线性代数 (B) 讲义草稿

李文威

北京大学数学科学学院

邮箱: wwli@pku.edu.cn

编译日期: 2020-10-03

目录

基于北京大学 2020 年秋季开设的线性代数 (B) 课程. 本课程教材为 [1]. 讲义仅是粗稿, 将持续更新和修正, 不建议打印或外传. 欢迎批评指正.

1 综观

1.1 何谓代数? 代数之义大矣. 按照经典视角, 代数是以抽象符号, 即变元 X, Y, Z 等等代替具体数字, 求解方程的一门技艺.

这个定义进一步引出一系列的问题: 何谓方程, 何谓数字, 以及更重要的是: 何谓技艺? 我们且从几个初步例子来审视这些问题.

首先回顾数学符号. 各位熟知的数系照例记为

$$\begin{array}{ccccccc} \mathbb{Z} & \subset & \mathbb{Q} & \subset & \mathbb{R} & \subset & \mathbb{C} \\ \text{整数集} & & \text{有理数集} & & \text{实数集} & & \text{复数集.} \end{array}$$

非负整数集记为 $\mathbb{Z}_{\geq 0}$, 正整数集记为 $\mathbb{Z}_{\geq 1}$, 依此类推.

▷ **二次方程** 考虑

$$X^2 + bX + c = 0,$$

其中 X 是变元, 代表我们所求的解, 而 b, c 是给定的复数. 求解公式是熟知的: 通过

$$X^2 + bX + c = \left(X + \frac{b}{2}\right)^2 + c - \frac{b^2}{4}$$

消去一次项, 于是公式

$$X = \frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

给出所有的复数解. 若 $b, c \in \mathbb{R}$, 则方程有实数解当且仅当 $b^2 - 4c > 0$. 古人仅关心实数解; 虚数 $\sqrt{-1}$ 或更一般的复数对他们而言并无现实意义.

▷ **三次方程** 一般的三次方程可以表作 $X^3 + aX^2 + bX + c = 0$ 的形式. 以 $X - \frac{a}{3}$ 代 X, 可以进一步消去 X^2 的系数. 因此不妨聚焦于形如

$$X^3 + pX + q = 0$$

的方程, 其中 p, q 是给定的复数. 三次方程的公式解是 G. Cardano 首先在 1545 年发表的. 为了说明他的公式, 首先取

$$D := -4p^3 - 27q^2.$$

观察到

$$\left(-\frac{27}{2}q+\frac{3}{2}\sqrt{-3D}\right)\left(-\frac{27}{2}q-\frac{3}{2}\sqrt{-3D}\right)=\frac{27^2q^2}{4}+\frac{27D}{4}$$
$$=\frac{27^2q^2-4\cdot 27\cdot p^3-27^2q^2}{4}=(-3p)^3.$$

因此可以令

$$u_1,u_2,u_3:\quad -\frac{27}{2}q+\frac{3}{2}\sqrt{-3D}\text{ 的立方根},$$
$$v_1,v_2,v_3:\quad -\frac{27}{2}q-\frac{3}{2}\sqrt{-3D}\text{ 的立方根},$$

使得 $u_iv_i=-3p$ 对 $i=1,2,3$ 都成立. 原三次方程的三个根 (计入重数) 表作

$$\alpha=\frac{u_1+v_1}{3},\quad \beta=\frac{u_2+v_2}{3},\quad \gamma=\frac{u_3+v_3}{3}.$$

这里考虑的都是方程的复根. 如果系数 $p,q\in\mathbb{R}$, 而 $D>0$, 则可以用初等方法说明方程的三根也都是实数. 尽管如此, 为了对一个现实的三次方程写下同样现实的三个根, Cardano 公式中的 $\sqrt{-3D}$ 和 u_i, v_i 却无可避免地要容许为复数. 这和二次方程的情形完全不同.

正因如此, Cardano 公式是促使数学家们接受复数的重要推力之一.

▷ **高次方程的公式解问题** 推而广之, 考虑形如

$$X^n+a_{n-1}X^{n-1}+\cdots+a_0=0$$

的 n 次方程, 其中 $a_0,a_1,\ldots,a_{n-1}$ 是给定的系数. 有了 $n=1,2,3$ 时的经验, 自然的问题是对一般的 n 寻求公式解. 这里所谓的公式, 仅容许用到系数 $a_0,\ldots,a_{n-1}$ 的四则运算 (当然, 分子非零) 和取 m 次根 $\sqrt[m]{\cdots}$ 的运算, 其中 $m\in\mathbb{Z}_{\geq 1}$.

四次方程的公式解是 G. Cardano 及其学生 L. Ferrari 的工作; $n\geq 5$ 的情形则长期困扰着此后的数学家们, 直至 N. H. Abel, P. Ruffini 和 E. Galois 等人在 18-19 世纪之交的工作才彻底解答了这个问题: 五次及以上的方程无公式解. 虽然这是一个否定性的结论, 其相关思想和技术却成为近世代数学的滥觞, 开启了数学发展史上的崭新一页.

▷ Fermat **方程** 考虑方程

$$X^n+Y^n=Z^n,\quad n\geq 3.$$

所谓的 Fermat 大定理, 断言的是此方程没有满足 $XYZ\neq 0$ 的整数解; 借由通分, 等价的说法是此方程没有满足 $XYZ\neq 0$ 的有理数解.

这个问题的完整解答是 R. Taylor 和 A. Wiles 在 1995 发表的工作. 几何观点在他们的工作中至关重要. 这里指的几何并不是简单地描绘 $X^n + Y^n = Z^n$ 的几何图形, 因为实数解和有理数解的脾性完全不同. 我们需要的是一套能整合几何直观和代数技巧, 从而能处理数论问题的几何理论; 当然, 不可或缺的还有那一瞬别开生面的直觉.

▷ **线性方程组** 线性方程意指一次方程. 线性方程组是形如

$$\begin{aligned} a_{11}X_1 + \cdots + a_{1n}X_n &= b_1 \\ a_{21}X_1 + \cdots + a_{2n}X_n &= b_2 \\ \vdots \quad & \quad \vdots \\ a_{m1}X_1 + \cdots + a_{mn}X_n &= b_m \end{aligned}$$

的方程组, 其中 a_{ij} 和 b_i 是给定的常数 ($1 \leq i \leq n$, $1 \leq j \leq m$), 而 $X_1, \ldots, X_n$ 是变元. 我们暂且不去明确所用的数系. 这样的方程可以在 $\mathbb{Q}$, $\mathbb{R}$ 或 $\mathbb{C}$ 上来考虑, 以后将会看到, 它们的解法和解集的结构和数系的选取基本无关.

这里出现的问题是: 如何判定方程组是否有解? 若有解, 如何高效地求解? 所有解 $(X_1, \ldots, X_n)$ 构成的集合 (顺理成章地称为**解集**) 有怎样的结构?

对于 $n = m = 2$ 的情形, 解法想必是读者熟知的, 公式可以用行列式表达. 对于变元更多的情形也有称为 Cramer 公式的行列式解法. 然而 Cramer 公式所需的计算量随变元变多而暴增, 它的地位在理论而不在计算层面. 我们行将介绍的 Gauss–Jordan 消元法则提供了一个简单快速的求解手段.

练习 1.1.1 请回顾之前讨论的三次方程 $X^3 + pX + q = 0$.

(i) 尝试验证 $(X-\alpha)(X-\beta)(X-\gamma) = X^3 + pX + q$. 换言之, Cardano 公式的确给出所有的根, 计入重数.

(ii) 设 $p, q \in \mathbb{R}$. 验证当 $D > 0$ 时 α, β, γ 都是实数. 〈提示〉 令 $\rho := \frac{-1+\sqrt{-3}}{2}$; 在复数平面上作图可见 $\rho^3 = 1$. 我们希望对 $i = 1, 2, 3$ 证明 $\overline{u_i + v_i} = u_i + v_i$, 这里 $z \mapsto \overline{z}$ 表复数的共轭运算. 由 $\overline{u_i}^3 = \overline{u_i^3}$ 可见 $u_i^3 = v_i^3$, 因而存在 $k \in \{0, 1, 2\}$ 使得 $\overline{u_i} = \rho^k v_i$. 再取一次共轭得到 $\overline{v_i} = \rho^k u_i$ 又由于

$$\overline{u_i v_i} = -3p = u_i v_i,$$

代入上述结果给出 $\rho^{2k} = 1$. 配合 $\rho^3 = 1$ 可得 $k = 0$.

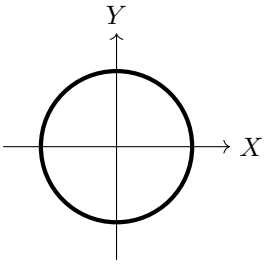
例子既已看过, 可以补全我们早先对 “何谓代数” 的解答.

⋆ **何谓方程** — 来自经过有限次的加, 减, 乘, 除 (分母非零) 四则运算得到的表达式.

- ⋆ **何谓数** — 至少包括 $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ 这些常用的数系; 它们的共性是都具备四则运算, 但除法要求分母非零. 注意到 $\mathbb{Z}$ 不在列表中, 因为除法在 $\mathbb{Z}$ 中不能通行无阻.
  从关于 Fermat 大定理的讨论可以看到方程的解的性状和 "数" 的界定密切相关, 采用的技术也随之而千变万化.
- ⋆ **何谓求解的技艺** — 判定方程是否有解, 如何精确求解, 给出一套尽量高效的算法, 或者至少给出逼近方程的解的手段. 算法是一切应用的核心.

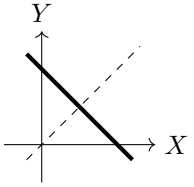
我们关心的还有解集的结构. 数学中的 "结构" 难以三言两语说清, 所以我们还是从简单例子入手. 结构的一个重要面向是**对称性**. 在几何的经典场景中, 对称性意指图像在一族刚体变换作业下的不变性; 这里所谓的刚体变换包括平移, 旋转, 镜射.

- ⋆ 考虑方程 $X^2+Y^2=1$, 其中 (X,Y) 取作平面 $\mathbb{R}^2$ 上的点. 它的解集是单位圆, 如下图:



  单位圆对任何以原点 $(0,0)$ 为圆心的转动都保持不变, 这是对称性的一个例子. 此外, 它相对于 X 轴或 Y 轴的镜射也都具有对称性.

- ⋆ 考虑线性方程组 $X+Y=1$, 具体起见, 仍在实数里求解. 其解集无非是平面上的直线, 如下图:



  直线上的点对于沿着 $(-1,1)$ 方向的所有平移都保持不变, 此外, 它相对于直线 $X=Y$ (上图虚线) 的镜射也具有对称性.

注记 1.1.2 上面给出了代数方程的几种典型例子, 那么何谓非代数方程? 典型的例子是涉及极限, 例如涉及无穷级数的操作, 这类问题是数学分析的主场. 另一类是涉及不

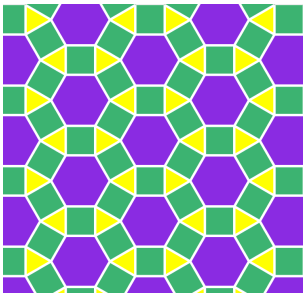
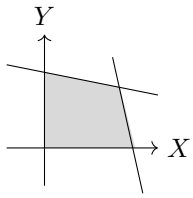


图 1.1: 这是编号为 $(6,4,3,4)$ 的平面镶嵌, 使用 Haskell 的 diagrams 包绘制. 您能从图中数出几种对称性? 几何学家证明了平面总共有 3 种正则镶嵌, 8 种半正则镶嵌; 正则镶嵌指的是由正多边形给出的平面镶嵌. 您能具体猜出是哪三种正多边形吗?

等式, 例如形如

$$\begin{aligned} a_{11}X_1 + \cdots + a_{1n}X_n &\le b_1 \\ a_{21}X_1 + \cdots + a_{2n}X_n &\le b_2 \\ \vdots \quad & \quad \vdots \\ a_{m1}X_1 + \cdots + a_{mn}X_n &\le b_m \end{aligned}$$

的方程组; 这里取 a_{ij} 和 b_i 为实数, 所求的解 $X_1, \ldots, X_n$ 亦然, 这是因为 $\mathbb{R}$ 相对于 $\mathbb{Q}$ 或 $\mathbb{C}$ 具有额外的 "序结构": 任两个实数可以合理地比大小. 涉及不等号的方程组也称为**半代数**的. 中学数学学过的线性规划便涉及这类方程组. 以 $n = 2$ 情形为例, 解空间一般是由有限多条直线围出的区域, 譬如



的形式. 这类解空间也有特殊的 "结构": 至少在有界的情形下, 它们是多边形 (高维情形: 多面体). 线性规划所求的是形如 $c_1X_1 + \cdots + c_nX_n$ 的函数在解空间上的极值. 当 $n = 2$ 时可以画图求解, $n = 3$ 时也可以发挥想象, 但实际应用场景中的 n 可以成千上万. 如何将低维的几何直觉可靠地推广到一般维数的线性规划? 尽管这是一个半代数的问题, 线性代数对此仍不可或缺.

1.2 Gauss–Jordan 消元法

现在聚焦于最简单的一类方程, 即线性方程组:

$$\begin{aligned} a_{11}X_1 + \cdots + a_{1n}X_n &= b_1 \\ a_{21}X_1 + \cdots + a_{2n}X_n &= b_2 \\ \vdots \quad & \quad \vdots \\ a_{m1}X_1 + \cdots + a_{mn}X_n &= b_m \end{aligned} \tag{1.1}$$

我们不对变元个数 n 施加任何限制. 为了讨论方便, 且先假设是在 $\mathbb{C}$ 中求解.

定义 1.2.1 如果以 $X_1, \ldots, X_n$ 为变元的两组线性方程组有相同的解集, 则称它们是**同解**的.

Gauss–Jordan 消元法的思路是在同解的方程组之间过渡, 直至方程组化为一类可直接求解的形式. 且先看个简单特例.

例 1.2.2 令 a, b, c 为给定的常数. 考虑

$$\begin{aligned} X_1 - X_2 + X_3 &= a && ① \\ X_1 - X_2 - X_3 &= b && ② \\ 2X_1 - 2X_2 - X_3 &= c && ③ \end{aligned}$$

右列是方程的编号, 或可谓 "行号". 将第一个方程两边乘以 -1 加到第二个方程; 类似地, 将第一个方程两边乘以 -2 加到第三个方程, 如是得到新的方程组

$$\begin{aligned} X_1 - X_2 + X_3 &= a && ① \\ -2X_3 &= b - a && ②' := ② - ① \\ -3X_3 &= c - 2a && ③' := ③ - 2 \cdot ① \end{aligned}$$

我们想反解 X_3, 所以将 ②′ 乘以 $\frac{1}{2}$, 然后用它消掉 ③′ 的 X_3. 产物是

$$\begin{aligned} X_1 - X_2 + X_3 &= a && ① \\ X_3 &= \frac{a-b}{2} && ②'' := \frac{1}{2}②' \\ 0 &= \frac{-a-3b+2c}{2} && ③'' := ③' + 3 \cdot ②'' \end{aligned}$$

每一步都给出同解的方程组. 解集于是明朗了: 我们由下而上地解方程, 得到

⋆ 如果 $-a - 3b + 2c \neq 0$, 则方程无解, 因为它将包含矛盾的 $0 =$ 非零项;

⋆ 设 $-a-3b+2c=0$, 则 ②′′ 给出 X_3, 代入 ①, 得出方程的通解

$$X_1 = a + X_2 - X_3 = \frac{a+b}{2} + X_2$$
$$X_3 = \frac{a-b}{2}.$$

注意到 X_2 在通解中是**自由变元**, 不受约束, 可以任取.

如果一切都取为实数, 将解集在三维空间中绘制, 则它或者是空集 (当 $-a-3b+2c \neq 0$), 或者是落在平面 $X_3 = \frac{a-b}{2}$ 上的一条直线, 由坐标 X_2 参数化. 套用物理学的术语, 后一情形下可以说解集的**自由度**为 1, 因为它有一个可变参数.

这里的自由度只是一个权宜说词, 随着线性代数理论的渐次铺展, 对之将有更加精确的界定.

回到一般的线性方程组. 形如 (1.1) 的写法现在显得有些累赘了, 我们引进较为紧凑的符号.

定义 1.2.3 我们将 (1.1) 的方程组以称为**矩阵**的方式记为

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \vdots & & & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{pmatrix}$$

的形式. 去掉最右一列得到的矩阵

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

称为该方程组的**系数矩阵**; 相对于此, 先前写下的带 $b_1, \ldots, b_m$ 的矩阵则称为**增广矩阵**.

矩阵行, 列的具体记法是

$$\begin{pmatrix} \vdots \\ \cdots\ a_{ij}\ \cdots \\ \vdots \end{pmatrix} \begin{matrix} \\ \text{第 } i \text{ 行} \\ \\ \end{matrix}$$
$$\text{第 } j \text{ 列}$$

每个矩阵元 a_{ij} 都等于 0 的矩阵称为**零矩阵**.

由于方程组中的 $b_1, \dots, b_m$ 角色毕竟不同于系数 a_{ij}, 有时在增广矩阵中宜作区隔, 如

$$\left(\begin{array}{ccc|c} a_{11} & \cdots & a_{1n} & b_1 \\ \vdots & & \vdots & \vdots \\ a_{m1} & \cdots & a_{mn} & b_m \end{array}\right)$$

Gauss–Jordan 消元法的思路是用以下三种操作来简化方程组, 或者换句话说, 简化相应的矩阵.

(A) 设 $1 \le i \ne k \le m$, 而 c 是任意常数. 我们将第 i 行乘以 c, 加到第 k 行, 其它的行保持不变:

$$A(i,k,c): \quad \begin{matrix} \\ \text{i} \\ \\ \text{k} \\ \\ \end{matrix} \begin{pmatrix} \vdots \\ \cdots\ a_{ij}\ \cdots \\ \vdots \\ \cdots\ a_{kj}\ \cdots \\ \vdots \end{pmatrix} \overset{\cdot c}{\circlearrowright} \quad \rightsquigarrow \quad \begin{pmatrix} \vdots \\ \cdots\ a_{ij}\ \cdots \\ \vdots \\ \cdots\ a_{kj} + ca_{ij}\ \cdots \\ \vdots \end{pmatrix}$$

(B) 设 $1 \le i \ne k \le m$. 我们交换第 i 行和第 k 行:

$$B(i,k): \quad \begin{matrix} \\ \text{i} \\ \\ \text{k} \\ \\ \end{matrix} \begin{pmatrix} \vdots \\ \cdots\ a_{ij}\ \cdots \\ \vdots \\ \cdots\ a_{kj}\ \cdots \\ \vdots \end{pmatrix} \overset{\text{交换}}{\circlearrowleft} \quad \rightsquigarrow \quad \begin{pmatrix} \vdots \\ \cdots\ a_{kj}\ \cdots \\ \vdots \\ \cdots\ a_{ij}\ \cdots \\ \vdots \end{pmatrix}$$

(C) 设 $1 \leq i \leq m$ 而 c 是非零常数. 我们将第 i 行的每一项都乘以 c:

$$C(i,c): \quad {}_i \begin{pmatrix} \vdots \\ \cdots \quad a_{ij} \quad \cdots \\ \vdots \end{pmatrix} \curvearrowleft \cdot c \quad \rightsquigarrow \quad \begin{pmatrix} \vdots \\ \cdots \quad ca_{ij} \quad \cdots \\ \vdots \end{pmatrix}$$

这些操作称为对矩阵的**初等行变换**. 我们仅容许交换行的顺序, 列的顺序不变, 所以变元 $X_1, \ldots, X_n$ 的顺序恒定. 注意到每一种操作都可以被相应的逆操作撤销, 以回到原来的矩阵, 具体言之:

- ⋆ $A(i,k,c)$ 的逆操作是 $A(i,k,-c)$,
- ⋆ $B(i,k)$ 的逆操作是 $B(k,i)$,
- ⋆ $C(i,c)$ 的逆操作是 $C(i,1/c)$,

有请读者顺手检验. 综上, 矩阵的初等行变换给出同解的方程组, 中间不丢失信息. 也请注意到如果矩阵的某一列全为 0, 则无论如何作初等行变换, 该列依然为 0.

陈述 Gauss–Jordan 消元法之前, 有必要先说明算法的目标—行梯矩阵, 这种矩阵对应的线性方程组易于求解.

定义 1.2.4 *考虑矩阵*

$$\begin{pmatrix} a_{11} & a_{12} & \cdots \\ a_{21} & a_{22} & \cdots \\ \vdots & \ddots & \\ a_{m1} & a_{m2} & \cdots \end{pmatrix} \tag{1.2}$$

*当它的形式如下所示时, 称之为***行梯矩阵**:

$$\begin{pmatrix} & & \\ & & \\ & & \vdots \end{pmatrix}$$

*其中左下空白部分的矩阵元皆为零, 涂灰的部分逐行向内严格缩进, 而且我们要求涂灰部分每一行的左端都是非零元, 它们称为此行梯矩阵的***主元**.

更加严格却不那么直观的定义如下:

- ⋆ *存在 $0 \leq r \leq m$ 使得第 i 行全为 0 当且仅当 $i > r$ (因此行梯矩阵中不全为 0 的行恰好是前 r 行);*

⋆ 对于每个 $1 \le k \le r$ (非零行的编号), 取

$$j_k := \min\{j : a_{k,j} \neq 0\},$$

则 $j_1 < j_2 < \cdots < j_r$ (相当于说涂灰部分逐行严格缩进).
上述的主元无非是 a_{k,j_k}, 其中 $1 \le k \le r$.

请读者沉思行梯矩阵的轮廓, 以下结果应该不言而喻.

练习 1.2.5 验证主元的个数 r 满足 $0 \le r \le \min\{n, m\}$. 无主元的行梯矩阵只能是零矩阵.

定义 1.2.6 在关于行梯矩阵的定义中, 倘若进一步对所有 $1 \le k \le r$ 要求:
⋆ $a_{k,j_k} = 1$, 换言之, 主元全为 1;
⋆ $i < k \implies a_{i,j_k} = 0$, 换言之, 落在主元以上的项全为 0;
则称此矩阵为**简化行梯矩阵**.

算法 1.2.7 (C. F. Gauss, C. Jordan) 对给定的矩阵如 (1.2), 按以下程序反复作初等行变换, 可以将之化为行梯矩阵.

1. 如果矩阵的第一列全为 0, 则跳过第一列, 继续对下图框出的 "子矩阵" 进初等行变换

$$\begin{pmatrix} 0 & a_{12} & a_{13} & \cdots & a_{1n} \\ 0 & a_{22} & a_{23} & \cdots & a_{2n} \\ \vdots & & \ddots & & \\ 0 & a_{m2} & a_{m3} & \cdots & a_{mn} \end{pmatrix}$$

   回忆到全为 0 的列不受后续初等行变换的影响, 可以放心舍去.

2. 设矩阵第一列有非零元, 设之为 a_{k1}. 进行先前标为 $B(k, 1)$ 的变换以交换第 k 行和第 1 行, 可以化到 $k = 1$ 亦即 $a_{11} \neq 0$ 的情形.

3. 设 $a_{11} \neq 0$. 接着对每个 $1 \le i \le m$, 进行先前标为 $A\left(1, i, -\frac{a_{i1}}{a_{11}}\right)$ 的变换, 将第一行乘以 $-\frac{a_{i1}}{a_{11}}$ 倍加到第 i 行. 如此的效果是将 a_{11} 以下的矩阵元全变为 0. 于是矩阵进一步化为

$$\begin{pmatrix} \mathbf{a_{11}} & a_{12} & \cdots & a_{1n} \\ 0 & & & \\ \vdots & \cdots & a_{ij} - \frac{a_{1j}a_{i1}}{a_{11}} & \cdots \\ 0 & & \vdots & \end{pmatrix}$$

然后我们对框出的子矩阵继续操作.

之所以将 $\mathbf{a_{11}}$ 加黑, 是代表该矩阵元为主元. 而对于框出的子矩阵, 它或者处处是 0, 或者经过初等行变换还会给出新的主元. 依此类推, 算法必然在有限步内停止, 给出行梯矩阵.

目前仅用到 (A), (B) 两种类型的运算. 为了从行梯矩阵进一步得到简化行梯矩阵, 我们对给定的行梯矩阵继续以下操作, 这里需要 (C) 型操作.

4. 对每个主元 a_{k,j_k}, 作变换 $C\left(k, a_{k,j_k}^{-1}\right)$ 以化约到行梯矩阵的主元全为 1 的情形.
5. 对每个主元 (取值为 1), 假设它位于第 k 行上, 对每个 $i<k$ 作变换 $A\left(k, i, -a_{ij_k}\right)$; 换言之, 将第 k 行乘以 $-a_{ij_k}$ 加到第 i 行上. 此操作将落在主元以上的矩阵元全化为 0.

显然, 最后得到的矩阵必然是简化行梯矩阵.

注意到消元法的执行方式并非唯一确定的. 比如步骤 2 涉及非零元 a_{k1} 的选法, 而且我们在选定非零元 a_{k1} 之前还可以进行若干次 (A) 或 (C) 型的初等行变换, 将各项化为更方便计算的形式. 当矩阵元全为整数时, 这种操作手法特别常见.

注记 1.2.8 同一个矩阵可以通过初等行变换过渡到种种不同的行梯矩阵. 相对于此, 初等行变换给出的简化行梯矩阵则是唯一确定的. 我们将在习题部分勾勒其证明.

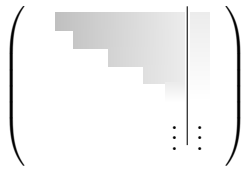
练习 1.2.9 假定读者对于编程有一定程度的了解. 令 $N:=\max\{n,m\}$. 试说明随着 N 增大, Gauss–Jordan 消元法的涉及的操作次数的增长约略被 N^3 的某个常数倍控制. 试说明 “约略” 一词何解.

1.3 回到线性方程组

莫忘原初问题是解方程 (1.1). 我们写下对应的增广矩阵

$$\left(\begin{array}{ccc|c} a_{11} & \cdots & a_{1n} & b_1 \\ \vdots & & \vdots & \vdots \\ a_{m1} & \cdots & a_{mn} & b_m \end{array}\right)$$

对之施行 Gauss–Jordan 消元法, 化之为简化行梯矩阵, 形如



相应的线性方程组与原方程组同解. 是故我们可以聚焦于简化行梯矩阵对应的线性方程组.

1. 如果简化行梯矩阵包含形如
$$(0 \ \cdots \ 0 \mid b_i)$$
的行, 或者换句话说, 方程组包含等式 $0 = b_i$, 而且 $b_i \neq 0$, 则方程组无解.

2. 假设没有如上形式的行. 记简化行梯矩阵主元的个数为 r, 将主元出现的列号依次排开, 记为
$$1 \leq j_1 < \cdots < j_r \leq n;$$
称它们对应的列为**主列**. 则矩阵的第 k 行对应到方程
$$X_{j_k} + \sum_{j>j_k} a_{kj} X_j = b_k;$$
注意到简化行梯矩阵的定义确保 $X_{j_{k+1}}, \ldots, X_{j_r}$ 在左式中的系数为 0. 由此立可对反解每个主列所对应的变元
$$X_{j_k} = b_k - \sum_{\substack{j>j_{k+1} \\ j \text{ 不对应到主列}}} a_{kj} X_j,$$
其中 k 遍历 $1, \ldots, r$.

注意到若第 j 列非主列, 则方程组对相应的变元 X_j 没有约束: 它们是 “自由变元”.

因此 n 元线性方程组 (1.1) 或者无解, 或者它的解集依赖于 $n-r$ 个自由变化的参数 (或者说其 “自由度” 为 $n-r$), 其中 r 是 Gauss–Jordan 消元法给出的主元个数.

注记 1.3.1 以上解方程 (1.1) 时对整个增广矩阵进行了消元. 包含 $b_1, \ldots, b_m$ 的增广列当然是重要的, 它会影响方程组是否有解. 但只要方程组有解, 主元就不可能出现在增广列, 否则简化行梯矩阵将有形如 $(0 \ \cdots \ 0 \mid 1)$ 的行.

这些讨论表明了, 一旦方程组 (1.1) 有解, 则增广矩阵的主元无非是系数矩阵的主元. 尽管系数矩阵的简化行梯形式是唯一确定的, 但主元仍然依赖于变元 $X_1, \ldots, X_n$ 的排序; 因此主元相对于方程组本身显得是一个外部的, 不尽自然的概念.

但另一方面, 上述讨论又表明一旦方程有解, 则主元个数 (等价地说, 系数矩阵的主元个数) r 是一个内在于方程组本身的概念, 它连同变元个数 n 一并决定了解集的自由度 $n-r$. 为了理清这些问题, 有必要为线性方程组建立更深刻也更自然的理论框架.

例 1.3.2 设线性方程组 (1.1) 的系数矩阵的主元个数等于变元个数 n. 以初等行变换

将系数矩阵化为简化行梯矩阵, 则增广矩阵也相应地化为

$$\left(\begin{array}{ccc|c} 1 & & & b'_1 \\ & \ddots & & \vdots \\ & & 1 & b'_n \\ & & & \vdots \\ & & & b'_m \end{array}\right)$$

的形式, 其中留白部分全为 0; 换言之, 分隔线左边矩阵仅在对角线上为 1, 其它全为 0.

- ⋆ 如果存在 $i > n$ 使得 $b'_i \neq 0$, 则对应的方程组无解.
- ⋆ 如果 $i > n \implies b'_i = 0$, 则第 n 行以下全对应到平凡等式 $0 = 0$, 由前 n 行则直接反解出 $X_i = b_i$, 其中 $i = 1, \ldots, n$.

因此这类方程组若有解则有唯一解, 符合先前的讨论.

注记 1.3.3 另一则观察则是 Gauss–Jordan 消元法的原理只涉及矩阵元的四则运算 (除法要求分母非零), 和我们具体选取的数系 $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ 等等并无关系. 然而若考虑系数在 $\mathbb{Z}$ 上的矩阵就会导致麻烦, 因为 Gauss–Jordan 消元法必须使用除法.

这就启发我们进一步放宽数系的概念, 转向容许四则运算的抽象代数结构, 称为**域**.

习题

1. ♣♣♣ 此处应有计算题.

2. 考虑两个大小相同的矩阵

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ & \ddots & \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}, \quad B = \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ & \ddots & \\ b_{m1} & \cdots & b_{mn} \end{pmatrix}.$$

如果可以通过一系列初等行变换从 A 过渡到 B, 则称 A 和 B 是**行等价**的.

(i) 取一列整数 $1 \leq c_1 < \cdots < c_h \leq n$. 从 A (或 B) 删除第 $c_1, \ldots, c_h$ 列得到的矩阵记为 A' (或 B'). 说明若 A 和 B 行等价, 则 A' 和 B' 行等价.

(ii) 设 A 和 B 形如

$$A=\begin{pmatrix} 1 & & & x_1 \\ & \ddots & & \vdots \\ & & 1 & x_m \\ & & & \\ & & & \\ & & & \end{pmatrix},\quad B=\begin{pmatrix} 1 & & & y_1 \\ & \ddots & & \vdots \\ & & 1 & y_m \\ & & & \\ & & & \\ & & & \end{pmatrix},$$

其中 $x_1,\dots,x_m$ 和 $y_1,\dots,y_m$ 是给定的数, 而矩阵中留白部分为 0. 说明若 A 和 B 行等价, 则对所有 $1\le i\le m$ 皆有 $x_i=y_i$.

提示〉 将 A 和 B 视为 m 元线性方程组的增广矩阵, 解之.

(iii) 对于一般情形, 证明若 A 和 B 是行等价的简化行梯矩阵, 则 $A=B$.

提示〉 设 $A\ne B$. 从左而右比较每一列, 设第一个相异的列为第 j 列. 从 A 和 B 删除所有 j 之后的列, 同时也删除第 j 列之前所有不含主元的列, 得到的矩阵分别记为 A' 和 B'.

- ⋆ 论证第 j 列不可能包含主元.
- ⋆ 论证 A' 和 B' 必然是 (ii) 的形式. 配合 (i) 来推导 $A'=B'$, 从而导出矛盾.

2 预备知识

2.1 整数的算术 设 $x,y\in\mathbb{Z}$. 如果存在 $d\in\mathbb{Z}$ 使得 $y=xd$, 则称 x 整除 y, 记为 $x\mid y$, 否则记为 $x\nmid y$; 此时称 d 为 x 的因数或因子.

对于一族整数 $x_1,\dots,x_n$, 记其最小公倍数为

$$\operatorname{lcm}(x_1,\dots,x_n):=\min\left\{m\in\mathbb{Z}_{\geq 1}:\forall 1\leq i\leq n,\ x_i\mid m\right\};$$

若 $x_1,\dots,x_n$ 不全为零, 定义其最大公因数为

$$\gcd(x_1,\dots,x_n):=\max\left\{d\in\mathbb{Z}_{\geq 1}:\forall 1\leq i\leq n,\ d\mid x_i\right\}.$$

若 $x_1,\dots,x_n$ 的最大公因数为 1, 则称它们互素.

命题 2.1.1 (带余除法) 对于任意 $a,d\in\mathbb{Z}$, 若 $d\neq 0$, 则存在唯一的 $q,r\in\mathbb{Z}$ 使得 $0\leq r<|d|$ 而 $a=dq+r$.

证明 不妨假设 $d>0$. 考虑集合 $R:=\{a-dq:q\in\mathbb{Z}\}\cap\mathbb{Z}_{\geq 0}$. 它是由非负整数组成的非空集, 故有最小元素 r; 相应地 $a=dq+r$. 必有 $r<d$, 否则 $a=d(q+1)+(r-d)$ 将给出 $r-d\in R$ 使得 $0\leq r-d<r$, 与 r 的极小性质矛盾. 这就说明 q,r 的存在性.

至于唯一性, 设 $dq+r=dq'+r'$, 其中 $q,q'\in\mathbb{Z}$ 而 $0\leq r\leq r'<d$. 因为 $r'-r=d(q-q')$ 既被 d 整除, 又有 $0\leq r'-r\leq r'<d$, 唯一可能是 $r'=r$. 证毕. □

根据唯一性, 带除法中的余数 $r=0$ 当且仅当 $d\mid a$.

对于一族整数 $x_1,\dots,x_n$, 定义 $\mathbb{Z}$ 的子集

$$\mathbb{Z}x_1+\cdots+\mathbb{Z}x_n:=\left\{\sum_{i=1}^{n}a_ix_i\in\mathbb{Z}:a_1,\dots,a_n\in\mathbb{Z}\right\}.$$

特别地, 定义 $x\mathbb{Z}:=\{xd:d\in\mathbb{Z}\}$.

引理 2.1.2 设 I 为 $\mathbb{Z}$ 的非空子集, 满足以下性质

$$x,y\in I\implies x+y\in I,\quad a\in\mathbb{Z},\ x\in I\implies ax\in I.$$

此时存在唯一的 $g\in\mathbb{Z}_{\geq 0}$ 使得 $I=g\mathbb{Z}$.

证明 不妨设 $I\neq\{0\}$, 否则唯一取法是 $g=0$. 注意到 $g\in I\iff -g\in I$. 取 g 为 I 中的最小正整数. 包含关系 $I\supset g\mathbb{Z}$ 是明白的. 至于 $\subset$, 设 $m\in I$, 用带余除法表为 $m=gq+r$, 其中 $0\leq r<g$. 于是 $r=m-gq$ 必为 0, 否则将给出 I 中比 g 更小的正整数, 矛盾.

最后, 如果正整数 g, g' 满足 $g\mathbb{Z} = g'\mathbb{Z}$, 则 $g' \mid g$ 而 $g \mid g'$, 唯一可能是 $g = g'$. □

命题 2.1.3 (É. Bézout) *设 $x_1, \dots, x_n$ 为不全为零的整数, 则*

$$\mathbb{Z}x_1 + \cdots + \mathbb{Z}x_n = \gcd(x_1, \dots, x_n)\mathbb{Z}.$$

证明 取引理 2.1.2 之 $g \in \mathbb{Z}_{\geq 1}$ 使得 $\mathbb{Z}x_1 + \cdots + \mathbb{Z}x_n = g\mathbb{Z}$. 注意到对于任意正整数 d, 我们有

$$(\forall 1 \leq i \leq n,\ d \mid x_i) \iff (\forall x \in \mathbb{Z}x_1 + \cdots + \mathbb{Z}x_n,\ d \mid x) \iff d \mid g.$$

这就表明 $g = \gcd(x_1, \dots, x_n)$. □

以上两条结果也说明我们可以合理地定义 $\gcd(0, \dots, 0) = 0$.

定义 2.1.4 *设 $p \in \mathbb{Z} \smallsetminus \{0, \pm 1\}$. 如果 p 除了 ± 1 和 $\pm p$ 之外没有别的因数, 则称 p 为* **素元**. *满足 $p \in \mathbb{Z}_{\geq 1}$ 的素元 p 称为* **素数**.

命题 2.1.5 (Euclid) *设 p 为素元, 若 $a, b \in \mathbb{Z}$ 使得 $p \mid ab$, 则必有 $p \mid a$ 或 $p \mid b$.*

证明 设 $p \nmid a$, 则因为 p 是素元, a 和 p 必然互素. 命题 2.1.3 蕴涵存在 $x, y \in \mathbb{Z}$ 使得 $1 = px + ay$. 于是 $p \mid pxb + aby = b$. □

定理 2.1.6 (算术基本定理) *任何非零整数 $n \in \mathbb{Z}$ 都有素因子分解*

$$n = \pm p_1^{a_1} \cdots p_r^{a_r},$$

其中 $r \in \mathbb{Z}_{\geq 0}$ (当 $r = 0$ 时右式规定为 ± 1), $p_1, \dots, p_r$ 是素数, $a_1, \dots, a_r \in \mathbb{Z}_{\geq 1}$, 而且此分解不论顺序是唯一的.

证明 对 $|n|$ 递归地操作. 如果 $|n| = 1$, 则 $n = \pm 1$ 已是所求的分解 ($r = 0$), 否则存在素数 p 使得 $p \mid n$, 对 $n' := n/p$ 继续操作, 最终可以将 $\pm n$ 写成若干个素数的积, 容许重复.

至于唯一性, 设 $p_1^{a_1} \cdots p_r^{a_r} = q_1^{b_1} \cdots q_s^{b_s}$, 其中 $p_1, \dots, p_r$ 是相异素数, $q_1, \dots, q_s$ 也是相异素数, 而 $a_i, b_j \in \mathbb{Z}_{\geq 1}$. 注意到 $r = 0$ 当且仅当 $s = 0$, 此时两边都是 1. 以下设 $r, s \geq 1$.

由于 $p_1 \mid q_1^{b_1} \cdots q_s^{b_s}$, 命题 2.1.5 蕴涵存在 $1 \leq j \leq s$ 使得 $p_1 \mid q_j$; 这进一步蕴涵 $p_1 = q_j$. 重排下标后不妨假设 $p_1 = q_1$, 必要时交换等号两边, 不妨假设 $a_1 \leq b_1$. 于是

$$p_2^{a_2} \cdots p_r^{a_r} = p_1^{b_1 - a_1} q_2^{b_2} \cdots q_s^{b_s}.$$

再次应用命题 2.1.5 可见 p_1 不整除左式, 故 $b_1 = a_1$. 继续递归地论证可得分解的唯一性. □

因此对于任何素数 p, 我们有 $p \nmid n$ 当且仅当 p 在 n 的素因子分解中出现, 相应的指数 $a \in \mathbb{Z}_{\geq 1}$ 由以下性质唯一确定: $p^a \mid n$ 而 $p^{a+1} \nmid n$.

推论 2.1.7 如果 $n = \pm\prod_{i=1}^r p_i^{a_i}$, $m = \pm\prod_{i=1}^r p_i^{b_i}$, 其中 $p_1, \dots, p_r$ 是相异素数而 $a_i, b_i \in \mathbb{Z}_{\geq 0}$, 则

$$\gcd(n, m) = \prod_{i=1}^r p_i^{\min\{a_i, b_i\}}, \quad \operatorname{lcm}(n, m) = \prod_{i=1}^r p_i^{\max\{a_i, b_i\}}.$$

任意多个数的 gcd 和 lcm 也有类似处理.

素数列 $2, 3, 5, 7, 11, \dots$ 是数论关切的基本对象; 这方面第一个重要的结果如下.

定理 2.1.8 (Euclid) 素数的个数无穷.

证明 给定素数 $p_1 < \cdots < p_n$, 考虑

$$m := p_1 \cdots p_n + 1,$$

则 $m > 1$ 不被 $p_1, \dots, p_n$ 中任一个素数整除. 考虑 m 的素因子分解式以得到新的素数. □

定义 2.1.9 (同余关系) 设 $N \in \mathbb{Z}$. 称 $a, b \in \mathbb{Z}$ 是 $\bmod N$ **同余**的, 如果 $N \mid a - b$; 此关系也写作

$$a \equiv b \pmod{N}.$$

显然 $a \equiv b \pmod{N}$ 连同 $b \equiv c \pmod{N}$ 蕴涵 $a \equiv c \pmod{N}$. 当 $N \neq 1$ 时, 带余除法表明 $a \equiv b \pmod{N}$ 当且仅当 a 和 b 除以 N 有相同的余数. 同样明白的是

$$a \equiv b \pmod{N} \implies \gcd(a, N) = \gcd(b, N);$$

特别地, 如果 $b > a \geq 1$ 而 b 用带余除法表作 $b = aq + r$, 其中 $0 \leq r < a$, 则

$$\gcd(a, b) = \gcd(r, a) \quad \begin{cases} = a, & \text{若 } r = 0 \\ \text{继续作带余除法}, & \text{若 } r \neq 0. \end{cases}$$

这是以辗转相除法求最大公因数的实质.

练习 2.1.10 证明若 $x \equiv x' \pmod{N}$, $y \equiv y' \pmod{N}$, 则有

$$x + y \equiv x' + y' \pmod{N}, \quad xy \equiv x'y' \pmod{N}.$$

作为同余等式的初步例子, 以下是称为 **Fermat 小定理**的著名结果. 它有简单的群

论诠释, 这里给出的则是初等的迂回论证.

定理 2.1.11 (P. Fermat) *设 p 为素数, 则对于所有 $x \in \mathbb{Z}$ 都有*

$$\gcd(p, x) = 1 \implies x^{p-1} \equiv 1 \pmod{p}. \tag{2.1}$$

证明 设 $p \nmid x$. 根据命题 2.1.3, 方程 $xy + pz = 1$ 有整数解 (y, z); 换言之存在 $y \in \mathbb{Z}$ 使得 $xy \equiv 1 \pmod{p}$. 现在考虑 $\{kx : k \in \mathbb{Z}\}$. 如果 $k_1 x \equiv k_2 x \pmod{p}$, 两边同乘以 y 并利用练习 2.1.10 可得 $k_1 \equiv k_2 \pmod{p}$. 另一方面, 素数的性质确保 $p \nmid k$ 时 $kx \not\equiv 0 \pmod{p}$. 这一切表明

$$kx, \quad k = 1, \ldots, p-1$$

两两不同余, 而且皆不 $\equiv 0 \pmod{p}$. 再次利用练习 2.1.10 可得

$$x^{p-1}(p-1)! = \underbrace{x \cdots ((p-1)x)}_{p-1 \text{ 项}} \equiv \underbrace{1 \cdots (p-1)}_{p-1 \text{ 项}} \equiv (p-1)! \pmod{N}.$$

因为 $p \nmid (p-1)!$, 仿照之前办法可从同余式两边消去 $(p-1)!$, 此即所求. □

定理 2.1.11 的逆命题并不成立. 满足 (2.1) 而非素数的正整数 p 称为 Carmichael 数, 其个数无穷; 前五个 Carmichael 数是 $561, 1105, 1729, 2465, 2821$. 尽管存在这些反例, 性质 (2.1) 仍然在一些概率素性检测算法中扮演要角.

定义 2.1.12 (Euler 函数) *设 $n \in \mathbb{Z}_{\geq 1}$, 定义 $\varphi(n)$ 为 $\leq n$ 而与 n 互素的正整数个数.*

练习 2.1.13 验证 Euler 函数 φ 的以下性质.

(i) 若 $n = \prod_{i=1}^{r} p_1^{a_1} \cdots p_r^{a_r}$ 是素因子分解, 其中 $a_i \in \mathbb{Z}_{\geq 1}$, 则

$$\varphi(n) = \prod_{i=1}^{r} \left(p_i^{a_i} - p_i^{a_i - 1}\right) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

(ii) 若 $n, m \in \mathbb{Z}_{\geq 1}$ 互素, 则 $\varphi(nm) = \varphi(n)\varphi(m)$.

(iii) 证明 $\sum_{\substack{d \geq 1 \\ d \mid n}} \varphi(d) = n$.

(iv) 证明 $\lim_{n \to +\infty} \varphi(n) = +\infty$.

2.2 集合与映射 近代数学的大厦以集合论为基石. 这套语言对于代数结构的研究尤其必要.

根据集合论创始人 G. Cantor 在 1895 年的界说, “集合意谓吾人感知或思想中一些确定的, 并且相互区别的对象汇集而成的整体, 这些对象称为该集合的元素.” 这段文字至少包含两条教益. 第一, 所论的数学对象是确定的, 当 x, y 给定, $x = y$ 或 $x \neq y$ 两者必居其一; 第二, 集合由其全体元素确定. 符号 $a \in A$ 意谓 a 是集合 A 的元素, 而 $a \notin A$ 意谓 $\neg(a \in A)$. 从属关系 $\in$ 是集合论语言的基本构件. 两个集合 A, B 相等当且仅当对于所有 x, 我们都有 $x \in A \iff x \in B$.

集合的元素既可以用枚举法 $\{x, y, \ldots\}$ 来表示, 或者用

$$\{x : x \text{ 满足 } \mathcal{P}\}, \quad \mathcal{P}: \text{ 某个给定的性质.}$$

的方式来描述; 但在后一情形必须小心: x 本身必须限制在某个已有的集合中, 否则可能产生矛盾.

例 2.2.1 著名的 Russell 悖论便是考虑了

$$\{\text{集合 } x : x \notin x\},$$

倘若这确实是集合, 记之为 R, 则 $R \in R$ 或 $R \notin R$ 俱不成. 根据现代集合论的观点, 问题在于所有集合的总体并不构成一个集合, 所以 R 的取法违背公理.

例 2.2.2 空集 $\varnothing$ 有一个直接然而稍微费解的刻画: $\varnothing = \{a \in A : a \neq a\}$, 其中 A 是任意集合. 从给定的集合 A 出发, $\{A\}$ 也是集合, $A \in \{A\}$ 而 $A \neq \{A\}$; 最简单的范例是 $\{\varnothing\}$, 无中生有!

今后视 “映射” 与 “函数” 为同义词. 从集合 A 到集合 B 的映射写作 $f : A \to B$ 或 $A \xrightarrow{f} B$ 的形式. 符号 $f : a \mapsto b$ 或 $a \xmapsto{f} b$ 代表 $f(a) = b$, 以此区别集合及其元素在映射下的像.

谨介绍关于映射的几则标准术语和符号.

术语	定义条件	符号
单射 (或**嵌入**)	$a \neq a' \implies f(a) \neq f(a')$	$f : A \hookrightarrow B$
满射	对每个 $b \in B$ 都存在 $a \in A$ 使得 $f(a) = b$	$f : A \twoheadrightarrow B$
双射 (或**一一对应**)	既单又满	$f : A \xrightarrow{1:1} B$

给定映射 $A \xrightarrow{f} B$ 和 $B \xrightarrow{g} C$, 其合成记为 $g \circ f$, 简记为 gf.

约定 2.2.3 图解映射的合成是一个特别方便的技巧, 其中将集合标作图的节点, 映射标作箭头; 如果图表中的映射 (即箭头) 在合成运算下殊途同归, 则称之为**交换图表**. 从以下图例应该可以看得明白:

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ & \searrow^{h} & \downarrow{\scriptstyle g} \\ & & C \end{array} \quad \text{交换} \iff gf = h,$$

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle u}\downarrow & & \downarrow{\scriptstyle g} \\ C & \xrightarrow[v]{} & D \end{array} \quad \text{交换} \iff vu = gf.$$

集合之间的常用操作罗列如下.

⋆ 设 A, B 为集合, 它们的**并**和**交**分别记为

$$A \cup B := \big\{x : x \in A \text{ 或 } x \in B\big\}, \quad A \cap B := \{x : x \in A \text{ 而且 } x \in B\}.$$

我们略而不谈的集合论公理足以确保定义合理. 推而广之, 对于一列集合 $A_1, \dots, A_n$, 同样可以定义它们的并 $\bigcup_{i=1}^n A_i$ 和交 $\bigcap_{i=1}^n A_i$.

⋆ **差集**的记法是

$$A \smallsetminus B := \{a \in A : a \notin B\}.$$

⋆ 符号 $A \subset B$ 意谓 A 是 B 的子集, 容许相等. 因此 $A = B$ 当且仅当 $A \subset B$ 而且 $B \subset A$. 严格包含关系写作 $A \subsetneq B$.

⋆ 定义 A 和 B 的 **Cartesius 积** (简称为**积**) 为

$$A \times B = \{(a, b) : a \in A,\ b \in B\},$$

其中 (a, b) 代表由 a 和 b 构成的有序对, 当 $a \neq b$ 时 $(a, b) \neq (b, a)$.

⋆ 推而广之, 对于一列集合 $A_1, A_2, \dots$, 可以定义其积 $\prod_{i=1,2,\dots} A_i$, 或写作 $A_1 \times A_2 \times \cdots$, 其元素是 n 元组 $a = (a_1, a_2, \dots)$, 计顺序, 使得对每个 i 都有 $a_i \in A_i$. 这些元素也表作 $a = (a_i)_i$ 的形式, 其中 a_i 称为 a 的第 i 个分量.

尽管 $A_1 \times (A_2 \times A_3)$, $A_1 \times A_2 \times A_3$ 和 $(A_1 \times A_2) \times A_3$ 严格来说是不同的集合, 但其元素间有自然的一一对应

$$\begin{array}{ccccc} A_1 \times (A_2 \times A_3) & \xleftrightarrow{1:1} & A_1 \times A_2 \times A_3 & \xleftrightarrow{1:1} & (A_1 \times A_2) \times A_3 \\ \cup & & \cup & & \cup \\ (a_1, (a_2, a_3)) & \longleftarrow\!\shortmid & (a_1, a_2, a_3) & \longmapsto & ((a_1, a_2), a_3). \end{array}$$

在此意义下, 集合的积满足结合律.

⋆ 设 A 为集合而 $n \in \mathbb{Z}_{\geq 1}$, 记 $A^n := \underbrace{A \times \cdots \times A}_{n\text{ 份}}$. 例如 $\mathbb{R}^2$ 无非是解析几何学探讨的平面, $\mathbb{R}^3$ 则为空间, 前提是平面或空间已配备坐标系.

⋆ 若集合 $A_1, A_2, \ldots$ 两两无交, 则它们的并也标作 $A_1 \sqcup A_2 \sqcup \cdots$ 的形式, 以强调这是**无交并**.

对于任意集合 $A_1, A_2, \ldots$, 我们有时也 "外在地" 构造无交并 $A_1 \sqcup A_2 \sqcup \cdots$, 想法是取 $A_1, A_2, \ldots$ 的适当 "副本" 迫使其两两无交, 再取并. 比如我们可以将 $A_1, A_2, \ldots$ 都嵌入为 $\left(\bigcup_{i=1,2,\ldots} A_i\right) \times \{1, 2, \ldots\}$ 的子集, 其中 A_i 嵌入第二个坐标等于 i 的部分, 然后取这些副本的并.

这里产生了一个问题: 无交并的外在构造在多大程度上依赖于副本的取法? 给定 $A_1, A_2, \ldots$ 如上, 设 $\mathcal{A}$ 和 $\mathcal{A}'$ 是无交并的两种取法, 对应的副本嵌入记为 $\iota_i : A_i \hookrightarrow \mathcal{A}$ 和 $\iota_i' : A_i \hookrightarrow \mathcal{A}'$, 其中 $i = 1, 2, \ldots$. 那么存在唯一的双射 φ 使得下图对 $i = 1, 2, \ldots$ 皆交换:

$$\begin{array}{ccc} \mathcal{A} & \xrightarrow[1:1]{\varphi} & \mathcal{A}' \\ & {\scriptstyle \iota_i} \nwarrow \quad \nearrow {\scriptstyle \iota_i'} & \\ & A_i & \end{array}$$

换言之, $\varphi\iota_i = \iota_i'$ 对所有 i 成立. 诚然, φ 能且仅能定义为 $\varphi(x) = \iota_i(a)$, 如果 i 和 $a \in A_i$ 使 $x = \iota_i(a)$. 正是这些唯一的双射确保我们能无歧义地谈论无交并.

⋆ 从集合 A 到 B 的所有映射构成一个集合, 记为

$$B^A := \{\text{映射 } f : A \to B\};$$

当 $A = \varnothing$ 时规定 $B^A = \{\varnothing\}$, 缘由可见稍后注记 2.2.5 的说明. 符号 B^A 的道理何在? 不妨考虑 $n \in \mathbb{Z}_{\geq 1}$ 和 $A = \{0, \ldots, n-1\}$, 这时有自然的一一对应

$$\begin{aligned} B^{\{0,\ldots,n-1\}} &\longleftrightarrow B^n \\ [f : \{0, \ldots, n-1\} \to B] &\longmapsto (f(i-1))_{i=1}^n . \end{aligned}$$

再考虑特例 $B = \{0, 1\}$, 这时有自然的一一对应

$$\begin{aligned} \{0,1\}^A &\xleftrightarrow{1:1} P(A) := \{A' \subset A : \text{子集}\} \\ f &\longmapsto \{a \in A : f(a) = 1\} . \end{aligned}$$

右式的 $P(A)$ 称为 A 的**幂集**; 注意到 $P(\varnothing) = \{\varnothing\}$.

记有任意限集 S 的元素个数为 $|S|$. 显然 $|A\times B|=|A|\cdot|B|$, $|A\sqcup B|=|A|+|B|$, 而 $\left|B^A\right|=|B|^{|A|}$ (此处约定 $0^0=1$), 前提是 A, B 都是有限集. 在关于 $\left|B^A\right|$ 的描述中取特例 $B=\{0,1\}$ 可见 $|P(A)|=2^{|A|}$.

以上等式也适用于无穷集, 问题在于如何为无穷集 S 定义其大小 $|S|$, 称为 S 的**基数**. 我们将待适当时机回到这个问题.

注记 2.2.4 关于并, 交, 无交并和积的定义不仅可用于一列集合 $A_1,A_2,\ldots$, 还可以进一步推广到任意一族集合 $(A_i)_{i\in I}$; 符号中的 I 是给定的集合 (称为指标集), 而对每个 $i\in I$ 都给定了集合 A_i. 对之可以依样画葫芦地定义

$$\begin{aligned}&\text{并 } \textstyle\bigcup_{i\in I}A_i, && \text{交 } \textstyle\bigcap_{i\in I}A_i, \quad (I\neq\varnothing),\\ &\text{无交并 } \textstyle\bigsqcup_{i\in I}A_i, && \text{积 } \textstyle\prod_{i\in I}A_i.\end{aligned}$$

这里我们规定当 $I=\varnothing$ 时, 相应的并与无交并都是 $\varnothing$, 而积是 $\{\varnothing\}$. 请读者思考 $I=\varnothing$ 时为何不定义 $\bigcap_{i\in I}A_i$. 提示: 交的定义要求对于任意集合 x, 我们有

$$x\in\bigcap_{i\in I}A_i \iff \forall i\in I,\ x\in A_i.$$

注记 2.2.5 集合论建立在公理系统的基础上. 这是数学的黑箱, 虽然与大部分应用无关, 这里不妨多说几句. 相关参考书籍包括但不限于 [3].

公理集合论当且的主流是 Zermelo–Fraenkel 体系, 其视角下的一切数学对象都是集合; 特别地, 集合的元素仍然是集合, 所以他们的集合论里没有 “原子”. 尽管乍看之下有些古怪, 由集合, 从属关系 $\in$ 和 Zermelo–Fraenkel 提出的几个简单公理出发, 竟足以撑起数学的基础, 即便从后见之明也是令人惊叹的.

- ⋆ 举例明之, 如何将积集 $A\times B$ 定义中的 (a,b) 化约为集合论的基本构件? 集合论的公理告诉我们如何对 $a\in A$ 和 $b\in B$ 构造并集 $\{a,b\}$, 但它无法区别顺序. 为了用集合论的语言描述顺序, 黑箱里的构造其实是

  $$(a,b):=\{\{a\},\{a,b\}\};$$

  而 (a,b,c) 等等的构造准此可知.

- ⋆ 其次, 如何阐释映射 $f:A\to B$? 办法是将映射 f 视同它的函数图形

  $$\Gamma:=\{(a,b)\in A\times B : b=f(a)\}.$$

  为了使子集 $\Gamma\subset A\times B$ 成为某映射的函数图形, 充要条件是对每个 $a\in A$, 存在唯一的 $b\in B$ 使得 $(a,b)\in\Gamma$. 这就使得 B^A 成为 $P(A\times B)$ 的子集. 如果取

$A=\varnothing$, 则 $A\times B=\varnothing$, $P(A\times B)=\{\varnothing\}$, 而 $\varnothing$ 本身平凡地满足关于函数图形的条件, 这就解释了 $B^{\varnothing}=\{\varnothing\}$ 的规定.

由于 Zermelo–Fraenkel 公理集合论确实有益于构筑一套简洁牢固的形式体系, 我们也依教奉行. 在随后的内容中, 不得不打开集合论黑箱的场合是很少的.

2.3 关于映射的进一步定义

下述定义尽管是形式化的, 但对于厘清相关概念将有切实的帮助.

任意集合 A 到自身的恒等映射 $a\mapsto a$ 记为 id_A, 或简记为 id. 显然地, 对于任意映射 $f:A\to B$ 都有

$$f\circ\mathrm{id}_A=f=\mathrm{id}_B\circ f.$$

双射 f 的逆映射记为 $f^{-1}:B\to A$. 逆映射的概念还有进一步的推广.

定义 2.3.1 *考虑一对映射 $A\underset{g}{\overset{f}{\rightleftarrows}}B$. 若 $gf=\mathrm{id}_A$, 则我们称 g 是 f 的***左逆***, 而 f 是 g 的***右逆***. 有左逆 (或右逆) 的映射称为是左可逆 (或右可逆) 映射.*

练习 2.3.2 说明集合之间的映射 f 左可逆当且仅当 f 单; 右可逆当且仅当 f 满. 说明当 f 不是双射, 则左逆或右逆一般不唯一.

现在可以重新梳理逆映射的概念.

定义 2.3.3 *如果映射 f 左, 右皆可逆, 则称 f 是***可逆***映射. 此时存在唯一的 $f^{-1}:B\to A$ 使得 $f^{-1}\circ f=\mathrm{id}_A$ 而 $f\circ f^{-1}=\mathrm{id}_B$.*

定义的后半段需要论证, 尽管这毫不困难. 首先设 f 可逆, g_L 为其左逆而 g_R 为其右逆. 映射合成满足结合律, 所以

$$g_R=\mathrm{id}_A\circ g_R=(g_L\circ f)\circ g_R=g_L\circ(f\circ g_R)=g_L\circ\mathrm{id}_B=g_L.$$

这就说明此时 f 有唯一的左逆, 它同时也是唯一的右逆, 可以合理地记为 f^{-1}.

练习 2.3.2 表明可逆映射无非是双射, 此时的 f^{-1} 无非是先前介绍的逆映射. 以上论证的特点在于它仅用到映射合成的结合律和 id 的性质, 毫不涉及集合的元素.

定义 2.3.4 *对于映射 $f:A\to B$ 和任意子集 $A'\subset A$, 记 A' 对 f 的像为 $f(A')$, 记 $f|_{A'}:A'\to B$ 为 f 在 A' 上的限制; 我们也记 $\mathrm{im}(f):=f(A)$.*

定义 2.3.5 *对于映射 $f:A\to B$ 和任意子集 $B'\subset B$, 记*

$$f^{-1}(B'):=\{a\in A:f(a)\in B'\},$$

*称为 B' 对 f 的***原像***或***逆像***. 若 $b\in B$, 记*

$$f^{-1}(b):=f^{-1}(\{b\})=\{a\in A:f(a)=b\}.$$

在和几何学相关的一些场景中, 大家偏好将 A 设想为竖在 B 上的空间, 而 f 类似于投影; 职是之故, $f^{-1}(b)$ 有时也称为 b 上的**纤维**. 相应地, A 分解为纤维的无交并

$$A = \bigsqcup_{b\in B} f^{-1}(a).$$

解方程可以看作是求映射纤维的问题. 回到 n 元线性方程组 (1.1) 具体地考察, 依然假设是在 $\mathbb{C}$ 上求解. 构造积集 $\mathbb{C}^n$ 和 $\mathbb{C}^m$, 并且定义映射

$$\begin{aligned} T : \mathbb{C}^n &\to \mathbb{C}^m \\ (x_i)_{i=1}^n &\mapsto \left(\sum_{i=1}^n a_{ij}x_i\right)_{j=1}^m . \end{aligned}$$

线性方程组的解集因而等于 $T^{-1}(b_1,\dots,b_m)$. 注意到 T 只依赖 (1.1) 的系数矩阵; 一旦系数矩阵给定, 求解方程组就相当于确定 T 的纤维.

当然, 问题不会因为抽象到这般程度就而自动解决. 在以上提纯过程中, 尚未用到的是映射 T 的特殊性质. 进一步的剖析将涉及向量空间的概念, 这是 §3 的任务.

2.4 二元关系

数学中经常需要谈论两个对象之间的关系, 比如说两个 n 元线性方程组是否同解. 按照惯例, 我们用集合论的语言来进行严格的表述.

定义 2.4.1 集合 A 和 B 之间的**二元关系**定义为 $A\times B$ 的子集. 对于二元关系 $R\subset A\times B$, 我们以符号 aRb 代表 $(a,b)\in R$. 当 $A=B$ 时, 我们也称 R 为 A 上的二元关系.

我们称关系 A 上的二元关系 R 具有

▷ **反身性** 如果所有 $a\in A$ 都满足 aRa;

▷ **传递性** 如果 aRb 且 bRc 蕴涵 aRc;

▷ **对称性** 如果 aRb 蕴涵 bRa;

▷ **反称性** 如果 aRb 且 bRa 蕴涵 $a=b$.

以下介绍最常用的两类二元关系: 偏序和等价.

最为人熟知的二元关系是比大小, 偏序关系是它的推广.

定义 2.4.2 集合 A 上的二元关系 $\leq$ 若满足反身性, 传递性和反称性, 则称资料 $(A,\leq)$ 为**偏序集**. 如果对于偏序集中的任两个元素 a,a' 皆可比大小 (换言之, $a\leq a'$ 或 $a'\leq a$ 必有一者成立), 则称此偏序集为**全序集**.

符号 $a<b$ 意指 $a\leq b$ 而且 $a\neq b$.

举例明之, 寻常的大小关系 $\leq$ 使得 $(\mathbb{Z},\leq)$, $(\mathbb{Q},\leq)$ 和 $(\mathbb{R},\leq)$ 都成为全序集. 设 A 为集合, 则幂集 $P(A)$ 对集合的包含关系 $\subset$ 构成偏序集, 然而非全序集. 正整数相对于整除关系也是偏序集然而非全序集的例子.

如果偏序集中的元素 m 满足 $x \geq m \implies x = m$, 则称 m 为**极大元**; 类似地定义**极小元**. 注意到偏序集未必有极大或极小元, 即使有, 它们往往也不唯一.

定义 2.4.3 *集合 A 上的二元关系 $\sim$ 若满足反身性, 传递性和对称性, 则称 $\sim$ 为 A 上的***等价关系***.*

最严格的等价关系是相等, 对应到对角子集 $\{(a,a) : a \in A\} \subset A \times A$. 顾名思义, 由给定的等价关系 $\sim$ 相联系的元素在某种意义下可以设想为相同的. 为了说清这点, 我们引进等价类的概念.

给定 A 上的等价关系 $\sim$. 形如 $[a] := \{a' \in A : a' \sim a\} \subset A$, 其中 $a \in A$ 的子集称为 A 中的**等价类**; 这时我们称 a 是等价类 $[a]$ 的一个**代表元**. 以下性质是容易的.

- $\star$ 任何 $a \in A$ 都包含于某个等价类: 取 $a \in [a]$ 便是.
- $\star$ 若 $a \sim a'$ 则 $[a] = [a']$: 这是传递性的直接结论, 留给读者自证.
- $\star$ 任两个等价类 $[a]$ 和 $[a']$ 作为 A 的子集或者无交, 或者相等. 这是因为若 $b \in [a] \cap [a']$, 则从 $a' \sim b \sim a$ 和上一步立得 $a \sim a'$.

这些性质蕴涵 A 是其中所有等价类的无交并.

定义 2.4.4 *设 $\sim$ 为集合 A 上的等价关系. 令 $A/\sim$ 为 A 中所有对 $\sim$ 的等价类构成的集合, 称为 A 对 $\sim$ 的***商集***. 映射*

$$\begin{aligned} q : A &\to A/\sim \\ a &\mapsto [a] \end{aligned}$$

*称为相应的***商映射***, 它显然满.*

命题 2.4.5 *设 $\sim$ 为集合 A 上的等价关系, $f : A \to B$ 为满足 $a \sim a' \implies f(a) = f(a')$ 的映射, 则存在唯一的映射 $\bar{f} : (A/\sim) \to B$ 使得 $\bar{f} \circ q = f$.*

证明 显然 $\bar{f} : q(a) = [a] \mapsto f(a)$ 确实给出从 $A/\sim$ 到 B 的映射: 它仅依赖等价类 $[a]$ 而非 a 的选取. 另一方面, 满足 $\bar{f} \circ q = f$ 的 $\bar{f}$ 也只能这般定义. □

练习 2.4.6 固定 $n, m \in \mathbb{Z}_{\geq 1}$. 考虑所有形如

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ & \ddots & \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$$

的矩阵构成的集合 $M_{m\times n}$, 其中要求 a_{ij} 属于 $\mathbb{C}$ (或者属于任何一个选定的域, 这不影响论证). 证明 §1 习题中介绍的行等价是 $M_{m\times n}$ 上的等价关系; 在 Gauss–Jordan 消元法的讨论中已经默认了这一则事实. 进一步用该节习题中的结果说明每个行等价类中存在唯一简化行梯矩阵.

例 2.4.7 考虑空间 $\mathbb{R}^3$. 在扣掉原点 $(0,0,0)$ 得到的子集 $\mathbb{R}^3\smallsetminus\{(0,0,0)\}$ 上定义二元关系

$$(x,y,z)\sim(x',y',z') \iff \exists t\in\mathbb{R},\ t\neq 0,\ (x',y',z')=(tx,ty,tz).$$

容易看出它是等价关系. 对应的商集有直观的描述:

$$\begin{aligned}\left(\mathbb{R}^3\smallsetminus\{(0,0,0)\}\right)/\sim &\xrightarrow{1:1} \left\{\ell\subset\mathbb{R}^3 : \text{过原点的直线}\right\}\\ [(x,y,z)] &\longmapsto \text{过 } (x,y,z) \text{ 和原点的唯一直线}.\end{aligned}$$

如果在 $\sim$ 的定义中以 $t>0$ 代替 $t\neq 0$, 则对应的商集和过原点的射线一一对应.

例 2.4.8 设 $N\in\mathbb{Z}$. 定义 2.1.9 定义的同余关系 $x\equiv y \pmod N$ 是 $\mathbb{Z}$ 上的等价关系. 相应的商集记为 $\mathbb{Z}/N\mathbb{Z}$, 有时也简记为 $\mathbb{Z}/N$. 包含 $a\in\mathbb{Z}$ 的等价类记为 $a+N\mathbb{Z}$. 以下设 $N\geq 1$.

当 $N\in\mathbb{Z}_{\geq 1}$ 固定, 对 a 取除以 N 的余数 $R_N(a)\in\{0,\dots,N-1\}$, 它仅依赖于 $a+N\mathbb{Z}$, 由此得到映射 $\overline{R_N}:\mathbb{Z}/N\mathbb{Z}\to\{0,\dots,N-1\}$. 这是双射. 所以 $\bmod N$ 的同余类可以通过 $\overline{R_N}$ 视同 $\{0,\dots,N-1\}$ 的元素; 当然余数的范围也可以改为 $\{1,\dots,N\}$ 等等. 取余数所呈现的经常是一种虚假的具体感; 多数场合下, 直接操作同余类更为简便.

命题 2.4.9 对于任意映射 $f:A\to B$, 在 A 上定义二元关系

$$a\sim_f a' \iff f(a)=f(a').$$

则 $\sim_f$ 是等价关系, 而且命题 2.4.5 给出双射 $\bar f:A\to\mathrm{im}(f)$.

证明 关于等价关系的验证是直截了当的. 命题 2.4.5 的前提对 f 和 $\sim_f$ 也显然成立, 由此得到 $\bar f: A/\sim_f\to B$ 使得 $\bar f([a])=f(a)$. 显然 $\mathrm{im}(\bar f)=\mathrm{im}(f)$. 如果 $\bar f([a])=\bar f([a'])$, 则 $f(a)=f(a')$, 从而 $[a]=[a']$. 这说明 f 也是单的. 证毕. □

以上命题虽然简单, 却有值得一提的内涵. 它说明尽管映射的像集 $\mathrm{im}(f)\subset B$ 相对于 A 是某种外在之物, 却可以从 A 透过等价关系内在地构造,. 往后探讨环, 向量空间等构造时, 这一主题还会反复回响.

2.5 环和域 自从 20 世纪初以降, 数学的目光开始从具体问题转向抽象集合上的抽象运算. 集合, 运算连同这些运算具备的基本性质, 一道构成了代数学中所谓的 "结构". 大而化之地说, 集合 S 上的 n 元运算 ($n \in \mathbb{Z}_{\geq 1}$) 指的无非是一个映射 $S^n \to S$; 譬如加法 $+$ 和乘法 $\cdot$ 都是 $\mathbb{Z}$ 上的二元运算. 对于一般的二元运算

$$\star : S \times S \to S,$$

习惯的作法是将 $\star(s_1, s_2)$ 写成 $s_1 \star s_2$.

行将介绍的环是代数结构的一个例子. 环是配备加法 $+$ 和乘法 $\cdot$ 两种二元运算的集合, 而且乘法和加法分别具有相应的幺元 (又称单位元, 加法情形也称零元). 细说如下.

定义 2.5.1 **环**是指资料 $(R, +, \cdot, 0_R, 1_R)$, 其中 R 是集合, $0_R, 1_R \in R$, 而 $+ : R \times R \to R$ 和 $\cdot : R \times R \to R$ 都是二元运算, 使得以下条件成立.

1. 加法运算满足以下条件:
   - ▷ **结合律** $(x + y) + z = x + (y + z)$;
   - ▷ **幺元性质** $x + 0_R = x = 0_R + x$.
   - ▷ **交换律** $x + y = y + x$.
   - ▷ **加法逆元** 对所有 x 皆存在 $-x$ 使得 $x + (-x) = 0_R$.
2. 乘法运算 $x \cdot y$ 也简写为 xy, 它满足以下条件:
   - ▷ **结合律** $(xy)z = x(yz)$;
   - ▷ **幺元性质** $x \cdot 1_R = x = 1_R \cdot x$;
3. 乘法对加法满足
   - ▷ **分配律** $(x + y)z = xz + yz, \quad z(x + y) = zx + zy$.

其中 x, y, z 代表 R 中的任意元素. 不致混淆时, 我们也把 0_R, 1_R 简记为 0, 1, 并以 R 总括资料 $(R, +, \cdot, 0_R, 1_R)$. 我们也将 $x + (-y)$ 写作 $x - y$.

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

以下介绍的几条运算性质都是定义的简单结论.

- ⋆ 结合律确保任意多个元素的加法和乘法可以不带括号地写作 $x + y + z$, xyz 等等.
- ⋆ 加法和乘法幺元都由各自的幺元性质唯一确定. 设若 0_R 和 $0'_R$ 皆满足加法幺元性质, 1_R 和 $1'_R$ 皆满足乘法幺元性质, 则

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

所以资料 $(R,+,\cdot,0_R,1_R)$ 中的 0_R 和 1_R 可以略去, 要求对加法或乘法都存在满足幺元性质的元素即可.

- ⋆ 加法满足消去律: 若 $x+y=x'+y$, 等式两边同加 $-y$, 应用加法结合律遂得 $x=x+0=x'+0=x'$.
- ⋆ 作为加法消去律的特例, 可以推知任何 x 的逆元 $-x$ 都是唯一的, 这是因为若 $x+x'=0=x+x''$, 则消去律蕴涵 $x'=x''$.
- ⋆ 从加法逆元的唯一性和 $x+(-x)=0=(-x)+x$ 立见 $-(-x)=x$.
- ⋆ 我们有恒等式 $x\cdot 0=0=0\cdot x$. 以第一个等号为例, 缘由是 $x\cdot 0=x\cdot(0+0)=x\cdot 0+x\cdot 0$, 对两端应用消去律可得 $x\cdot 0=0$.
- ⋆ 我们有 $(-1)\cdot x=-x$, 这是缘于

$$(-1)\cdot x+x=(-1)\cdot x+1\cdot x=(-1+1)\cdot x=0\cdot x=0$$

和加法逆元的唯一性. 代入 $x=-1$ 遂有 $(-1)\cdot(-1)=1$.

注意到对于一般的环, 乘法未必有交换律. 往后探讨的矩阵环将给出非交换环的自然实例.

注记 2.5.2 最平凡的环是**零环**: 这是只有单个元素 $1=0$ 的环, 从环论观点看是无趣的. 另一方面, 非零环必然满足 $1\neq 0$, 论证基于前述性质, 细节留给读者.

定义 2.5.3 *如果环 R 的乘法也满足交换律 $xy=yx$, 则称 R 为***交换环***.*

定义 2.5.4 *设 x 是环 R 的元素. 若存在 $y\in R$ 使得 $xy=1$ (或 $yx=1$), 则称 y 为 x 的右逆 (或左逆), 而 x 右可逆 (或左可逆). 若 x 左右皆可逆, 则称 x* **可逆**. *由可逆元构成的子集记为 $R^\times$.*

如果 x 可逆, 则 x 的左逆也必然是右逆, 而且存在唯一的 $x^{-1}\in R$ 使得 $x^{-1}x=1=xx^{-1}$. 论证和逆映射的版本 (见定义 2.3.3) 如出一辙, 以幺元 1 代替该处的 id 便是. 由此也立即看出 $(x^{-1})^{-1}=x$.

注意到 $R^\times$ 包含 1, 对乘法运算和乘法取逆 $x\mapsto x^{-1}$ 封闭. 进一步, $y^{-1}x^{-1}xy=1=xyy^{-1}x^{-1}$ 蕴涵

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

现在万事俱备, 可以引入域的概念: 它们是能作除法的交换环, 前提是除数非零. 如果不要求乘法交换, 得到的概念称为除环.

定义 2.5.5 *满足 $R^\times=R\smallsetminus\{0\}$ (换言之, 非零元皆可逆) 的非零环称为***除环***. 交换除环称为***域***. 域的子环如果也构成域, 则称之为子域.*

在域中可以合理地将 xy^{-1} 写作 x/y 或 $\frac{x}{y}$, 前提是 $y \neq 0$.

例 2.5.6 相对于寻常的乘法和加法运算, $\mathbb{C}$ 是域, 而 $\mathbb{R}, \mathbb{Q}$ 都是 $\mathbb{C}$ 的子域, 而子环 $\mathbb{Z}$ 不是域; 事实上 $\mathbb{Z}^\times = \{\pm 1\}$.

比域宽松的一个概念是整环, 它以环 $\mathbb{Z}$ 为模板.

定义 2.5.7 非零交换环 R 若满足 $x, y \neq 0 \implies xy \neq 0$, 则称为**整环**.

整环的子环显然也是整环.

以上举出的域都是 $\mathbb{C}$ 的子域. 另一方面, 在数学其它领域和线性代数的应用中将不可避免地遇到**有限域**. 下一则例子将包含最简单的一类有限域, 其元素个数为素数.

例 2.5.8 设 $N \in \mathbb{Z}_{\geq 1}$. 例 2.4.8 考察了 mod N 同余类构成的集合 $\mathbb{Z}/N\mathbb{Z}$. 在其上定义加法和乘法运算如下

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

其中 $x, y \in \mathbb{Z}$. 容易看出这是良定义的, 也就是说运算产物仅依赖同余类 $[x]$ 和 $[y]$ 而不是 x 和 y 的具体取法; 见练习 2.1.10. 取 $0_{\mathbb{Z}/N\mathbb{Z}} := [0]$, $1_{\mathbb{Z}/N\mathbb{Z}} := [1]$, 立见 $\mathbb{Z}/N\mathbb{Z}$ 对此运算成为交换环, 它的元素个数是 N.

注意到 $[x] \in (\mathbb{Z}/N\mathbb{Z})^\times$ 相当于说同余方程 $xy \equiv 1 \pmod{N}$ 有整数解 y. 基于命题 2.1.3, 此方程有解当且仅当 x 和 N 互素; 换言之,

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

特别地, 考虑等价类在 $\{1, \ldots, N\}$ 中的唯一代表元, 可见 $|(\mathbb{Z}/N\mathbb{Z})^\times| = \varphi(N)$.

由此推知 $\mathbb{Z}/N\mathbb{Z}$ 为域当且仅当 N 为素数. 设 p 为素数. 域 $\mathbb{Z}/p\mathbb{Z}$ 是**有限域**的初步例子. 鉴于它的重要性, 我们另外引入符号 $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

练习 2.5.9 取无交并 $\mathbb{R} \cup \{\infty\}$, 其中 ∞ 仅作为一个符号来理解. 在其上定义运算

$$x \oplus y := \min\{x, y\}, \quad x \odot y := x + y,$$

其中涉及 ∞ ("正无穷大") 的运算按直观的方式理解.

(i) 证明 $(\mathbb{R} \cup \{\infty\}, \oplus, \odot, \infty, 0)$ 非环. 说明它缺乏哪一条性质.

(ii) 另一方面, 对所有 $n \in \mathbb{Z}_{\geq 1}$, 验证 $(x \oplus y)^{\odot n} := (x \oplus y) \odot \cdots \odot (x \oplus y)$ 等于 $x^{\odot n} \oplus y^{\odot n}$.

练习 2.5.10 设 $D \in \mathbb{Z}$ 是无平方因子的非零整数.

(i) 验证

$$\mathbb{Q}\left(\sqrt{D}\right) := \left\{a + b\sqrt{D} \in \mathbb{C} : a, b \in \mathbb{Q}\right\}$$

是 $\mathbb{C}$ 的子域, 称为**二次域**. 具体说明非零元的求逆公式.

(ii) 验证 $\mathbb{Z}[\sqrt{D}] := \left\{a+b\sqrt{D} : a,b\in\mathbb{Z}\right\}$ 是整环. 验证当 $D\equiv 1 \pmod 4$ 时, 它包含于更大的整环

$$\mathcal{O}_D := \left\{ \begin{array}{l|l} \frac{x+y\sqrt{D}}{2} & x,y\in\mathbb{Z} \\ & a\equiv b \pmod 2 \end{array} \right\}.$$

迄今考虑的环主要是交换环. 稍后研究矩阵时, 非交换环将会自然地出现.

例 2.5.11 若 R 是环, A 是任意集合, 则函数集 $R^A=\{f:A\to R\}$ 相对于

$$(f+g)(a)=f(a)+g(a),\quad (fg)(a)=f(a)g(a),\quad a\in R$$

构成环, 其中 0_{R^A} 取为常值映射 $a\mapsto 0_R$, 而 1_{R^A} 取为常值映射 $a\mapsto 1_R$. 请读者自行验证

$$\left(R^A\right)^\times = \left\{f\in R^A : \forall a\in A,\ f(a)\in R^\times\right\}.$$

这般定义的运算可以合理地称为是函数集上的**逐点**运算.

2.6 环的同态和同构

设 R 和 R' 为环. 在环论的研究及其应用中, 我们所关心的映射 $f:R\to R'$ 并非任意的, 它应该和环结构兼容; 或者更形象地说, f 应该将 R 中的环论运算反映在 R' 中. 将这一想法严谨地表述, 便引出环同态的概念.

定义 2.6.1 设 $f:R\to R'$ 为环之间的态射. 当以下条件成立时, 称 f 为**环同态**:

- ⋆ $f(x+y)=f(x)+f(y)$,
- ⋆ $f(xy)=f(x)f(y)$,
- ⋆ $f(1_R)=1_{R'}$,

其中 x,y 取遍 R 的元素.

几点简单观察:

- ⋆ 定义未要求 $f(0_R)=0_{R'}$, 因为这是自动的: 从 $f(0_R)=f(0_R+0_R)=f(0_R)+f(0_R)$, 配合 R' 中的加法消去律, 即得 $f(0_R)=0_{R'}$;
- ⋆ $f(-x)=-f(x)$ 成立, 这是 $0_{R'}=f(x+(-x))=f(x)+f(-x)$ 的推论;
- ⋆ 若 $x\in R^\times$, 则 $f(x)\in(R')^\times$ 而 $f(x^{-1})=f(x)^{-1}$.

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

♣♣♣ 环同构的概念

2.7 多项式的算术

设 R 为非零环. 以 X 为变元, 系数在 R 上的**多项式**定义为形如

$$f=\sum_{n\geq 0}a_nX^n,\quad a_n\in R,\quad \text{至多有限个 } a_n \text{ 非零}$$

的形式和, $a_n=0$ 的项可以省去; 须凸显变元时也将 f 写作 $f(X)$. 所谓形式和, 意指我们并非真在某个环中作加法. 严格的说法应当是: 多项式是 $\mathbb{Z}_{\geq 0}$ 份 R 的积 $R^{\mathbb{Z}_{\geq 0}}$ 中的元素, 按分量写作 $(a_n)_{n\geq 0}$ 的形式, 要求仅有至多有限个 n 使得 $a_n\neq 0$. 乍看之下, X^n 在写法中仅起到记录下标 n 的作用; 稍后定义多项式乘法时, 符号 X^n 的便利性就会凸显.

以上关于形式和的讨论也表明

$$\sum_{n\geq 0}a_nX^n=\sum_{n\geq 0}b_nX^n\iff \forall n\in\mathbb{Z}_{\geq 0},\ a_n=b_n.$$

我们称 a_n 是多项式 $f=\sum_n a_nX^n$ 的 n 次系数; 称 a_0 为 f 的常数项. 仅有常数项系数非零的多项式称为常数多项式; 所有系数皆为零者称为零多项式.

多项式的加法定为逐项相加

$$\sum_{n\geq 0}a_nX^n+\sum_{n\geq 0}b_nX^n:=\sum_{n\geq 0}(a_n+b_n)X^n,$$

乘法则定为

$$\left(\sum_{n\geq 0}a_nX^n\right)\cdot\left(\sum_{n\geq 0}b_nX^n\right):=\sum_{n\geq 0}\left(\sum_{\substack{h,k\geq 0,\\ h+k=n}}a_hb_k\right)X^n.$$

系数在 R 上, 以 X 为变元的所有多项式构成集合 $R[X]$. 注意到 R 自然地嵌入为 $R[X]$ 的子集, 方式是映 $r\in R$ 为相应的常数多项式.

命题 2.7.1 *以上运算使得 $R[X]$ 成为环, 其中 $0_{R[X]}$ 是所有系数全为 0_R 的多项式, 而 $1_{R[X]}$ 是常数项为 1_R, 其余系数全为 0_R 的多项式; R 是 $R[X]$ 的子环.*

如果 R 是交换环, 则 $R[X]$ 亦然.

证明 这些无非是定义的直接操演, 比如乘法的交换律归结为 R 的乘法交换律和 $X^i(X^jX^k)=X^{i+j+k}=(X^iX^j)X^k$. □

非零多项式 f 的次数定义为

$$\deg f:=\max\{n\in\mathbb{Z}_{\geq 0}:a_n\neq 0\};$$

一般不考虑零多项式的次数; 确实有需要时, 定义 $\deg 0 = -\infty$.

引理 2.7.2 设 R 为整环, 则 $R[X]$ 也是整环; 事实上对所有非零的 $f, g \in R[X]$ 都有 $\deg(fg) = \deg f + \deg g$.

证明 设 $f = a_n X^n +$ 低次项, $g = b_m X^m +$ 低次项, 其中 $a_n, b_m \neq 0$. 那么 $fg = a_n b_m X^{m+n} +$ 低次项, 而 $a_n b_m \neq 0$. □

举例明之, 整系数多项式构成整环 $\mathbb{Z}[X]$. 线性代数的研究中主要遇到的是域上的多项式环.

♣♣♣ 多项式 vs. 多项式函数

♣♣♣ 多项式的算术

3 向量空间和线性映射

本节选定域 F.

3.1 向量空间 域 F 上的向量空间又称为线性空间. 这是具有加法, 数乘运算以及零元的一种代数结构; 加法是空间上的二元运算, 数乘则涉及域 F 元素的作用. 细说如下.

定义 3.1.1 域 F 上的向量空间简称 F-向量空间, 这是指资料 $(V,+,\cdot,0_V)$, 其中 V 是集合, $0_V\in V$, 而 $+:V\times V\to V$ 和 $\cdot:F\times V\to V$ 分别写作 $(u,v)\mapsto u+v$ 和 $(t,v)\mapsto t\cdot v$ 的形式, 使得以下条件成立.

1. 加法满足以下条件:
   - ▷ **结合律** $(u+v)+w=u+(v+w)$;
   - ▷ **幺元性质** $v+0_V=v=0_V+v$;
   - ▷ **交换律** $u+v=v+u$;
   - ▷ **加法逆元** 对所有 v 皆存在 $-v$ 使得 $v+(-v)=0_V$.
2. 数乘或纯量乘法 $t\cdot v$ 也简写为 tv, 它满足以下条件:
   - ▷ **结合律** $s\cdot(t\cdot v)=(st)\cdot v$;
   - ▷ **幺元性质** $1\cdot v=v$.
3. 数乘对加法满足
   - ▷ **分配律** $(s+t)\cdot v=sv+tv,\quad s\cdot(u+v)=su+sv$.

其中 u,v,w (或 s,t) 代表 V (或 F) 中的任意元素. 不致混淆时, 我们也简记 0_V 为 0, 将 $u+(-v)$ 写作 $u-v$, 并以 V 总括资料 $(V,+,\cdot,0)$.

如果 V 的子集 V_0 包含 0, 而且在加法和数乘运算下封闭, 则 $(V_0,+,\cdot,0)$ 也是 F-向量空间, 称之为 V 的**子空间**.

向量空间经常简称为空间. 向量空间 V 的元素也称为 V 中的**向量**. 定义中的加法幺元 0_V 又称为 V 的零元, 或零向量. 与向量相对, 域 F 的元素则称为纯量.

一切和环的定义 2.5.1 明显相似. 由之推出的以下几条性质也出于同样理路, 细节不劳重复.

- ⋆ 零元 0_V 由相应的幺元性质唯一确定, 所以资料中的 0_V 其实可以略去, 要求存在满足该性质的元素即可.
- ⋆ 加法满足消去律: $u+v=u'+v$ 蕴涵 $u=u'$. 作为推论, 任何 v 的加法逆元 $-v$ 都是唯一的.
- ⋆ 逆元的唯一性也蕴涵 $-(-v)=v$.

⋆ 我们有恒等式 $0\cdot v=0$; 等号左边纯量积中的 $0\in F$, 而右边的 $0\in V$. 这是缘于 $0\cdot v=(0+0)\cdot v=0\cdot v+0\cdot v$ 和消去律.

⋆ 我们有 $(-1)\cdot v=v$. 这是缘于 $(-1)\cdot v+v=(-1)\cdot v+1\cdot v=(-1+1)\cdot v=0\cdot v=0$.

子空间的定义中未要求 V_0 对取逆 $v\mapsto -v$ 封闭, 这是因为 $-v=(-1)\cdot v$, 所以要求数乘的封闭性已经足够.

例 3.1.2 (零空间) 最平凡的向量空间是 $\{0\}$, 它是所有 F-向量空间的子空间.

例 3.1.3 平面向量对加法和数乘构成 $\mathbb{R}$-向量空间, 空间向量亦同. 这是向量空间最直观的例子.

♣♣♣ 平行四边形法则图解, 伸缩图解.

例 3.1.4 设 $n\in\mathbb{Z}_{\geq 0}$. 按以下方式赋予 F^n 向量空间的结构

$$(x_1,\dots,x_n)+(y_1,\dots,y_n):=(x_1+y_1,\dots,x_n+y_n),\quad x_i,y_i\in F;$$
$$t(x_1,\dots,x_n):=(tx_1,\dots,tx_n),\quad t\in F.$$

其中的零元取为 $(0,\dots,0)$. 定义所需的性质都是明显的. 注意到当 $n=0$ 时, F^n 定义为零空间 $\{0\}$. 作为特例, F 对域的加法和乘法 (在此作为数乘) 也是 F-向量空间; 这是最简单的非零 F-向量空间.

例 3.1.5 回忆一些符号: 对任意集合 V 和 I, 我们记 $V^I:=\{\text{映射 } I\to V\}$, 其元素写作 $(v_i)_{i\in I}$ 或简写为 $(v_i)_i$, 其中对每个 i 都有 $v_i\in A$; 换言之, V^I 由 V 中的元素族构成, 集合 I 在此充当下标的角色.

进一步要求 V 是 F-向量空间, 则 V^I 自然对逐项的运算构成向量空间, 即

$$(v_i)_i+(w_i)_i=(v_i+w_i)_i,\quad t(v_i)_i=(tv_i)_i.$$

当 $I=\varnothing$ 时约定 $V^I:=\{0\}$. 这是例 3.1.4 的推广: 不难看出 F^n 即是 $F^{\{0,\dots,n-1\}}$.

3.2 实例: 矩阵空间

矩阵在 §1 已经多次用到, 当时我们对矩阵元的取值在哪个数系含糊其词. 现在既然有了域的概念, 便可以清楚地定义一般的矩阵.

定义 3.2.1 (域上的矩阵) 设 $m,n\in\mathbb{Z}_{\geq 1}$. 域 F 上的 $m\times n$ **矩阵**是指形如如下的资料

$$A=(a_{ij})_{\substack{1\leq i\leq m\\1\leq j\leq n}}=\begin{pmatrix}a_{11}&\cdots&a_{1n}\\ \vdots&\ddots&\vdots\\ a_{m1}&\cdots&a_{mn}\end{pmatrix}=\begin{pmatrix}&\vdots&\\ \cdots&a_{ij}&\cdots\\ &\vdots&\end{pmatrix}\begin{matrix}\\ \\ \text{第 } i \text{ 行}\\ \\ \\ \text{第 } j \text{ 列}\end{matrix}$$

其中 $a_{ij}\in F$, 称为该矩阵的第 (i,j) 个矩阵元或 (i,j)-项. 所有 $m\times n$ 矩阵构成的集合记为 $M_{m\times n}(F)$. 作为特例, $n\times n$ 矩阵也称为 n 阶**方阵**.

按惯例, 我们经常将矩阵 $A=(a_{ij})_{\substack{1\leq i\leq m\\1\leq j\leq n}}$ 简记为 $(a_{ij})_{i,j}$.

现在赋予集合 $M_{m\times n}(F)$ 向量空间所需的运算.

⋆ 对 $M_{m\times n}(F)$ 的任两个元素 $A=(a_{ij})_{i,j}$ 和 $B=(b_{ij})_{i,j}$, 定义

$$A+B:=(a_{ij}+b_{ij})_{\substack{1\leq i\leq m\\1\leq j\leq n}}.$$

⋆ 对任意 $t\in F$ 和 $A=(a_{ij})_{i,j}\in M_{m\times n}(F)$, 定义

$$t\cdot A:=(ta_{ij})_{\substack{1\leq i\leq m\\1\leq j\leq n}}.$$

换言之, 加法无非是逐项相加, 数乘是对每一项乘以同样的 t.

命题 3.2.2 这些运算使得 $M_{m\times n}(F)$ 成为 F-向量空间. 其中的零元为零矩阵 $0_{m\times n}=(0)_{i,j}$, 而任意矩阵 $A=(a_{ij})_{i,j}$ 的加法逆元为 $-A=(-a_{ij})_{i,j}$.

证明 理应是明显的. 一切运算性质都逐项地化约到 F 中来验证. □

对于特例 $n=1$, 向量空间 $M_{m\times 1}(F)$ 化约为例 3.1.4 讨论的 F^m; 出于直观的理由, $M_{m\times 1}(F)$ 的元素也称为 m 维的**列向量**. 同样道理, 向量空间 $M_{n\times 1}(F)$ 可以等同于 F^n, 其元素称为 n 维的**行向量**.

一旦定义了一般的域 F 上的矩阵, §§1.2—1.3 介绍的线性方程组, 行运算和 Gauss–Jordan 消元法理论可以一字不易地推广到任意域 F 上.

定义 3.2.3 考虑域 F 上的 n 元线性方程组

$$\begin{aligned} a_{11}X_1 + \cdots + a_{1n}X_n &= b_1 \\ \vdots \qquad & \quad \vdots \\ a_{m1}X_1 + \cdots + a_{mn}X_n &= b_m. \end{aligned}$$

如果 $b_1 = \cdots = b_m = 0$, 则称此方程组为**齐次**的.

给定线性方程组, 总是可以把其中的常数项 (或者说是零次项) $b_1, b_2, \ldots$ 全代为 0, 从而得到相应的齐次方程组. 从矩阵的观点看, 这相当于删除增广矩阵的最后一列, 只看系数矩阵.

除了加法和数乘. 矩阵还有相乘的运算.

定义 3.2.4 (矩阵乘法) 矩阵乘法是按以下方式定义的映射

$$\begin{aligned} M_{m\times n}(F) \times M_{n\times r}(F) &\longrightarrow M_{n\times r}(F) \\ (A, B) &\longmapsto AB \end{aligned}$$

若 $A = (a_{ij})_{\substack{1\le i\le m\\ 1\le j\le n}}$, $B = (b_{jk})_{\substack{1\le j\le n\\ 1\le k\le r}}$, 则 $AB = (c_{ik})_{\substack{1\le i\le m\\ 1\le k\le r}}$, 其中

$$c_{ik} := \sum_{j=1}^{n} a_{ij}b_{jk}.$$

注意到只有行数和列数合乎规格的矩阵才能相乘.

命题 3.2.5 矩阵乘法满足以下性质:

▷ **结合律** $(AB)C = A(BC)$;

▷ **分配律** $A(B + C) = AB + AC$, $(B + C)A = BA + CA$;

▷ **线性** $A(tB) = t(AB) = (tA)B$;

其中 $t \in F$ 和矩阵 A, B, C 是任意的, 前提是它们的行数和列数使矩阵运算有意义.

这些运算规律可以从定义验证, 不过我们更愿意从线性映射的角度来理解矩阵. 见 §3.4. 稍后的推论 3.4.11 还将进一步明确 $M_{n\times n}(F)$ 的环结构.

练习 3.2.6 以矩阵乘法的定义直接证明命题 3.2.5

3.3 基和维数

对于经典的平面向量或空间向量, 我们熟知一旦选定坐标系, 所有向量都能按坐标唯一地展开. 将此思路扩及一般的向量空间, 就引向了基的概念. 按定义, 基的元素个数即是向量空间空间的维数.

向量空间的基并不唯一, 通常也没有标准的取法. 在许多应用中 (例如中学物理力学中的静态平衡), 适当选基, 自由换基还是解决问题的关键手段. 阐明基与基之间如何变换是本节的重要任务.

为了严谨地解释这些概念, 需要先引进一系列的术语.

选定域 F. 设 S 为 F-向量空间 V 的子集, 或有限或无穷. 形如

$$a_1v_1 + \cdots + a_mv_m, \quad m \in \mathbb{Z}_{\geq 0},\ a_i \in F,\ v_i \in S,$$

的向量称为 S 中的元素**线性组合**. 注意到上式取 $m = 0$ 对应到 "空和", 约定为 0. 记

$$\langle S\rangle := \big\{S \text{ 中的元素的线性组合}\big\}.$$

按定义立见 $\langle S\rangle$ 是 V 的子空间. 事实上, $\langle S\rangle$ 是包含 S 的最小子空间: 包含 S 的子空间必然也包含 $\langle S\rangle$. 这同样是线性组合定义的直接结论.

职是之故, 我们也称 $\langle S\rangle$ 为 S 的线性包, 或 S 张成的子空间. 平凡的情形是 $\langle\varnothing\rangle = \{0\}$. 我们经常将 S 中元素的线性组合写作

$$\sum_{s\in S} a_s s$$

的形式, 其中的系数 $a_s \in F$, 而且至多仅有限多个 $a_s \neq 0$, 因此这实际上是有限和; 今后凡是写下诸如 $\sum_s a_s s$ 的公式时, 都作如是假设.

定义 3.3.1 设 S 为 F-向量空间 V 的子集.

- ⋆ 如果 $\langle S\rangle = V$, 则称 S 是 V 的一族生成元, 或简称为生成系.
- ⋆ 称形如
$$\sum_{s\in S} a_s s = 0$$
的等式为 S 中的线性关系; 如果系数 a_s 不全为 0, 则称此关系非平凡. 若 S 中存在非平凡的线性关系, 则称 S **线性相关**, 否则称 S **线性无关**.
- ⋆ 若 S 是线性无关的生成系, 则称 S 是 V 的一组**基**.

注意到如果 S 线性无关, 则任何线性组合 $v = \sum_{s\in S} a_s s$ 中的系数 a_s 都由 v 唯一确定, 这是因为

$$\sum_{s\in S} a_s s = \sum_{s\in S} b_s s \iff \sum_{s\in S}(a_s - b_s)s = 0.$$

所以如果 S 是 V 的基, 则所有 v 都能够表成线性组合 $v=\sum_{s\in S}a_s s$, 而且其中的系数 $(a_s)_{s\in S}$ 由 v 唯一确定.

向量空间 V 的所有生成族 (或线性无关子集) 可以按集合包含关系 $\subset$ 比较大小, 由此可以谈论其中的极大或极小元; 参见定义 2.4.2 的相关讨论.

引理 3.3.2 *对于 F-向量空间 V 的任意子集 S, 我们有*

$$S \text{ 是极小生成系} \iff S \text{ 是基} \iff S \text{ 是极大线性无关子集}.$$

证明 设 S 是极小生成系. 以下验证 S 线性无关, 从而说明 S 为基. 设 S 中存在非平凡线性关系 $a_1s_1+\cdots+a_ms_m=0$, 其中 $s_i\in S$ 相异; 不失一般性, 可设 $a_1\neq 0$. 那么

$$s_1=-a_1^{-1}\left(\sum_{i=2}^{m}a_i s_i\right),$$

由此可见 $S\smallsetminus\{s_1\}$ 和 S 生成同一个向量空间 V, 和 S 的极小性矛盾.

接着设 S 为基并且证明 S 是极大线性无关子集. 基的定义已包含线性无关. 倘若 $w\in V\smallsetminus S$, 则可将之表作 $w=\sum_s a_s s$, 或等价地说 $w-\sum_s a_s s=0$, 可见 $S\cup\{w\}$ 线性相关. 故 S 是极大线性无关子集.

最后设 S 是极大线性无关子集. 对于任意 $v\in V$, 若 $v\in S$ 则 $v\in\langle S\rangle$; 若 $v\notin S$, 则存在非平凡线性关系

$$av+\sum_s a_s s=0.$$

此处必有 $a\neq 0$, 否则 $\sum_s a_s s=0$ 给出 S 中的非平凡线性关系. 于是 $v=-a^{-1}\sum_s a_s s\in\langle S\rangle$. 故 S 也是生成系; 它必然极小, 否则存在 $s\in S$ 使得 $\langle S\smallsetminus\{s\}\rangle=V$, 按此将 s 表为线性组合

$$s=\sum_{t\in S\smallsetminus\{s\}}a_t t,$$

则 $s-\sum_{t\in S\smallsetminus\{s\}}a_t t=0$ 将导致 S 线性相关, 矛盾. □

所有向量空间都有基, 而且不同的基有相同的元素个数. 证明虽不难, 却需要一些集合论的背景知识, 感兴趣的读者可参考 [2, §6.4]. 简单起见, 我们只考虑有限的情形如下.

引理 3.3.3 *设 S 是 F-向量空间 V 的生成系, S 有限, 则存在子集 $B\subset S$ 使得 B 是 V 的基.*

证明 设 S 中存在非平凡的线性关系, 适当调整系数后不妨将其写作

$$s-\sum_{t\in S\smallsetminus\{s\}}a_t t=0,$$

其中 $s \in S$. 那么 $S \smallsetminus \{s\}$ 仍是生成系. 由于 S 有限, 反复操作将得到极小生成系 $B \subset S$. □

引理 3.3.4 设 $\{s_1, \dots, s_n\}$ 生成 F-向量空间 V, 则当 $m > n$ 时, 任意 m 个向量 $v_1, \dots, v_m \in V$ 都线性相关.

证明 取系数 $a_{ij} \in F$, 其中 $1 \leq i \leq m$ 而 $1 \leq j \leq n$, 使得对所有 $1 \leq i \leq m$ 都有

$$v_i = a_{1i}s_1 + \cdots a_{ni}s_n.$$

我们断言若 $(x_1, \dots, x_m) \in F^m$ 是 m 元齐次线性方程组

$$\begin{aligned} a_{11}X_1 + \cdots + a_{1m}X_m &= 0 \\ \vdots \qquad & \quad \vdots \\ a_{n1}X_1 + \cdots + a_{nm}X_m &= 0 \end{aligned} \tag{3.1}$$

的一组解, 则 $x_1v_1 + \cdots + x_mv_m = 0$. 这是因为

$$\sum_{i=1}^{m} x_i v_i = \sum_{i=1}^{m} x_i \left(\sum_{j=1}^{n} a_{ji} s_j \right) = \sum_{j=1}^{n} \left(\sum_{i=1}^{m} a_{ji} x_i \right) s_j = 0;$$

这里用到了求和次序的交换 $\sum_i \sum_j = \sum_j \sum_i$. 所以问题化为证 $m > n$ 时方程组 (3.1) 有不全为 0 的解. 为此, 对其系数矩阵

$$\begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nm} \end{pmatrix} \qquad (m > n)$$

进行 Gauss–Jordan 消元法, 得出的简化行梯矩阵的主元个数 $\leq \min\{n, m\} < m$ (练习 1.2.5); 换言之, 其解集至少包含一个自由变量. 这就说明 (3.1) 有不全为 0 的解. □

定义–命题 3.3.5 设 F-向量空间 V 有一族有限的生成元, 则它有基, 而且每组基的元素个数皆有限而且彼此相等. 满足此条件的 F-向量空间 V 称为**有限维向量空间**, 而任一组基的元素个数称为 V 的**维数**, 记为 $\dim_F V$ 或 $\dim V$.

证明 引理 3.3.3 说明 V 有一组基 $\{v_1, \dots, v_n\}$, 其中 $n \in \mathbb{Z}_{\geq 0}$. 设 B 是 V 的任一组基, 则引理 3.3.4 说明 B 必然有限, 而且 $|B| \leq n$. 同理, $n \leq |B|$. 因此每组基的元素个数皆相等. □

推论 3.3.6 设 $\dim V = n$, 而 $v_1, \dots, v_n \in V$ 是相异的向量. 当以下任一条件成立时, $\{v_1, \dots, v_n\}$ 是 V 的基:

- ⋆ $\{v_1, \dots, v_n\}$ 线性无关;
- ⋆ $\{v_1, \dots, v_n\}$ 生成 V.

证明 对于线性无关的情形, $\{v_1, \dots, v_n\}$ 可以扩充为基; 对于生成系的情形, 它包含一组基作为子集. 然而任何基都恰有 n 个元素. □

注意到对于零空间 $\{0\}$, 定义导致它的基是空集 $\varnothing$. 对于一般的 V, 我们有

$$\dim V = 0 \iff V = \{0\}.$$

注记 3.3.7 按以上定义, 有限维向量空间 V 的基是一类特殊的子集, 基的元素不计顺序. 如果进一步为基的元素排了序, 写作 $v_1, \dots, v_n$ 等等, 则称之为**有序基**以资区别.

例 3.3.8 向量空间 F^n 是 n 维的. 它有标准基 $e_1, \dots, e_n$, 其中

$$e_i := (0, \dots, \underbrace{1}_{i\text{-分量}}, \dots, 0), \quad i = 1, \dots, n.$$

理由直截了当: 任何 $v = (x_1, \dots, x_n) \in F^n$ 都可以表成

$$v = x_1 e_1 + \cdots + x_n e_n;$$

反过来说, 如果 v 写作以上形式, 则 x_i 是 v 的第 i 个分量, 因此表法是唯一的.

例 3.3.9 推而广之, 矩阵空间 $M_{m\times n}(F)$ 是 mn 维的. 它有标准基 E_{ij}, 其中 E_{ij} 是第 (i,j) 个矩阵元为 1, 其它矩阵元全为 0 的 $m \times n$ 矩阵, 此处 $1 \le i \le m$ 而 $1 \le j \le n$. 任何矩阵 A 都能唯一地展开为

$$A = \sum_{\substack{1\le i\le m\\ 1\le j\le n}} a_{ij} E_{ij};$$

系数 a_{ij} 正是 A 的第 (i,j) 个矩阵元.

3.4 线性映射和矩阵

线性映射是保持向量结构的一类映射. 在代数学的框架中, 更合理的称呼应当是向量空间的同态. 本节依然选定域 F.

定义 3.4.1 设 V 和 W 是 F-向量空间. 若映射 $T : V \to W$ 满足

$$T(v_1 + v_2) = T(v_1) + T(v_2), \quad v_1, v_2 \in V,$$
$$T(tv) = tT(v), \quad t \in F,\ v \in V,$$

则称 T 为线性映射, 或称线性变换.

线性映射保持零元, 这是由于 $T(0) = T(0 + 0) = T(0) + T(0)$ 和加法的消去律蕴涵 $T(0) = 0$; 此处以 0 同时代表 V 和 W 的零元, 不致混淆. 类似地, $0 = T(0) = T(-v + v) = T(-v) + T(v)$ 蕴涵 $T(-v) = -T(v)$, 所以线性映射自动保持加法取逆的运算.

简便起见, 我们经常将 $T(v)$ 简写为 Tv.

线性映射的初步例子是空间 V 到自身的恒等映射 id_V. 另一个平凡的例子则是零映射 $0 : V \to W$, 映所有 $v \in V$ 为 0.

引理 3.4.2 设 $T : U \to V$ 和 $S : V \to W$ 都是线性映射, 则其合成 $ST : U \to W$ 也是线性映射.

证明 直接验证 $ST(v_1 + v_2) = S(Tv_1 + Tv_2) = STv_1 + STv_2$ 和 $ST(tv) = S(t \cdot Tv) = t \cdot ST(v)$. □

以下概念和映射情形的定义 2.3.1, 差别仅是此处的映射都要求为线性.

定义 3.4.3 考虑一对线性映射 $V \underset{S}{\overset{T}{\rightleftarrows}} W$. 若 $ST = \mathrm{id}_V$, 则我们称 S 是 T 的**左逆**, 而 T 是 S 的**右逆**. 有左逆 (或右逆) 的映射称为是左可逆 (或右可逆) 线性映射.

定义 3.4.4 如果线性映射 $T : V \to W$ 左右皆可逆, 则称为**可逆**线性映射, 也称为**同构**. 这时存在唯一的线性映射 $T^{-1} : W \to V$ 使得 $T^{-1}T = \mathrm{id}_V$ 而 $TT^{-1} = \mathrm{id}_W$, 称为 T 的逆; 它同时是 T 的唯一左逆和唯一右逆.

对于可逆的 T, 左逆, 右逆的唯一性证都照搬集合映射的情形 (定义 2.3.3) 进行论证. 如果 $T : V \to W$ 是同构, 这也写作 $T : V \xrightarrow{\sim} W$. 如果 $U \xrightarrow{T} V \xrightarrow{S} W$, 则合成 ST 也是同构, 其逆为 $T^{-1}S^{-1}$; 一切既是套话, 按下不表.

然而这里也出现了新问题: 如果一个线性映射作为集合的映射是可逆的, 它作为线性映射是否可逆? 答案是肯定的.

命题 3.4.5 设 $T : V \to W$ 为线性映射, 则 T 可逆当且仅当它作为集合之间的映射是可逆的, 或者等价地说 (练习 2.3.2), 当且仅当它是集合之间的双射.

证明 设 T 作为线性映射可逆, 则逆线性映射 T^{-1} 同时也是它作为集合映射的逆映射.

接着设存在集合之间的映射 $T^{-1}: W \to V$ 使得 $T^{-1}T = \mathrm{id}_V$ 而 $TT^{-1} = \mathrm{id}_W$. 今将说明 T^{-1} 必然是线性映射. 首先 T 是集合的双射. 对任何 $w_1, w_2 \in W$, 我们有

$$T\left(T^{-1}(w_1) + T^{-1}(w_2)\right) = TT^{-1}(w_1) + TT^{-1}(w_2) = w_1 + w_2;$$

两边取 T^{-1} 的像, 可得 $T^{-1}(w_1) + T^{-1}(w_2) = T^{-1}(w_1 + w_2)$.

同理, 对任何 $t \in F$ 和 $w \in W$, 我们有

$$T\left(tT^{-1}(w)\right) = tTT^{-1}(w) = tw.$$

两边取 T^{-1} 的像可得 $tT^{-1}(w) = T^{-1}(tw)$. □

♣♣♣ 需要更详细的说明

同构是代数学的核心概念之一. 同构是向量空间之间的等价关系. 如果 $T: V \xrightarrow{\sim} W$, 那么 V 和 W 不但作为集合能通过 T 在元素之间建立一一对应, 而且元素的对应还保持所论的代数结构, 也就是加法与数乘; 这表明 V 和 W 在向量空间的研究中可以透过 T 来等同.

观察到

- ⋆ 如果 $T_1, T_2: V \to W$ 都是线性映射, 则 $T_1 + T_2: v \mapsto T_1(v) + T_2(v)$ 仍是线性映射;
- ⋆ 如果 $t \in F$ 而 $T: V \to W$ 是线性映射, 则 $tT: v \mapsto t \cdot T(v)$ 仍是线性映射.

这就启发我们将所有从 V 到 W 的线性映射作成向量空间, 其加法和数乘由上述 "逐点" 的加法和数乘运算给出.

定义 3.4.6 设 V 和 W 为 F-向量空间. 定义 $\mathrm{Hom}(V, W)$ 为所有从 V 到 W 的线性映射所成的集合. 加法和数乘分别按 $(T_1 + T_2)(v) = T_1(v) + T_2(v)$ 和 $(tT)(v) = t \cdot Tv$ 确定. 空间 $\mathrm{Hom}(V, W)$ 的零元由零映射 $0: V \to W$ 给出.

线性映射的性质即刻给出关于映射合成的以下性质.

命题 3.4.7 设 U, V, W 为 F-向量空间. 映射的合成

$$\begin{aligned} \circ: \mathrm{Hom}(V, W) \times \mathrm{Hom}(U, V) &\to \mathrm{Hom}(U, W) \\ (S, T) &\mapsto ST \end{aligned}$$

满足

$$(tS) \circ T = t(S \circ T) = S \circ (tT), \quad t \in F$$

和分配律

$$(S_1+S_2)\circ T = S_1\circ T + S_2\circ T,\quad S\circ(T_1+T_2) = S\circ T_1 + S\circ T_2.$$

将线性映射对合成的分配律和 Hom-空间是向量空间这一性质合并使用, 我们就得到环的新例子.

推论 3.4.8 *设 V 为向量空间, 则 $\mathrm{End}(V) := \mathrm{Hom}(V,V)$ 成为环, 其加法运算是线性映射的逐点加法, 乘法是线性映射的合成 $(S,T)\mapsto ST$; 零元是零映射, 乘法幺元是恒等映射 id_V. 此外, $\mathrm{End}(V)$ 是零环当且仅当 $V=\{0\}$.*

证明 环的条件已经含藏于上述讨论. 注意到一个环 R 是零环当且仅当 $1_R = 0_R$. 而对于向量空间 V, 显然有 $\mathrm{id}_V = 0$ 当且仅当 $V=\{0\}$. □

眼下的任务当然是尽量具体地了解并操作 $\mathrm{Hom}(V,W)$. 这点可以透过基来达成.

1. 首先假定对 V 已经选定了一组基 $\{v_j\}_{j\in J}$, 此处 J 是充当下标的某个集合. 任意 $v\in V$ 都能唯一地展开为线性组合 $v=\sum_{j\in J} c_j v_j$. 若 $T\in\mathrm{Hom}(V,W)$, 则

$$Tv = \sum_{j\in J} c_j\cdot T(v_j).$$

所以 T 由它在 $\{v_j\}_{j\in J}$ 上的限制, 亦即资料 $(Tv_j)_{j\in J}\in W^J$ 完全确定. 反过来说, 假定已给定 W 中的一族向量 $(\underline{w}_j)_{j\in J}\in W^J$, 定义

$$\begin{aligned} T: V &\longrightarrow W\\ \sum_{j\in J} c_j v_j &\longmapsto \sum_{j\in J} c_j \underline{w}_j. \end{aligned}$$

由定义立见这是线性映射. 综上, 得到双射

$$\begin{aligned} \mathrm{Hom}(V,W) &\xrightarrow{1:1} W^J\\ T &\longmapsto (Tv_j)_{j\in J}. \end{aligned}$$

2. 承上, 进一步选定 W 的基 $\{w_i\}_{i\in I}$, 此处 I 仍是某个充当下标的集合. 对每个 $j\in J$, 将 Tv_j 表作

$$Tv_j = \sum_{i\in I} a_{ij} w_i$$

其中 $a_{ij}\in F$ 是唯一确定的一族系数, 而且当 j 固定, 至多仅对有限个 i 非零. 因

此

$$\mathrm{Hom}(V,W) \xrightarrow{1:1} \big\{(a_{ij}) \in F^{I\times J} : \forall j,\ \exists \text{ 至多有限个 } i \text{ 使得 } a_{ij}\neq 0\big\}$$

其中 $(a_{ij})_{i,j}$ 对应的线性映射由下式刻画:

$$v_j \mapsto \sum_{i\in I} a_{ij}v_j, \quad j\in J. \tag{3.2}$$

3. 由此可以将 $\mathrm{Hom}(V,W)$ 的向量空间结构转译到 $F^{I\times J}$ 上:
   - ⋆ 若 $T,T'\in\mathrm{Hom}(V,W)$ 分别对应到 $(a_{ij})_{i,j}$ 和 $(a'_{ij})_{i,j}$, 则 $T+T'$ 对应到 $(a_{ij}+a'_{ij})_{i,j}$.
   - ⋆ 若 T 对应到 $(a_{ij})_{i,j}$ 而 $t\in F$, 则 tT 对应到 $(ta_{ij})_{i,j}$.

   这些断言都直接导自 (3.2) 的刻画.

4. 现在来探讨线性映射的合成. 给定 F-向量空间 U, V, W, 分别带有给定的基 $\{u_k\}_{k\in K}$, $\{v_j\}_{j\in J}$, $\{w_i\}_{i\in I}$, 其中 I,J,K 依然是充当下标的集合. 考虑线性映射

$$\begin{aligned} S\in\mathrm{Hom}(V,W) &\leftrightarrow (a_{ij})_{i,j}\\ T\in\mathrm{Hom}(U,V) &\leftrightarrow (b_{jk})_{j,k}. \end{aligned}$$

   为了描述 ST, 对每个 $k\in K$ 来计算

$$ST(u_k)=S\left(\sum_{j\in J} b_{jk}v_j\right)=\sum_{j\in J} b_{jk}S(v_j)=\sum_{j\in J}\sum_{i\in I} a_{ij}b_{jk}w_i;$$

   注意到每一步求和都只有有限项非零. 因此相对于选定的基及其下标集 I 和 K, 线性映射 $ST:U\to W$ 对应的资料 $(c_{ik})_{i,k}$ 无非是

$$c_{ik}=\sum_{j\in J} a_{ij}b_{jk}, \quad i\in I,\ k\in K \tag{3.3}$$

   留意到上式的 $\sum_j$ 对每个 (i,k) 都有限.

将上述讨论应用于有限维向量空间, 则下述结果水到渠成. 请回忆 §3.2 介绍的矩阵空间 $M_{m\times n}(F)$.

定理 3.4.9 设 V 和 W 为有限维向量空间, 分别带选定的有序基 $v_1,\dots,v_n$ 和

$w_1,\dots,w_m$, 其中 $n,m\in\mathbb{Z}_{\geq 1}$. 此时有向量空间的同构

$$\begin{aligned}\mathcal{M}:\mathrm{Hom}(V,W)&\xrightarrow{1:1}M_{m\times n}(F)\\ T&\longmapsto (a_{ij})_{\substack{1\leq i\leq m\\1\leq j\leq n}}\end{aligned}$$

其中 $(a_{ij})_{i,j}=\mathcal{M}(T)$ 由以下性质刻画:

$$Tv_j=\sum_{i=1}^{m}a_{ij}w_i,\quad 1\leq j\leq n.$$

证明 相当于在之前的讨论中取 $I=\{1,\dots,m\}$ 和 $J=\{1,\dots,n\}$. 关于 "存在至多有限个 i 使得 $a_{ij}\neq 0$" 的条件在此是多余的. □

映射合成的描述也同样转译到矩阵空间上. 请先回忆矩阵乘法的定义 3.2.4 和关于交换图表的约定 2.2.3.

定理 3.4.10 设 U, V, W 为有限维向量空间, 分别带选定的有序基 $u_1,\dots,u_r$, $v_1,\dots,v_n$ 和 $w_1,\dots,w_m$. 以下图表交换:

$$\begin{array}{ccc}\mathrm{Hom}(V,W)\times\mathrm{Hom}(U,V) & \xrightarrow{\text{映射合成}} & \mathrm{Hom}(U,W)\\ \downarrow{\scriptstyle\mathcal{M}}\quad\downarrow{\scriptstyle\mathcal{M}} & & \downarrow{\scriptstyle\mathcal{M}}\\ M_{m\times n}(F)\times M_{n\times r}(F) & \xrightarrow[\text{矩阵乘法}]{} & M_{m\times r}(F)\end{array}$$

换言之, $\mathcal{M}(ST)=\mathcal{M}(S)\mathcal{M}(T)$, 左式是映射合成, 右式是矩阵乘法.

证明 比较矩阵乘法的定义和 (3.3), 其中代入 $K=\{1,\dots,r\}$. □

基于上述结果, 足以用一句话说明矩阵乘法的交换律, 分配律等性质.

证明 (命题 3.2.5) 化约为线性映射相对于合成运算的种种相应性质, 如命题 3.4.7 所述. □

且看矩阵的两个特殊例子.

⋆ 无论如何选取 V 和 W 的基, 零映射 $0:V\to W$ 对应的矩阵都是**零矩阵**:

$$0=0_{m\times n}:=\begin{pmatrix}0&\cdots&0\\ \vdots&\ddots&\vdots\\ 0&\cdots&0\end{pmatrix}\in M_{m\times n}(F).$$

⋆ 任取 V 的有序基 $v_1, \ldots, v_n$, 借以将 $\mathrm{End}(V) := \mathrm{Hom}(V, V)$ 等同于 $M_{n\times n}(F)$. 此时恒等映射 id_V 由 $v_i \mapsto v_i$ 刻画, 因而对应到**单位矩阵**:

$$1 = 1_{n\times n} := \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix} \in M_{n\times n}(F),$$

其中留白部分全为 0; 换言之, $1_{n\times n}$ 只有对角矩阵元取为 1, 其余矩阵元全为 0.

推论 3.4.11 *对所有 $n \in \mathbb{Z}_{\geq 1}$, 集合 $M_{n\times n}(F)$ 对矩阵加法和乘法成为非零环, 其乘法幺元是 $1_{n\times n}$, 零元是 $0_{n\times n}$.*

证明 这不外是推论 3.4.8 的转译. □

参考文献

[1] 丘维声. **简明线性代数**. 北京: 北京大学出版社, 2002 (引用于 p. 1).

[2] 李文威. **代数学方法 (第一卷)**. Vol. 67.1. 现代数学基础丛书. 北京: 高等教育出版社, 2019. ISBN: 978-7-04-050725-6 (引用于 p. 39).

[3] 郝兆宽, 杨跃. **集合论：对无穷概念的探索**. 逻辑与形而上学教科书系列. 上海: 复旦大学出版社, 2014. ISBN: 978-7-309-10710-4 (引用于 p. 23).