Chapter 1

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：

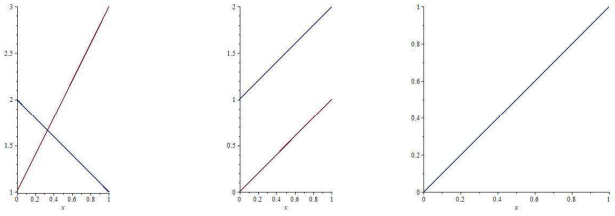
1. 解方程与数系的扩张：

   - $2x = 1 \Rightarrow x = 1/2$. 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。”



(a) 相交 (b) 平行 (c) 重合

图 1.1: 直线的位置关系

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：

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

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

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

   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：

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

   再令 $y=z-\frac{p}{3z}$，得

$$z^6+qz^3-\frac{p^3}{27}=0(预解式)$$

   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

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

其中 a_{ij}, b_i 都是实数，$i = 1, 2\cdots m, j = 1, 2\cdots n$. $x_1 \cdots x_n$ 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

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

称为实数上 $m \times n$ 的矩阵，称 $\overrightarrow{A_i} = (a_{i1}, \cdots, a_{in})$ 为 A 的第 i 行，$\overrightarrow{A^{(j)}} = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix}$ 为第 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 $\overrightarrow{u}=(u_1,\dots,u_n),\overrightarrow{v}=(v_1,\dots,v_n)$，其中 $u_i,v_i,i=1,\dots,n$ 是实数，另外 $\alpha\in\mathbb{R}$。则

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

$$\alpha\overrightarrow{u}=(\alpha u_1,\dots,\alpha u_n).$$

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:

$$\left(\begin{array}{ccc:c}2&-1&3&1\\4&-2&5&5\\2&-1&4&-1\end{array}\right)\xrightarrow{r_2-2r_1}\left(\begin{array}{ccc:c}2&-1&3&1\\0&0&-1&3\\2&-1&4&-1\end{array}\right)$$

$$\xrightarrow{r_3-r_1}\left(\begin{array}{ccc:c}2&-1&3&1\\0&0&-1&3\\0&0&1&-2\end{array}\right)\xrightarrow{r_3+r_2}\left(\begin{array}{ccc:c}2&-1&3&1\\0&0&-1&3\\0&0&0&1\end{array}\right)$$

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 $x_1,\cdots x_n$ 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 $\begin{cases}x_1=\alpha_1\\ \vdots\\ x_n=\alpha_n\end{cases}$ 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

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

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

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

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：

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

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：

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

(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 $\left(\begin{array}{c:c}A&\begin{matrix}b_1\\\vdots\\b_m\end{matrix}\end{array}\right)$ 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 $\left(\begin{array}{c:c}A'&\begin{matrix}b_1\\\vdots\\b_m\end{matrix}\end{array}\right)$，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

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

于是有

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

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

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

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

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

而取任意的 $1 \leqslant i \leqslant n,\ i \neq k_1, k_2, \cdots k_r, x_i = 1$，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 $\left(\begin{array}{c:c} A & \begin{matrix}b_1\\ \vdots\\ b_m\end{matrix}\end{array}\right)$ 为增广矩阵的线性方程组为 (L)，其中 $b_1,\cdots,b_m\in\mathbb{R}$。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。 □

思考题 1.2.1 设 A 是 $m\times n$ 阶矩阵，$m<n$, $b_1,\cdots,b_m\in\mathbb{R}$。试证明：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或者不相容，或者不确定。

命题 1.2.2 设 A 是 $m\times n$ 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：

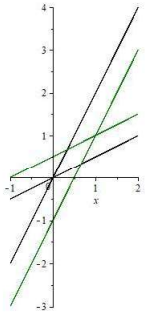


图 1.2: 平移

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

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

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

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

也有所有正偶数的集合

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

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	$\mathbb{Z}^+ = \{1, 2, 3 \cdots\}$
自然数集	$\mathbb{N} = \{0, 1, 2, \cdots\}$
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 $S \subset T$。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：
$S \cup T = \{a \mid a \in S\text{或}a \in T\}$；$S$ 和 T 的交：$S \cup T = \{a \mid a \in S\text{且}a \in T\}$。

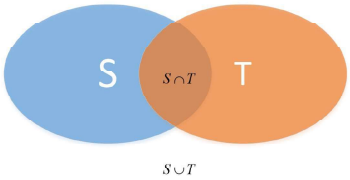


图 1.3: S 和 T 的并与交

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

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

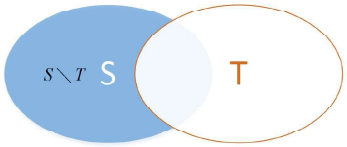


图 1.4: S 和 T 的差集

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 $S_1, S_2, \cdots, S_n$ 是 n 个集合，定义

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

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

- $\mathbb{R}^{1\times n} = \{(x_1, \cdots, x_n) | x_1, \cdots, x_n \in \mathbb{R}\}$，$n$ 维行向量空间；
- $\mathbb{R}^{1\times n} = \{\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} | x_1, \cdots, x_n \in \mathbb{R}\}$，$n$ 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；
- $v = \left\{ (x_1, \cdots, x_n) \middle| \begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = 0 \\ \cdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = 0 \end{cases} \right\} \subset \mathbb{R}^n$ 线性子空间。

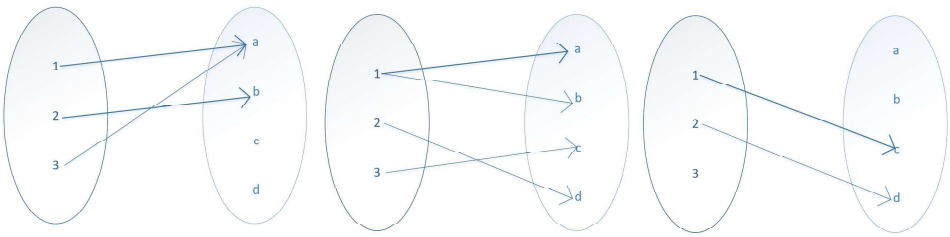
1.3.3 映射

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。



(a) f (b) g (c) h

图 1.5:

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)。显然 $f^{-1}(T)=S$。

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

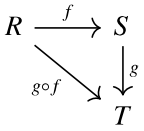
- f 是单射 $\Longleftrightarrow \forall t\in T$, $f^{-1}(\{t\})$ 至多含有一个元素;
- f 是满射 $\Longleftrightarrow \forall t\in T$, $f^{-1}(\{t\})$ 非空。

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

$$g\circ f(x)=g(x^2)=x^2+1;$$
$$f\circ g(x)=f(x+1)=(x+1)^2.$$

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 $f\circ h=\mathrm{id}_S$，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

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

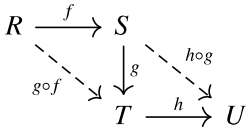
于是 f 是可逆映射，且逆映射为 g。 □

由定理的证明过程我们可以得到一个有用的结论：设 $f : S \to T, g : T \to S$ 是映射，若 $gf = \mathrm{id}_S$，则 g 是满射，f 是单射。

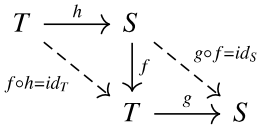
例 1.3.15 $\sin : [-\frac{\pi}{2}, \frac{\pi}{2}] \to [-1, 1]$ 是可逆映射。

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 $\{1, \cdots, n\}$ 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 1.3.3 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。

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 $f^k(x) = f(f \cdots f(x)), k = 0, 1, 2, \cdots$，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]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

1.4 等价关系和序关系

1.4.1 二元关系

定义 1.4.1 设 S 是非空集合，$R \subset S \times S$，则称 R 是 S 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。

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

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

(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 $r\in\{0,1,\cdots,|b|-1\}$ 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。

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

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

称 $\bar{a}$ 是 a 关于 $\sim$ 的等价类。

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

命题 1.4.1 设 $\sim$ 是集合 S 上的等价关系，$a,b\in S$，则

(1) $a\sim b\Longleftrightarrow \bar{a}=\bar{b}$;

(2) $a\nsim b\Longleftrightarrow \bar{a}\cap\bar{b}=\emptyset$.

证明: (i) ($\Longrightarrow$)
设 $x\in\bar{a}$，则 $x\sim a$，因为 $a\sim b$，所以 $x\sim b$，即 $x\in\bar{b}$。故 $\bar{a}\subset\bar{b}$。同理 $\bar{b}\subset\bar{a}$。故 $\bar{a}=\bar{b}$。
($\Longleftarrow$)
由 $b\in\bar{b},\bar{a}=\bar{b}$ 知 $b\in\bar{a}$，即 $a\sim b$。

(ii) ($\Longrightarrow$)
用反证法。若 $\bar{a}\cap\bar{b}\neq\emptyset$，则存在 $x\in\bar{a}\cap\bar{b}$，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 $\bar{a}$ 中的任意元素为 $\bar{a}$ 的代表元。

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

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

例如，$\mathbb{Z}/\equiv_2=\{\bar{0},\bar{1}\}$，$\mathbb{Z}/\equiv_n=\{\bar{0},\cdots,\overline{n-1}\}$。我们通常把 $\{\bar{0},\cdots,\overline{n-1}\}$ 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。

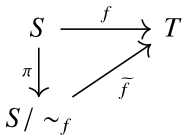
定义 1.4.9 设 $\sim$ 是 S 上的等价关系，定义映射

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

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

例 1.4.3 $\pi:\mathbb{Z}\to\mathbb{Z}_n,k\mapsto\bar{k}=\overline{\mathrm{rem}(k,n)}$ 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

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

首先 $\widetilde{f}$ 是良定义的: 设 $\bar{a}=\bar{b}$，则 $a\sim_f b$，即 $f(a)=f(b)$，所以 $\widetilde{f}(\bar{a})=\widetilde{f}(\bar{b})$，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 $\bar{a}\neq\bar{b}$，则 $a\nsim_f b$，即 $f(a)\neq f(b)$，所以 $\widetilde{f}(\bar{a})\neq\widetilde{f}(\bar{b})$，即 $\widetilde{f}$ 是单射。
最后验证 $f=\widetilde{f}\circ\pi$: 对 $\forall a\in S$，$\widetilde{f}\circ\pi(a)=\widetilde{f}(\bar{a})=f(a)$，即 $f=\widetilde{f}\circ\pi$。 □

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 $U = \bar{a}$ 且 $U \subset S$ 非空；若 $\bar{a} \neq \bar{b}$，则 $\bar{a} \cap \bar{b} = \emptyset$。另外，$\forall a \in S$, $a \in \bar{a}$。综上，$S = \bigcup\limits_{u \in S/\sim} U$。 □

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 $\bar{s} = S_i$，所以 $S/\sim_T = T$。 □

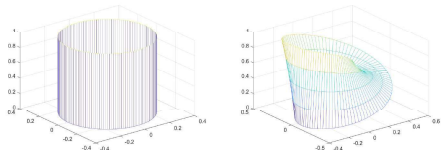
例 1.4.5 考虑将正方形的对边“粘合”过程中的集合分割及对应的等价类。
设正方形为 $[0,1] \times [0,1]$，分割

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

则 $S/\sim_{T_1}$ 是圆柱；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 $S/\sim_{T_2}$ 是莫比乌斯 (Möbius) 带。



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

图 1.6:

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。

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 $S = \{a,b,c\}, T = 2^S, T_0 = T \setminus \{S\}$，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) 在整除关系 ”$|$” 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 在序 “$a|b \Longleftrightarrow b \preceq a$” 下的最大元称为最小公倍数 (least common multiple)，记为 $\mathrm{lcm}(a,b)$。

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。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 $\sigma,\sigma^2,\cdots,\sigma^n,\cdots$ 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 $m = kq + r$, $r \in \{0, 1, \cdots, k-1\}$, 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 $i_1, \cdots, i_k \in X$ 两两不同, $\pi \in S_n$, 如果

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

且对 $\forall j \in X \setminus \{i_1, \cdots, i_k\}$, 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 $\forall m \in \{1, 2, \cdots, k-1\}$, 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 $\{i_1, \cdots, i_k\} \cap \{j_1, \cdots, j_l\} = \emptyset$, 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 $\tau_1, \cdots, \tau_p$ 是 $\pi_1, \cdots, \pi_p$ 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

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

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

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

下面验证 $\sigma = \pi \circ \tau$。
$\forall i \in \{i_1, \cdots, i_k\},\ \pi\tau(i) = \pi(i) = \sigma(i)$;
$\forall j \in J,\ \pi(\tau(j)) = \tau(j) = \sigma(j)$.
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，$\pi_1, \cdots, \pi_p$ 中也只有一个循环改变 i，设为 π_a，则 $\sigma(i) = \pi_a(i) = \tau_1(i)$，注意到 σ 与 π_a 和 τ_1 都交换 (反复运用引理 1.5.4)，于是

$$\sigma^2(i) = \sigma\pi_a(i) = \pi_a^2(i) = \tau_1^2(i).$$

重复以上做法可得对任意的正整数 h 有 $\sigma^h(i) = \pi_a^h(i) = \tau_1^h(i)$。设 c 是使得 $\sigma^c(i) = i$ 的最小正整数，那么 $\pi_a = \tau_1 = \left(i\ \sigma(i)\ \sigma^2(i) \cdots \sigma^{c-1}(i)\right) = \tau_1$。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 $\sigma = (1\ 5)(2\ 3)(4)$.

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 $\mathrm{ord}(\sigma) = \mathrm{lcm}(\mathrm{ord}(\pi_1), \cdots, \mathrm{ord}(\pi_s))$。

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

[1] 关于数学归纳法，我们会在习题课讲义中详细介绍。

$l = k_i q_i,\ i = 1, \cdots, s$。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 $r_1 \in \{1, 2, \cdots, k_1 - 1\}$。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 $\pi_2^k, \cdots, \pi_s^k$ 与 $\pi_1^{r_1}$ 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 $\mathrm{ord}(\sigma)$。

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

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 $\tau'_{k-1},\ \tau'_k$，使得

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

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！故后一个或者不会发生，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 $\lambda_1,\cdots,\lambda_k,\mu_1,\cdots,\mu_m$ 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 $\pi_1,\cdots,\pi_s$ 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)。显然有 (1) 如果 σ 是偶置换, 那么

$$\begin{aligned}L_\sigma(A_n)&=R_\sigma(A_n)=A_n.\\L_\sigma\left(\overline{A_n}\right)&=R_\sigma\left(\overline{A_n}\right)=\overline{A_n}.\end{aligned}$$

(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

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

称函数 $g = \pi \circ f$ 是由 π 作用到 f 上得到的。我们称一个函数是对称的，若 $\forall \pi \in S_n$, $\pi \circ f = f$; 称一个函数是斜对称 (反对称) 的，若 $\forall \pi \in S_n$, $\pi \circ f = \varepsilon_\pi f$。

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 $(\alpha\beta) \circ f = \alpha \circ (\beta \circ f)$。

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 $x_1, \cdots, x_n$ 两两不同时，$\Delta_n(x_1, x_2, \cdots, x_n) \neq 0$。

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

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

由于 $\sigma \circ f$ 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 (我们会在第四章证明它)。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。

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 $r_0 = q_2 r_1 + r_2$，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 $r_1 = q_3 r_2 + r_3$，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 $r_2 = q_4 r_3 + r_4, \cdots, r_{k-2} = q_k r_{k-1} + r_k$, $r_{k-1} = q_{k+1} r_k$，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 $r_{i-2} = q_i r_{i-1} + r_i$ 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

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

令 $u_{k-2} = -q_k$, $v_{k-2} = 1 + q_k q_{k-1}$。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 $g = u_1 a + v_1 b$。 □

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 1.6.1 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 $\Longleftrightarrow \exists u,v\in\mathbb{Z}$ 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 $\mathrm{lcm}(a,b) = ab$。

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 $\mathrm{lcm}(a,b) = \dfrac{ab}{\gcd(a,b)}$。

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 $\mathrm{lcm}(a,b) = cdg$。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，$\mathrm{lcm}(a,b) = cdg = \frac{ab}{\gcd(a,b)}$。 □

下面我们介绍一些素数的性质。

定义 1.6.2 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]

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。

[1] 1 既不是素数也不是合数。

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 $m_1,\cdots,m_s$ 两两互素的情形，证明留作思考。