平方等于自身, 证明该环是交换环. 若任意元素的立方等于自身, 结论是否成立?

22. 证明交换环的满同态像仍是交换环.

23. 证明任意有限整环 R 是一个域.

24. 设 p 是素数, R 是有单位元的交换环, 使得任取 $x\in R, px=0$. 证明

$$(x+y)^{p^m}=x^{p^m}+y^{p^m},\quad m=1,2,\cdots.$$

(提示: 对 m 作归纳, 注意到二项系数 $\left(\begin{array}{c}p\\k\end{array}\right)$ 当 $0<k<p$ 时被 p 整除.)

25. 证明含有 5 个元素的环或同构于 $\mathbb{Z}_5$, 或是带有零乘法的环 (注: 含有两个或以上元素的零乘法环不是幺环).

26. 环 R 的非零元素 x 称为幂零的, 若存在 $n \in \mathbb{N}$, 使得 $x^n = 0$. 证明:
    1) 若 R 是任意有单位元的环, x 是幂零元, 则 $1 - x$ 是可逆元;
    2) 环 $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ 包含有幂零元, 当且仅当 m 可以被一个大于 1 的整数的平方整除.

27. 若环 R 有单位元 e, 且基数 $|R|$ 是无限的, 则非零不可逆元素的个数不可能是一个有限整数. (提示: 用反证法. 设 $N = \{a_1, \cdots, a_n\}$ 是环 R 中所有的非 0 不可逆元素的集合. 对任意 $x \in R\backslash(N \cup \{0\})$, 可以定义左平移映射 $\rho_x : N \to N,\ a_i \mapsto xa_i$, 注意我们可以视作 $\rho_x \in S_n$, 而 $\rho : R^\times \to S_n,\ x \mapsto \rho_x$ 是一个同态, 故 $\ker(\rho) = \{x \in R^\times :\ \rho_x = \mathrm{id}\}$ 是一个无限集. 然而另一方面, 我们可以证明 $\ker(\rho) \subset \{e + a_1, \ldots, e + a_n\}$, 从而得到矛盾.)

28. 证明矩阵 $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, 其中 $a, b \in \mathbb{Z}/3\mathbb{Z}$, 构成一个 9 元域, 而这个域的乘法群是 8 阶循环群.

29. 域 $\mathbb{Q}(\sqrt{2})$ 和 $\mathbb{Q}(\sqrt{3})$ 是否同构?

30. 设 p 是奇素数. 证明 $\mathbb{Z}/p\mathbb{Z}$ 中的非零元有一半是平方元 (即是 $\mathbb{Z}/p\mathbb{Z}$ 中某个元素的平方), 且如果 a 和 b 不是平方元, 则 ab 是平方元.

31. 证明: 自然同态 $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ 诱导的群同态 $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ 是满同态, 其中 p 是素数.

32. 特征是素数的环不一定是无零因子环, 试构造这样的反例.

第五章　复数域

在中学我们就已经学习过复数了。这一章我们将介绍复数的更多性质。

5.1　复数的定义和运算

我们在数学分析课程中已经学习过实数 $\mathbb{R}$ 的严格定义，并且知道 $\mathbb{R}$ 是一个域。我们自然地可以考虑 $\mathbb{R}$ 的扩域。那么我们应该如何将 $\mathbb{R}$ 嵌入到一个更大的域中呢？一个容易想到的办法是往 $\mathbb{R}$ 里添加一些新元素，然后让新元素与原来的元素进行运算，从而得到一个关于加减乘除封闭的集合，这就是我们所需要的扩域。具体地说，我们有如下定义：

定义 5.1.1. 令 $\mathbb{C} = \{x + y\mathrm{i} \mid x, y \in \mathbb{R}\}$，其中 i 满足 $\mathrm{i}^2 = -1$(即 i 是 $x^2 + 1 = 0$ 的一个根)，在 $\mathbb{C}$ 上定义如下的加法和乘法：

$$
\begin{aligned}
+ :&\mathbb{C} \times \mathbb{C} \longrightarrow \mathbb{C} \\
&(a + b\mathrm{i}, c + d\mathrm{i}) \longmapsto (a + c) + (b + d)\mathrm{i} \\
\times :&\mathbb{C} \times \mathbb{C} \longrightarrow \mathbb{C} \\
&(a + b\mathrm{i}, c + d\mathrm{i}) \longmapsto (ac - bd) + (ad + bc)\mathrm{i}
\end{aligned}
$$

则容易验证 $(\mathbb{C}, +, 0, \times, 1)$ 是域，并且 $a + b\mathrm{i} (\neq 0)$ 的负元是 $-a - b\mathrm{i}$，乘法逆元是 $\dfrac{a - b\mathrm{i}}{a^2 + b^2}$，并且 $\mathbb{R} \to \mathbb{C}$, $x \mapsto x + 0_{\mathbb{R}}\mathrm{i}$ 是域同态。我们称 $\mathbb{C}$ 是复数域，其中的元素称为复数 (complex number)。

我们称 i 为虚数单位；若 $z = x + y\mathrm{i} \in \mathbb{C}$，则称 x 为 z 的实部，记作 $x = \mathrm{Re}(z)$；y 为 z 的虚部，记作 $y = \mathrm{Im}(z)$；如果 $\mathrm{Re}(z) = 0$，则称 z 为纯虚数；我们称 $\overline{z} = x - y\mathrm{i}$ 是 z 的**共轭复数**。容易验证：$z + \overline{z} \in \mathbb{R}$, $z\overline{z} \in \mathbb{R}$, $\overline{\overline{z}} = z$。于是我们有：

命题 5.1.1. $\varphi : \mathbb{C} \to \mathbb{C}$, $z \mapsto \overline{z}$ 是 $\mathbb{C}$ 的自同构，并且 $\varphi^2 = \mathrm{id}_{\mathbb{C}}$。[1]

由定义即可证明，留作练习。

符号 i 的解释

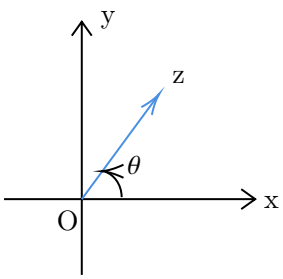
我们知道，i 是实系数方程 $x^2 + 1 = 0$ 的一个根，然而，这样假设似乎并不是很自然，下面我们找到一个“实体”满足这个“方程”。

注意到实数域 $\mathbb{R}$ 与二阶方阵环的子环 $\{\lambda E_2 \mid \lambda \in \mathbb{R}\}$ 同构，而我们可以找到矩阵 $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$，它满足 $J^2 + E = O$，于是我们可以考虑由 E, J 通过加法、实数乘法和矩阵乘法生成的子矩阵环 (代数)，即 $F = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$，很容易验证 F 是一个域 (练习：找出 F 中非零元的逆矩阵)。我们作映射 $\varphi : \mathbb{C} \to F$, $a + b\mathrm{i} \mapsto aE + bJ$，容易验证 φ 是一个域同构。这样我们就给虚数单位 i 找到了一个合适的“实体”：矩阵方程 $X^2 + E = O$ 的解。我们在下册复化与实化一节中会更深入地学习这一点。

我们也可以将复数 $x + y\mathrm{i}$ 视作二维平面上的点 (x, y)，即将 $\mathbb{C}$ 视作向量空间 $\mathbb{R}^2$。于是，设 $z = x + y\mathrm{i}$，我们定义 z 的**模长** $|z| = \sqrt{x^2 + y^2} = \sqrt{z\overline{z}}$，容易验证 $z \neq 0$ 时 $z^{-1} = \dfrac{\overline{z}}{|z|^2}$。我们

[1] 还可以证明 φ 是 $\mathbb{C}$ 上的连续函数，这是分析学的内容。

称射线 Oz 与 x 轴正半轴的夹角 θ 为 z 的**辐角**，记作 $\theta = \arg(z)$，我们通常规定 $0 \leqslant \theta < 2\pi$。于是我们立刻有 $x = |z|\cos\theta$, $y = |z|\sin\theta$，那么 $z = x + y\mathrm{i} = |z|(\cos\theta + \mathrm{i}\sin\theta)$，我们把或者称为**复数的三角形式或极坐标形式**。



复数的三角形式的一个优点是方便我们做乘法。

命题 5.1.2. 设 $z_1 = r_1(\cos\theta_1 + \mathrm{i}\sin\theta_1)$, $z_2 = r_2(\cos\theta_2 + \mathrm{i}\sin\theta_2)$，其中 $r_1, r_2 > 0$, $\theta_1, \theta_2 \in \mathbb{R}$。则 $z_1 z_2 = r_1 r_2(\cos(\theta_1 + \theta_2) + \mathrm{i}\sin(\theta_1 + \theta_2))$。特别地，如果 $z = r(\cos\theta + \mathrm{i}\sin\theta)$, $r > 0, \theta \in \mathbb{R}$，则 $z^n = r^n(\cos n\theta + \mathrm{i}\sin n\theta)$(称为 De Moivre(棣莫弗) 公式)；如果 $z \neq 0$，则 $z^{-1} = \dfrac{1}{r}(\cos\theta - \mathrm{i}\sin\theta)$。

证明是容易的，留作练习。

复数的指数形式

我们定义 $e^{\mathrm{i}\theta} = \cos\theta + \mathrm{i}\sin\theta$ $(\theta \in \mathbb{R})$，则我们可以将复数的三角形式 $z = r(\cos\theta + \mathrm{i}\sin\theta)$ 写成更简单的 $z = re^{\mathrm{i}\theta}$，并且将复数的乘法写成更简单的形式 $z_1 z_2 = r_1 r_2 e^{\mathrm{i}(\theta_1+\theta_2)}$。这个定义的合理性来自如下的 Taylor 级数形式推导 [1]：

$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}, \quad \sin x = \sum_{k=1}^{\infty} (-1)^k \frac{x^{2k+1}}{(2k+1)!}, \quad \cos x = \sum_{k=0}^{\infty} (-1)^k \frac{x^{2k}}{(2k)!}$$

于是

$$\begin{aligned} e^{\mathrm{i}\theta} &= \sum_{k=0}^{\infty} \frac{(\mathrm{i}\theta)^k}{k!} \\ &= \sum_{k=0}^{\infty} (-1)^k \frac{\theta^{2k}}{(2k)!} + \mathrm{i} \sum_{k=1}^{\infty} (-1)^k \frac{\theta^{2k+1}}{(2k+1)!} \\ &= \cos\theta + \mathrm{i}\sin\theta \end{aligned}$$

特别地，取 $\theta = \pi$ 即得到 $e^{\mathrm{i}\pi} + 1 = 0$，这就是著名的欧拉公式。

借助棣莫弗公式我们可以方便地对复数进行开方运算：设 $z = r(\cos\theta + \mathrm{i}\sin\theta)$，如果 ω 满足 $\omega^n = z$，不妨设 $\omega = r_0(\cos\theta_0 + \mathrm{i}\sin\theta_0)$，则 $\omega^n = r_0^n(\cos n\theta_0 + \mathrm{i}\sin n\theta_0)$，对比 z 的形式可得 $r_0^n = r$, $n\theta_0 = \theta + 2k\pi, k \in \mathbb{Z}$，即 $r_0 = \sqrt[n]{r}$, $\theta_0 = \dfrac{\theta + 2k\pi}{n}, k \in \mathbb{Z}$。

特别地，我们关注 1 在 $\mathbb{C}$ 中的 n 次方根。

定义 5.1.2. 设 $n \in \mathbb{Z}^+$, $\omega \in \mathbb{C}$，如果 $\omega^n = 1$，则称 ω 是一个 n 次单位根。

定理 5.1.1. 设 $n \in \mathbb{Z}^+$，则 $\mathbb{C}$ 中有且仅有 n 个互不相同的 n 次单位根，并且它们在复数的乘法下构成 n 阶循环群。

[1] 我们会在复变函数课程中更严谨地定义复数域上的初等函数。

证明. 由上面的复数开方法可知全部的 n 次单位根为 $e^{\frac{2k\pi\mathrm{i}}{n}}, \forall k \in \mathbb{Z}$。实际上这些数有且只有 n 个，这是因为如果 $s \equiv t \mod n$，即 $t - s = mn, m \in \mathbb{Z}$，则

$$e^{\frac{2s\pi\mathrm{i}}{n}} - e^{\frac{2t\pi\mathrm{i}}{n}} = e^{\frac{2t\pi\mathrm{i}}{n}}(e^{\frac{2(t-s)\pi\mathrm{i}}{n}} - 1) = e^{\frac{2t\pi\mathrm{i}}{n}}(e^{2m\pi\mathrm{i}} - 1) = 0$$

同样的方法可以证明如果 $s \not\equiv t \mod n$，则 $e^{\frac{2s\pi\mathrm{i}}{n}} \neq e^{\frac{2t\pi\mathrm{i}}{n}}$。于是 $U_n = \{e^{\frac{2k\pi\mathrm{i}}{n}} \mid k = 0, 1, \ldots, n-1\}$ 是全部的 n 次单位根。下面说明 U_n 在复数乘法下成群。设 $a, b \in U_n$，则 $(ab^{-1})^n = \dfrac{a^n}{b^n} = 1$，所以 $ab^{-1} \in U_n$，即 U_n 是群。

最后我们说明 U_n 是循环群，这只需要在 U_n 中找到一个 n 阶元素即可。注意到 $(e^{\frac{2\pi\mathrm{i}}{n}})^n = 1$，而对任意的 $l \in \{1, \ldots, n-1\}$，有 $(e^{\frac{2\pi\mathrm{i}}{n}})^l = e^{\frac{2l\pi\mathrm{i}}{n}} \neq 1$，即 $e^{\frac{2\pi i}{n}}$ 是 n 阶元，所以 $U_n =< e^{\frac{2\pi\mathrm{i}}{n}} >$ 是循环群。 □

实际上，我们可以证明，任何域的有限阶乘法子群都是循环群。证明需要用到 Sylow 定理，我们会在抽象代数课程中学习。

我们把 n 次单位根群记作 U_n。U_n 的生成元称为 n 次本原单位根。下面我们考虑 n 次本原单位根的性质。

命题 5.1.3. $e^{\frac{2k\pi\mathrm{i}}{n}}$ 是 n 次本原单位根 $\iff \gcd(k, n) = 1$。

证明. $(\Longrightarrow)$ 用反证法，如果 $\gcd(k, n) = r > 1$，那么令 $m = \dfrac{n}{r} < n$，有 $(e^{\frac{2k\pi\mathrm{i}}{n}})^m = e^{2\frac{k}{r}\pi\mathrm{i}}$，而 $\dfrac{k}{r}$ 是整数，故 $(e^{\frac{2k\pi\mathrm{i}}{n}})^m = 1$，即 $e^{\frac{2k\pi\mathrm{i}}{n}}$ 的阶小于 n，从而与 $e^{\frac{2k\pi\mathrm{i}}{n}}$ 是 n 次本原单位根矛盾！
$(\Longleftarrow)\gcd(k, n) = 1 \Longrightarrow \exists a, b \in \mathbb{Z}$ 使得 $an + bk = 1$，于是

$$e^{\frac{2\pi\mathrm{i}}{n}} = e^{\frac{2(an+bk)\pi\mathrm{i}}{n}} = (e^{\frac{2k\pi\mathrm{i}}{n}})^b$$

所以 $\forall l \in \{1, \ldots, n-1\}$，有

$$e^{\frac{2l\pi\mathrm{i}}{n}} = (e^{\frac{2k\pi\mathrm{i}}{n}})^{bl}$$

即 $e^{\frac{2k\pi\mathrm{i}}{n}}$ 是生成元。 □

于是我们立刻有：

推论 5.1.1. $\mathbb{C}$ 中 n 次本原单位根有且只有 $\varphi(n)$ 个，其中 φ 是欧拉函数。

实际上，命题5.1.3的结论可以推广到一般的循环群，证明方法类似，留作思考。

例 5.1.1. $\mathbb{C}$ 中 4 次单位根为 $\pm 1, \pm\mathrm{i}$，其中本原单位根为 $\pm\mathrm{i}$。

5.2 实数域的二次扩张

本节的主要结论是：复数域在同构意义下是唯一的，即下面的定理。

定理 5.2.1. 设 F 是 $\mathbb{R}$ 上的 2 维向量空间，在 F 上有一个乘法使得 F 在自然的加法和该乘法下是整环，则 F 是域并且与 $\mathbb{C}$ 同构。

证明. 设 $\mathbf{1}$ 是 F 的乘法幺元，则 $\mathbb{R} \to \mathbb{R}\cdot\mathbf{1}$ 是环同构，即我们可以将 $\mathbb{R}$ 嵌入 F 中。由于 F 是 $\mathbb{R}$ 上的 2 维向量空间，故由基扩充定理可以找到 $\mathbf{e} \in F \setminus \mathbb{R}\cdot\mathbf{1}$ 使得 $\mathbf{1},\mathbf{e}$ 是 F 的一组基。于是 $\forall \mathbf{a} \in F$, $\exists \alpha,\beta \in \mathbb{R}$ 使得 $\mathbf{a} = \alpha\mathbf{1} + 2\beta\mathbf{e}$，特别地，$\mathbf{e}^2 = \alpha\mathbf{1} + 2\beta\mathbf{e}$。[1] 于是可令 $\mathbf{f} = -\beta\mathbf{1} + \mathbf{e} \notin \mathbb{R}\cdot\mathbf{1}$，则

$$\mathbf{f}^2 = (-\beta\mathbf{1} + \mathbf{e})^2 = \mathbf{e}^2 - 2\beta\mathbf{e} + \beta^2\mathbf{1} = (\alpha + \beta^2)\mathbf{1}$$

注意到 $\mathbf{f} \notin \mathbb{R}\cdot\mathbf{1}$，则 $\alpha + \beta^2 < 0$，于是可以令 $\alpha + \beta^2 = -\delta$, $\delta > 0$，则 $(\frac{1}{\sqrt{\delta}}\mathbf{f})^2 = -\mathbf{1}$，取 $\mathbf{j} = \frac{1}{\sqrt{\delta}}\mathbf{f}$, $\mathbf{j}^2 = -\mathbf{1}$，容易验证 $\varphi : \mathbb{C} \to F$, $a + b\mathrm{i} \mapsto a\mathbf{1} + b\mathbf{j}$ 是环同构，从而 F 是域并且同构于复数域。这样我们就完成了证明。 □

上面的定理告诉我们：$\mathbb{R}$ 的二次扩张在同构意义下是唯一的。那么，有理数域的二次扩张是什么情况呢？设 d 是一个整数 (可以是负数)，如果 $\sqrt{d}$ 不是有理数，则 $\mathbb{Q}(\sqrt{d}) = \{\alpha + \beta\sqrt{d} \mid \alpha,\beta \in \mathbb{Q}\}$ 是有理数域上的二维向量空间，并且是有理数域的一个扩域，称为 $\mathbb{Q}$ 的二次扩域 (验证之)，$d > 0$ 时 $\mathbb{Q}(\sqrt{d})$ 称为实二次扩域，$d < 0$ 时 $\mathbb{Q}(\sqrt{d})$ 称为虚二次扩域。显然 $\mathbb{Q}$ 的二次扩域不是唯一的 (思考：证明 $\mathbb{Q}(\sqrt{2})$ 与 $\mathbb{Q}(\sqrt{3})$ 之间不是域同构)。我们可以类似地定义 $\mathbb{Q}(\sqrt{d})$ 中元素的共轭和范数，感兴趣的读者可以自行推导它们的性质。二次扩域是数论的研究对象，有些问题至今尚未解决。

[1] 这样构造的原因是，我们希望找到满足 $\mathbf{j}^2 = -\mathbf{1}$ 的元素，如果这样的元素存在，则可设 $\mathbf{e} = a\mathbf{1} + b\mathbf{j}$, $b \neq 0$，于是 $\mathbf{e}^2 = (a^2 - b^2)\mathbf{1} + 2ab\mathbf{j} = (-a^2 - b^2)\mathbf{1} + 2a(a\mathbf{1} + b\mathbf{j}) = (-a^2 - b^2)\mathbf{1} + 2a\mathbf{e}$，这启示了 $\mathbf{j}$ 的构造。

5.3 * 复数的初等几何

我们已经知道，复数可以视作 $\mathbb{R}$ 上的二维向量空间 (即复平面)，于是许多平面几何的问题可以化成复数运算的问题来解决。下面我们简单提供一些用复数来解决平面几何问题的例子。

设 $z_1 = x_1 + y_1\mathrm{i}$, $z_2 = x_2 + y_2\mathrm{i}$，我们定义内积 $< z_1, z_2 >= x_1x_2 + y_1y_2 = \mathrm{Re}(z_1\overline{z_2})$，则内积满足：

(1) 双线性性：$\forall \lambda_1, \lambda_2 \in \mathbb{C}$, $< \lambda_1 z_1 + \lambda_2 z_2, z_3 >= \lambda_1 < z_1, z_3 > + \lambda_2 < z_2, z_3 >$, $< z_3, \lambda_1 z_1 + \lambda_2 z_2 >= \lambda_1 < z_3, z_1 > + \lambda_2 < z_3, z_2 >$。

(2) 对称性：$< z_1, z_2 >=< z_2, z_1 >$。

(3) 正定性：对任意 $z \in \mathbb{C}$, $< z, z >\geqslant 0$，并且等号当且仅当 $z = 0$ 时成立。

于是显然有 $|z| = \sqrt{< z, z >}$，并且我们可以定义两个非零复数的夹角 θ：

$$\cos\theta = \frac{< z_1, z_2 >}{|z_1| \cdot |z_2|}$$

(一般规定 $0 \leqslant \theta < \pi$)。特别地，如果 $< z_1, z_2 >= 0$，则称 z_1, z_2 正交 (规定 0 与任意复数正交)。

于是，复平面上过两个点 $u, v \in \mathbb{C}$ 的直线可以用参数方程 $\overline{uv} : w = u + (v - u)t$, $t \in \mathbb{R}$ 表示 (w 是直线上任意一点对应的复数，t 为参数)。于是我们立刻有：

(1) 三个不同的点共线 $\iff$ 它们对应的复数 z_1, z_2, z_3 满足 $z_3 = z_1 + (z_1 - z_2)t$, $t \in \mathbb{R}$，即 $\dfrac{z_3 - z_2}{z_1 - z_2} \in \mathbb{R}$。

(2) 两条直线 $\overline{z_1z_2}$, $\overline{z_3z_4}$ 垂直 $\iff < z_2 - z_1, z_4 - z_3 >= 0$。

定理 5.3.1. *不共线的四点 z_1, z_2, z_3, z_4 共圆 $\iff$ 其交比 $[z_1, z_2, z_3, z_4] = \dfrac{(z_1 - z_2)(z_3 - z_4)}{(z_1 - z_4)(z_3 - z_2)} \in \mathbb{R}$。*

证明. 注意到交比在任意一个平移 $z \mapsto z + a$, $\forall a \in \mathbb{C}$ 下保持不变 (验证留作练习)，则可以将坐标原点平移到 z_1, z_2, z_3 这个三角形的外心处，此时四点共圆 $\iff \|z_1\| = \|z_2\| = \|z_3\| = \|z_4\|$，而后者等价于交比是实数 (验证留作练习)。 □

最后我们关注一下三大古典作图难题：三等分角、倍立方体、化圆为方。它们的结论都是不能用尺规作图的方法做出。为了证明这一点，我们需要讨论尺规作图可以作出哪些对象。

平面上的点与复数一一对应，给定单位长度 1，则我们可以用无刻度的直尺和圆规完成加、减、乘、取倒数、开平方的操作，于是我们通过尺规作图可以得到的数构成一个域 CS，称为**可构造数域**。显然 $\mathbb{Q} \subset CS \subset \mathbb{C}$。并且可以证明如下的结论：

定理 5.3.2. *$\alpha \in CS \iff$ 存在二次扩张序列 $\mathbb{Q} \subset \mathbb{K}_1 \subset \mathbb{K}_2 \subset \cdots \subset \mathbb{K}_n$ 使得 $\alpha \in \mathbb{K}_n$，其中每个 $\mathbb{K}_i/\mathbb{K}_{i-1}$ 都是二次扩张*[1]。

证明细节可以参考 Algebra, Thomas.W.Hungerford,GTM73 的 *ChapterV, Appendix*。我们可以证明，三等分任意角和倍立方体都需要构造 $\mathbb{Q}$ 的三次扩张，化圆为方需要 $\mathbb{Q}$ 的超越扩张，于是它们都不能由尺规作图得到。

[1] 即 $\mathbb{K}_i$ 是 $\mathbb{K}_{i-1}$ 的 2 维向量空间。

5.4 习题

1. 验证命题5.1.1.

2. 验证 $F=\left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a,b\in\mathbb{R}\right\}$ 在矩阵的加法和乘法下是一个域.

3. 验证命题5.1.2.

4. 找出使 $z^2+(1+i)z$ 为纯虚数的所有模为 1 的复数 z. 在复平面 $\mathbb{C}$ 上画出这些点的轨迹.

5. 设复数 δ 满足方程 $\delta^4=-1$, 域 $\mathbb{R}(\delta)$ 由 $\mathbb{R}$ 添加 δ 得到. 关于 $\mathbb{R}(\delta)$ 我们能说些什么?

6. 设 $A,B\in M_n(\mathbb{R})$. 根据命题5.1.1证明 $\overline{\det(A+\mathrm{i}B)}=\det(A-\mathrm{i}B)$ (加横线表示复共轭).

7. 设 $A,B\in M_n(\mathbb{R})$,
$$C=\begin{pmatrix} A & B \\ -B & A \end{pmatrix}\in M_{2n}(\mathbb{R}).$$
对实矩阵 C 施行复数域 $\mathbb{C}$ 上的 I 型和 II 型初等变换证明
$$\det C=|\det(A+\mathrm{i}B)|^2.$$

8. (波利亚和塞格). 利用上面两题给出下述“奇怪”现象的解释. 带有复系数 $d_{kl}=a_{kl}+\mathrm{i}b_{kl}$ 和未知数 $z_i=x_i+\mathrm{i}y_i$ 的方形齐次线性方程组
$$\begin{gathered} d_{11}z_1+\cdots+d_{1n}z_n=0 \\ \cdots\cdots\cdots\cdots \\ d_{n1}z_1+\cdots+d_{nn}z_n=0 \end{gathered} \tag{$*$}$$
有非平凡解 $(z_1,\cdots,z_n)$, 当且仅当 $\det(d_{kl})=a+\mathrm{i}b=0$. 这个条件引出了两个方程 $a=0,b=0$, 它们联系到 $2n^2$ 个实数值 a_{kl}, b_{kl}. 另一方面, 方程组 $(*)$ 可以写成带有 $2n$ 个实未知数 x_i,y_i 的 $2n$ 个齐次线性方程组. 现在非平凡解存在的条件是, 单独一个 $2n$ 阶实行列式等于零, 它仅由关于 a_{kl}, b_{kl} 的一个方程给出. 这两个结果是怎样相容的?

9. 找出二次域 $\mathbb{Q}(\sqrt{d})$ 的自同构, 它应该保持有理数不变. 提示: 恒等映射和映射 $a+b\sqrt{d}\mapsto a-b\sqrt{d}$.

10. 当 $n>1$ 时, 1 的所有 n 次方根的和等于什么? 求 1 的 12 次本原根的和, 以及 15 次本原根的和.

11. 证明 $\zeta=(2+\mathrm{i})/(2-\mathrm{i})$ 不是 1 的根, 尽管 $|\zeta|=1$. 提示: $\zeta^n=1\Rightarrow(2-\mathrm{i})^n=(2+\mathrm{i})^n=(2-\mathrm{i}+2\mathrm{i})^n=(2-\mathrm{i})^n+\cdots+(2\mathrm{i})^n\Rightarrow(2-\mathrm{i})(a+b\mathrm{i})=(2\mathrm{i})^n\Rightarrow 5\left(a^2+b^2\right)=2^{2n}\Rightarrow 5\mid 2^{2n}$, 得到矛盾.

12. 集合 $S^1=\left\{e^{\mathrm{i}\varphi}\mid\varphi\in\mathbb{R}\right\}$ (以 1 为半径的圆周) 组成 $\mathbb{C}$ 的乘法群 $(\mathbb{C}^*,\cdot)$ 的一个子群. 如果 $\mathbb{R}-$ 线性映射 $f:\mathbb{C}\to\mathbb{C}$ 满足 $<f(z),f(z')>=<z,z'>$, 即 f 保存向量的长度 (两点间的距离), 则我们称 f 是正交的. 证明如果 $f(z)=cz$ 或 $f(z)=c\bar{z}$, 其中 $c\in S^1$, 则 $f:\mathbb{C}\to\mathbb{C}$ 是正交的.

13. 证明

$$\begin{vmatrix} x_0 & x_1 & x_2 & \cdots & x_{n-1} \\ x_{n-1} & x_0 & x_1 & \cdots & x_{n-2} \\ x_{n-2} & x_{n-1} & x_0 & \cdots & x_{n-3} \\ \cdots\cdots & \cdots\cdots & \cdots & \cdots & \cdots\cdots \\ x_1 & x_2 & x_3 & \cdots & x_0 \end{vmatrix} = \prod_{k=0}^{n-1} \left(x_0 + \zeta^k x_1 + \zeta^{2k} x_2 + \cdots + \zeta^{(n-1)k} x_{n-1} \right),$$

其中 ζ 是一个 n 次本原单位根.

14. 证明不等式

$$|z_1 - z_2| \leqslant \left| |z_1| - |z_2| \right| + \min\{|z_1|, |z_2|\} \cdot \left| \arg z_1 - \arg z_2 \right|.$$

在什么情形下这个不等式变成等式?

15. 利用复数的三角形式证明等式:

a) $\cos x + \cos 2x + \cdots + \cos nx = \frac{\sin \frac{nx}{2} \cos \frac{(n+1)x}{2}}{\sin \frac{x}{2}} \quad (x \neq 2k\pi, k \in \mathbb{Z})$;

b) $\sin x + \sin 2x + \cdots + \sin nx = \frac{\sin \frac{nx}{2} \sin \frac{(n+1)x}{2}}{\sin \frac{x}{2}} \quad (x \neq 2k\pi, k \in \mathbb{Z})$.

16. 设 A, B 是 m 阶实矩阵, 并且满足 $A^2 + B^2 = AB$, 若 $AB - BA$ 是可逆矩阵, 求证: m 是 3 的倍数.

第六章　多项式环

这一章我们主要讨论单变元和多变元的多项式，以及多项式的根。

6.1　单变元多项式

6.1.1　一元多项式环的定义与赋值同态

我们首先来讨论单变元多项式的构造。

设 $(R,+,0,\cdot,1)$ 是一个交换环，x 是一个符号 (未定元)，我们可以形式地说 $f(x)=a_0+a_1x+\cdots+a_nx^n,\ a_i\in R,\ i=0,1,\ldots,n$ 是一个多项式。例如，$\mathbb{R}$ 上 $f(x)=x^2+2x+3$ 就是一个多项式。但这样并不严谨，因为我们没有说清楚 x 究竟是什么。为此，我们给出下面的定义。

首先，我们注意到多项式是由其“系数”决定的，而与未定元的名字是 x 还是 y 没有关系。因此，我们定义

$$\widetilde{R}=\{(a_0,a_1,a_2,\cdots)\mid a_0,a_1,a_2,\cdots\in R\text{ 且其中只有有限多个非 }0.\}$$

我们记 $(a_0,a_1,a_2,\cdots)=\widetilde{a}$，且 $\widetilde{a}$ 的第 k 个位置的元素记为 a_k(从第 0 个开始计数，下同)。特别地，$\widetilde{0}=(0,0,\cdots),\ \widetilde{1}=(1,0,\cdots)$。我们在 $\widetilde{R}$ 上定义如下的加法和乘法：

$$\begin{aligned}&+:\widetilde{R}\times\widetilde{R}\longrightarrow\widetilde{R}\\&\quad(\widetilde{a},\widetilde{b})\longmapsto\widetilde{c},\quad c_k=a_k+b_k,\forall k\in\mathbb{N}.\\&\cdot:\widetilde{R}\times\widetilde{R}\longrightarrow\widetilde{R}\\&\quad(\widetilde{a},\widetilde{b})\longmapsto\widetilde{c},\quad c_k=\sum_{i=0}^{k}a_ib_{k-i},\forall k\in\mathbb{N}.\end{aligned}$$

容易验证上面的加法和乘法是良定义的 ($\widetilde{c}$ 中只有有限多个位置的元素非 0)，并且 $(\widetilde{R},+,\widetilde{0},\cdot,\widetilde{1})$ 是交换幺环 (验证 $\widetilde{R}$ 关于加法成交换群，于是可以定义自然的减法，乘法成交换幺半群，乘法关于加法有分配律，留作练习)。

引进符号 (未定元，indeterminate, variable)

$$x=(0,1,0,\cdots)$$

并规定单项式 (monomials)

$$x^0=\widetilde{1},\ x^i=(0,\ldots,0,1,0,\cdots)\text{ (第 }i\text{ 个位置是 1)。}$$

我们看到这个规定与 $\widetilde{R}$ 上的乘法是相容的。于是我们有：

命题 6.1.1. 令 $\tau:R\to\widetilde{R},\ r\mapsto\widetilde{r}=(r,0,0,\cdots)$，则 φ 是单的环同态。

证明是容易的，留作练习。

于是我们通常将 $\widetilde{r}\in\widetilde{R}$ 与 $r\in R$ 等同起来，即将 R 视作 $\widetilde{R}$ 的子环。我们也可以定义“数乘”多项式 $r\widetilde{a}=\widetilde{ra}=(ra_0,ra_1,\cdots)$。于是对任意 $\widetilde{a}\in\widetilde{R}$，不妨设 $\widetilde{a}$ 的第 n 个位置以后 (不含

n) 全为 0，则容易验证 $\widetilde{a} = a_0 + a_1 x + \cdots + a_n x^n$，即

$$\widetilde{R} = \left\{ \sum_{i=0}^{n} a_i x^i \mid n \in \mathbb{N},\ a_0, \ldots, a_n \in R. \right\}$$

我们也把 $\widetilde{R}$ 记作 $R[x]$，称为 R 上的**一元多项式环** (the ring of univariate polynomials over R)，其中的元素称为一元**多项式** (univariate polynomial)。

定理 6.1.1. (1) 设 $p = p_0 + p_1 x + \cdots + p_d x^d \in R[x]$，则 $p = 0 \iff p_0 = \cdots = p_d = 0$；
(2) 设 $p = p_0 + p_1 x + \cdots + p_s x^s$，$q = q_0 + q_1 x + \cdots + q_t x^t \in R[x]$，则 $p = q \iff s = t$ 且 $\forall i = 0, 1, \ldots, s,\ p_i = q_i$。

证明. (1)$p = 0 \iff (p_0, p_1, \ldots, p_d, 0, \cdots) = (0, 0, \cdots) \iff p_0 = p_1 = \cdots = p_d = 0$；
(2)$p = q \iff (p_0, \ldots, p_s, 0, \cdots) = (q_0, \ldots, q_t, 0, \cdots) \iff p_i = q_i,\ \forall i \in \mathbb{N}$，即得结论。

□

定义 6.1.1. 设 $p = p_0 + p_1 x + \cdots + p_d x^d \in R[x]$，$p_i \in R, p_d \neq 0$，则我们称 d 为多项式 p 的次数 (degree)，记作 $\deg_x(p) = d$ 或 $\deg(p) = d$。我们把 p_i 称为 x^i 在 p 中的系数 (coefficient)，特别地，p_d 称为 p 的首项系数 (leading coefficient)，记作 $\mathrm{lc}_x(p) = p_d$ 或 $\mathrm{lc}(p) = p_d$。如果 $\deg(p) = 0$，则称 p 为常多项式 (constant polynomial)；如果 $\mathrm{lc}(p) = 1$，则称 p 为首一多项式 (monic polynomial)。另外，特别规定 $\deg(0) = -\infty$。

由定义立刻有

命题 6.1.2. 设 $p, q \in R[x]$，则
(1)$\deg(p + q) \leqslant \max(\deg(p), \deg(q))$；
(2)$\deg(pq) \leqslant \deg(p) + \deg(q)$，当且仅当 $\mathrm{lc}(p)\mathrm{lc}(q) \neq 0$ 时 $\deg(pq) = \deg(p) + \deg(q)$ 并且 $\mathrm{lc}(pq) = \mathrm{lc}(p)\mathrm{lc}(q)$。

证明是显然的，留作练习。

例 6.1.1. 在 $\mathbb{Z}_6[x]$ 中 $f = \overline{2}x^2 + \overline{3}x + \overline{1}$，$g = \overline{3}x + \overline{4}$，求 $f + g$ 和 fg。

解. 计算可得

$$f + g = \overline{2}x^2 + (\overline{3} + \overline{3})x + (\overline{1} + \overline{4}) = \overline{2}x^2 + \overline{5};$$
$$fg = (\overline{2}x^2 + \overline{3}x + \overline{1})(\overline{3}x + \overline{4}) = \overline{0}x^3 + \overline{3}x^2 + \overline{3}x + \overline{2}x^2 + \overline{0}x + \overline{4} = \overline{5}x^2 + \overline{3}x + \overline{4}.$$

□

定理 6.1.2. 设 D 是整环，则 $D[x]$ 也是整环。

证明. 只需证明 $D[x]$ 无零因子。设 $f, g \in D[x]$ 且 $f \neq 0, g \neq 0$，则 $\mathrm{lc}(f) \neq 0,\ \mathrm{lc}(g) \neq 0$。于是由 D 是整环可知 $\mathrm{lc}(f)\mathrm{lc}(g) \neq 0$，即 $fg \neq 0$。 □

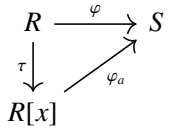
注 6.1.1. 当 $\mathbb{F}$ 是域时，由上面的定理知 $\mathbb{F}[x]$ 是整环，于是可以作 $\mathbb{F}[x]$ 的分式域

$$\mathbb{F}(x) = \left\{ \frac{f(x)}{g(x)} \mid f, g \in \mathbb{F}[x], g \neq 0 \right\}.$$

我们称 $\mathbb{F}(x)$ 为 $\mathbb{F}$ 上关于 x 的有理分式域。

在中学我们接触的多项式都是可以“代入数值”进行计算的，那么，如何严格地定义这一操作呢？这就是下面的**赋值同态** (evaluation homomorphism)。

定理 6.1.3. 设 $\varphi : R \to S$ 是两个环之间的非零同态，任意固定 $a \in S$，如命题6.1.1那样将 R 视作 $R[x]$ 的子环，则存在唯一的环同态 $\varphi_a : R[x] \to S$ 满足 $\varphi_a\big|_R = \varphi$，并且 $\varphi_a(x) = a$。



证明. 先证存在性。构造如下的 φ_a：

$$\begin{aligned} \varphi_a : R[x] &\longrightarrow S \\ p = \sum_{i=0}^{d} p_i x^i &\longmapsto \sum_{i=0}^{d} \varphi(p_i) a^i \quad (\text{规定} a^0 = 1_S) \end{aligned}$$

首先 φ_a 是良定义的 (多项式由系数唯一确定，定理6.1.1)。下面我们证明 φ_a 是环同态。设 $f = \sum_{i=0}^{n} f_i x^i$，$g = \sum_{i=0}^{m} g_i x^i$，$f_n, g_m \neq 0$，令 $d = \max(m, n)$，首先我们有

$$\begin{aligned} \varphi_a(f+g) &= \varphi_a\Big(\sum_{i=0}^{d} (f_i + g_i) x^i\Big) \\ &= \sum_{i=0}^{d} \varphi(f_i + g_i) a^i && (\varphi_a\text{的定义}) \\ &= \sum_{i=0}^{d} (\varphi(f_i) + \varphi(g_i)) a^i && (\varphi\text{是环同态}) \\ &= \sum_{i=0}^{d} \varphi(f_i) a^i + \sum_{i=0}^{d} \varphi(g_i) a^i \\ &= \varphi_a(f) + \varphi_a(g). \end{aligned}$$

同理可证 $\varphi_a(fg) = \varphi_a(f)\varphi_a(g)$，即 φ_a 是环同态。而且我们有 $\varphi(1_R) = \varphi(1_R)a^0 = 1_S \cdot 1_S = 1_S$，于是对 $\forall r \in R$，有

$$\varphi_a(r) = \varphi_a(rx^0) = \varphi(r)a^0 = \varphi(r)$$

即 $\varphi_a|_R = \varphi$，并且 $\varphi_a(x) = \varphi(1_R)a = 1_S a = a$。即我们构造的 φ_a 满足我们的所有要求。

再证唯一性。设 $\psi : R[x] \to S$ 也是满足上面要求的环同态，则

$$\begin{aligned} \psi(f) &= \psi\Big(\sum_{i=0}^{n} f_i x^i\Big) \\ &= \sum_{i=0}^{n} \psi(f_i)\psi(x)^i && (\psi\text{是环同态}) \\ &= \sum_{i=0}^{n} \varphi(f_i) a^i && (\psi\text{的性质}) \\ &= \varphi_a(f). \end{aligned}$$

唯一性证完。 □

定理的证明过程实际上给出了把元素“代入”多项式的具体操作。设 $f \in R[x]$，我们把 $\varphi_a(f)$ 也简记作 $f(a)$。

例 6.1.2. 在定理6.1.3中，令 $\varphi : \mathbb{Z} \to \mathbb{Z}_5$，$u \mapsto \overline{u}$ 以及 $a = \overline{3} \in \mathbb{Z}_5$，取 $f(x) = x^2 - 4 \in \mathbb{Z}[x]$，求 $\varphi_a(f)$。

解. $\varphi_a(f) = \varphi(1)a^2 - \varphi(4)a^0 = \overline{1} \cdot \overline{3}^2 - \overline{4} \cdot \overline{1} = \overline{5} = \overline{0}$。 □

特别地，在上面的定理中取 $S = R$，$\varphi = \mathrm{id}_R$ 就得到了我们熟悉的赋值操作。在没有特别说明时的赋值我们都是指这种情形。

此外，这个定理也告诉了我们如何将矩阵代入多项式中。

命题 6.1.3. 设 $\mathbb{F}$ 是域，$A \in M_n(\mathbb{F})$，则 $\mathbb{F}[A] = \{\sum_{i=0}^{m} a_i A^i \mid a_i \in \mathbb{F},\ m \in \mathbb{N}\}$（定义 $A^0 = E_n$）在矩阵加法和乘法下是一个交换环，注意到嵌入 $\rho : \mathbb{F} \to \mathbb{F}[A]$，$a \mapsto aE_n$ 是环同态，于是由定理6.1.3可以将 ρ 扩张到 $\mathbb{F}[x] \to \mathbb{F}[A]$ 上：

$$\begin{aligned} \rho_A : \mathbb{F}[x] &\longrightarrow \mathbb{F}[A] \\ f = \sum_{i=0}^{m} f_i x^i &\longmapsto \sum_{i=0}^{m} f_i A^i \end{aligned}$$

ρ_A 是环同态。

我们把 $\rho_A(f)$ 简记为 $f(A)$。

例 6.1.3. $f(x) = x^2 - 4 \in \mathbb{R}[x]$，$A = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$，则 $f(A) = A^2 - 4E = \begin{pmatrix} 0 & 4 \\ 0 & 0 \end{pmatrix}$。

6.1.2 一元多项式的带余除法

命题 6.1.4. 设 R 是交换环，$f, g \in R[x]$ 且 $g \neq 0$，如果 $\mathrm{lc}(g)$ 乘法可逆，则 $\exists!$ 一组 $q, r \in R[x]$ 满足 $f = qg + r$ 且 $\deg(r) < \deg(g)$。我们称 $q = \mathrm{quo}(f, g)$ 为商，$r = \mathrm{rem}(f, g)$ 为余式。

证明. 先证存在性。若 $\deg(f) < \deg(g)$，则取 $q = 0$，$r = f$ 即满足条件。于是我们只需考虑 $\deg(f) = \deg(g) + k$，$k \geqslant 0$ 的情形。不妨设 $\deg(g) = n$，对 k 做数学归纳法。

- $k = 0$ 时，设 $\mathrm{lc}(f) = f_n$，$\mathrm{lc}(g) = g_n$，令 $r = f - f_n g_n^{-1} g + r$，则 $\deg(r) < n$ 并且 $f = (f_n g_n^{-1})g + r$。取 $q = f_n g_n^{-1}$ 即可。
- 如果 $k \geqslant 1$ 并且存在性对次数差小于 k 的 f 和 g 成立，那么，令 $h = f - f_{n+k} g_n^{-1} x^k g$，则 $\deg(h) < n + k$，于是由归纳假设，存在 $q_1, r_1 \in R[x]$ 使得 $h = q_1 g + r_1$，满足 $\deg(r_1) < \deg(g)$，则 $f = (f_{n+k} g_n^{-1} x^k + q_1)g + r_1$，取 $q = f_{n+k} g_n^{-1} x^k + q_1$，$r = r_1$，则 $f = qg + r$ 且 $\deg(r) < \deg(g)$。

这样我们就证明了存在性。

再证唯一性。如果另有一组 q'，r' 满足 $f = q'g + r'$ 并且 $\deg(r') < \deg(g)$，则 $qg + r = q'g + r'$，即 $(q - q')g = r' - r$，注意到 $\deg(r' - r) < \deg(g)$，于是只能是 $q - q' = 0$，所以 $r' - r = 0$。这样我们就证明了唯一性。 □

特别地，如果 $\exists q(x) \in R[x]$ 使得 $f = qg$，则我们称多项式 f 能被 g 整除，记作 $g \mid f$。易证 $\mathrm{rem}(f, g) = 0 \Rightarrow g \mid f$，并且整除是 $R[x]$ 上的一个偏序关系。与整数上的竖式除法类似，我们也可以用竖式计算多项式的带余除法。我们用下面的例子展示具体的计算过程。

例 6.1.4. $f = x^3 + 2x + 1$, $g = 2x^2 + 1 \in \mathbb{R}[x]$, 求 $q, r \in \mathbb{R}[x]$ 使得 $f = qg + r$ 且 $\deg(r) < \deg(g)$。

解.

$$
\begin{array}{rcl}
 & & \frac{1}{2}x \\
\hline
2x^2 + 1 &) & x^3 + 2x + 1 \\
 & & x^3 + \frac{1}{2}x \\
\hline
 & & \frac{3}{2}x + 1
\end{array}
$$

□

特别地，域上的多项式一定可以作带余除法。

定理 6.1.4. 设 $\mathbb{F}$ 是域，$f, g \in \mathbb{F}[x]$，$g \neq 0$，则 $\exists!$ 一组 $q, r \in R[x]$ 满足 $f = qg + r$ 且 $\deg(r) < \deg(g)$。

证明. 由于 $g \neq 0$，$\mathbb{F}$ 是域，故 $\mathrm{lc}(g) \in \mathbb{F} \setminus \{0\}$ 可逆，再由命题 6.1.4即得结论。 □

定理 6.1.5 (余式定理). 设 R 是交换环，$f \in R[x]$，$\alpha \in R$，则 $f(\alpha) = \mathrm{rem}(f, x - \alpha)$。

证明. 在环 R 中 1 显然是乘法可逆元，故可以作带余除法 $f(x) = q(x)(x - \alpha) + r(x)$，由 $\deg(r(x)) < \deg(x - \alpha) = 1$ 可知 $\deg(r(x)) = 0$，即 $r(x) = r \in R$。再由赋值同态可知 $f(\alpha) = q(\alpha)(\alpha - \alpha) + r$，即 $r = f(\alpha)$。 □

于是我们可以简单地讨论一下一元多项式的根。

定义 6.1.2. 设 $\mathbb{F}, \mathbb{K}$ 是域且 F 是 $\mathbb{K}$ 的子域，设 $f \in \mathbb{F}[x]$, $\alpha \in \mathbb{K}$，如果 $f(\alpha) = 0$，则称 α 是 f 在 $\mathbb{K}$ 中的一个根。

例如 $f(x) = x^4 - x^2 - 2 \in \mathbb{Q}[x]$ 在 $\mathbb{Q}$ 中没有根，在 $\mathbb{R}$ 中有两个根 $\pm\sqrt{2}$，在 $\mathbb{C}$ 中有四个根 $\pm\sqrt{2}, \pm i$。

定理 6.1.6. 设 $\mathbb{F}$ 是域 $\mathbb{K}$ 的子域，$\alpha \in \mathbb{K}$，$f \in \mathbb{F}[x]$ 且 $d = \deg(f) > 0$，则

(i) $f(\alpha) = 0 \iff \mathrm{rem}(f, x - \alpha) = 0$;

(ii) f 在 $\mathbb{K}$ 中至多有 d 个互不相同的根。[1]

证明. (i) 显然可以将 f 放在 $\mathbb{K}[x]$ 中，于是由余式定理立刻可证。
(ii) 不妨设 f 在 $\mathbb{K}$ 中所有互不相同的根为 $\alpha_1, \alpha_2, \ldots, \alpha_m$，则由 (i) 可知 $f(x) = q_1(x)(x - \alpha_1)$，则 $0 = f(\alpha_2) = q_1(\alpha_2)(\alpha_2 - \alpha_1)$，由 $\alpha_1 \neq \alpha_2$ 可知 $q_1(\alpha_2) = 0$ 即 $q_1(x) = q_2(x)(x - \alpha_2)$，所以 $(x - \alpha_1)(x - \alpha_2) \mid f$。重复上面的过程归纳可得 $(x - \alpha_1) \cdots (x - \alpha_m) \mid f$，即 $f = q_m(x)(x - \alpha_1) \cdots (x - \alpha_m)$，而 $(x - \alpha_1) \cdots (x - \alpha_m)$ 是一个 m 次多项式，则由命题6.1.2易得 $m \leqslant d$。 □

6.1.3 一元多项式的最大公因子与辗转相除法

在介绍辗转相除法之前，我们先介绍一般的整环上的整除关系与最大公因子。

定义 6.1.3. 设 D 是整环，$a, b \in D$ 且 $a \neq 0$，如果存在 $c \in D$ 使得 $b = ca$，则称 a 是 b 的因子，b 是 a 的倍式 (b 能被 a 整除)，记作 $a \mid b$。如果 b 不能被 a 整除，则记作 $a \nmid b$。如果 $a \mid b$, $b \nmid a$，则称 a 是 b 的真因子。

显然这个定义包含了 $\mathbb{Z}$ 和 $R[x]$ 上关于因子和整除的定义。注意整除关系依赖于 D 的选取。

[1] 这个命题的条件可以减弱到整环上，留作练习。

定义 6.1.4. 设 D 是整环，$a,b\in D$，如果存在 $u\in D^\times$(D 中乘法可逆元) 使得 $a=ub$，则称 a 与 b 相伴 (a and b are associates)，记作 $a\approx b$。

例如 $\mathbb{Z}$ 中 n 和 $-n$ 相伴。容易验证相伴是一个等价关系。

引理 6.1.1. 设 D 是整环，$a,b,c\in D$，则
(1)$a\mid b, b\mid c\Longrightarrow a\mid c$;
(2)$a\mid b, a\mid c\Longrightarrow \forall f,g\in D,\ a\mid (fb+gc)$。

证明是简单的，留作练习。

引理 6.1.2. 设 D 是整环，$a,b\in D^*=D\setminus\{0\}$，则 $a\approx b\iff a\mid b$ 且 $b\mid a$。

证明. ($\Longrightarrow$)$a\approx b\Longrightarrow \exists u\in D^\times$ 使得 $a=ub$，所以 $u^{-1}a=b$，即 $a\mid b$ 且 $b\mid a$。
($\Longleftarrow$) 如果 $a\mid b$ 且 $b\mid a$ 成立，即 $\exists p,q\in D$ 使得 $a=pb,\ b=qa$，则 $a=pqa$，即 $(1-pq)a=0$，由 D 是整环即有 $1-pq=0$，即 $p,q\in D^\times$，所以 $a\approx b$。 □

定义 6.1.5. 设 D 是整环，$a,b\in D^*$，如果 $c\in D^*$ 同时满足 $c\mid a,\ c\mid b$，则称 c 是 a,b 的公因子 (common divisor)。设 g 是 a,b 的某个公因子，如果 g 还满足如下条件：任取 $c\in D^*$ 也是 a,b 的公因子，则 $c\mid g$，则我们称 g 是 a,b 的最大公因子 (greatest common divisor)，记作 $g=\gcd(a,b)$。

最大公因子在相伴的意义下是唯一的，即下面的命题。

命题 6.1.5. 设 D 是整环，$a,b\in D^*$，g,h 都是 a,b 的最大公因子，则 $g\approx h$。

证明. 由最大公因子的定义立刻有 $g\mid h,\ h\mid g$，于是由引理6.1.2即得结论。 □

例 6.1.5. 在 $\mathbb{Z}$ 中 $\gcd(35,21)=7$或 -7。(当然习惯上我们取 7，取 -7 也不影响结果。)

下面的定理是本小节的核心结论。

定理 6.1.7. 设 $\mathbb{F}$ 是域，则 $\mathbb{F}[x]$ 是整环 (定理6.1.2)，我们有：$\forall p,q\in\mathbb{F}[x]\setminus\{0\}$，$\gcd(p,q)$ 都存在并且 $\exists u,v\in\mathbb{F}[x]$ 使得 $up+vq=\gcd(p,q)$(Bezout 关系)。

证明. 令集合 $I=\{ap+bq\mid a,b\in\mathbb{F}[x]\}$，显然 $I\setminus\{0\}$ 是非空集合，于是我们可以设 g 是 I 中次数最低的非零多项式，我们只要证明 g 是 p,q 的最大公因子即可。

首先，我们可以做带余除法 $p=hg+r$，其中 $\deg(r)<\deg(g)$。由于 $g\in I$，按 I 的定义有：$\exists u,v\in\mathbb{F}[x]$ 使得 $up+vq=g$，代入 $p=hg+r$ 并整理有：

$$p=h(up+vq)+r\Longrightarrow r=(1-hu)p+(-hv)q$$

于是按 I 的定义，$r\in I$，但由于 $\deg(r)<\deg(g)$，如果 $r\neq 0$ 就会与 g 是 I 中次数最低的非零多项式矛盾，于是 $r=0$，即 $p=hg$，$g\mid p$。同理做 $q=h'g+r'$ 即可得到 $g\mid q$。即我们证明了 g 是 p,q 的公因子。

最后我们证明 g 的最大性。另取 $c\in\mathbb{F}[x]$ 也是 p,q 的公因子，则 $c\mid p, c\mid q\Longrightarrow c\mid up+vq$，即 $c\mid g$。这样我们就完成了证明。 □

实际上，证明中出现的 I 是 p,q 生成的 $\mathbb{F}[x]$ 的理想，这个证明告诉我们 $\mathbb{F}[x]$ 是一个主理想整环 (principal ideal domain,PID)[1]。

[1]即 $\mathbb{F}[x]$ 的每个理想都可以由一个元素生成，我们会在抽象代数课程中继续学习。

下面我们考虑如何计算 $\mathbb{F}[x]$ 中非零多项式 f,g 的最大公因子。类似于 1.6 节中的做法，我们反复做带余除法如下：
令 $r_0=f, r_1=g$，我们有

$$\begin{aligned}
r_0 &= q_2 r_1 + r_2 && \deg(r_1) > \deg(r_2)\\
r_1 &= q_3 r_2 + r_3 && \deg(r_2) > \deg(r_3)\\
&\vdots && \vdots\\
r_{k-2} &= q_k r_{k-1} + r_k && \deg(r_{k-1}) > \deg(r_k)\\
r_{k-1} &= q_{k+1} r_k && r_{k+1} = 0
\end{aligned}$$

这个算法能够终止 (即必存在 $k\in\mathbb{N}$ 使得 $r_{k+1}=0$) 是因为 $\deg(r_1)>\deg(r_2)>\cdots>\deg(r_k)$，而 $\deg(r_1)$ 是有限的。结合定理6.1.7, 用类似于第 1.6 节的证明方法我们就可以证明上面的 r_k 就是我们所需要的 $\gcd(f,g)$，并且将上面的带余除法的式子从下向上回代即可得到 Bezout 关系，详细的步骤我们留给读者作为练习。这个算法仍称作辗转相除法或者 Euclidean 算法。

例 6.1.6. 设 $f(x)=x^4+\overline{1}, g(x)=x^3+\overline{1}\in\mathbb{Z}_2[x]$，求 $\gcd(f,g)$。

解. 做带余除法 (利用竖式) 如下：

$$\begin{aligned}
x^4+\overline{1} &= x(x^3+\overline{1}) + x + \overline{1}\\
x^3+\overline{1} &= (x^2+x+\overline{1})(x+\overline{1})
\end{aligned}$$

即 $\gcd(f,g)=x+\overline{1}$。 □

定义 6.1.6. 设 $\mathbb{F}$ 是域，$f,g\in\mathbb{F}[x]\setminus\{0\}$，如果 $\gcd(f,g)=1$，则我们称 f,g 互素 (relatively prime)。

定理 6.1.8. 设 $\mathbb{F}$ 是域，$f,g\in\mathbb{F}[x]\setminus\{0\}$，则 f,g 互素 $\iff$ $\exists u,v\in\mathbb{F}[x]$ 使得 $uf+vg=1$。

由定义立刻可证。

定义 6.1.7. 设整环 R 满足如下条件：存在尺度函数 $\delta: R\setminus\{0\}\to\mathbb{N}$ 满足：
(1)$\forall a,b\in R^*$, $\delta(ab)\geqslant\delta(a)$; [1]
(2) 对 $\forall a\in R, b\in R^*$, $\exists q,r\in R$ 使得 $a=qb+r$，其中 $\delta(r)<\delta(b)$ 或者 $r=0$。
则我们称 R 是欧几里得环 (欧氏环,Euclidean ring)。

显然在欧氏环中我们可以做辗转相除法。类似于定理6.1.7的证明，我们可以得到：

定理 6.1.9. 欧氏环 R 中任意两个非零元素 a,b 都有最大公因子 $d=\gcd(a,b)$，并且存在 $u,v\in R$ 使得 $d=ua+vb$。

如果欧氏环 R 中 $\gcd(a,b)=1$，则我们称 a,b 互素。显然仍有 a,b 互素 $\iff$ $\exists u,v\in R$ 使得 $ua+vb=1$。

在下一节，我们的主要任务就是证明：欧氏环一定是唯一因子分解整环。

[1]这个条件可以去掉，但后面证明欧氏环是唯一因子分解整环会复杂一些。参考 Basic Algrbra I, N.Jacobson, DOVER PUBLICATIONS, INC 的 2.15 节。

6.2 多项式的因式分解

6.2.1 唯一因子分解整环

这一节中我们统一用 D 表示整环，$\mathbb{F}$ 表示域。记 $D^* = D \setminus \{0\}$, $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$。

定义 6.2.1. 设 $a \in D^* \setminus D^\times$，如果不存在 $b, c \in D^* \setminus D^\times$ 使得 $a = bc$，则称 a 是不可约元 (irreducible element)，称分解 $a = bc$ 是非平凡的；如果 $\forall b, c \in D^*$，由 $a \mid (bc)$ 都能得到 $a \mid b$ 或 $a \mid c$，则称 a 是素元 (prime element)。

例 6.2.1. 在 $\mathbb{Z}$ 中不可约元和素元都是素数；在 $\mathbb{Q}[x]$ 中 $x^2 - 2$ 是不可约元，同时也是素元，但在 $\mathbb{R}[x]$ 中 $x^2 - 2$ 既不是不可约元也不是素元。

命题 6.2.1. 设 $p \in D^*$ 是素元，则 p 一定是不可约元。

证明. 用反证法。假设 p 不是不可约元，即 $\exists a, b \in D^* \setminus D^\times$ 使得 $p = ab$，由 p 是素元可知 $p \mid a$ 或 $p \mid b$。不妨设 $p \mid a$，则 $\exists c \in D^*$ 使得 $cp = a$，那么我们有 $p = ab = cpb$，即 $p(1 - cb) = 0$。由于 D 是整环，$p \neq 0$，故 $bc = 1$，这与 $b \notin D^\times$ 矛盾！这样我们就证明了命题。 □

但上面命题的逆命题是不成立的，我们看下面的例子。

例 6.2.2. 显然 $\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$ 在通常的加法和乘法下是整环，在 $\mathbb{Z}[\sqrt{-3}]$ 上定义范数 $N(a + b\sqrt{-3}) = a^2 + 3b^2$，容易验证对 $\forall \alpha, \beta \in \mathbb{Z}[\sqrt{-3}]$，有 $N(\alpha\beta) = N(\alpha)N(\beta)$ 成立。

首先我们考虑 2 在 $\mathbb{Z}[\sqrt{-3}]$ 上的分解。设 $2 = (a + b\sqrt{-3})(c + d\sqrt{-3})$, $a, b, c, d \in \mathbb{Z}$，如果 $b = 0$ 或 $d = 0$，则 $a + b\sqrt{-3}$ 或 $c + d\sqrt{-3}$ 中至少有一个是 ± 1，这样的分解显然不是非平凡的；如果 b, d 均不为 0，则取范数即得 $4 = (a^2 + 3b^2)(c^2 + 3d^2) \geqslant 3 \cdot 3 = 9$，矛盾！故 2 没有非平凡的分解，即 2 是 $\mathbb{Z}[\sqrt{-3}]$ 中的不可约元。

然而，$2 \mid (1 + \sqrt{-3})(1 - \sqrt{-3})$，但 $2 \nmid (1 + \sqrt{-3})$, $2 \nmid (1 - \sqrt{-3})$，故 2 不是素元。

上面的例子告诉我们不可约元不一定是素元。但在一些特殊的环中，不可约元和素元是等价的。

引理 6.2.1. 设 $\mathbb{F}$ 是域，则 $\mathbb{F}[x]$ 中不可约元都是素元。

证明. 设 $p \in \mathbb{F}[x]$ 不可约，$f, g \in \mathbb{F}[x]$ 且 $p \mid (fg)$，我们只需证明：如果 $p \nmid f$，则必有 $p \mid g$。由于 $p \nmid f$ 且 p 不可约，则必有 $\gcd(p, f) = 1$，于是存在 $u, v \in \mathbb{F}[x]$ 使得 $uf + vp = 1$，则 $ufg + vpg = g$，由于 $p \mid (fg)$ 且 $p \mid vp$，故 $p \mid g$。 □

定义 6.2.2. 设 $a \in D^*$，如果存在 $\alpha \in D^\times$ 及不可约元 $p_1, p_2, \ldots, p_s$ 使得 $a = \alpha p_1 \cdots p_s$，则称 a 在 D 中有有限的不可约分解，称 $p_1, \ldots, p_s$ 为 a 的不可约因子。

例如，$\mathbb{Z}$ 中每个非零的整数都有有限的不可约分解 (证明是显然的，留作练习)。

命题 6.2.2. $\mathbb{F}[x]$ 中每个非零多项式都有不可约分解。

证明. 用数学归纳法。设 $f \in \mathbb{F}[x]$, $\deg(f) = d$。

(1) $d = 0, 1$ 时 f 本身不可约，这是显然的。

(2) 设 $d > 1$ 且命题对一切次数小于 d 的多项式成立。现在 $\deg(f) = d$，如果 f 本身是不可约元，则结论直接成立；否则必存在 $g, h \in \mathbb{F}[x] \setminus \{0\}$ 使得 $f = gh$，且 $g, h \notin \mathbb{F}[x]^\times$，即 $0 < \deg(g) < d$, $0 < \deg(h) < d$。由归纳假设，g, h 有有限的不可约分解，则将它们乘在一起就得到了 f 的不可约分解。 □

定义 6.2.3. 如果 D^* 中的每个元素都有有限的不可约分解并且如果 $a \in D^*$ 有两个不可约分解 $a = up_1 \cdots p_m = vq_1 \cdots q_n$(其中 $u, v \in D^\times$, $p_1, \ldots, p_m, q_1, \ldots, q_n$ 都是不可约元)，则有 $m = n$ 且经过适当地调整顺序后 $\forall k \in \{1, 2, \ldots, m\}$, $p_k \approx q_k$，那么我们称 D 是唯一因子分解整环 (unique factorization domain,UFD)。

我们解释一下分解的唯一性。例如，在 $\mathbb{Z}$ 中 $24 = 2 \times 2 \times 2 \times 3 = -3 \times (-2) \times 2 \times 2$，则调整顺序后有 $3 \approx 3, 2 \approx (-2), 2 \approx 2, 2 \approx 2$。

定理 6.2.1. 设 D^* 中每个元素都有有限的不可约分解，则 D 是唯一因子分解整环 $\iff$ D 中的不可约元都是素元。

证明. ($\Longrightarrow$) 设 p 是 D 中的不可约元，如果有 $a, b \in D^*$ 满足 $p \mid (ab)$ 且 $p \nmid a$，我们只需证 $p \mid b$。设

$$a = up_1 \cdots p_m,\ b = vq_1 \cdots q_n,\ u, v \in D^\times$$

分别是 a, b 的不可约分解，由 $p \mid (ab)$ 可知存在 $c \in D^*$, $ab = cp$。设 c 的不可约分解为 $c = wr_1 \cdots r_s$，其中 $w \in D^\times$，$r_1, \ldots, r_s$ 是不可约元，于是

$$w(r_1 \cdots r_s p) = uv(p_1 \cdots p_m q_1 \cdots q_n)$$

由于 D 是唯一因子分解整环，故 $s + 1 = m + n$ 并且调整顺序后每个 $r_1, \ldots, r_s, p$ 唯一地与 $p_1, \ldots, p_m, q_1, \ldots, q_n$ 中的某个元素相伴。由于 $p \nmid a$，故 p 不能与 $p_1, \ldots, p_m$ 当中的元素相伴，于是存在 $j \in \{1, \ldots, n\}$ 使得 $p \approx q_j$。不妨设 $p \approx q_1$，即 $p = \alpha q_1, \alpha \in D^\times$，则

$$b = v\alpha^{-1}(\alpha q_1)q_2 \cdots q_n = (v\alpha^{-1})pq_2 \cdots q_n.$$

即 $p \mid b$ 成立。这个方向就证完了。
($\Longleftarrow$) 任取 $a \in D^*$，设 $a = up_1 \cdots p_m = vq_1 \cdots q_n$，其中 $u, v \in D^\times$, $p_1, \ldots, p_m, q_1, \ldots, q_n$ 都是不可约元。不妨设 $m \leqslant n$，则由 $p_1 \mid q_1 \cdots q_n$(因为 $p_1 \mid v^{-1}up_1 \cdots p_m = q_1 \cdots q_n$) 及 p_1 是素元可知 $\exists j \in \{1, \ldots, n\}$ 使得 $p_1 \mid q_j$。不妨设 $j = 1$，由 q_1 不可约可知 $p_1 \approx q_1$，即 $\exists \rho_1 \in D^\times$ 使得 $q_1 = \rho_1 p_1$。那么我们有：

$$up_1 p_2 \cdots p_m = v\rho_1 p_1 q_2 \cdots q_n$$

由消去律可知 $up_2 \cdots p_m = v\rho_1 q_2 \cdots q_n$,其中 $v\rho_1 \in D^\times$。重复以上步骤可以得到 $p_1 \approx q_1, \ldots, p_m \approx q_m$ 并且

$$u = (v\rho_1 \cdots \rho_m)(q_{m+1} \cdots q_n).$$

于是如果 $m < n$,就有 $1 = (u^{-1}v\rho_1 \cdots \rho_m)(q_{m+1} \cdots q_n)$,即 $(q_{m+1} \cdots q_n)$ 是可逆元,这与 $q_{m+1}, \ldots, q_n$ 是不可约元矛盾！即必有 $m = n$ 并且 $\forall i \in \{1, \ldots, n\}$, $p_i \approx q_i$。这样我们就完成了证明。 □

注 6.2.1. 如果 D^* 的元素不一定有有限的不可约分解，那么 D 不是唯一分解整环。例如，取 $D = \mathbb{R}[x^{\frac{1}{2^n}} \mid n \in \mathbb{Z}^+]$ 为包含 $\mathbb{R}$ 和所有 $\{x^{\frac{1}{2^n}} \mid n \in \mathbb{Z}^+\}$ 的最小子环，那么 $x \in D$ 可以分解成 $x = x^{\frac{1}{2}}x^{\frac{1}{2}} = x^{\frac{1}{4}}x^{\frac{1}{4}}x^{\frac{1}{4}}x^{\frac{1}{4}} = \cdots$，我们找不到一个有限的不可约分解，于是它当然不是唯一分解整环。

我们在上一节的末尾已经定义了欧氏环。显然 $\mathbb{Z}, \mathbb{F}[x]$ 都是欧氏环，其尺度函数分别是绝对值和多项式的次数。下面我们来证明本节的主要结论。

定理 6.2.2. 欧氏环是唯一因子分解整环。

证明. 设 R 是欧氏环，尺度函数为 δ. 我们首先证明：R^* 中的每一个元素都有有限的不可约分解。首先，如果 $a \in R^\times$，那么 a 本身就是不可约分解；其次，a 本身是不可约元的情形也是平凡的。于是我们只需考虑 $a \notin R^\times$ 且 a 有真因子的情形。设 $a = bc$，其中 $b, c \notin R^\times$，我们先来证明 $\delta(b) < \delta(a)$。

事实上，由尺度函数的定义，首先我们有 $\delta(b) \leqslant \delta(a)$。如果 $\delta(b) = \delta(a)$，做带余除法 $b = qa + r$，则 $\delta(r) < \delta(a)$ 且 $r \neq 0$(如果 $r = 0$，即 $a \mid b$，于是 $a \approx b$ 与 b 是 a 的真因子矛盾!)。显然 $1 - qc \neq 0$(否则 $c \in R^\times$ 矛盾！)，则有

$$\delta(a) = \delta(b) \leqslant \delta(b(1 - qc)) = \delta(b - qa) = \delta(r) < \delta(a)$$

这是一个矛盾！故 a 有真因子 $b \Longrightarrow \delta(b) < \delta(a)$。

现在我们可以证明不可约分解是有限的了。设 $a = a_1 a_2 a_3 \cdots$，其中每个 $a_i, i \in \mathbb{Z}^+$ 都不可逆，则每个 $a_{i+1} a_{i+2} \cdots$ 都是 $a_i a_{i+1} a_{i+2} \cdots$ 的真因子，于是

$$\delta(a) = \delta(a_1 a_2 a_3 \cdots) > \delta(a_2 a_3 \cdots) > \delta(a_3 \cdots) > \cdots$$

由于 $\delta(a) \in \mathbb{N}$ 是一个有限数，故这个不等式链必然在某一步终止，即必有 $a = a_1 a_2 a_3 \cdots a_n$ 且 $n \leqslant \delta(a)$。所以 a 的长度最长的因子链就是 a 的不可约分解 (如果其中某个元素可约，则可以分解成不可约元的乘积，这会导致因子链变长，矛盾！)。

最后我们利用定理6.2.1来证明欧氏环是唯一因子分解整环。设 p 是 R 中的不可约元，我们只需证 p 是素元。设 $p \mid (ab)$ 且 $ab \neq 0$，不妨设 $p \nmid a$，由 p 不可约知 $\gcd(p, a) = 1$，那么由定理 6.1.9得 $\exists u, v \in R$ 使得 $up + va = 1$，于是 $upb + vab = b$，由 $p \mid upb$，$p \mid ab$ 可知 $p \mid b$，即 p 是素元。这样我们就完成了证明。 □

推论 6.2.1. $\mathbb{Z}$ 和 $\mathbb{F}[x]$ 都是唯一因子分解整环。[1]

由 $\mathbb{Z}$, $\mathbb{F}[x]$ 都是欧氏环即可证明。

然而，$\mathbb{F}[x, y]$ 就不是欧氏环[2]，但它仍然是唯一因子分解整环。证明参见习题课讲义。

下面我们利用唯一因子分解整环的性质来更精细地讨论多项式的根。

定义 6.2.4. 设 D 是唯一因子分解整环，$p \in D$ 是不可约元，$a \in D^*$。如果 $\exists m \in \mathbb{N}$ 使得 $p^m \mid a$ 但 $p^{m+1} \nmid a$，则称 m 是 p 在 a 中的重数。

例如，$\mathbb{Z}$ 上 2 在 24 中的重数为 3，$\mathbb{Q}[x]$ 中 $3x + 1$ 在 $f(x) = (x - 1)(3x + 1)^2(x^2 + 1)$ 中的重数为 2。

定义 6.2.5. 设 $\mathbb{F}$ 是 $\mathbb{K}$ 的子域，$\alpha \in \mathbb{K}$，$f(x) \in \mathbb{F}[x] \setminus \mathbb{F}$ 并且 $f(\alpha) = 0$，则 $\mathbb{K}[x]$ 上 $x - \alpha$ 在 f(视作 $\mathbb{K}[x]$ 中的元素) 中的重数称为根 α 的重数。特别地，当重数为 1 时，我们称 α 是 f 的单根；当重数等于 $m(> 1)$ 时，称 α 是 f 的 m 重根。

例如，在 $\mathbb{C}[x]$ 中 $f(x) = (x - 1)(3x + 1)^2(x^2 + 1)$ 有单根 $x = 1, \pm i$ 和 2 重根 $x = -\frac{1}{3}$。

命题 6.2.3. 设 $\mathbb{F}$ 是 $\mathbb{K}$ 的子域，$f(x) \in \mathbb{F}[x] \setminus \mathbb{F}$，并且 $f(x)$ 在 $\mathbb{K}$ 中的所有互不相同的根为 $\alpha_1, \ldots, \alpha_s$，其重数分别为 $m_1, \ldots, m_s$，则我们有 $m_1 + \cdots + m_s \leqslant \deg(f)$。

证明. 设 $d = \deg(f)$，对 d 做数学归纳法。

(1)$d = 1$ 时 f 只有一个单根，命题显然成立。

[1] 前者被称为算术基本定理。

[2] 多元多项式的严格定义在下一节。

(2) 设命题对 $\mathbb{F}[x]$ 中所有次数小于 d 的多项式成立，则对 f 而言，考虑 $\alpha_s \in \mathbb{K}$ 是 f 的 m_s 重根，即存在 $g(x) \in \mathbb{K}[x]$ 使得 $f(x) = g(x)(x-\alpha_s)^{m_s}$，并且 $g(\alpha_s) \neq 0$，$\deg(g) < \deg(f)$。我们需要证明 $\alpha_1, \ldots, \alpha_{s-1}$ 是 $g(x)$ 分别是 $g(x)$ 的 $m_1, \ldots, m_{s-1}$ 重根。

首先，由于对 $\forall i \in \{1, 2, \ldots, s-1\}$，有 $\alpha_i \neq \alpha_s$，则 $(x-\alpha_i)^{m_i}$ 与 $(x-\alpha_s)^{m_s}$ 在 $\mathbb{K}[x]$ 上互素 (UFD)，即存在 $u, v \in \mathbb{K}[x]$ 使得 $u(x)(x-\alpha_i)^{m_i} + v(x)(x-\alpha_s)^{m_s} = 1$，于是 $u(x)(x-\alpha_i)^{m_i} g(x) + v(x)(x-\alpha_s)^{m_s} g(x) = g(x)$，也即

$$u(x)(x-\alpha_i)^{m_i} g(x) + v(x) f(x) = g(x)$$

由于 $(x-\alpha_i)^{m_i} \mid (x-\alpha_i)^{m_i} g(x)$，$(x-\alpha_i)^{m_i} \mid f(x)$，故 $(x-\alpha_i)^{m_i} \mid g(x)$。

另一方面，对 $\forall i \in \{1, 2, \ldots, s-1\}$，由于 α_i 是 f 的 m_i 重根，即 $(x-\alpha_i)^{m_i+1} \nmid f$，所以 $(x-\alpha_i)^{m_i+1} \nmid g$，这说明 α_i 在 g 中的重数不超过 m_i。于是由归纳假设，$\deg(g) \geqslant m_1 + \cdots + m_{s-1}$，于是 $\deg(f) = \deg(g) + m_s \geqslant m_1 + \cdots + m_s$。 □

于是我们立刻有：

推论 6.2.2. 设 $\mathbb{F}$ 是 $\mathbb{K}$ 的子域，$f, g \in \mathbb{F}[x] \setminus \mathbb{F}$ 且 $\deg(f), \deg(g) \leqslant n$。如果 $\exists \alpha_1, \ldots \alpha_{n+1} \in \mathbb{K}$ 使得 $\forall i \in \{1, \ldots, n+1\}$，$f(\alpha_i) = g(\alpha_i)$，则 $f = g$。

证明. 反证法，如果命题不成立，则令 $h = f - g \neq 0$，注意到 h 有 $n+1$ 个不同的根 $\alpha_1, \ldots \alpha_{n+1}$，这与命题6.2.3矛盾！ □

6.2.2 多项式函数与插值

设 D 是整环，任取多项式 $f \in D[x]$，则赋值同态给出了一个 D 到 D 的映射 (函数) $\widetilde{f} : D \to D,\ a \mapsto f(a)$。我们把所有 $\widetilde{f}$ 放在一起做成一个集合 D_{pol}，并在 D_{pol} 上定义加法和乘法运算如下：

$$\widetilde{f} + \widetilde{g} : D \to D,\ a \mapsto f(a) + g(a); \qquad \widetilde{f} \cdot \widetilde{g} : D \to D,\ a \mapsto f(a)g(a).$$

则 D_{pol} 在上述加法和乘法下构成环，称为 D 上的多项式函数环。我们显然有：$\varphi : D[x] \to D_{pol},\ f(x) \mapsto \widetilde{f}$ 是一个满同态，但这个同态不一定是同构。例如，$\mathbb{Z}_p$(p 是素数) 上 $x^p - x$ 是一个非零多项式，但 $\varphi(x^p - x) = \widetilde{0}$，即 $\ker(\varphi) \neq \{0\}$。那么，φ 何时是同构呢？我们有下面的定理。

定理 6.2.3. 如果整环 D 满足 $|D| = \infty$，则 $\varphi : D[x] \to D_{pol},\ f(x) \mapsto \widetilde{f}$ 是同构。

证明. 只需证明此时 $\ker(\varphi) = \{\widetilde{0}\}$。反证法，如果存在非零多项式 $f \in D[x]$ 使得 $\widetilde{f} = \widehat{0}$，即 D 中的元素都是 f 的根，这与 f 只有有限多个不同的根 (定理6.1.6) 矛盾！于是命题得证。 □

由上面的定理，我们可以把无限域 $\mathbb{F}$ 上的多项式 $f(x) \in \mathbb{F}[x]$ 视作 $\mathbb{F} \to \mathbb{F}$ 的函数，那么，我们自然会有这样的问题：给定这个多项式函数在一些点上的取值，如何确定这个函数的表达式 (即多项式) 呢？这就是我们下面讨论的**插值** (interpolation) 问题。

定理 6.2.4. 设 $\mathbb{F}$ 是无限域，$\alpha_1, \ldots, \alpha_n \in \mathbb{F}$ 两两不同，$\beta_1, \ldots, \beta_n \in \mathbb{F}$，则存在唯一的 $f \in \mathbb{F}[x]$ 满足 $\deg(f) < n$ 且 $\forall i \in \{1, \ldots, n\}$，$f(\alpha_i) = \beta_i$。

证明. 一个自然的解决这个问题的思路是我们在中学就已经学过的待定系数法。由于我们要求 $\deg(f) < n$，故可设 $f = f_0 + f_1 x + \cdots + f_{n-1} x^{n-1}$，则由 $\forall i \in \{1, \ldots, n\}$，$f(\alpha_i) = \beta_i$ 可以列出

如下的线性方程组：

$$\begin{cases} f_0 + \alpha_1 f_1 + \cdots + \alpha_1^{n-1} f_{n-1} = \beta_1 \\ f_0 + \alpha_2 f_1 + \cdots + \alpha_2^{n-1} f_{n-1} = \beta_2 \\ \qquad\qquad\qquad\qquad\qquad\vdots \\ f_0 + \alpha_n f_1 + \cdots + \alpha_n^{n-1} f_{n-1} = \beta_n \end{cases}$$

即

$$\begin{pmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_n & \cdots & \alpha_n^{n-1} \end{pmatrix} \begin{pmatrix} f_0 \\ f_1 \\ \vdots \\ f_n \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix}.$$

记上面方程组的系数矩阵为 A。注意到系数矩阵是 Vandermonde 矩阵，由 $\alpha_1, \ldots, \alpha_n$ 互不相同可知 $\det(A) = \prod_{1 \leqslant i < j \leqslant n} (\alpha_j - \alpha_i) \neq 0$，于是上面的方程组存在唯一解。

事实上，我们可以验证

$$f(x) = \sum_{i=1}^{n} \beta_i \frac{(x-\alpha_1)\cdots(x-\alpha_{i-1})(x-\alpha_{i+1})\cdots(x-\alpha_n)}{(\alpha_i-\alpha_1)\cdots(\alpha_i-\alpha_{i-1})(\alpha_i-\alpha_{i+1})\cdots(\alpha_i-\alpha_n)} \tag{6.2.1}$$

就是满足条件的解。这是因为：对每个 $i \in \{1, \ldots, n\}$，令

$$l_i(x) = \frac{(x-\alpha_1)\cdots(x-\alpha_{i-1})(x-\alpha_{i+1})\cdots(x-\alpha_n)}{(\alpha_i-\alpha_1)\cdots(\alpha_i-\alpha_{i-1})(\alpha_i-\alpha_{i+1})\cdots(\alpha_i-\alpha_n)},$$

则 $l_i(x)$ 满足：

$$l_i(\alpha_j) = \delta_{ij} = \begin{cases} 1, & i = j; \\ 0, & i \neq j. \end{cases}.$$

由于 $f(x) = \sum_{i=1}^{n} \beta_i l_i(x)$，所以对每个 α_j，$j \in \{1, \ldots, n\}$，我们有

$$f(\alpha_j) = \sum_{i=1}^{n} \beta_i l_i(\alpha_j) = \sum_{i=1}^{n} \beta_i \delta_{ij} = \beta_j.$$

这样我们就完成了证明。 □

我们把上面证明过程中出现的式 (6.2.1) 称为 Lagrange **插值** (interpolation) **公式**。从上面的证明过程中可以看出，Lagrange 插值公式中 $l_i(x)$ 的构造与我们证明中国剩余定理 (定理1.6.5) 时 um 和 vn 的构造是类似的。实际上，Lagrange 插值公式是一般交换环上中国剩余定理的特例。此外，定理也可以在有限域上使用，但需要注意的是，此时必须有限制条件 $\deg(f) < |\mathbb{F}|$ (思考之)。

我们也可以用另一种办法解决插值问题。条件同上，我们不妨设 $f(x)$ 的形式为

$$f(x) = u_0 + u_1(x-\alpha_1) + u_2(x-\alpha_1)(x-\alpha_2) + \cdots + u_{n-1}(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_{n-1})$$

依次代入 $\alpha_1, \alpha_2, \ldots, \alpha_n$ 可以得到关于 $u_0, u_1, \ldots, u_{n-1}$ 的一元一次方程，这样即可确定 f。这种方法称为牛顿插值。

插值问题在理论研究和实际应用中都有重要的意义。我们在以后的学习中还会经常遇到它。

6.2.3 多项式的形式微分与无平方分解

我们在分析学中学过导数，也知道 $\mathbb{R}[x]$ 中的多项式函数是可微函数。注意到多项式函数的导数可以直接利用法则计算，而不需要依赖其分析学的意义。那么，我们是否可以在一般域的多项式环上定义代数风格的“导数”呢？这就是下面讨论的内容。

定义 6.2.6. 设 $\mathbb{K}$ 是域，在 $\mathbb{K}[x]$ 上定义如下映射：

$$\frac{\mathrm{d}}{\mathrm{d}x} : \mathbb{K}[x] \to \mathbb{K}[x]$$
$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \mapsto \frac{\mathrm{d}f}{\mathrm{d}x} = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}.$$

我们把 $\dfrac{\mathrm{d}}{\mathrm{d}x}$ 称为 $\mathbb{K}[x]$ 上的形式导数或形式微分算子。显然这个定义与分析学中的定义是一致的。我们也把 $\dfrac{\mathrm{d}f}{\mathrm{d}x}$ 记作 $f'(x)$，对 f 求 n 次导数记作 $f^{(n)}(x)$ 或 $\frac{\mathrm{d}^n f}{\mathrm{d}x^n}$。

容易验证形式微分算子满足以下性质：对 $\forall f, g \in \mathbb{K}[x]$, $\lambda \in \mathbb{K}$，我们有

(1) $\dfrac{\mathrm{d}(f+g)}{\mathrm{d}x} = \dfrac{\mathrm{d}f}{\mathrm{d}x} + \dfrac{\mathrm{d}g}{\mathrm{d}x}$;

(2) $\dfrac{\mathrm{d}\lambda f}{\mathrm{d}x} = \lambda \dfrac{\mathrm{d}f}{\mathrm{d}x}$;

(3) $\dfrac{\mathrm{d}(fg)}{\mathrm{d}x} = \dfrac{\mathrm{d}f}{\mathrm{d}x} g + f \dfrac{\mathrm{d}g}{\mathrm{d}x}$(称为 Leibniz 法则).

更一般地，我们可以利用这些性质在一般的环上定义导数运算如下：

定义 6.2.7. 设 A 是任意交换环，K 是 A 的子环，如果映射 $D_K : A \to A$ 满足：对 $\forall x, y \in A$ 及 $\lambda \in K$，有：

(i) $D_K(x+y) = D_K(x) + D_K(y)$;

(ii) $D_K(\lambda x) = \lambda D_K(x)$;

(iii) $D_K(xy) = D_K(x)y + x D_K(y)$.

则称 D_K 是 A 上的一个 K-导子 (或 K-导数，K-derivative)。我们把 A 上的所有 K-导子组成的集合记作 $\mathrm{Der}(A)$，称为 A 上的 K-导子代数，它是李代数 (Lie algebra) 的重要研究对象。

例 6.2.3. 设 $\mathbb{K}$ 是域，令 $A = \mathbb{K}[x]$，则由上面的定义可知 A 中的所有 $\mathbb{K}$-导子必然满足 $\forall f \in \mathbb{K}[x]$, $D(f) = \dfrac{\mathrm{d}f}{\mathrm{d}x} D(x)$ (提示：利用 $D(x^n) = xD(x^{n-1}) + x^{n-1}D(x)$，归纳得到 $D(x^n) = nx^{n-1}D(x)$，再利用算子 D 的线性性质，细节留作练习)。于是 $\mathbb{K}[x]$ 中的任意 $\mathbb{K}$-导子由 $D(x)$ 的值唯一确定。特别地，当 $D(x) = 1$ 时，D 就回到了形式微分算子的情形。

此外，由定义6.2.7的 (iii) 可知，导子 D 满足 $D^n(xy) = \sum_{k=0}^{n} \binom{n}{k} D^k(x) D^{n-k}(y)$，这个性质称为 Leibniz 公式。

下面我们考虑多项式的因子的重数和形式微分的关系。设 $\mathbb{F}$ 是域，则 $\mathbb{F}[x]$ 是唯一因子分解整环，即 $\forall f \in \mathbb{F}[x]$，存在唯一的不可约分解 $f(x) = \lambda p_1(x)^{k_1} \cdots p_r(x)^{k_r}$, $\lambda \in \mathbb{F}$, $p_1, \ldots, p_r \in \mathbb{F}[x]$ 是不可约多项式，我们把 k_i 称为素因子 p_i 的重数。

定理 6.2.5. 设 $p(x)$ 是 $f(x) \in \mathbb{F}[x]$ 的 k 重不可约因子，且 $\mathrm{char}(\mathbb{F}) \nmid k$，则 p 是 f' 的 $k-1$ 重因子。特别地，设 p 是 f 的不可约因子，则 p 的重数是 $1 \iff \gcd(p, f') = 1$。

证明. 设 $f(x)=[p(x)]^k g(x)$，其中 $\gcd(p(x),g(x))=1$，则 $f'(x)=[p(x)]^{k-1}(kp'(x)g(x)+p(x)g'(x))$，由于 $p(x)$ 不可约，故 $p'(x)\neq 0$，又 $k\nmid \mathrm{char}(\mathbb{F})$，故 $kp'(x)g(x)\neq 0$，于是 $p(x)\nmid kp'(x)g(x)$ (注意 p 是素元)，即 $p(x)\nmid kp'(x)g(x)+p(x)g'(x)$，所以 p 是 f' 的 $k-1$ 重因子。特例可以由定理的结论直接得到。 □

推论 6.2.3. (1) 设 $\mathbb{F}$ 是域，$f(x)\in\mathbb{F}[x]$，$p(x)$ 是 f 的不可约因子，$\mathrm{char}(\mathbb{F})\nmid k!$。则 p 在 f 中的重数是 $k \iff \forall i\in\{0,1,\dots,k-1\}$ 都有 $p(x)\mid f^{(i)}(x)$，但 $p(x)\nmid f^{(k)}(x)$。
(2) 设 $\mathbb{F}$ 是 $\mathbb{K}$ 的子域，$\mathrm{char}(\mathbb{F})\nmid k!$，则 $\alpha\in\mathbb{K}$ 是 $f(x)\in\mathbb{F}[x]$ 的 k 重根 $\iff f(\alpha)=f'(\alpha)=\cdots=f^{(k-1)}(\alpha)=0,\ f^{(k)}(\alpha)\neq 0$。
(3) 令 $f(x)=\lambda p_1(x)^{k_1}\cdots p_r(x)^{k_r}$，$\lambda\in\mathbb{F}$ 是 $f(x)$ 的不可约分解，其中 $k_i>0$，如果对每个 $i\in\{1,\dots,r\}$ 都有 $\mathrm{char}(\mathbb{F})\nmid k_i$，则 $\gcd(f,f')=p_1(x)^{k_1-1}\cdots p_r(x)^{k_r-1}$。

证明. (1)($\Longrightarrow$) 注意到 $\mathrm{char}(\mathbb{F})\nmid k! \Longrightarrow \forall i\in\{0,1,\dots,k-1\},\mathrm{char}(\mathbb{F})\nmid k-i$，于是由定理6.2.5可以归纳地得到 p 是 f' 的 $k-1$ 重因子，p 是 f'' 的 $k-2$ 重因子，……p 是 $f^{(k-1)}$ 的 1 重因子，所以 p 与 $f^{(k)}$ 互素，这样就证明了该方向。
($\Longleftarrow$) 设 p 是 f 的 l 重因子，我们只需要证明 $l=k$ 即可。由 ($\Longrightarrow$) 方向可知，p 是 f 的 l 重因子立刻有：$\forall i\in\{0,1,\dots,l-1\}$ 都有 $p(x)\mid f^{(i)}(x)$，但 $p(x)\nmid f^{(l)}(x)$。显然这只有当 $l=k$ 时才成立，否则与条件 “$\forall i\in\{0,1,\dots,k-1\}$ 都有 $p(x)\mid f^{(i)}(x)$，但 $p(x)\nmid f^{(k)}(x)$” 矛盾。
(2) 我们把 f 视作 $\mathbb{K}[x]$ 中的多项式，取 $p(x)=x-\alpha$，由 (1) 及定理6.1.6(i) 即得结论。
(3) 由于每个 k_i 都不能被 $\mathrm{char}(\mathbb{F})$ 整除，故对每个 i，$f'(x)$ 可以写成 $[p_i(x)]^{k-1}g_i(x)$ 的形式，其中 $\gcd(p_i,g_i)=1$。于是由 (1) 可得：对 $\forall i\in\{1,\dots,r\}$，$p_i(x)$ 是 f' 的 k_i-1 重因子，即 $\exists g\in\mathbb{F}[x]$，$f'(x)=p_1(x)^{k_1-1}\cdots p_r(x)^{k_r-1}g(x)$，且 $\gcd(p_i,g)=1$ 对每个 $i\in\{1,\dots,r\}$ 成立。于是对任意一组非负整数 $l_1,\dots,l_r$，我们有 $\gcd(p_1(x)^{l_1}\cdots p_r(x)^{l_r},g(x))=1$，特别地，$\gcd(f,g)=1$，于是 $\gcd(f,f')=p_1(x)^{k_1-1}\cdots p_r(x)^{k_r-1}$。 □

定义 6.2.8. 设 $\mathbb{F}$ 是域，$f(x)=\lambda p_1(x)^{k_1}\cdots p_r(x)^{k_r}$，$\lambda\in\mathbb{F}$ 是 $f(x)$ 的不可约分解，其中 $k_i>0$，令 $g(x)=\dfrac{f(x)}{\gcd(f,f')}$，则 $g(x)$ 与 $p_1(x)\cdots p_r(x)$ 相伴，我们称 $g(x)$ 是 f 的无平方部分。若 $f=\lambda q_1^{l_1}\cdots q_s^{l_s}$，其中 $q_1,\dots,q_s$ 两两互素且在 $\mathbb{F}$ 上都没有重数大于 1 的因子，则称这个分解是 f 的无平方分解。

由于求 f 的无平方部分只需要求导和求最大公因子，因此我们并不需要知道 f 的素因子分解。因此，对 $\mathrm{char}(\mathbb{F})=0$ 的情形，我们可以通过反复地求导和辗转相除来求 f 的无平方分解。

例 6.2.4. 设 $f(x)=x^5-3x^4+2x^3+2x^2-3x+1\in\mathbb{Q}[x]$，求 f 的无平方分解。

解. 进行如下计算 (相伴意义下)：

$$
\begin{aligned}
&h_1(x)=\gcd(f,f')=x^3-3x^2+3x-1, && g_1(x)=\frac{f}{h_1}=x^2-1 && \\
&h_2(x)=\gcd(h_1,h_1')=x^2-2x+1, && g_2(x)=\frac{h_1}{h_2}=x-1, && f_1=\frac{g_1}{g_2}=x+1\\
&h_3(x)=\gcd(h_2,h_2')=x-1, && g_3(x)=\frac{h_2}{h_3}=x-1, && f_2=\frac{g_2}{g_3}=1\\
&h_4(x)=\gcd(h_3,h_3')=1, && g_4(x)=\frac{h_3}{h_4}=x-1, && f_3=\frac{g_3}{g_4}=1\\
&h_5(x)=\gcd(h_4,h_4')=1, && g_5(x)=\frac{h_4}{h_5}=1, && f_4=\frac{g_4}{g_5}=x-1.
\end{aligned}
$$

由于 $g_5=1$，算法停止，故 $f(x)=f_1f_2^2f_3^3f_4^4=(x+1)(x-1)^4$。 □

思考题 6.2.1. (1) 按上面例子的思路，写出一般的算法 (有余力的读者可以用计算机实现该算法)；
(2) 当域的特征不为 0 时算法应该做什么样的改动 (此时会遇到 $f'=0$ 的问题，思考之)？

6.2.4 整系数多项式的因子分解

这一小节我们来考虑整系数多项式的素因子分解。由于 $\mathbb{Z}$ 中除了 ± 1 之外的数关于乘法都不可逆，这给我们做分解带来了许多额外的困扰 (比如 $2x^2+3x+1$ 就不能再写成 $2(x+1)(x+\frac{1}{2})$ 了)。为此，我们需要新的工具来处理整系数多项式。

定义 6.2.9. 设 $f(x)\in\mathbb{Z}\setminus\{0\}$，我们称 f 的所有系数的最大公因子为 f 的 **容度** (content)，记作 $\mathrm{cont}(f)$。如果 $\mathrm{cont}(f)=1$，则称 f 是本原多项式 (primitive polynomial)。

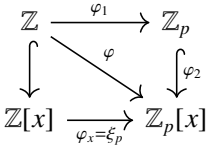
例如，$\mathrm{cont}(2x^2+3x+1)=1$，$\mathrm{cont}(24x^3+3x-12)=3$。设 $a\in\mathbb{Z}$，显然我们有 $\mathrm{cont}(af)=a\mathrm{cont}(f)$。

在讨论整系数多项式时，将系数模掉一个素数是一种常用的方法，这可以在使系数变小的同时保留原多项式的一些信息。

引理 6.2.2. 设 p 是任意素数，则
(1) 令

$$\begin{aligned}\xi_p:\mathbb{Z}[x]&\longrightarrow\mathbb{Z}_p[x]\\ f=\sum_{i=0}^{d}f_ix^i&\longmapsto\overline{f}=\sum_{i=0}^{d}\overline{f_i}x^i.\end{aligned}$$

其中 $\overline{f_i}$ 是 f_i 模 p 的剩余类。则 ξ_p 是满的环同态。
(2) 如果 $f\in\mathbb{Z}[x]$ 是本原多项式，则 $\xi_p(f)\neq\overline{0}$。



证明. (1) 显然 $\varphi_1:\mathbb{Z}\to\mathbb{Z}_p$，$a\mapsto\overline{a}$ 和 $\varphi_2:\mathbb{Z}_p\to\mathbb{Z}_p[x]$，$\overline{1}\mapsto\overline{1}$ 都是环同态，于是 $\varphi=\varphi_2\circ\varphi_1:\mathbb{Z}\to\mathbb{Z}_p[x]$ 也是环同态，由赋值同态 (定理6.1.3) 可知 $\varphi_x=\xi_p:\mathbb{Z}[x]\to\mathbb{Z}_p[x]$，$x\mapsto x$ 也是环同态。ξ_p 是满射显然。
(2) 若 $\xi_p(f)=\overline{0}$，则 $\overline{f_0}=\cdots=\overline{f_d}=\overline{0}$，即 $p\mid f_0,\ldots,p\mid f_d$，这与 $\mathrm{cont}(f)=1$ 矛盾！ □

下面我们先看一些例子。

例 6.2.5. $\mathbb{Z}_2[x]$ 中二次多项式只有 x^2，$x^2+x=x(x+\overline{1})$，$x^2+\overline{1}=(x+\overline{1})^2$，$x^2+x+\overline{1}$，其中只有最后一个是不可约多项式。

例 6.2.6. 求证 $f(x)=x^4+x+1\in\mathbb{Z}[x]$ 在 $\mathbb{Z}[x]$ 上不可约。

解. 考虑 $\xi_2:\mathbb{Z}[x]\to\mathbb{Z}_2[x]$，如果 f 在 $\mathbb{Z}[x]$ 上可约，那么 $\xi_2(f)$ 在 $\mathbb{Z}_2[x]$ 上也可约。用反证法。如果 $\xi_2(f)=\xi_2(g)\xi_2(h)$，其中 $\xi_2(g),\xi_2(h)$ 的次数都大于 1 而小于 4，那么，我们讨论两种情况：
(1)$\xi_2(g),\xi_2(h)$ 中有一个是 1 次多项式，这说明 $\xi_2(f)$ 在 $\mathbb{Z}_2$ 上有根，而 $\xi_2(f)(\overline{0})=\xi_2(f)(\overline{1})=\overline{1}$，

矛盾！此情形不成立。
(2)$\xi_2(g),\xi_2(h)$ 都是 $\mathbb{Z}_2[x]$ 中的 2 次不可约多项式，则由上一个例子可知 $\xi_2(f)$ 只能是 $(x^2+x+\overline{1})^2 = x^4+x^2+\overline{1}$，这与 $\xi_2(f) = x^4+x+\overline{1}$ 矛盾！此情形亦不成立。
综上所述，$\xi_2(f)$ 在 $\mathbb{Z}_2[x]$ 上不可约，所以 f 在 $\mathbb{Z}[x]$ 上不可约。 □

引理 6.2.3 (Gauss 引理). 设 $f,g \in \mathbb{Z}[x]$ 是本原多项式，则 fg 也是本原多项式。

证明. 用反证法。假设 fg 不是本原多项式，则存在素数 p 使得 $p \mid \mathrm{cont}(fg)$，于是 $\xi_p(fg) = \overline{0}$。由于 ξ_p 是环同态，故 $\xi_p(f)\xi_p(g) = 0$，然而 $\mathbb{Z}_p[x]$ 是整环，故 $\xi_p(f) = \overline{0}$ 或 $\xi_p(g) = \overline{0}$，即 $p \mid \mathrm{cont}(f)$ 或 $p \mid \mathrm{cont}(g)$，这与 f,g 都是本原多项式矛盾！ □

注 6.2.2. 显然对 $\forall f \in \mathbb{Z}[x]\setminus\{0\}$，$f$ 可以唯一地写成 $\mathrm{cont}(f)g$ 的形式，其中 g 是本原多项式。

推论 6.2.4. 设 $f,g \in \mathbb{Z}[x]$，则 $\mathrm{cont}(fg) = \mathrm{cont}(f)\mathrm{cont}(g)$

证明. 设 $f = \mathrm{cont}(f)u(x)$，$g = \mathrm{cont}(g)v(x)$，其中 $u,v \in \mathbb{Z}[x]$ 是本原多项式。于是

$$fg = \mathrm{cont}(f)\mathrm{cont}(g)\cdot uv$$

由 Gauss 引理，uv 是本原多项式，故 $\mathrm{cont}(fg) = \mathrm{cont}(f)\mathrm{cont}(g)$。 □

定理 6.2.6. 设 $f(x) \in \mathbb{Z}[x]\setminus\mathbb{Z}$，如果 f 不能写成 $\mathbb{Z}[x]$ 中两个正次数多项式的乘积，则 f 在 $\mathbb{Q}[x]$ 中不可约。

证明. 用反证法。如果 f 在 $\mathbb{Q}[x]$ 中可约，即 $\exists g,h \in \mathbb{Q}[x]\setminus\mathbb{Q}$ 使得 $f = gh$。设 g,h 的所有系数的分母的最小公倍数分别为 a,b，则 $ag,bh \in \mathbb{Z}[x]$，不妨设 $ag = \mathrm{cont}(ag)u(x)$，$bh = \mathrm{cont}(bh)v(x)$，其中 $u,v \in \mathbb{Z}[x]$ 是正次数的本原多项式，则由 $(ab)f = ag\cdot bh$ 可知

$$ab\,\mathrm{cont}(f) = \mathrm{cont}(abf) = \mathrm{cont}(ag)\mathrm{cont}(bh)$$

则 $abf = ag\cdot bh = \mathrm{cont}(ag)\mathrm{cont}(bh)uv = \mathrm{cont}(abf) = ab\,\mathrm{cont}(f)uv$，即 $f = \mathrm{cont}(f)uv$，这与 f 不能写成 $\mathbb{Z}[x]$ 中两个正次数多项式的乘积矛盾！ □

推论 6.2.5. 设 $f(x) = f_0 + f_1x + \cdots + f_nx^n \in \mathbb{Z}[x]$，如果 f 有有理数根 $\frac{r}{s}$，$\gcd(r,s) = 1$，则 $r \mid f_0$，$s \mid f_n$。

证明. 由命题的条件可知在 $\mathbb{Q}[x]$ 上 $x - \frac{r}{s}$ 是 f 的因子，于是 $sx - r$ 是本原多项式并且由定理6.2.6的证明过程可得 $sx - r \mid f$，于是可设 $f = (sx-r)(a_0 + \cdots + a_{n-1}x^{n-1})$，其中 $a_0,\ldots,a_{n-1} \in \mathbb{Z}$，展开上式右边并对比系数可知 $a_0r = -f_0$，$a_{n-1}s = f_{n-1}$，即 $r \mid f_0$，$s \mid f_n$。 □

这个推论可以帮助我们快速判断一个整系数 (或有理系数) 多项式是否有有理数根，即试根法。

下面我们给出一个判断整系数多项式是否可约的方法。

定理 6.2.7 (Eisenstein 判别法). 设 $n \in \mathbb{Z}, n \geqslant 2$，$f = x^n + f_{n-1}x^{n-1} + \cdots + f_1x + f_0 \in \mathbb{Z}[x]$。如果存在素数 $p \in \mathbb{Z}$ 使得 $p \mid f_{n-1},\ldots,p \mid f_1, p \mid f_0$ 都成立但 $p^2 \nmid f_0$，则 f 在 $\mathbb{Q}[x]$ 上不可约。

证明. 用反证法。假设 f 在 $\mathbb{Q}[x]$ 中可约，则由定理6.2.6可知，存在 $g,h \in \mathbb{Z}[x]\setminus\mathbb{Z}$ 使得 $f = gh$。不妨设 $\deg(g) = d$，$\deg(h) = e$，则 $1 < d < n$，$1 < e < n$，并且设

$$g = x^d + g_{d-1}x^{d-1} + \cdots + g_0, \quad h = x^e + h_{e-1}x^{e-1} + \cdots + h_0.$$

由于 $p \mid f_{n-1}, \ldots, p \mid f_1, p \mid f_0$，在 $f = gh$ 两边同时取 ξ_p 可得 $\xi_p(f) = \xi_p(g)\xi_p(h)$，即

$$x^n = (x^d + \overline{g_{d-1}}x^{d-1} + \cdots + \overline{g_0})(x^e + \overline{h_{e-1}}x^{e-1} + \cdots + \overline{h_0}) \tag{6.2.2}$$

对比上式中常数项的系数即得 $\overline{g_0 h_0} = 0$, 因此 $\overline{g_0} = 0$ 或 $\overline{h_0} = 0$，即 $p \mid g_0$ 或 $p \mid h_0$。因为 $p^2 \nmid f_0$，我们可以假设 $p|g_0$，$p \nmid h_0$。设 i 是最小满足 $\overline{g_i} \neq 0$ 的指标，由上面的论证可知 $1 \leqslant i \leqslant d$，那么 x^i 在式 (6.2.2) 右边的系数是 $\overline{g_i}\overline{h_0} \neq 0$，这与 (6.2.2) 的左边矛盾！这样我们就完成了证明。 □

需要说明的是，Eisenstein 判别法的逆命题不成立，例如 $x^{105} - 9$ 在 $\mathbb{Q}[x]$ 上不可约 (试证明之 [1])。然而我们显然找不到素数 p 满足 Eisenstein 判别法的条件。

推论 6.2.6. *设 $n \in \mathbb{Z}, n \geqslant 2$，$f = f_n x^n + f_{n-1}x^{n-1} + \cdots + f_1 x + f_0 \in \mathbb{Z}[x]$。如果存在素数 $p \in \mathbb{Z}$ 使得 $p \nmid f_n$ 但 $p \mid f_{n-1}, \ldots, p \mid f_1, p \mid f_0$，而且 $p^2 \nmid f_0$，则 f 在 $\mathbb{Q}[x]$ 上不可约。*

证明是类似的，留作练习。

在本小节的最后，我们看几个证明多项式不可约的例题。

例 6.2.7. *求证 $x^5 + 2x + 2$ 在 $\mathbb{Q}[x]$ 上不可约。*

证明. 取 $p = 2$，则 $p \mid 2$，$p^2 \nmid 2$，由 Eisenstein 判别法即得结论。 □

例 6.2.8. *设 $p \in \mathbb{Z}^+$ 是素数，求证 $f(x) = x^{p-1} + \cdots + x + 1$ 在 $\mathbb{Q}[x]$ 上不可约。*

证明. 作变量替换 $x \mapsto x + 1$(注意 $\mathbb{Q}[x] \to \mathbb{Q}[x]$, $x \mapsto x + 1$ 是环同构)，则

$$\begin{aligned} h(x) = f(x+1) &= (x+1)^{p-1} + \cdots + (x+1) + 1 \\ &= \frac{(x+1)^p - 1}{(x+1) - 1} \quad \text{(形式计算，可省略)} \\ &= x^{p-1} + \binom{p}{1}x^{p-2} + \cdots + \binom{p}{p-2}x + \binom{p}{p-1} \end{aligned}$$

显然 f 不可约 $\iff$ h 不可约。由于 $p \mid \binom{p}{k}$ 对每个 $k \in \{1, 2, \ldots, p-1\}$ 都成立，但 $p^2 \nmid \binom{p}{p-1}$，故由 Eisenstein 判别法可知 h 不可约。这样我们就完成了证明。 □

6.2.5 有理函数的准素分解

最后我们简单讨论一下形如多项式的“比值”的表达式的化简。

在 §4.4 节中，我们已经讨论了如何从一个整环出发，通过局部化的方法得到其分式域。特别地，我们知道域 $\mathbb{F}$ 上的多项式环 $\mathbb{F}[x]$ 是整环，则可以构造 $\mathbb{F}[x]$ 的分式域

$$\mathbb{F}(x) = \left\{ \frac{f}{g} \mid f, g \in \mathbb{F}[x],\ g \neq 0 \right\}.$$

注意 $\mathbb{F}(x)$ 中的元素是等价类，并且可以将 $\mathbb{F}[x]$ 自然地嵌入到 $\mathbb{F}(x)$ 中。$\mathbb{F}(x)$ 上的加法和乘法的定义与性质已经在 §4.4 中讨论过了。我们把 $\mathbb{F}(x)$ 称为**有理函数域** (rational function field)，其中的元素称为 $\mathbb{F}$ 上的**有理函数**或有理分式。

定义 6.2.10. *设 $\mathbb{F}$ 是域，$\dfrac{f}{g} \in \mathbb{F}[x]$，我们称 f 为分子，g 为分母，定义有理函数的次数 $\deg(\dfrac{f}{g}) = \deg(f) - \deg(g)$。这个定义是良定义的，因为如果 $\dfrac{f}{g} = \dfrac{f'}{g'}$，即 $fg' = f'g$，于是*

[1] 提示：反设 $x^{105} - 9 = fg$，则在 $\mathbb{C}$ 上有 $f = \prod_{k=1}^{s}(x - \sqrt[105]{9}e^{2m_k\pi i})$, $m_1, \ldots, m_s \in \{0, 1, \ldots, 104\}$，证明 $|f(0)| \notin \mathbb{Z}$ 即可。

$\deg(f)+\deg(g')=\deg(fg')=\deg(f'g)=\deg(f')+\deg(g)$，即 $\deg(f)-\deg(g)=\deg f'-\deg(g')$。如果 $\deg(\frac{f}{g})<0$，则称 $\frac{f}{g}$ 是真分式；如果 $\frac{f}{g}$ 中 $\gcd(f,g)=1$，则称 $\frac{f}{g}$ 是既约分式。显然每个有理分式都会等价于一个既约分式，因此，下面我们提到的有理分式默认都是既约的。

对有理分式 $\frac{f}{g}$ 来说，如果 $\deg(f)\geqslant\deg(g)$，那么我们可以做带余除法 $f(x)=q(x)g(x)+r(x)$，$\deg(r)<\deg(g)$ 或 $r(x)=0$，则

$$\frac{f(x)}{g(x)}=q(x)+\frac{r(x)}{g(x)}$$

其中 $\frac{r(x)}{g(x)}$ 是真分式。由带余除法的唯一性可得该分解的唯一性。此外，我们称形如 $\frac{f(x)}{p(x)^n}$ (其中 $p(x)\in\mathbb{F}[x]$ 是不可约多项式，$\deg(f)<\deg(p)$) 的有理分式为最简分式。下面我们讨论如何将真分式写成最简分式的和。

引理 6.2.4. 设 $p(x)\in\mathbb{F}[x]$ 是不可约多项式，则对 $\forall f(x)\in\mathbb{F}[x]$，存在唯一一组 $q_0(x),q_1(x),\ldots,q_k(x)$ 使得 $\forall i\in\{0,\ldots,k\}$，$\deg(q_i)<\deg(p)$ 并且

$$f(x)=\sum_{i=0}^{k}q_i(x)(p(x))^i.$$

证明. 如果 $\deg(f)<\deg(p)$，则直接取 $q_0=f$ 即得结论；否则，我们可以反复做带余除法

$$\begin{aligned}
&f=h_1p+q_0, && \deg(q_0)<\deg(p);\\
&h_1=h_2p+q_1, && \deg(q_1)<\deg(p);\\
&\cdots && \cdots\\
&h_{k-1}(x)=h_kp+q_{k-1}, && \deg(q_{k-1})<\deg(p);\\
&h_k=q_k, && \deg(h_k)<\deg(p).
\end{aligned}$$

算法终止是因为 $\deg(f)\geqslant\deg(h_1)+\deg(p)$，$\deg(h_1)\geqslant\deg(h_2)+\deg(p),\cdots\cdots$，于是进行到某一步必然有 $\deg(h_k)<\deg(p)$，即算法终止。

将上面的式子从下向上依次代入即得 $f(x)=\sum_{i=0}^{k}q_i(x)(p(x))^i$。 □

现在我们可以对真分式进行分解了。

定理 6.2.8. 有理函数域 $\mathbb{F}(x)$ 中的每个真分式都可以分解成一些分母不同的最简分式的和，而且和式中的最简分式由原来的真分式唯一确定 (即不计加法次序下该分解唯一)。

证明. 设 $\frac{f}{g}\in\mathbb{F}(x)$，$\deg(f)<\deg(g)$。显然我们可以将 $\mathrm{lc}(g)$ 放到分子上，即将 g 简化为首一多项式。下面我们分以下三步证明原命题。

(1) 如果 g 本身是不可约多项式的方幂，则直接进行第 (3) 步。反之，如果 $g(x)=g_1(x)g_2(x)$，其中 g_1,g_2 首一，互素且 $1\leqslant\deg(g_i)<\deg(g)$，$\forall i=1,2$，则存在 $u_1(x),v_1(x)\in\mathbb{F}[x]$ 使得 $u_1g_1+v_1g_2=1$，于是 $f(x)=u_1(x)g_1(x)f(x)+v_1(x)g_2(x)f(x)$，做带余除法

$$v_1(x)f(x)=u_2(x)g_1(x)+f_1(x),\quad \deg(f_1)<\deg(g_1)$$

再令 $f_2(x)=u_1(x)f(x)+u_2(x)g_2(x)$，则

$$\begin{aligned}f(x)&=u_1(x)g_1(x)f(x)+v_1(x)g_2(x)f(x)\\&=(u_1(x)f(x)+u_2(x)g_2(x))g_1(x)+f_1(x)g_2(x)\\&=f_2(x)g_1(x)+f_1(x)g_2(x)\end{aligned}$$

于是

$$\frac{f(x)}{g(x)}=\frac{f(x)}{g_1(x)g_2(x)}=\frac{f_2(x)}{g_2(x)}+\frac{f_1(x)}{g_1(x)}$$

此时，由于 $\deg(f)<\deg(g)=\deg(g_1)+\deg(g_2)$，利用 $f(x)=f_2(x)g_1(x)+f_1(x)g_2(x)$ 可得

$$\deg(f_2)+\deg(g_1)\leqslant\max\{\deg(f_2g_1),\deg(f_1g_2)\}=\deg(f)<\deg(g_1)+\deg(g_2)$$

即 $\deg(f_2)<\deg(g_2)$。这样我们就把 $\dfrac{f(x)}{g(x)}$ 分解成了两个真分式的和。

我们还需要证明 f_1,f_2 由 g_1,g_2 唯一确定。设另有 f_1',f_2' 也满足

$$\frac{f(x)}{g(x)}=\frac{f_2'(x)}{g_2(x)}+\frac{f_1'(x)}{g_1(x)},\quad \deg(f_1')<\deg(g_1),\ \deg(f_2')<\deg(g_2)$$

则

$$\frac{f_2'(x)}{g_2(x)}+\frac{f_1'(x)}{g_1(x)}=\frac{f(x)}{g_1(x)g_2(x)}=\frac{f_2(x)}{g_2(x)}+\frac{f_1(x)}{g_1(x)}$$

通分整理即有

$$(f_2'(x)-f_2(x))g_1(x)=(f_1(x)-f_1'(x))g_2(x)$$

又因为 $\gcd(g_1,g_2)=1$，所以 $g_1(x)\mid(f_1(x)-f_1'(x))$，然而由于

$$\deg(f_1-f_1')\leqslant\max(\deg(f_1),\deg(f_1'))<\deg(g_1)$$

所以只能是 $f_1-f_1'=0$，即 $f_1(x)=f_1'(x)$。同理 $f_2(x)=f_2'(x)$，即 f_1,f_2 由 g_1,g_2 唯一确定。

(2) 设 $g(x)$ 有素因子分解 $g(x)=(p_1(x))^{n_1}(p_2(x))^{n_2}\cdots(p_s(x))^{n_s}$，其中 $p_i(x),\ i=1,\dots,s$ 是两两不同的首一的不可约多项式。则由 (1)，对 s 归纳即可得到

$$\begin{aligned}\frac{f(x)}{g(x)}&=\frac{f_1(x)}{(p_1(x))^{n_1}}+\frac{h_1(x)}{(p_2(x))^{n_2}\cdots(p_s(x))^{n_s}}\\&=\frac{f_1(x)}{(p_1(x))^{n_1}}+\frac{f_2(x)}{(p_2(x))^{n_2}}+\frac{h_2(x)}{(p_3(x))^{n_3}\cdots(p_s(x))^{n_s}}\\&=\cdots\\&=\frac{f_1(x)}{(p_1(x))^{n_1}}+\frac{f_2(x)}{(p_2(x))^{n_2}}+\cdots+\frac{f_s(x)}{(p_s(x))^{n_s}}\end{aligned}$$

其中 $\deg(f_i)<\deg(p_i^{n_i})$。下面我们只需把形如 $\dfrac{f_i(x)}{(p_i(x))^{n_i}}$ 的分式分解成最简分式之和即可。

(3) 由引理6.2.4，对 (2) 中的每个 $f_i(x)$，存在唯一一组 $q_{0i}(x),q_{1i}(x),\dots,q_{n_i-1,i}(x)$ 使得 $f_i(x)=\sum_{j=0}^{n_i-1}q_{ji}(x)(p_i(x))^j$，其中 $\deg(q_{ji})<\deg(p_i),\ j=1,\dots,n_i-1$，于是

$$\frac{f_i(x)}{(p_i(x))^{n_i}}=\sum_{j=0}^{n_i-1}\frac{q_{ji}(x)}{(p_i(x))^{n_i-j}}.$$

所以

$$\frac{f(x)}{g(x)} = \sum_{i=1}^{s} \sum_{j=0}^{n_i-1} \frac{q_{ji}(x)}{(p_i(x))^{n_i-j}}.$$

上式右边的每一项都是最简分式，而且由 (1)(3) 两步的唯一性可知整个分解是唯一的。这样我们就完成了证明。 □

这个定理的证明过程实际上也给出了将真有理分式分解成最简分式的算法。此外，我们也可以用待定系数法来计算该分解，细节留给读者思考。准素分解在分析学中有很大的作用，它是计算有理函数的不定积分的重要工具。另外，由此出发我们可以建立起一套判定一个函数的积分是否是初等函数的理论 (类比 Galois 理论)，并由此得到 Γ 函数不是初等函数等有意义的结果。

6.3 多元多项式简介

6.3.1 定义与对称多项式

定义 6.3.1. 设 R 是交换环，$x_1,\dots,x_n$ 是未定元，则我们称 $R[x_1][x_2]\cdots[x_n]$ 是 R 上的 n 元多项式环，记作 $R[x_1,\dots,x_n]$。

注 6.3.1. 显然 $R[x_1,\dots,x_n]$ 是交换环。注意到 $R[x_1][x_2]$ 与 $R[x_2][x_1]$ 是同构的，因此 R 上的 n 元多项式环在同构意义下是唯一的。

定理 6.3.1. (1) 若 R 是整环，则 $R[x_1,\dots,x_n]$ 也是整环。
(2) 若 R 是唯一因子分解整环，则 $R[x_1,\dots,x_n]$ 也是唯一因子分解整环。

(1) 的证明是显然的，(2) 的证明我们放在习题课讲义中。

一个多元多项式可以整理成不同的形式。例如在 $\mathbb{Q}[x,y]$ 中

$$\begin{aligned} f &= (x^2+1)y^2+(x+1)y+x^5+2x \\ &= x^2y^2+y^2+xy+y+x^5+2x \\ &= x^5+y^2x^2+(y+2)x+y^2+y \end{aligned}$$

定义 6.3.2. 设 $R[x_1,\dots,x_n]$ 是交换环 R 上的 n 元多项式环，令

$$X_n=\left\{x_1^{i_1}\cdots x_n^{i_n}\mid i_1,\dots,i_n\in\mathbb{N}\right\}\subset R[x_1,\dots,x_n]$$

则我们称 X_n 中的元素为单项式 (monomial)。

与单变元多项式相比，定义多元多项式的次数更复杂一些。

定义 6.3.3. 设 $M=x_1^{i_1}\cdots x_n^{i_n}\in X_n$，我们称 $i_1+\cdots+i_n$ 为单项式 M 的全次数 (total degree)，记为 $\deg(M)$；相对应地我们称 i_k 为 M 关于变元 x_k 的次数，记作 $\deg_{x_k}(M)=i_k$。特别地，我们同样规定 $M\in R^*$ 的次数是 0，0_R 的次数是 $-\infty$。

显然，若 $M=x_1^{i_1}\cdots x_n^{i_n}$，$N=x_1^{j_1}\cdots x_n^{j_n}\in X_n$，则两个单项式的乘积 $MN=x_1^{i_1+j_1}\cdots x_n^{i_n+j_n}$，于是 $\deg(MN)=\deg(M)+\deg(N)$。

我们可以将多项式写成单项式的线性组合，即下面的命题。

命题 6.3.1. 设 $f\in R[x_1,\dots,x_n]\backslash\{0\}$，则存在唯一一组两两不同的 $\alpha_1,\dots,\alpha_k\in R$ 及 $M_1,\dots,M_k\in X_n$ 使得 $f=\sum_{i=1}^k\alpha_iM_i$。此时我们称 α_i，$i\in\{1,\dots,k\}$ 是 M_i 的系数，称 f 的这个形式为分布式 (distributive form)。

利用多元多项式的定义即可证明。

定义 6.3.4. 设 $f=\sum_{i=1}^k\alpha_iM_i$ 是分布式，则我们称 f 的全次数为 $\max\{\deg(M_1),\dots,\deg(M_k)\}$，记作 $\deg(f)$；称 f 关于变元 x_i 的次数为 $\max\{\deg_{x_i}(M_1),\dots,\deg_{x_i}(M_k)\}$。显然后者与将 f 视作关于 x_i 的单变元多项式时 x_i 的次数是一致的。

例如，设 $f=x^2y^2+y^2+xy+y+x^5+2x\in\mathbb{Q}[x,y]$，则 $\deg(f)=\deg_x(f)=5$，$\deg_y(f)=2$。

利用组合中的挡板法容易证明，X_n 中次数不超过 d 的单项式有 $\binom{n+d}{n}$ 个。

定义 6.3.5. 设 $h=\sum_{i=1}^k\alpha_iM_i\in R[x_1,\dots,x_n]$ 是分布式，如果 $\forall i\in\{1,\dots,k\}$，$\deg(M_1)=\deg(M_2)=\cdots=\deg(M_k)=d$，则我们称 h 是 d 次的齐次多项式 (homogeneous polynomial)。特别地，0 是任意次的齐次多项式。

于是，若 $f \in R[x_1,\dots,x_n]$，$\deg(f)=d$，则 f 可以唯一的写成 $f=h_d+\cdots+h_0$，其中 h_i 是 i 次的齐次多项式。

定理 6.3.2. 设 $p,q \in R[x_1,\dots,x_n]$，$\deg(p)=d$，$\deg(q)=e$，则 $\deg(p+q) \leqslant \max\{\deg(p),\deg(q)\}$，$\deg(pq) \leqslant \deg(p)+\deg(q)$。当 R 是整环时后者的等号成立。

类比于单变元多项式的赋值同态，我们有下面的定理。

定理 6.3.3. 设 R,S 是交换环，$\varphi: R \to S$ 是环同态，则对任意的 $s_1,\dots s_n \in S$，存在唯一的环同态 $\varphi_{s_1,\dots,s_n}: R[x_1,\dots,x_n] \to S$ 使得 $\varphi_{s_1,\dots,s_n}\big|_R = \varphi$ 并且 $\forall i \in \{1,\dots,n\}$，有 $\varphi_{s_1,\dots,s_n}(x_i)=s_i$。

利用单变元情形时的赋值同态定理及数学归纳法即可证明，细节留作练习，或者参考 Algebra, Thomas W. Hungerford, GTM73 的 Chapter III, Theorem5.5。

特别地，如果 $\mathbb{F}$ 是域，则恒等映射 $\mathrm{id}: \mathbb{F} \to \mathbb{F}$ 诱导了 $\mathbb{F}[x_1,\dots,x_n] \to \mathbb{F}$ 上的通常的赋值（“代入”操作)。于是，设 $f \in \mathbb{F}[x_1,\dots,x_n]$，$a_1,\dots,a_n \in \mathbb{F}$，如果 $f(a_1,\dots,a_n)=0$，则我们称 $(a_1,\dots,a_n)$ 是 f 在 $\mathbb{F}$ 上的一个零点。

下面我们讨论在变元的置换下多元多项式的变化。

例 6.3.1. 我们可以考虑嵌入 $\varphi: R \to R[x_1,\dots,x_n]$ 诱导的赋值同态。设 $\sigma \in S_n$，则由上面的定理可知，存在唯一的环同态 φ_σ 使得

$$\varphi_\sigma(x_i)=x_{\sigma(i)},\ \text{且}\varphi_\sigma\big|_R=\varphi$$

并且，容易证明 φ_σ 有逆映射 $\varphi_{\sigma^{-1}}$，且逆映射也是环同态。于是 φ_σ 是 $R[x_1,\dots,x_n]$ 上的自同构。

例如，在 $\mathbb{Q}[x_1,x_2,x_3]$ 上，取 $\sigma=(12)$，$f=x_1+2x_2^2-x_3$，则 $\varphi_\sigma(f)=x_2+2x_1^2-x_3$。

下面我们就可以定义对称多项式 (symmertric polynomial) 了。

定义 6.3.6. 设 $p \in R[x_1,\dots,x_n]$，如果对任意 $\sigma \in S_n$，都有 $\varphi_\sigma(p)=p$，则称 p 是关于 $x_1,\dots,x_n$ 的 n 元对称多项式。容易证明所有的 n 元对称多项式构成 $R[x_1,\dots,x_n]$ 的子环。

下面我们考虑一类特殊的对称多项式，它们被称为初等对称多项式。设 $p=(x_{n+1}-x_1)(x_{n+1}-x_2)\cdots(x_{n+1}-x_n) \in R[x_1,\dots,x_n,x_{n+1}]$，我们也可以将 p 视作关于 x_{n+1} 的单变元多项式，这样 p 的系数就落在 $R[x_1,\dots,x_n]$ 中，即

$$p=x_{n+1}^n-s_1x_{n+1}^{n-1}+\cdots+(-1)^{n-1}s_{n-1}x_{n+1}+(-1)^n s_n,\ \text{其中}s_1,\dots,s_n \in R[x_1,\dots,x_n].$$

直接展开计算可得

$$\begin{aligned}
&s_1=x_1+x_2+\cdots+x_n\\
&s_2=x_1x_2+x_1x_3+\cdots\cdots+x_{n-1}x_n\\
&\cdots\cdots\\
&s_k=\sum_{1\leqslant i_1<i_2<\cdots<i_k\leqslant n} x_{i_1}x_{i_2}\cdots x_{i_k}\\
&\cdots\cdots\\
&s_n=x_1x_2\cdots x_n.
\end{aligned} \tag{6.3.1}$$

容易验证上面的 s_k，$k=1,\dots,n$ 是 k 次的齐次对称多项式，称为 n 元 k 次初等对称多项式或基本对称多项式 (elementary symmertric polynomial)。利用上面的计算过程我们也可以得到单变元多项式根与系数的关系。

定理 6.3.4 (Vieta, 韦达定理). 设 $\mathbb{F}$ 是域，$f(x) = a_0 + \cdots + a_n x^n \in \mathbb{F}[x]$，并且 f 在域 $\mathbb{K} \supset \mathbb{F}$ 上有 n 个根 (计重数)$\alpha_1, \ldots, \alpha_n$(允许重复)，则

$$\frac{a_i}{a_n} = (-1)^{n-i} s_{n-i}(\alpha_1, \ldots, \alpha_n)$$

其中 $s_{n-i} \in \mathbb{F}[y_1, \ldots, y_n]$ 是 $n-i$ 次的 n 元 $n-i$ 次初等对称多项式。

在 $p = (x_{n+1} - x_1)(x_{n+1} - x_2) \cdots (x_{n+1} - x_n)$ 中取 $x_{n+1} = x$, $\forall i = 1, \ldots, n$, $x_i = \alpha_i$，展开 p 并与 f 对比系数即可。细节留作练习。

特别地，当 $\deg(f) = 2$ 时，上面的定理就回到了我们中学学过的情形。

设 $p \in \mathbb{Z}^+$ 是素数，我们考虑 $\mathbb{Z}_p[x]$ 中的多项式 $f = x^{p-1} - \overline{1}$。显然 $\deg f = p-1$ 并且 f 在 $\mathbb{Z}_p$ 上有 $p-1$ 个根 $\overline{1}, \overline{2}, \ldots, \overline{p-1}$，于是由韦达定理，$-\overline{1} = (-1)^{p-1} s_{p-1}(\overline{1}, \ldots, \overline{p-1})$，即 $\mathbb{Z}_p$ 中 $\overline{(p-1)!} = -\overline{1}$(分 $p = 2$ 和 $p \neq 2$ 讨论一下)，即 $(p-1)! + 1 \equiv 0 \mod p$。反之，如果 $p = p_1 p_2$, $1 < p_1, p_2 < p$，那么 $(p-1)! \equiv 0 \mod p_1$，于是 $(p-1)! + 1 \neq 0 \mod p_1$，即 $(p-1)! + 1 \neq 0 \mod p$。综上所述，我们有

定理 6.3.5 (Wilson). $p \in \mathbb{Z}^+$ 是素数 $\iff (p-1)! + 1 \equiv 0 \mod p$。

证明如前所述。

之所以我们把式 (6.3.1) 中的 s_k 称作“基本”对称多项式，是因为我们有下面的定理。

定理 6.3.6 (对称多项式基本定理). 设 R 是整环，$f(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$ 是对称多项式，则存在唯一的多项式 $g(y_1, \ldots, y_n) \in R[y_1, \ldots, y_n]$ 使得 $f(x_1, \ldots, x_n) = g(s_1, \ldots, s_n)$，其中 $s_1, \ldots, s_n$ 是 $R[x_1, \ldots, x_n]$ 上的初等对称多项式。而且，g 的系数是 f 系数的整数线性组合。

为了证明这个定理，我们首先介绍单项式的项序的概念。

定义 6.3.7. 设 X_n 是 $R[x_1, \ldots, x_n]$ 中所有单项式的集合，”$\preceq$”是 X_n 上的一个全序关系。如果”$\preceq$”还满足：

(1) $1 \preceq t$, $\forall t \in X_n$;

(2) 如果单项式 $m \preceq n$，那么 $\forall s \in X_n$，都有 $sm \preceq sn$。

那么我们称”$\preceq$”是 X_n 上的一个项序 (term order)。设 $s, t \in X_n$，我们把 $s \preceq t$ 且 $s \neq t$ 的情形记作 $s \prec t$。设 $f = \sum_{i=1}^{k} \alpha_i M_i \in R[x_1, \ldots, x_n]$ 是分布式，我们把 $\{\alpha_i M_i : i = 1, \ldots, k\}$ 在项序”$\preceq$”下的最大元 $\alpha_j M_j$ 称为 f 在该项序下的首项 (leading term)，记为 $\mathrm{LT(f)} = \alpha_{\mathrm{j}} \mathrm{M_j}$.

利用定义6.3.7的 (2) 很容易验证以下引理：

引理 6.3.1. 设 $f_1, \ldots, f_r \in R[x_1, \ldots, x_n]$，则 $\mathrm{LT(f_1 \cdots f_r)} = \mathrm{LT(f_1)} \cdots \mathrm{LT(f_r)}$。

证明留作练习。

一个典型的项序是如下所述的字典序：

定义 6.3.8. 我们把单项式简记成 $\mathbf{x}^\alpha = x_1^{a_1} \cdots x_n^{a_n}$, $\alpha = (a_1, \ldots, a_n)$ 的形式，设 $\mathbf{x}^\alpha, \mathbf{x}^\beta \in X_n$，在 X_n 上定义如下的全序关系：

$$\mathbf{x}^\alpha \prec \mathbf{x}^\beta \iff \beta - \alpha \text{的第 1 个非零分量为正.}$$

则容易验证这是一个项序，我们称其为 $x_1 \succ \cdots \succ x_n$ 的字典序 (Lexicographic order)。

定理6.3.6的证明. 首先，我们设 f 的全次数是 m，则 f 可以唯一地写成 $f = f_0 + f_1 + \cdots + f_m$ 的形式，其中 f_i 是 i 次齐次多项式。容易看出对称多项式的每个齐次部分也是对称的。那么，我们只需要证明每个齐次对称多项式都能写成初等对称多项式的多项式，即可证明原命题。于是我们不妨假设 f 是 m 次齐次对称多项式。

设 f 在字典序下的首项 $\mathrm{LT(f)} = \mathrm{a}x_1^{\mathrm{i_1}} \cdots x_n^{\mathrm{i_n}}$，则由于 f 是齐次对称多项式，我们有 $i_1 \geqslant i_2 \geqslant \cdots \geqslant i_n$。若不然，如果存在某个 $i_k < i_{k+1}$，$k \in \{1, \ldots, n-1\}$，则置换 x_k 和 x_{k+1} 可知单项式 $u = ax_1^{i_1} \cdots x_k^{i_{k+1}} x_{k+1}^{i_k} \cdots x_n^{i_n}$ 也是 f 中的项，而在字典序下 $\mathrm{LT(f)} \preceq \mathrm{u}$ 且 $\mathrm{LT(f)} \neq \mathrm{u}$，这显然是一个矛盾!

接下来我们构造命题中所要求的多项式 g。令

$$f_{(1)}(x_1, \ldots, x_n) = f(x_1, \ldots, , x_n) - as_1^{i_1 - i_2} s_2^{i_2 - i_3} \cdots s_{n-1}^{i_{n-1} - i_n} s_n^{i_n},$$

其中 $s_1, \ldots, s_n$ 是初等对称多项式。由引理6.3.1，注意到 $as_1^{i_1 - i_2} s_2^{i_2 - i_3} \cdots s_{n-1}^{i_{n-1} - i_n} s_n^{i_n}$ 在字典序下的首项是各个 s_i，$i = 1, \ldots, n$ 的乘积，即

$$\mathrm{LT}(\mathrm{as_1^{i_1 - i_2} s_2^{i_2 - i_3} \cdots s_{n-1}^{i_{n-1} - i_n} s_n^{i_n}}) = \mathrm{a} \cdot \mathrm{x_1^{i_1 - i_2}} \cdot (\mathrm{x_1 x_2})^{\mathrm{i_2 - i_3}} \cdots (\mathrm{x_1 \cdots x_{n-1}})^{\mathrm{i_{n-1} - i_n}} \cdot (\mathrm{x_1 \cdots x_n})^{\mathrm{i_n}} = \mathrm{LT(f)},$$

因此在字典序下只能是 $\mathrm{LT(f_{(1)})} \prec \mathrm{LT(f)}$，并且 $f_{(1)}$ 的系数一定形容 $c - q \cdot a$，c为 f 的系数，$q \in \mathbb{Z}$ 的形式 (因为 $s_1, \ldots, s_n$ 里的系数都是 1)。显然 $f_{(1)}$ 仍然是齐次对称多项式，设 $f_{(1)}$ 的首项是 $bx_1^{j_1} \cdots x_n^{j_n}$，对 $f_{(1)}$ 重复上述操作得到 $f_{(2)}$，

$$f_{(2)}(x_1, \ldots, x_n) = f_{(1)}(x_1, \ldots, , x_n) - bs_1^{j_1 - j_2} \cdots s_n^{j_n},$$

则 $f_{(2)}$ 仍满足 $\mathrm{LT(f_{(2)})} \prec \mathrm{LT(f_{(1)})}$，且 $f_{(2)}$ 的系数一定形容 $d - q \cdot b$，d为$f_{(1)}$的系数，$q \in \mathbb{Z}$ 的形式。这样重复有限步以后，由于项序的最小元是 1，我们必然会得到某个 $f_{(l)} = 0$。将上述过程相加我们就得到了所需要的 g:

$$g(s_1, \ldots, s_n) = as_1^{i_1 - i_2} s_2^{i_2 - i_3} \cdots s_{n-1}^{i_{n-1} - i_n} s_n^{i_n} + bs_1^{j_1 - j_2} \cdots s_n^{j_n} + \cdots,$$

且其系数是 f 系数的整数线性组合。

最后我们来说明 g 的唯一性。如果 $g_1(y_1, \ldots, y_n)$ 和 $g_2(y_1, \ldots, y_n)$ 同时满足

$$f(x_1, \ldots, x_n) = g_1(s_1, \ldots, s_n) = g_2(s_1, \ldots, s_n),$$

并且 $g_1(y_1, \ldots, y_n) - g_2(y_1, \ldots, y_n) \neq 0$(也就是说，$g_1, g_2$ 只是在代入 $s_1, \ldots, s_n$ 时相等，一般情形下可能不相等)，那么，任取 $g_1 - g_2$ 中的一个非零单项式 $ay_1^{k_1} \cdots y_n^{k_n}$，将 $s_1, \ldots, s_n$ 代入其中并求其字典序下的首项，可得:

$$\mathrm{LT}(\mathrm{as_1^{k_1} \cdots s_n^{k_n}}) = \mathrm{a} \cdot \mathrm{x_1^{k_1 + \cdots + k_n} x_2^{k_2 + \cdots + k_n} \cdots x_n^{k_n}} \neq 0.$$

从上式可以看出，如果 $g_1 - g_2$ 中的两个单项式 $M_1(y_1, \ldots, y_n) \neq M_2(y_1, \ldots, y_n)$，那么 $\mathrm{LT(M_1(s_1, \ldots, s_n))} \neq \mathrm{LT(M_2(s_1, \ldots, s_n))}$，而 $g_1(s_1, \ldots, s_n) - g_2(s_1, \ldots, s_n)$ 的首项是

$$\{\mathrm{LT(M(s_1, \ldots, s_n))} \mid \mathrm{M(y_1, \ldots, y_n)}\text{是}\mathrm{g_1 - g_2}\text{中的单项式}\}$$

中字典序下的最大者,因此 $\mathrm{LT}(g_1(s_1,\ldots,s_n)-g_2(s_1,\ldots,s_n))\neq 0$,这与 $g_1(s_1,\ldots,s_n)=g_2(s_1,\ldots,s_n)$ 矛盾！这样我们就完成了证明。 □

对称多项式基本定理说明，对称多项式一定是初等对称多项式的多项式，并且定理的证明过程实际上也是计算这种表达式的方法。在实际计算中，我们也常用待定系数法计算如何用初等对称多项式表出一般的对称多项式。我们看下面的例子。

例 6.3.2. 将对称多项式 $f=x_1^2x_2+x_1x_2^2+x_1^2x_3+x_1x_3^2+x_2^2x_3+x_2x_3^2$ 写成初等对称多项式的多项式。

解. (法一) f 在字典序 $x_1>x_2>x_3$ 的字典序下的首项是 $x_1^2x_2$，于是我们作

$$f_{(1)}=f-s_1s_2=f-(x_1+x_2+x_3)(x_1x_2+x_1x_3+x_2x_3)=-3x_1x_2x_3$$

而 $f_{(1)}+3s_3=0$，因此 $f=s_1s_2-3s_3$。

(法二) 由于 f 的全次数是 3,我们不妨设 $f=\sum_{k_1,k_2,k_3}a_{k_1,k_2,k_3}s_1^{k_1}s_2^{k_2}s_3^{k_3}$,则非负整数 k_1,k_2,k_3 都不超过 3，并且 $k_1+2k_2+3k_3=\deg(f)=3$，因此只能是

$$\begin{cases}k_1=3\\k_2=0\\k_3=0\end{cases}\quad\text{或}\quad\begin{cases}k_1=1\\k_1=0\\k_3=0\end{cases}\quad\text{或}\quad\begin{cases}k_1=0\\k_2=0\\k_3=1\end{cases},$$

即 f 用 s_1,s_2,S_3 表示时只能出现 s_1^3,s_1s_2,s_3 单项。设 $f=as_1^3+bs_1s_2+cs_3$，分别取 (x_1,x_2,x_3) 为 $(1,0,0)$, $(1,1,0)$, $(1,1,1)$ 代入上式得

$$\begin{cases}a=0\\2a+2b=2\\27a+9b+c=6\end{cases}$$

解得 $a=0,b=1,c=-3$，即 $f=3s_1s_2-3s_3$。 □

下面我们考虑一类特殊的对称多项式：幂和。我们称 $p_k(x_1,\ldots,x_n)=x_1^k+\cdots+x_n^k\in\mathbb{R}[x_1,\ldots,x_n]$ 为 k 次幂和，由对称多项式基本定理，p_k 一定可以用初等对称多项式 $s_1,\ldots,s_n$ 表出，那么，具体的表出形式是什么呢?

命题 6.3.2 (Newton 公式). p_k,s_k 记号的意义如上，则
(1) 如果 $1\leqslant k\leqslant n$，则 $p_k-p_{k-1}s_1+\cdots+(-1)^{k-1}p_1s_{k-1}+(-1)^kks_k=0$;
(2) 如果 $k>n$，则 $p_k-p_{k-1}s_1+\cdots+(-1)^{n-1}p_{k-n+1}s_{n-1}+(-1)^np_{k-n}s_n=0$。

证明. 用数学归纳法可以直接证明该定理。这里我们给出一个更巧妙的方法。

令 $\lambda(t)=(1+x_1t)(1+x_2t)\cdots(1+x_nt)$，对 $\lambda(t)$ 按 t 展开，则由初等对称多项式的定义(或韦达定理) 可知 $\lambda(t)=1+s_1t+\cdots+s_nt^n$，那么

$$\frac{\mathrm{d}\ln(\lambda(t))}{\mathrm{d}t}=\frac{s_1+2s_2t+\cdots+ns_nt^{n-1}}{1+s_1t+\cdots+s_nt^n}.\tag{6.3.2}$$

另一方面，对 $\ln(\lambda(t))$ 不展开直接求导可得

$$\frac{\mathrm{d}\ln(\lambda(t))}{\mathrm{d}t}=\frac{x_1}{1+x_1t}+\frac{x_2}{1+x_2t}+\cdots+\frac{x_n}{1+x_nt}.$$

利用习题课关于形式幂级数的结论 $(1+x)^{-1} = 1 - x + x^2 - \cdots + (-1)^k x^k + \cdots$ 可知

$$\begin{aligned}\frac{\mathrm{d}\ln(\lambda(t))}{\mathrm{d}t} &= x_1(1 - x_1 t + x_1^2 t^2 - \cdots) + x_2(1 - x_2 t + x_2^2 t^2 - \cdots) + \cdots + x_n(1 - x_n t + x_n^2 t^2 - \cdots) \\ &= p_1 - p_2 t + p_3 t^2 - \cdots + (-1)^k p_{k+1} t^k + \cdots\end{aligned} \tag{6.3.3}$$

对比式 (6.3.2) 和 (6.3.3) 可知

$$s_1 + 2s_2 t + \cdots + n s_n t^{n-1} = (1 + s_1 t + \cdots + s_n t^n)(p_1 - p_2 t + p_3 t^2 - \cdots + (-1)^k p_{k+1} t^k + \cdots)$$

展开上式右边并依次与左边对比 $t^i, i = 0, 1, \ldots, n-1, \cdots$ 的系数即可得到定理的结论。 □

6.3.2 判别式与结式

我们看到韦达定理是用对称多项式表示单变元多项式的根与系数的关系。那么，单变元多项式是否有重根这一问题应该如何判定呢？这就需要我们下面讨论的判别式 (discriminant)。

定义 6.3.9. 设 $\mathbb{F}$ 是域并且 $f = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{F}[x]$ 在 $\mathbb{F}$ 上有 n 个根 $x_1, \ldots, x_n$(计重数)，我们定义

$$D(f) = a_n^{2n-2} \prod_{1 \leqslant j < i \leqslant n} (x_i - x_j)^2$$

称 $D(f)$ 为多项式 f 的判别式。

之所以我们要这样定义判别式，首先基于这样的观察：f 有重根 $\iff D(f) = 0$。注意到 $D(f)$ 是关于 $x_1, \ldots, x_n$ 的对称多项式，因此它一定可以用初等对称多项式表出。$D(f)$ 前面的系数 a_n^{2n-2} 不是本质的，取这个系数的目的是和后面的结式对应起来。下面我们讨论如何将 $D(f)$ 用根的初等对称多项式表出，进而由韦达定理，将 $D(f)$ 用 f 的系数表出。

首先，注意到

$$\prod_{1 \leqslant j < i \leqslant n} (x_i - x_j) = \begin{vmatrix} 1 & 1 & 1 & \cdots & 1 \\ x_1 & x_2 & x_3 & \cdots & x_n \\ x_1^2 & x_2^2 & x_3^2 & \cdots & x_n^2 \\ \vdots & \vdots & \vdots & & \vdots \\ x_1^{n-1} & x_2^{n-1} & x_3^{n-1} & \cdots & x_n^{n-1} \end{vmatrix},$$

于是

$$
\begin{aligned}
D(f) &= a_n^{2n-2}\begin{vmatrix} 1 & 1 & 1 & \cdots & 1 \\ x_1 & x_2 & x_3 & \cdots & x_n \\ x_1^2 & x_2^2 & x_3^2 & \cdots & x_n^2 \\ \vdots & \vdots & \vdots & & \vdots \\ x_1^{n-1} & x_2^{n-1} & x_3^{n-1} & \cdots & x_n^{n-1} \end{vmatrix}^2 \\
&= a_n^{2n-2}\begin{vmatrix} 1 & 1 & 1 & \cdots & 1 \\ x_1 & x_2 & x_3 & \cdots & x_n \\ x_1^2 & x_2^2 & x_3^2 & \cdots & x_n^2 \\ \vdots & \vdots & \vdots & & \vdots \\ x_1^{n-1} & x_2^{n-1} & x_3^{n-1} & \cdots & x_n^{n-1} \end{vmatrix}\begin{vmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ 1 & x_3 & x_3^2 & \cdots & x_3^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{vmatrix} \\
&= a_n^{2n-2}\begin{vmatrix} n & p_1 & p_2 & \cdots & p_{n-1} \\ p_1 & p_2 & p_3 & \cdots & p_n \\ p_2 & p_3 & p_4 & \cdots & p_{n+1} \\ \vdots & \vdots & \vdots & & \vdots \\ p_{n-1} & p_n & p_{n+1} & \cdots & p_{2n-2} \end{vmatrix}
\end{aligned}
$$

由 Newton 公式，p_i 可以用 s_i(即 $(-1)^i\dfrac{a_{n-i}}{a_n}$) 表示出来，这样我们就可以用 f 的系数表示 $D(f)$ 了。当然在 $\deg(f)$ 比较小时，我们也可以直接用待定系数法计算。后面学完结式以后我们会有更简单的计算方法。

特别地，如果 $f = x^2 - bx + c \in \mathbb{C}[x]$ 在 $\mathbb{C}$ 上有根 x_1, x_2，则 $s_1(x_1, x_2) = b$，$s_2(x_1, x_2) = c$，而

$$
D(f) = \begin{vmatrix} 2 & p_1 \\ p_1 & p_2 \end{vmatrix} = \begin{vmatrix} 2 & s_1 \\ s_1 & s_1^2 - 2s_2 \end{vmatrix} = s_1^2 - 4s_2.
$$

即 $D(f) = b^2 - 4c$。这与我们中学时学过的一元二次方程的判别式是一致的。

下面我们来定义两个多项式的 Sylvester 结式，结式也是通过研究多项式的最大公因子得到的。

定义 6.3.10. 设 $\mathbb{F}$ 是域，$f = a_0 + a_1x + \cdots + a_nx^n$，$g = b_0 + b_1x + \cdots + b_mx^m \in \mathbb{F}[x]$，$a_n, b_m \neq 0$，我们称下面的行列式

$$
\begin{vmatrix}
a_n & a_{n-1} & \cdots & a_0 & & & \\
 & a_n & \cdots & a_1 & a_0 & & \\
 & & \ddots & & \ddots & \ddots & \\
 & & & a_n & \cdots & a_1 & a_0 \\
b_m & \cdots & b_0 & & & & \\
 & b_m & \cdots & b_0 & & & \\
 & & b_m & \cdots & b_0 & & \\
 & & & \ddots & & \ddots & \\
 & & & & b_m & \cdots & b_0
\end{vmatrix}
\begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\}\text{m 行} \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\}\text{n 行} \end{matrix}
\qquad (\text{空白部分为 } 0)
$$

为 f 和 g 的 Sylvester 结式 (Sylvester Resultant)，记作 $\mathrm{Res}_x(f,g)$ 或简记为 $\mathrm{Res}(f,g)$ (称对应的矩阵为 Sylvester 矩阵)。特别地，如果 $f=a_0\in\mathbb{F}$，则 $\mathrm{Res}(f,g)=a_0^m$；如果 $g=b_0\in\mathbb{F}$，则 $\mathrm{Res}(f,g)=b_0^n$；如果 f,g 都在 $\mathbb{F}\setminus\{0\}$ 中，则 $\mathrm{Res}(f,g)=1$，如果 $f=g=0$，则 $\mathrm{Res}(f,g)=0$。

引理 6.3.2. 设 $\mathbb{F}$ 是域，$f,g\in\mathbb{F}[x]\setminus\mathbb{F}$，则存在非零多项式 $u(x),v(x)\in\mathbb{F}[x]$ 使得 $uf+vg=\mathrm{Res}(f,g)$，并且 $\deg(u)<\deg(g)$，$\deg(v)<\deg(f)$。

证明. 对 f,g 的 Sylvester 矩阵 S 作如下的初等列变换：对 $i\in\{1,2,\dots,m+n-1\}$，将 S 的第 i 列乘以 x^{m+n-i} 后加到最后一列，得到矩阵 S'：

$$S'=\begin{pmatrix}
a_n & a_{n-1} & \cdots & a_0 & & & x^{m-1}f\\
 & a_n & \cdots & a_1 & a_0 & & x^{m-2}f\\
 & & \ddots & & \ddots & \ddots & \vdots\\
 & & & a_n & \cdots & a_1 & f\\
b_m & \cdots & b_0 & & & & x^{n-1}g\\
 & b_m & \cdots & b_0 & & & x^{n-2}g\\
 & & b_m & \cdots & b_0 & & x^{n-3}g\\
 & & & \ddots & & \ddots & \vdots\\
 & & & & b_m & \cdots & g
\end{pmatrix}$$

则 $\det(S')=\det(S)$。将 $\det(S')$ 按最后一列展开，再分别按含有 f 和 g 合并同类项，即得存在 $u,v\in\mathbb{F}[x]$ 使得 $\mathrm{Res}(f,g)=\det(S')=u(x)f(x)+v(x)g(x)$。而次数关系可以直接由行列式展开时最后一列关于 x 的次数得到。

下面我们证明 u,v 均不是 0。当 $\mathrm{Res}(f,g)\neq0$ 时结论显然。如果 $\mathrm{Res}(f,g)=0$，则我们不妨设 $u(x)=u_{m-1}x^{m-1}+\cdots+u_0$，$v(x)=v_{n-1}x^{n-1}+\cdots+v_0$，则将 $\mathrm{Res}(f,g)=\det(S')=u(x)f(x)+v(x)g(x)$ 的右边展开并对比系数可知 $u_{m-1},\dots,u_0,v_{m-1},\dots,v_0$ 满足

$$(u_{m-1},\dots,u_0,v_{m-1},\dots,v_0)\begin{pmatrix}
a_n & a_{n-1} & \cdots & a_0 & & & \\
 & a_n & \cdots & a_1 & a_0 & & \\
 & & \ddots & & \ddots & \ddots & \\
 & & & a_n & \cdots & a_1 & a_0\\
b_m & \cdots & b_0 & & & & \\
 & b_m & \cdots & b_0 & & & \\
 & & b_m & \cdots & b_0 & & \\
 & & & \ddots & & \ddots & \\
 & & & & b_m & \cdots & b_0
\end{pmatrix}=(0,\dots,0,0,\dots,0)$$

由 $\mathrm{Res}(f,g)=0$ 可知这个关于 $u_{m-1},\dots,u_0,v_{m-1},\dots,v_0$ 的方程组有非零解，即 u,v 均不为 0(注意此时 u,v 有一个是 0 即可得到 $u=v=0$)。这样我们就完成了证明。 □

定理 6.3.7. 设 $\mathbb{F}$ 是域，$f,g\in\mathbb{F}[x]$，则 $\mathrm{Res}(f,g)=0\iff f=g=0$ 或者 $\deg(\gcd(f,g))>0$。

证明. ($\Longleftarrow$) 用反证法。如果 $\mathrm{Res}(f,g)\neq0$，由上面的引理，必有 $\gcd(f,g)\mid\mathrm{Res}(f,g)$，而 $\mathrm{Res}(f,g)\in\mathbb{F}$ 是常数，故 $\gcd(f,g)$ 与 1 相伴，即 $\deg(\gcd(f,g))=0$，矛盾!
($\Longrightarrow$) 如果 $\mathrm{Res}(f,g)=0$，则 $f=g=0$ 的情形显然，下设 f,g 不同时为 0。不妨设 $f\neq0$，

则由上面的引理，$\exists u(x), v(x) \in \mathbb{F}[x]$ 使得 $u(x)f(x) = -v(x)g(x)$，如果 $\deg(\gcd(f,g)) = 0$，即 f 和 g 互素，那么 $f(x) \mid v(x)$，这与 $\deg(v) < \deg(f)$ 矛盾！ □

下面我们考虑结式和判别式之间的联系。为此我们需要下面的命题。

命题 6.3.3. 设 $\mathbb{F}$ 是域，$f, g \in \mathbb{F}[x]$ 并且在 $\mathbb{F}[x]$ 中可以分解成一次因子的乘积：

$$f(x) = a_n(x-\alpha_1)\cdots(x-\alpha_n)$$
$$g(x) = b_m(x-\beta_1)\cdots(x-\beta_m)$$

那么

$$\operatorname{Res}(f,g) = a_n^m \prod_{i=1}^{n} g(\alpha_i) = b_m^n \prod_{j=1}^{m} f(\beta_j) = a_n^m b_m^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j).$$

证明. 首先，由结式的定义容易验证 $\operatorname{Res}(f,g) = (-1)^{mn}\operatorname{Res}(g,f)$，因此我们只需证明 $\operatorname{Res}(f,g) = a_n^m \prod_{i=1}^{n} g(\alpha_i)$ 即可。引入一个新的参变元 y，考虑 $\operatorname{Res}_x(f, g-y)$（即将 g 的常数项 b_0 换成 $b_0 - y$）。由结式的定义可知 $\operatorname{Res}_x(f,g-y)$ 是一个关于 y 的 n 次多项式，并且其关于 y 的常数项恰为 $\operatorname{Res}(f,g)$。注意到 $\operatorname{Res}_x(f,g-y)$ 关于 y^n 的系数为 $(-1)^n a_n^m$，即

$$\operatorname{Res}_x(f,g-y) = (-1)^n a_n^m y^n + \cdots + \operatorname{Res}(f,g)$$

由于 $\forall i \in \{1,\ldots,n\}$，$f(\alpha_i) = g(\alpha_i) - g(\alpha_i) = 0$，即 $x-\alpha_i \mid f$，$x-\alpha_i \mid g(x) - g(\alpha_i)$，所以

$$\operatorname{Res}_x(f(x), g(x) - g(\alpha_i)) = 0.$$

那么反过来，关于 y 的多项式 $\operatorname{Res}_x(f,g-y)$ 有根 $y = g(\alpha_i)$，即 $\forall i \in \{1,\ldots,n\}$，$g(\alpha_i) - y \mid \operatorname{Res}_x(f,g-y)$。于是取遍 $i = 1,\ldots,n$ 并对比首项系数和次数就有

$$\operatorname{Res}_x(f,g-y) = a_n^m \prod_{i=1}^{n}(g(\alpha_i) - y)$$

在上式中令 $y = 0$，即得 $\operatorname{Res}(f,g) = a_n^m \prod_{i=1}^{n} g(\alpha_i)$。这样我们就完成了证明。 □

命题 6.3.4. 设 $f \in \mathbb{F}[x]$，$\deg(f) = n$，$\operatorname{lc}(f) = a_n$，则

$$D(f) = (-1)^{\frac{n(n-1)}{2}} a_n^{-1} \operatorname{Res}(f, f').$$

证明. 不妨设 f 在 $\mathbb{F}$ 上恰有 n 个根 $\alpha_1,\ldots,\alpha_n$（计重数）[1]，由上面的命题立刻有

$$\operatorname{Res}(f,f') = a_n^{n-1} \prod_{i=1}^{n} f'(\alpha_i).$$

对 $f = a_n(x-\alpha_1)\cdots(x-\alpha_n)$ 求导数得

$$f'(x) = a_n \sum_{i=1}^{n} \prod_{j\neq i}(x-\alpha_j).$$

[1] 任何一个域的代数闭包都存在，我们会在抽象代数课程中证明这一点。

以 $x=\alpha_i$ 代入上式得

$$f'(\alpha_i)=a_n\prod_{j\neq i}(\alpha_i-\alpha_j).$$

于是

$$\begin{aligned}\mathrm{Res}(f,f')&=a_n^{2n-1}\prod_{i=1}^{n}\prod_{j\neq i}(\alpha_i-\alpha_j)\\&=a_n^{-1}(-1)^{\frac{n(n-1)}{2}}a_n^{2n-2}\prod_{j<i}(\alpha_i-\alpha_j)^2\\&=a_n^{-1}(-1)^{\frac{n(n-1)}{2}}D(f).\end{aligned}$$

这样我们就完成了证明。 □

例 6.3.3. 分别计算 $\mathbb{Q}[x]$ 中多项式 $f(x)=x^2+bx+c$ 和 $g(x)=x^3+px+q$ 的判别式。

解. (1)$D(f)=-\mathrm{Res}(f,f')=\begin{vmatrix}1&b&c\\2&b&0\\0&2&b\end{vmatrix}=b^2-4c;$

(2)$D(g)=-\mathrm{Res}(g,g')=\begin{vmatrix}1&0&p&q&\\&1&0&p&q\\3&0&p&&\\&3&0&p&\\&&3&0&p\end{vmatrix}=-4p^3-27q^2.$ □

最后我们证明下面的结论。

命题 6.3.5. f,g 的条件同定义6.3.10，则 $\mathrm{Res}(f,g)$ 是关于 $a_n,\dots,a_0,b_m,\dots,b_0$ 的不可约多项式 (将系数视作符号)。

证明. 用反证法。容易验证 $\mathrm{Res}(f,g)$ 分别是关于 f,g 的根 $\alpha_1,\dots,\alpha_n$ 和 $\beta_1,\dots,\beta_m$ 的对称多项式，若其可约，则可设 $\mathrm{Res}(f,g)=AB$，其中 A,B 都是关于 $\alpha_1,\dots,\alpha_n$ 和 $\beta_1,\dots,\beta_m$ 的正次数对称多项式 (思考之)。由命题6.3.3，$\alpha_1-\beta_1\mid\mathrm{Res}(f,g)$，则 $\alpha_1-\beta_1\mid AB$，不妨设 $\alpha_1-\beta_1\mid A$，则由 A 是对称多项式，可知 $\forall i,j$，有 $\alpha_i-\beta_j\mid A$，于是 $\prod_{i,j}(\alpha_i-\beta_j)\mid A$。这说明 $B\mid a_n^m b_m^n$，于是 $B=\lambda a_n^p b_m^q$，$0\leqslant p\leqslant m$，$0\leqslant q\leqslant n$，$\lambda\neq 0$。但容易验证 $a_n\nmid\mathrm{Res}(f,g)$，$b_m\nmid\mathrm{Res}(f,g)$，于是 $p=q=0$，这与 B 是正次数的相矛盾! □

有关结式的更多内容,可以参考 Using Algebraic Geometry, David A.Cox, e.t.c., GTM185 的 Chapter 3。

6.4 实根隔离与近似求根简介

6.4.1 实根隔离

这一小节我们简单地讨论一下实系数多项式 $f(x)$ 在闭区间 $[a,b]$ 内有多少个根的问题。

我们首先需要有限实数序列的变号数这一概念。设一个有限的实数序列为 $S=\{c_1,\ldots,c_m\}$，记 V_S 为使 $c_ic_{i+1}<0,\ i\in 1,\ldots,m-1$ 的 i 的个数，并称 V_S 为序列 S 的变号数。如果序列 S 中含有 0，则 S 的变号数等于将 S 中的 0 都去掉后所得序列的变号数。例如，序列 $\{1,0,-1,1,-1\}$ 的变号数为 3。

下面我们回到本节一开始的问题。不失一般性，我们可以设 $f\in\mathbb{R}[x]$ 是无平方的 (否则取 f 的无平方部分即可)。我们直接给出以下定义。

定义 6.4.1. 给定非零实系数多项式 $f(x)$ 和闭区间 $[a,b]$，称多项式序列

$$f_0(x)=f(x),f_1(x),\cdots,f_s(x)$$

是多项式 $f(x)$ 在闭区间 $[a,b]$ 上的 Sturm 序列，如果这些多项式都是实系数多项式且以下条件成立:

(1) 最后一个多项式 $f_s(x)$ 在 $[a,b]$ 上没有根;

(2) $f(a)f(b)\neq 0$;

(3) 对 $c\in[a,b]$ 和 $1\leqslant k\leqslant s-1$，若 $f_k(c)=0$，则 $f_{k-1}(c)f_{k+1}(c)<0$;

(4) 对 $c\in[a,b]$，若 $f(c)=0$，则 $(f_0(x)f_1(x))'\big|_{x=c}>0$。

由条件 (3) 知 Sturm 序列中相邻的多项式在 $[a,b]$ 上没有公共根。对 $c\in[a,b]$，序列 $f_0(c),f_1(c),\cdots,f_s(c)$ 的变号数记作 V_c 或 $V_c(f)$，即

$$V_c=V_c(f)=V(\{f_0(c),f_1(c),\ldots,f_s(c)\}).$$

我们有以下定理。

定理 6.4.1 (Sturm). 设 $f_0=f,f_1,\ldots,f_s$ 是正次数多项式 $f(x)\in\mathbb{R}[x]$ 在闭区间 $[a,b]$ 上的一个 Sturm 序列，则 f 在开区间 (a,b) 内的不同实根的个数 (不计重数) 为 Sturm 序列在 a,b 两点处的变号数之差，即 V_a-V_b。

证明从略。

那么，Sturm 序列具体应该如何构造呢? 可以证明 (过程从略) 以下的序列 $f_0(x)=f(x),f_1(x),\ldots,f_s(x)$ 是 Sturm 序列:

$$\begin{aligned}
f_0(x)&=f(x)\\
f_1(x)&=f'(x)\\
f_2(x)&=-\mathrm{rem}(f_0,f_1)\\
f_3(x)&=-\mathrm{rem}(f_1,f_2)\\
&\cdots\cdots\\
f_s(x)&=-\mathrm{rem}(f_{s-2},f_{s-1})\neq 0\\
&\quad(\mathrm{rem}(f_{s-1},f_s)=0)
\end{aligned}$$

以上的序列称为标准 Sturm 序列。

例 6.4.1. 设 $f(x)=x^4-2x^2-3x+3$，求 f 的实根个数。

解. f 在闭区间 $[-M,M](M>0$ 充分大) 上的标准 Sturm 序列为

$$\begin{aligned} f_0 &= f \\ f_1 &= 4x^3-4x-3 \\ f_2 &= x^2+\frac{9}{4}x-3 \\ f_3 &= -\frac{113}{4}x+30 \\ f_4 &= -\frac{6603}{113^2} \end{aligned}$$

于是 Sturm 序列在 $x=-M,\ x=M$ 处的符号如下表:

	f_0	f_1	f_2	f_3	f_4
$x=-M$	+	-	+	+	-
$x=M$	+	+	+	-	-

从而 $V_{-M}=3,\ V_M=1$，于是 f 只有两个不同的实根。 □

我们还有以下的结论。

定理 6.4.2 (Descartes). 设 $f\in\mathbb{R}[x]$，则 f 的正根个数 (计重数) 不超过其系数序列的变号数，且两者有相同的奇偶性。如果 f 没有虚根，则两者相等。

证明从略。

6.4.2 根的近似求解

我们中学时就已经接触过用二分法近似地求解一个多项式的根，在数学分析课程中又证明了其收敛性。那么，是否有更快速的近似解算法呢? 本小节介绍的牛顿法就是一个更快的算法。

如果我们已知多项式 f 在 $x=c$ 附近有根，那么，我们令

$$c_0=c,\ c_{k+1}=c_k-\frac{f(c_k)}{f'(c_k)},\ k=0,1,2,\dots$$

如果序列 $\{c_k\}$ 收敛到 a，则 $f(a)=0$。因此我们可以通过以上的迭代公式，计算某个 $c_n(n$ 足够大) 使得 $|c_n-a|$ 满足我们所需要的精度要求，即我们把 c_n 当作 $f(x)=0$ 的近似解。这种做法称为牛顿迭代法，其几何意义是不断作函数的切线与 x 轴的交点会越来越接近函数的零点。需要注意的是牛顿迭代并不总是收敛的，关于牛顿法的收敛性判别与收敛速度的分析，读者可以在一般的数值分析教材中找到。

6.5 代数基本定理

定理 6.5.1 (代数基本定理). *任何正次数的复系数多项式都至少有一个复数根。*

证明从略。代数基本定理至今尚没有纯代数的证明，最简单的证明是利用复分析中的刘维尔定理 (有界整函数必为常数) 给出的，《代数学引论》给出的则是一个常见的应用代数知识稍多的证明。

推论 6.5.1. *设 $f \in \mathbb{C}[x]$，$\deg(f) = n > 0$，则 f 在 $\mathbb{C}$ 上有且只有 n 个根 (计重数)。*

对 n 归纳即可证明。

下面我们列举一些关于实系数多项式的结论，利用代数基本定理可以很快证明它们。

定理 6.5.2. *设 $f \in \mathbb{R}[x]$，$c \in \mathbb{C}$ 是 f 的根，则 $\overline{c}$ 也是 f 的根，并且 $\overline{c}$ 的重数与 c 的重数相同。*

证明. 设 $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{R}[x]$，由 c 是 f 的根可知 $a_n c^n + \cdots + a_1 c + a_0 = 0$，于是

$$\begin{aligned} 0 = \overline{f(c)} &= \overline{a_n c^n} + \cdots + \overline{a_1 c} + \overline{a_0} \\ &= a_n(\overline{c})^n + \cdots + a_1\overline{c} + a_0 \quad \text{(利用了} a_i = \overline{a_i},\ i \in \{0,\ldots,n\}.\text{)} \\ &= f(\overline{c}), \end{aligned}$$

即 $\overline{c}$ 也是 f 的根。类似地，可以证明 $f^{(k)}(c) = 0 \iff f^{(k)}(\overline{c}) = 0$，即 c 与 $\overline{c}$ 具有相同的重数。 □

推论 6.5.2. (1) *实系数不可约多项式的次数不超过 2；*
(2) *设 $f \in \mathbb{R}[x]$，$\deg(f) = 2$，则 f 在 $\mathbb{R}[x]$ 中不可约 $\iff D(f) < 0$。*
(3) *$\mathbb{R}[x]$ 中的每个正次数多项式都可以分解成一些一次和二次实系数多项式的乘积。*

证明. (1) 设 f 是 $\mathbb{R}[x]$ 中次数大于 1 的不可约多项式，则 f 没有实根 (否则它有一次的因子)。由代数基本定理，不妨设 c 是 f 的一个虚根，由定理6.5.2，$\overline{c}$ 也是 f 的根，那么

$$(x-c)(x-\overline{c}) = x^2 - (c+\overline{c})x + c\overline{c} \mid f(x).$$

注意到 $c+\overline{c}$ 和 $c\overline{c}$ 都是实数，而 f 不可约，因此只能是 f 和 $(x-c)(x-\overline{c})$ 相伴，即 $\deg(f) = 2$，此即 (1) 成立。
(2) 不妨设 f 是首一多项式，则 f 不可约 $\iff$ f 没有实根，由代数基本定理及定理6.5.2可知 f 有两个共轭的虚根 $c, \overline{c}$，不妨设 $f(x) = a(x-c)(x-\overline{c})$，$c = u + v\mathrm{i}$，$\mathrm{a}, \mathrm{u}, \mathrm{v} \in \mathbb{R}$，那么其判别式 $D(f) = a^2(c-\overline{c})^2 = -4a^2v^2 < 0$；反之 $D(f) < 0$ 可知 f 的两个根是共轭虚根。此即 (2) 成立。
(3) 这是 (1) 和 (2) 的直接推论。 □

多项式是线性代数和抽象代数的重要研究对象，也是数学各个领域最基础和最通用的工具之一。我们不在这里推荐相关的进阶参考书，读者可以根据自己的需求来了解不同方向的进阶内容。

6.6 习题

单变元多项式

1. 验证命题6.1.1中定义的 $\widetilde{R}$ 确实是一个交换幺环, 并证明命题6.1.1.

2. 验证命题6.1.2.

3. 验证引理6.1.1.

4. 验证关于域上多项式环 $\mathbb{F}[x]$ 的辗转相除法的正确性.

5. 对哪些正整数 n, 在多项式环 $\mathbb{Z}_n[x]$ 中, x^2+x+1 整除 $x^4+3x^3+x^2+7x+5$?

6. 设 R 是含幺的交换环, 加法零元和乘法幺元分别记作 $0_R, 1_R$. 命 $R[[x]]$ 为所有映射 $f:\mathbb{N}\to R$ 形成的集合. 定义这些映射间的加法和乘法为

$$(f+g)(k)=f(k)+g(k),\quad (fg)(k)=\sum_{\substack{i+j=k\\ i,j\in\mathbb{N}}} f(i)g(j).$$

   证明: $R[[x]]$ 连同这些运算成为一个带 $\mathbf{1}$ 的交换结合环, 称为 R 上的形式幂级数环, 乘法单位元 $\mathbf{1}$ 是如下映射 $\mathbf{1}(k)=\begin{cases}1_R, & k=0;\\ 0_R, & k\neq 0.\end{cases}$.

7. 记号同第 6 题. 命 $x\in R[[x]]$ 为映射 $x(k)=\begin{cases}1_R, & k=1;\\ 0_R, & k\neq 1.\end{cases}$. 定义 $r\in R$ 与映射 x 的乘法为: $(rx)(k)=r\cdot(x(k))$. 那么

   (1) 验证: x^i(映射 x 按照第6题的规则自乘 i 次) 满足: $x^i(k)=\begin{cases}1_R, & k=i;\\ 0_R, & k\neq i.\end{cases}$. 从而 $R[[x]]$ 中的任意元素 f 有下面的形式

$$f=f(0)\mathbf{1}+f(1)x+f(2)x^2+f(3)x^3+\cdots.$$

   (2) $R[x]$ 是 $R[[x]]$ 的子环.
   (3) 确定 $R[[x]]$ 中的可逆元.

8. 记号同第 6 题. 对非零元 $f\in R[[x]]$, 定义 $\omega(f)$ 为最小的非负整数 k 使得 $f(k)\neq 0_R$. 约定 $\omega(\mathbf{0})=-\infty$. 证明
   (1) $\omega(f+g)\geqslant\min\{\omega(f),\omega(g)\}$.
   (2) $\omega(fg)\geqslant\omega(f)+\omega(g)$.
   (3) 如果 R 是整环, 则 $\omega(fg)=\omega(f)+\omega(g)$. 从而此时 $R[[x]]$ 是整环.

9. 确定 $\mathbb{Z}[x]$ 的所有环自同构.

10. 证明: 多项式 $f\in R[x_1,\cdots,x_n]$ 是 m 次齐次多项式当且仅当对任意的 $t\in R[x_1,\cdots,x_n]$ 有

$$f(tx_1,\cdots,tx_n)=t^m f(x_1,\cdots,x_n).$$

多项式的因式分解

1. 证明 $\mathbb{Z}$ 中每个非零整数都有有限的不可约分解.

2. 证明推论6.2.6.

3. 在 $\mathbb{Z}_p[x]$ 中找出下列多项式的素因子分解.
   (1) $x^3+x^2+x+1, p=2$;
   (2) $x^2-3x-3, p=5$;
   (3) $x^2+1, p=7$.

4. 在 $\mathbb{Q}[x]$ 中求出 $x^6+x^4+x^3+x^2+x+1$ 和 $x^5+2x^3+x^2+x+1$ 的最大公因子.

5. 多项式 x^2-2 在 $\mathbb{Z}_8$ 中有多少个根?

6. 证明: 素数 p 是 $\mathbb{Z}[\sqrt{-3}]$ 中的素元当且仅当 x^2+3 在 $\mathbb{Z}_p[x]$ 是不可约的.

7. 设
$$f(x,y)=a_0x^n+a_1x^{n-1}y+\cdots+a_{n-1}xy^{n-1}+a_ny^n\in\mathbb{Q}[x,y]$$
   是齐次多项式. 证明:
   (1) $f(x,y)$ 的不可约因子也是齐次的.
   (2) $f(x,y)$ 是不可约的当且仅当 $f(x,1)=a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n\in\mathbb{Q}[x]$ 是不可约的.

8. 设 F 是域. 确定形式幂级数环 $F[[x]]$ 的素元并证明这个环是唯一因子分解环.

9. 设 $x_{ij}, 1\leqslant i,j\leqslant n$ 是未知元. 证明 $\det\left(x_{ij}\right)\in F\left[x_{11},x_{12},\cdots,x_{nn}\right]$ 是不可约的 (提示: 每个 x_{ij} 在 $\det\left(x_{ij}\right)$ 的单项中的幂至多为 1).

10. 证明下列多项式在 $\mathbb{Q}[x]$ 中是不可约的.
    (1) $x^5-12x^3+36x-12$;
    (2) $x^{105}-9$;
    (3) $(x-a_1)(x-a_2)\cdots(x-a_n)-1$, 其中 $a_1,a_2,\cdots,a_n$ 是整数.

11. 确定多项式 $f(x)$ 在根 c 处的重数:
    (1) $f(x)=x^5-5x^4+7x^3-2x^2+4x-8, c=2$;
    (2) $f(x)=3x^5+2x^4+x^3-10x-8, c=-1$.

12. 求出下列多项式的有理根:
    (1) $x^3-6x^2+15x-14$;
    (2) $24x^4-42x^3-77x^2+56x+60$.

13. 多项式 x^5-ax^2-ax+1 在 a 取何值时以 -1 为一个根, 且重数至少是 2 ?

14. 证明 1 是以下多项式的三重根:
    (1) $x^{2n}-nx^{n+1}+nx^{n-1}-1$;
    (2) $(n-2m)x^n-nx^{n-m}+nx^m-(n-2m)$.

15. 证明多项式
$$1+x+\frac{x^2}{2!}+\cdots+\frac{x^n}{n!}$$
    没有重根.

16. 证明多项式

$$a_1x^{n_1}+a_2x^{n_2}+\cdots+a_kx^{n_k}\quad(n_1<n_2<\cdots<n_k)$$

的非零根的重数不超过 $k-1$.

17. 考虑递归方程

$$u(n+k)=a_0u(n)+a_1u(n+1)+\cdots+a_{k-1}u(n+k-1),\quad k\neq 0,a_0\neq 0.$$

令 $f(x)=x^k-a_{k-1}x^{k-1}-\cdots-a_0$. 证明:

(1) 函数 $u(n)=n^rc^n, r\geqslant 0, c\neq 0$ 是递归方程的解当且仅当 c 是 $f(x)$ 的根, 重数不小于 $r+1$;

(2) 如果 $c_1,\cdots,c_m$ 是 $f(x)$ 的所有的根, 重数分别是 $s_1,\cdots,s_m$, 那么, 递归方程的任何解都有如下形式

$$u(n)=\sum_{i=1}^{m}g_i(n)c_i^n,$$

其中 $g_i(x)(i=1,\cdots,m)$ 是次数不超过 s_i-1 的多项式.

18. 如果 f 是域 K 上的不可约多项式, $\operatorname{char}K=0$, 那么 $\gcd(f,f')=1$, 其中 f' 是 f 的导数.

19. 假设域 K 上的多项式 f 的导数为 0 . 证明:

(1) 如果 $\operatorname{char}K=0$, 则 f 为常数;

(2) 如果 $\operatorname{char}K=p>0$, 则 $f(x)=g(x^p)$, 其中 g 是某个多项式.

20. 假设一个次数小于 n 的多项式在 n 个连续的整数点上取值整数. 证明: 这个多项式在所有的整数点上取整数值. 这个多项式的系数是否都是整数?

21. 设 F 是有限域, 含 q 个元素. 证明: 任何映射 $f:F\to F$ 都可以唯一地表成一个次数小于 q 的多项式函数.

22. 设 R 是唯一因子分解环. 证明: $R[x]$ 是唯一因子分解环.

23. 把下列分式写成最简分式之和.

(1) $\dfrac{x^2}{(x-1)(x+2)(x+3)}$;

(2) $\dfrac{x}{(x^2-1)^2}$.

多元多项式

1. 验证6.3.1.

2. 证明6.3.1.

3. 证明定理6.3.3和6.3.4.

4. 验证引理6.3.1.

5. 计算如下多项式的所有根的平方和及所有根的乘积:

(1) $3x^3+2x^2-3x-5$;

(2) x^4+x^2-2x+3.

6. 计算如下多项式的所有根的倒数的和:
   (1) $5x^3+2x^2-3$;
   (2) x^4-2x^2-3x+1.

7. 已知多项式 $x^3-7x+\lambda$ 有两个根的比值是 2 , 求 λ.

8. 把下面的对称多项式写成初等对称多项式的代数表达式:
   (1) $(x_1x_2+x_3x_4)(x_1x_3+x_2x_4)(x_1x_4+x_2x_3)$;
   (2) $(x_1+x_2-x_3-x_4)(x_1-x_2+x_3-x_4)(x_1-x_2-x_3+x_4)$;
   (3) $(2x_1-x_2-x_3)(2x_2-x_1-x_3)(2x_3-x_1-x_2)$;

9. 设 K 是无限域, $f\in K[x_1,\cdots,x_n]$ 是非零多项式. 利用定理6.2.3并对 n 作归纳法证明: 存在 $a_1,\cdots,a_n\in K$ 使得 $f(a_1,\cdots,a_n)\neq 0$. 于是 $K[x_1,\cdots,x_n]$ 和域 K 上的 n 个变量的多项式函数环同构.

10. 证明:
    (1) 每个变元的次数皆小于 p 的非零多项式 $f\in\mathbb{Z}_p[X_1,\cdots,X_n]$ 具有上面的习题9 所述的性质: 存在 $a_1,\cdots,a_n\in P$, 使 $f(a_1,\cdots,a_n)\neq 0$.
    (2) 任意多项式 $f\in\mathbb{Z}_p[X_1,\cdots,X_n]$ 可表示为形式

$$f(X_1,\cdots,X_n)=\sum_{i=1}^{n}g_i(X_1,\cdots,X_n)\left(X_i^p-X_i\right)+f^*(X_1,\cdots,X_n),$$

    其中 f^* 是一个约化多项式 $\left(\deg_{X_i}f^*\leqslant p-1,i=1,2,\cdots n\right)$, 它的全次数 $\deg f^*\leqslant\deg f$. 由此断定, 从多项式环 $\mathbb{Z}_p[X_1,\cdots,X_n]$ 到 $\mathbb{Z}_p$ 上的 n 变元多项式函数环的映射 $f\mapsto\tilde{f}=\tilde{f^*}$ 是一个满射, 其核为 $L=\sum_{i=1}^{n}\left(X_i^p-X_i\right)\mathbb{Z}_p[X_1,\cdots,X_n]$.

11. (Chevalley) 设 $f(X_1,\cdots,X_n)$ 是域 $\mathbb{Z}_p$ 上的 r 次齐次多项式 $(r<n)$. 证明方程 $f(X_1,\cdots,X_n)=0$ 至少有一个非平凡解.

    提示: 因为 f 是齐次的, 显然有 $f(0,\cdots,0)=0$. 用反证法假设 $(a_1,\cdots,a_n)\neq 0\Rightarrow f(a_1,\cdots,a_n)\neq 0$. 根据上题和费马小定理, $g(X_1,\cdots,X_n)=1-f(X_1,\cdots,X_n)^{p-1}$ 的约化多项式为 $g^*(X_1,\cdots,X_n)=\left(1-X_1^{p-1}\right)\cdots\left(1-X_n^{p-1}\right)$. 但是

$$\deg g=(p-1)\deg f=(p-1)r<(p-1)n=\deg g^*.$$

    得到矛盾, 定理得证.

    对论述稍加修改, 证明更一般的结论: 方程 $f(X_1,\cdots,X_n)=0$ 的解的个数可以被 p 整除, (用两种方法计算和式 $\sum_{x_1,\cdots,x_n\in\mathbb{Z}_p}g(X_1,\cdots,X_n)$).

12. 利用牛顿公式和克拉默公式证明:

$$p_k=\begin{vmatrix} s_1 & 1 & 0 & 0 & \cdots & 0\\ 2s_2 & s_1 & 1 & 0 & \cdots & 0\\ 3s_3 & s_2 & s_1 & 1 & \cdots & 0\\ \vdots & \vdots & \vdots & \vdots & & \vdots\\ (k-1)s_{k-1} & s_{k-2} & s_{k-3} & s_{k-4} & \cdots & 1\\ ks_k & s_{k-1} & s_{k-2} & s_{k-3} & \cdots & s_1 \end{vmatrix},$$

$$s_k = \frac{1}{k!}\begin{vmatrix} p_1 & 1 & 0 & 0 & \cdots & 0 \\ p_2 & p_1 & 1 & 0 & \cdots & 0 \\ p_3 & p_2 & p_1 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ p_{k-1} & p_{k-2} & p_{k-3} & p_{k-4} & \cdots & 1 \\ p_k & p_{k-1} & p_{k-2} & p_{k-3} & \cdots & p_1 \end{vmatrix}.$$

13. 假设域 K 的特征不等于 2. 称多项式 $f \in K[x_1, \cdots, x_n]$ 为斜对称的 (或交错的) 如果

$$f(x_{\pi(1)}, \cdots, x_{\pi(n)}) = \varepsilon_\pi f(x_1, \cdots, x_n), \quad \forall \pi \in S_n,$$

其中 ε_π 是 π 的符号. 证明: 如果 $f \in K[x_1, \cdots, x_n]$ 是斜对称的, 那么存在对称多项式 $g \in K[x_1, \cdots, x_n]$ 使得

$$f = g \prod_{n \geqslant i > j \geqslant 1} (x_i - x_j).$$

14. 证明: 一般三次多项式 $f = a_0x^3 + a_1x^2 + a_2x + a_3$ 的判别式为

$$D(f) = a_1^2a_2^2 - 4a_1^3a_3 - 4a_0a_2^3 + 18a_0a_1a_2a_3 - 27a_0^2a_3^2.$$

15. 计算下列多项式的结式:
(1) $x^3 - 3x^2 + 2x + 1, 2x^2 - x - 1$;
(2) $2x^3 - 3x^2 - x + 2, x^4 - 2x^2 - 3x + 4$;
(3) $2x^4 - x^3 + 3, 3x^3 - x^2 + 4$.

16. 求 λ 以使下面的方程对有公共根:
(1) $x^3 - \lambda x + 2, x^2 + \lambda x + 2$;
(2) $x^3 + \lambda x^2 - 9, x^3 + \lambda x - 3$.

17. 计算下列多项式的判别式:
(1) $x^n + a$;
(2) $x^n + px + q$.

18. 假设多项式 f, g, h 都可以分解成线性因子的乘积. 证明

$$\mathrm{Res}(fg, h) = \mathrm{Res}(f, h)\,\mathrm{Res}(g, h).$$

(注: 以后会证明, 域 K 上的任何多项式都可以在 K 的某个扩域中分解成线性因子的乘积).

19. 证明:

$$D(fg) = D(f)D(g)[\mathrm{Res}(f, g)]^2.$$

实根隔离, 代数基本定理

1. 用 Sturm 定理证明 $x^3 - 7x - 7$ 在开区间 $(-2, -1)$ 内有两个实根. 这个多项式还有一个正根, 这个正根的近似值, 要求精确到小数点后第二位.

2. 证明: 如果整系数多项式 $f(x)$ 在 0 和 1 处的取值 $f(0)$ 和 $f(1)$ 都是奇数, 那么 $f(x)$ 没有整数根.

3. 设 $f(x)$ 是首一整系数多项式. 证明: 若有三个不同的整数 a,b,c 使得

$$|f(a)| = |f(b)| = |f(c)| = 1,$$

则 $f(x)$ 没有整数根.

4. 设 n 是正整数. 求满足条件

$$f(f(x)) = f(x)^n + a_1 f(x)^{n-1} + \cdots + a_{n-1} f(x) + a_n$$

的所有 n 次复系数多项式 $f(x)$ (提示: 用代数基本定理).

5. 设 $2n$ 次实系数多项式 $f(x)$ 的所有复数根都是纯虚数. 证明: 它的导数 $f'(x)$ 的所有根, 除了一个例外 0, 其余都是纯虚数 (提示: 令 $g(x^2) = \dfrac{f'(x)}{x}$, 证明 g 恰有 $n-1$ 个实根).

6. 如果任取 $x \in \mathbb{R}, f(x) \geqslant 0$, 则实多项式 $f(x)$ 可以表示成

$$f(x) = g(x)^2 + h(x)^2$$

的形状, 其中 $g,h \in \mathbb{R}[x]$. 提示: 利用恒等式

$$\left(p^2+q^2\right)\left(r^2+s^2\right) = (pr+qs)^2 + (ps-qr)^2.$$

7. 证明自由项 $w \neq 0$ 的多项式 $f(x) = x^5 + ux^4 + vx^3 + w \in \mathbb{R}[x]$ 的根不可能全是实的.

提示: 考虑其相关多项式 $x^5 f\left(\frac{1}{x}\right)$ 的根, 利用韦达定理和牛顿公式导出矛盾.

8. 设 $f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n$ 是一个 n 次实系数多项式. 证明: 知道了多项式 $f(x), x^n f\left(\frac{1}{x}\right), f(-x), x^n f\left(\frac{-1}{x}\right)$ 的正根的一个上界, 就得出了多项式 $f(x)$ 的正根和负根的下界和上界。

9. 用上题8的记号, 设 $a_0 > 0, m$ 是使 $a_m < 0$ 的最小指标, B 是负系数的绝对值的最大值. 证明对于多项式 $f(x)$ 的任何正实根 c 都有

$$c \leqslant 1 + \sqrt[m]{\frac{B}{a_0}}$$

提示: 当 $x > 1$ 时, 使用估计式

$$f(x) \geqslant a_0 x^n - B\frac{x^{n-m+1}-1}{x-1} > \frac{x^{n-m+1}}{x-1}\left[a_0 x^{m-1}(x-1) - B\right]$$

10. 设 $\mathbb{F}$ 是零特征域, $a \in \mathbb{F}$. 证明任意 n 次多项式 $f \in \mathbb{F}[x]$ 满足公式（泰勒公式）

$$f(x) = f(a) + \frac{1}{1!}f'(a)(x-a) + \frac{1}{2!}f''(a)(x-a)^2 + \cdots + \frac{1}{n!}f^{(n)}(a)(x-a)^n$$

提示: 对形式表达式 $f(x) = \sum b_i (x-a)^i$ 逐项求导 k 次然后令 $x = a$.