线性代数 I 笔记

Linear Algebra I Notes

丁毅

中国科学院大学，北京 100049

Yi Ding

University of Chinese Academy of Sciences, Beijing 100049, China

2023.10 - 2024.1

序言

本书为笔者本科时的代数笔记，包含线性代数和抽象代数中的常见内容，以及少部分拓展内容。本书用黑色表示笔记内容的主干框架，用灰色以及有色方框等表示对主干内容的补充、对晦涩概念的理解、定理的具体证明过程等，采用红色对重点知识进行强调，同时适当配有插图。这样的颜色和结构安排既突出了知识的主要框架，也保持了笔记的深度和广度，并且不会因为颜色过多而导致难以锁定文本内容，乃是尝试了多种安排后挑选出的最佳方案。如果读者有更佳的颜色和排版方案，可以将建议发送到笔者邮箱，在此感谢。

由于个人精力及知识水平有限，书中难免有不妥、错误之处，望不吝指正，在此感谢。

目录

序言 **I**

1 代数的起源 **1**

1.1 从代数起源到低阶行列式 1

1.2 集合 (set) 与映射 (map) 1

1.2.1 集合的相关概念 1

1.3 二元关系与商映射 2

1.3.1 二元关系 2

1.3.2 等价关系 2

1.3.3 偏序关系 2

1.4 置换 3

1.4.1 置换的基本概念 3

1.4.2 与置换相关的定理/推论 5

1.5 整数的算术 6

1.5.1 与整数相关的定理/推论 6

1.6 第一章思考题 7

2 矩阵 (matrices) **8**

2.1 向量空间 8

2.1.1 向量空间的基本概念 8

2.1.2 向量空间的定理/推论 9

2.1.3 线性方程组的解集情况 10

2.1.4 线性方程组与向量空间的联系补充 10

2.1.5 线性相关与线性无关补充 10

2.1.6 分块矩阵 10

2.2 线性映射与矩阵运算 11

2.2.1 线性映射的基本概念 11

2.2.2 矩阵运算的基本概念 11

2.2.3 常见的特殊矩阵 11

2.2.4 线性方程组中的向量空间 11

2.2.5 理解矩阵是一种线性映射 11

2.3 第二章思考题 11

3 行列式 (determinant) 12
3.1 行列式的构造和刻画 . . . 12
3.1.1 线性、多重线性映射 . . . 12
3.1.2 对称、斜对称函数 . . . 12
3.1.3 行列式的定义 . . . 12
3.1.4 行列式基本计算方法 . . . 12
3.2 行列式的特性 . . . 12
3.2.1 常见的特殊行列式 . . . 12
3.2.2 由伴随矩阵求矩阵逆 . . . 12
3.2.3 斜对称多重线性函数的重要性质 . . . 12
3.2.4 行列式的性质 . . . 12
3.2.5 伴随矩阵和 Cramer's Rule . . . 12
3.3 Laplace Expansion 和 Binet-Cauthy Theorem . . . 12
3.3.1 Laplace Expansion（拉普拉斯展开） . . . 12
3.3.2 Binet-Cauthy Theorem（比内-柯西定理） . . . 12
3.3.3 “子式”的辨析 . . . 12
3.4 八大常见行列式及其解法 . . . 12
3.5 第三章思考题 . . . 12

4 群 (group)、环 (ring)、域 (field) 13
4.1 群的概念与类型 . . . 13
4.1.1 群的基本概念 . . . 13
4.1.2 一些特殊的群 . . . 13
4.1.3 与群有关的定理/推论 . . . 13
4.2 群同态 . . . 13
4.2.1 陪集与 Lagrange Theorem . . . 14
4.2.2 正规子群 . . . 14
4.2.3 群同态与群同构 . . . 14
4.3 群作用在集合上 . . . 14
4.3.1 群对集合的作用及其推论 . . . 14
4.3.2 Sylow Theorem . . . 14
4.4 有限群的结构特点 . . . 14
4.4.1 有限群的结构及其推论 . . . 14
4.4.2 三大同构定理 . . . 14
4.4.3 其它常用结论 . . . 14
4.5 群思维导图 . . . 14
4.6 环和域 . . . 14
4.6.1 环的相关概念 . . . 14

4.6.2 一些特殊的环 . . . 14
4.6.3 域的相关概念 . . . 14
4.6.4 一些特殊的域 . . . 14
4.7 环思维导图 . . . 14
4.8 群环域典型问题深入 . . . 14
4.8.1 “模”与商空间 . . . 15
4.8.2 子群/正规子群的传递性、交、积 . . . 15
4.8.3 子环/理想的传递性、交、积 . . . 15
4.8.4 群、环、域同态 . . . 15
4.8.5 证明某个群非单 . . . 15
4.8.6 主理想的定义与表示 . . . 15
4.8.7 从环过渡到域 . . . 15
4.8.8 p^2 阶群、p 群、pq 群的性质 . . . 15
4.9 第四章思考题 . . . 15

5 多项式 **16**
5.1 一元多项式环 . . . 16
5.2 因式分解 . . . 16
5.3 上多项式的根 . . . 16
5.4 对称多项式 . . . 16
5.5 第五章思考题 . . . 16

参考文献 **17**

第1章 代数的起源

1.1 从代数起源到低阶行列式

一般方程根式解：n 次一般方程 $(n \geq 5)$ 没有根式解: $a_n x^n + a_{n-1}x^{n-1} + ... + a_0 = 0$

对角矩阵：n 阶对角矩阵 (diagnal matrix)：

$$D = \begin{bmatrix} a_{11} & 0 & ... & 0 \\ 0 & a_{22} & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & ... & ... & a_{nn} \end{bmatrix}$$

当 $a_{11} = a_{22} = ... = a_{nn} = a$ 时，D 称为纯量矩阵，记为 $diag_n(a)$，其中 $diag$ 指代英文中的 diagnal (adj. 对角的)。矩阵 $diag_n(1)$ 称为 n 阶单位矩阵 (identity matrix of order n)，记作 I_n 或 I。

低阶行列式：一阶、二阶、三阶行列式（略）

1.2 集合 (set) 与映射 (map)

1.2.1 集合的相关概念

差集： $X \backslash Y$ 或 $X - Y$，表示集合 $\{x \mid x \in X, x \notin Y\}$。

笛卡尔积： $X \times Y = \{(x, y) \mid x \in X, x \in Y\}$，$n$ 阶笛卡尔积：$X^n = X \times X \times X ... X$（$n$ 个 X 相乘）

集合的势（基数）：设 X, Y 为两集合，如果存在双射 $f : X \to Y$，则称 X 与 Y 等势（或有相同的基数），记为 $cardX = cardY$，或 $X \sim Y$。其中 $card$ 代指英文中的 cardinal（n. 基数）。容易证明，基数满足如下运算，设 X 为 n 元集合，Y 为 m 元集合，则有：$|X| = cardX = n$，$|Y| = cardY = m$，$|X \times Y| = card(X \times Y) = nm$, $|X \cup Y| + |X \cap Y| = n + m$.

容斥原理： $|S \cup T| + |S \cap T| = |S| + |T|$

映射的原像与像：“原像”即为映射 f 的定义域，也就是 X，“像”即为映射 f 的值域，并且值域 $Im(f) \subseteq Y$，当且仅当 f 为满射时取等。$Im(f)$ 表示映射 f 的值域，也可以用 $f(X)$ 表示 f 的值域。

映射的逆：

$$f\text{有逆} \iff f\text{为双射}$$
$$f\text{有左逆} \iff f\text{为单射}$$
$$f\text{有右逆} \iff f\text{为满射}$$
$$\text{若映射}f\text{有逆，则逆唯一}$$

集合的幂集：集合 X 的所有子集构成的集合称为 X 的幂集，记为 $\mathcal{P}(X)$.

1.3 二元关系与商映射

1.3.1 二元关系

二元关系定义：给定两个集合 X,Y，且 $\omega \subset X \times Y$，则称 ω 为 X,Y 之间的一个二元关系。若 $(x,y) \in \omega$, 则称 x,y 有二元关系 ω，记为 $x\omega y$.

对二元关系定义的理解：给定集合 $X = \{$喜羊羊，沸羊羊，美羊羊，灰太狼，红太狼$\}$，定义 $\heartsuit = \{$（沸羊羊，美羊羊），（美羊羊，喜羊羊），（灰太狼，红太狼），（红太狼，灰太狼）$\}$，显然 $\heartsuit$ 是 X,Y 之间的一个二元关系，且对沸羊羊，美羊羊 $\in X$，有沸羊羊 $\heartsuit$ 美羊羊，但是反之则不成立，也即美羊羊 $\heartsuit$ 沸羊羊不成立。

1.3.2 等价关系

等价关系定义：等价关系是一种（一类）特殊的二元关系。满足下面三条性质的二元关系称为等价关系.

$$\text{反身性（自反性）：} x \sim x$$
$$\text{对称性：} x \sim y \Longrightarrow y \sim x$$
$$\text{传递性：} x \sim y,\ y \sim z \Longrightarrow x \sim z$$

等价类：设 $\sim$ 是 X 上的一个等价关系，对元素 $x \in X$，定义 X 关于 $\sim$ 的、含有元素 x 的等价类为 $\bar{x} = \{x \in X \mid x \sim x'\}$

商集： X 关于等价关系 $\sim$ 的全体等价类构成的集合称为 X 关于 $\sim$ 的商集，记为 $X/\sim$

划分：通过某种依据，将集合 X 分为数份并构成新集合，这个新集合叫作 X 的一种划分。且有定理：X 上的等价关系与它的划分一一对应

1.3.3 偏序关系

偏序关系定义：偏序关系是一种特殊的二元关系 ω。满足下面三条性质的二元关系称为偏序关系.

$$\text{反身性（自反性）：} x \sim x$$
$$\text{反对称性：} x \sim y,\ y \sim x \Longrightarrow y = x$$
$$\text{传递性：} x \sim y,\ y \sim z \Longrightarrow x \sim z$$

可比： $x,y \in A, x$ 与 y 可比 $\Longleftrightarrow x \preceq y$ 或 $y \preceq x$

全序（集）：全序是一种特殊的偏序关系。若集合 X 上的一个偏序关系 $\preceq_0$ 满足：$\forall x, y \in A$, 都有 x, y 可比，也即 $\forall x, y \in A$, 有 $x \preceq_0 y$ 或 $y \preceq_0 x$，则称偏序关系 $\preceq_0$ 为全序，同时称集合 X 为全序集。

覆盖： $x, y \in A, x \preceq y$, 若不 $\exists z \in A$ 使得 $x \preceq z \preceq y$, 则称 y 覆盖 x.

例如 $A = \{1, 2, 4, 9\}$ 上的整除关系，9 覆盖 1，4 覆盖 2，4 不覆盖 1

偏序集：由集合 A 和 A 上的一个偏序关系构成的“数对”，称为偏序集，记作 $(A, \preceq)$

如 $(\mathbb{N}, \leq)$ 和 $(\mathcal{P}(A), \subseteq)$，其中 $\mathcal{P}(A)$ 表示 A 的全体子集构成的集合。

偏序图（哈赛图）：

哈赛图是一种简化的偏序关系图 (一般由下向上看), 以 $(\{1, 2, 3, 4, 5, 6, 7\}$, 整除) 的哈赛图为例：

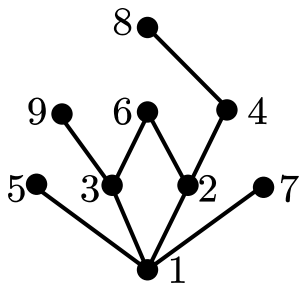

图 1.1: 哈赛图示例

1.4 置换

1.4.1 置换的基本概念

置换的定义：置换是由 $X \longrightarrow X$ 的一个双射，其中 X 为 n 元有限非空集合。

可以思考一下“置换”和“排列”之间的联系

对称群的定义： n 元有限非空集合 X 的全体置换构成集合 S_n，称 S_n 为集合 X 上的对称群。且易证:

$$|S_n| = card(S_n) = n!$$

置换的乘法（置换的复合）：关键思路：“谁变成谁”。满足结合律，不一定满足交换律。

$$\text{设}\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \nu = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \text{则：}$$

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

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

注意：置换乘法从右向左计算（置换是一个双射，想想映射的复合）

循环：设置换 σ 是一个循环，如果 σ“移动了”X 中的 r 个元素，则称 σ 为 r 循环（常写作 $r-cycle$），记为 $\sigma=(i_1,i_2,...,i_r)$，且可以用循环图表示，举两个例子：

$$\sigma=\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}=(1\ 2\ 3)\text{ 为 }3-cycle\text{，如图 1.2}$$

$$\nu=\begin{pmatrix}1&2&3&4&5\\5&1&4&2&3\end{pmatrix}=(1\ 5\ 3\ 4\ 2)\text{ 为 }5-cycle\text{，如图 1.3}$$

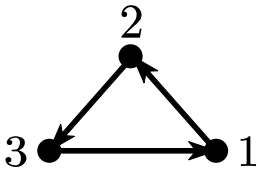

图 1.2: $\sigma=(1\ 2\ 3)$ 循环图

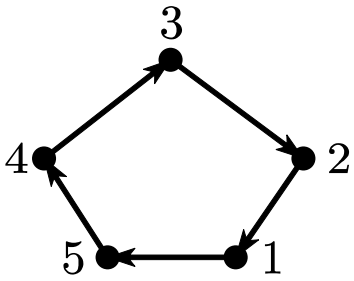

图 1.3: $\nu=(1\ 5\ 3\ 4\ 2)$ 循环图

特别地, 不移动（即固定）所有元素的循环为 1 循环，也即恒等置换 (恒等变换)。一个 $2-cycle$ 仅交换 X 中的一对元素，故称为对换。

循环的乘法（复合）：循环的乘法可按置换乘法来做：

$$\begin{pmatrix}1&2\end{pmatrix}\begin{pmatrix}1&3&4&2&5\end{pmatrix}=\begin{pmatrix}1&2&3&4&5\\2&1&3&4&5\end{pmatrix}\begin{pmatrix}1&2&3&4&5\\3&5&4&2&1\end{pmatrix}=\begin{pmatrix}1&2&3&4&5\\3&5&4&1&2\end{pmatrix}$$
$$=\begin{pmatrix}1&3&4\end{pmatrix}\begin{pmatrix}2&5\end{pmatrix}$$

也可以按照循环的意义来做：从右向左依次复合，谁变成谁、再变成谁。

从右向左算，得到哪个数字就继续看这个数字的变化，如得到“(14”下一步便看 4 变成了谁，直至形成闭环，打上右括号。然后为避免遗漏，从小到大考虑暂未变换的数。

置换相交/不相交：两个置换 σ_1,σ_2 称为不相交的如果：$\forall i\in\{1,2,...,n\},i$ 至多被 σ_1,σ_2 中的一个置换移动。反之则称 σ_1,σ_2 相交。另外，由于置换可以通过置换基本定理写为循环乘积的形式，那么不相交可等价的定义为：两个置换的循环表示中不存在相同元素。

置换的奇偶性：若一个置换 σ 以写成奇数（偶数）个对换的乘积，则称置换 σ 为奇置换，并定义符号：

$$\varepsilon_\sigma=\begin{cases}-1&,\sigma\text{为奇置换}\\1&,\sigma\text{为偶置换}\end{cases}$$

由置换基本定理、循环的对换分解，有结论：

$$\varepsilon_\sigma=(-1)^{\sum_{i=1}^m(r_i-1)},\varepsilon_{\sigma\nu}=\varepsilon_\sigma\varepsilon_\nu$$

置换的逆：略

置换的阶：对于一个置换 $\sigma \in S_n$, 若 $\sigma^p = e$，则称 σ 为一个 p 阶置换。且有定理：

$$\forall\, r-cycle\ \sigma \in S_n,\ 有 \sigma^r = e$$

也即 $r-cycle$ 是一个 r 阶循环。再由置换基本定理，可推得：

$$\forall\, \sigma = \begin{pmatrix} i_1 & i_2 & ... & i_{r_1} \end{pmatrix} ... \begin{pmatrix} j_1 & j_2 & ... & j_{r_s} \end{pmatrix},\ \sigma的阶数为\ p = l.c.m(r_1, r_2, ..., r_n)$$

补充：S_n 中元素的最高阶为 $m = l.c.m(1,2,3,...,n)$，经查阅资料，$l.c.m(1,2,3,...,n) = f(n)$ 为 $Landau's function$， 渐近于 e

置换作用于函数：

设 $f(x_1, x_2, ..., x_n)$ 为 n 元函数，定义：$\sigma \circ f(x_1, x_2, ..., x_n) = f(x_{\sigma(1)}, x_{\sigma(2)}, ..., x_{\sigma(n)})$

对称/斜对称函数：对称函数：一个定义在 X^n 上的函数称为对称的如果：

$$\forall\, x_i, x_j \in I, f(x_1, x_2, ..., x_i, ..., x_j, ..., x_n) = f(x_1, x_2, ..., x_j, ..., x_i, ..., x_n)$$

上述定义可等价地写为：

$$\forall\, \sigma \in S_n, \sigma \circ f = f$$

斜对称函数：一个定义在 X^n 上的函数称为斜对称的如果：

$$\forall\, x_i, x_j \in I, f(x_1, x_2, ..., x_i, ..., x_j, ..., x_n) = -f(x_1, x_2, ..., x_j, ..., x_i, ..., x_n)$$

常见的对称函数如：

$$f(x_1, x_2, ..., x_n) = \sum_{i=1}^{n} x_i^2, \quad g(x_1, x_2, ..., x_n) = \sum_{1 \le i \le j \le n} x_i x_j = \sum_{j=1}^{n} \sum_{i=1}^{j} x_i x_j$$

常见的斜对称函数如 n 元列向量行列式（n 元行向量行列式同理）：

$$det(\vec{x}_1 \vec{x}_2, ..., \vec{x}_n) = \begin{vmatrix} \vec{x}_1 & \vec{x}_2 & ... & \vec{x}_n \end{vmatrix} = \begin{vmatrix} x_{11} & x_{12} & ... & x_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1} & x_{n2} & ... & x_{nn} \end{vmatrix},\ \vec{x}_i = \begin{bmatrix} x_{1i} \\ \vdots \\ x_{ni} \end{bmatrix} 为n维列向量$$

1.4.2 与置换相关的定理/推论

置换基本定理：每一个非恒等置换都可分解为数个不相交的循环之积，且这样的分解唯一（不考虑顺序），也即：

$$\forall\, \sigma \in S_n,\ \exists\ 唯一确定的循环\ \nu_1, \nu_2, ..., \nu_n\ 满足：\ \sigma = \nu_1 \nu_2 ... \nu_n$$

循环的对换分解：对任意长度为 r 的循环 ν，ν 可以写为 $(r-1)$ 个对换的乘积，也即：

$$\nu = \begin{pmatrix} i_1 & i_2 & ... & i_r \end{pmatrix} = \begin{pmatrix} i_1 & i_r \end{pmatrix} \begin{pmatrix} i_1 & i_{r-1} \end{pmatrix} ... \begin{pmatrix} i_1 & i_2 \end{pmatrix}$$

这里要注意是倒序：从 r 到 2。并且由此可以推得任意置换的对换分解，略。

奇偶置换个数相同：一个 n 元对称群 S_n 中，全体奇置换 $\overline{S_n}$ 与全体偶置换 $\underline{S_n}$ 的个数相同，即 $card\ \overline{S_n} = card\ \underline{S_n} = \frac{n!}{2}$

置换的共轭作用： $\forall\ \sigma,\ \nu \in S_n,$ 设 $\nu = (i_1\ i_2\ ...\ i_{r_1})...(j_1\ j_2\ ...\ j_{r_s})$，有：

$$\sigma\nu\sigma^{-1} = \begin{pmatrix}\sigma(i_1) & \sigma(i_2) & ... & \sigma(i_{r_1})\end{pmatrix}...\begin{pmatrix}\sigma(j_1) & \sigma(j_2) & ... & \sigma(j_{r_s})\end{pmatrix}$$

证明：置换的共轭作用

先证 ν 为循环的情况。设 $\nu = \begin{pmatrix}i_1 & i_2 & ... & i_r\end{pmatrix}$，则知 $i_1, i_2, ..., i_r \in \{1, 2, ..., n\}$, 设 $k \in \{1, 2, ..., n\}$, 下面分类：

当 $\sigma^{-1}(k) \in \{1, 2, ..., n\} \setminus \{i_1, i_2, ..., i_r\}$ 时，ν 不移动 $\sigma^{-1}(k)$, 即:

$$\nu\sigma^{-1}(k) = \nu(\sigma^{-1}(k)) = \sigma^{-1}(k) \Longrightarrow \sigma\nu\sigma^{-1}(k) = \sigma(\nu\sigma^{-1}(k)) = \sigma\sigma^{-1}(k) = e(k)$$

当 $\sigma^{-1}(k) \in \{i_1, i_2, ..., i_r\}$ 时，设 $\sigma^{-1}(k) = i_s,\ s \in \{1, 2, ..., r\}$, 则 $k = \sigma(i_s)$, 有：

$s \leq r-1$ 时：

$$\nu(\sigma^{-1}(k)) = \nu(i_s) = i_{s+1} \Longrightarrow \sigma\nu\sigma^{-1}(\sigma(i_s)) = \sigma\nu\sigma^{-1}(k) = \sigma(\nu(\sigma^{-1}(k))) = \sigma(i_{s+1})$$

$s = r$ 时：

$$\nu(\sigma^{-1}(k)) = \nu(i_r) = i_1 \Longrightarrow \sigma\nu\sigma^{-1}(\sigma(i_s)) = \sigma\nu\sigma^{-1}(k) = \sigma(\nu(\sigma^{-1}(k))) = \sigma(i_1)$$

于是$\sigma^{-1}(k) \in \{i_1, i_2, ..., i_r\}$ 时，令$g = \sigma\nu\sigma^{-1}$, 则有：$g(\sigma(i_s)) = \begin{cases}\sigma(i_{s+1}) & , s \leq r-1 \\ \sigma(i_1) & , \ s = r\end{cases}$

综上，写为循环形式即得：

$$\sigma\nu\sigma^{-1} = \begin{pmatrix}\sigma(i_1) & \sigma(i_2) & ... & \sigma(i_r)\end{pmatrix}$$

再由置换基本定理进行推广，命题得证。

1.5 整数的算术

1.5.1 与整数相关的定理/推论

算术基本定理： $\forall\ n \in \mathbb{N}_+,\ n \geq 2,\ \exists!\ p_1, p_2, ..., p_r, k_1, k_2, ..., k_r,$ 其中p_i为素数, $k_i \in \mathbb{N}_+$，使得：

$$n = p_1^{k_1} p_2^{k_2} ... p_r^{k_r}$$

欧几里得定理：素数有无穷多个。

带余除法： $\forall a, b \in \mathbb{N},\ \exists! q, r \in \mathbb{N}$ 使得 $a = bq + r$, 其中 $0 \leq r < b$

欧几里得算法（辗转相除法）： $\forall\, a,b\in\mathbb{N}_+$, 令 $r_0=a, r_1=b$ 并定义 $r_i=q_{i+1}r_{i+1}+r_{i+2}$, 其中 $0\le r_{i+2}<r_{i+1}$, 则存在最小的整数 n 使得 $r_{n+2}=0$, 且有 $r_{n+1}=g.c.d(a,b)$

定理： 三个整数的最大公因数与最小公倍数满足如下结论：

$$g.c.d(a,b,c)=g.c.d(a,g.c.d(b,c)) \qquad l.c.m(a,b,c)=l.c.m(a,l.c.m(b,c))$$

互质定理： $\forall\, m,n\in\mathbb{Z}, mn\neq 0, \exists\, s,t\in Z$, 使得 $g.c.d(m,n)=s\,|m|+t\,|n|$ 。特别地，当 m,n 互质时，$g.c.d(m,n)=1$，于是得到互质定理：正整数 m,n 互质 $\Longleftrightarrow \exists\ s,t\in Z$, 使得 $sm+tn=1$.

补充：由欧几里得算法求互质定理中的整数 s,t

以 $g.c.d(54,20)$ 为例，作辗转相除如下：

$r_0=54,\ r_1=20$

$r_0=q_1r_1+r_2$

$\Longrightarrow q_1=2,\ r_2=14$

$r_1=q_2r_2+r_3$

$\Longrightarrow q_2=1,\ r_3=6$

$r_2=q_3r_3+r_4$

$\Longrightarrow q_3=2,\ r_4=2$

$r_3=q_4r_4+r_5$

$\Longrightarrow q_4=3,\ r_5=0$

$\Longrightarrow g.c.d(54,20)=r_4=2$

$$\begin{aligned}
g.c.d(54,20)&=r_4\\
&=r_2-q_3r_3\\
&=r_2-q_3(r_1-q_2r_2)\\
&=-q_3r_1+(1+q_2q_3)r_2\\
&=-q_3r_1+(1+q_2q_3)(r_0-q_1r_1)\\
&=(1+q_2q_3)r_0+(-q_1-q_1q_2q_3-q_3)r_1
\end{aligned}$$

$$\Longrightarrow\begin{cases}s=1+q_2q_3=3\\ t=-q_1-q_1q_2q_3-q_3=-8\end{cases}$$

1.6 第一章思考题

1. $\forall\, r-cycle\ \sigma\in S_n$, **是否有** $\sigma^r=e$**?**

> **解：1.** $\forall\, r-cycle\ \sigma\in S_n$, **是否有** $\sigma^r=e$**?**
>
> 容易证明，$\forall\, r-cycle\ \sigma\in S_n$，有 $\sigma^r=e$，因此 $r-cycle$ 也是一个 r 阶置换。

第 2 章　矩阵 (matrices)

2.1　向量空间

2.1.1　向量空间的基本概念

n 维向量空间：

我们将向量与其直角坐标等同，则 n 维向量空间 $\mathbb{R}^n = \{\vec{x} = (x_1, ..., x_n) \mid x_1, x_2, ..., x_n \in \mathbb{R}\}$ 是一个由向量组成的集合, 且容易验证其对线性运算封闭，称为 n 维向量空间，更严谨的称法是“n 维欧式几何空间”。

n 维向量空间是线性空间 (vector space) 的一种，下面我们给出线性空间的定义。

设 F 是域，V 是一集合。在 V 中定义运算加法：

$$\forall\, v, u \in V,\ \exists!\, \mu \in V \text{ 使 } \mu = v + u$$

且 $(V,\ +)$ 构成 *Abel* 群 (也即：V 对加法封闭，满足加法结合律和交换律，具有加法单位元，任意元素对加法可逆)。在 F, V 之间定义数乘：

$$\forall\, a \in F,\ v \in V,\ \exists!\, u \in V \text{ 使 } u = a \cdot v$$

且构成数乘满足结合律、具有单位元，加法和数乘满足左右分配率。此时称集合 V 是域 F 上的线性空间，F 中的元素称为纯量或数量，V 中的元素称为向量。在本书中，如无特别说明，我们的“向量空间”都指的是“n 维欧氏几何空间”。

下面是一些常见的线性空间：

实数域上的全体 m 行 n 列矩阵构成一个线性空间，称为实数矩阵空间，记为 $M_{m\times n}(\mathbb{R})$。

实区间 $[a, b] \subseteq \mathbb{R}$ 上的全体连续函数构成一个线性空间，称为连续函数空间，记为 $C_{[a,b]}$。

子空间：若 n 维向量空间 $\mathbb{R}^n$ 的非空子集满足 V 满足：$\forall\, \vec{a}, \vec{b} \in V, \alpha, \beta \in \mathbb{R},\ (\alpha\vec{a} + \beta\vec{b}) \in V$, 则称 V 为 $\mathbb{R}^n$ 的子空间。

容易证明，$\forall\, n \geq 2, \mathbb{R}^n$ 有无数个子空间。

向量组的线性张成 *Span*：设有限集 $A = \{\vec{a}_1, \vec{a}_2, ..., \vec{a}_n\} \subset \mathbb{R}^n$, 定义 A 的线性张成：

$$Span\ A = \{\alpha_1\vec{a}_1 + \alpha_2\vec{a}_2 + ... + \alpha_n\vec{a}_n \mid \alpha_1, \alpha_2, ..., \alpha_n \in \mathbb{R}\}$$

有的教材也记作 $Span(A)$。

容易验证，$Span\ A$ 是 $\mathbb{R}^n$ 的一个子空间。且有推论：设 U, V 为 $\mathbb{R}^n$ 的两个子空间，则 $U \cap V$ 和 $U + V$ 也是 $\mathbb{R}^n$ 的一个子空间，但 $U \cup V$ 不一定是子空间。

特别地，我们有：$\mathbb{R} = Span\,\{\vec{e}_1, \vec{e}_2, ..., \vec{e}_n\}$

线性方程组、$\mathbb{R}^n$、行列式间的联系：定理：m 行 n 列齐次线性方程组 $A\vec{x} = \vec{0}$ 的解集 $X = \left\{\vec{x} \mid A\vec{x} = \vec{0}\right\}$ 构成 $\mathbb{R}^n$ 的子空间。

定理：m 行 n 列线性方程组 $A\vec{x}=\vec{b}$ 有解 $\Longleftrightarrow \vec{b}\in Span\ A$

定理：若 $m=n$，且行列式 $det(A)\neq 0$，则 $\forall\ \vec{b}\in\mathbb{R}^n$，方程 $A\vec{x}=\vec{b}$ 有唯一解

线性相关：设向量组 $A=\{\vec{a}_1,\vec{a}_2,...,\vec{a}_n\}$，其中 $\vec{a}_i\in\mathbb{R}^m$，若存在不全为零的常数 $\alpha_1,\alpha_2,...,\alpha_n$ 使得 $\alpha_1\vec{a}_1+\alpha_2\vec{a}_2+...+\alpha_1\vec{a}_n=\vec{0}$，则称向量组 A 线性相关。

我们常说的“矩阵 A 线性相关”，或者“A 的某几列线性相关”，实际上是指由这些向量构成的向量组线性相关，只是为了简洁与方便，我们直接称为“矩阵 A 线性相关”。

并且设 $A=[\vec{a}_1,\vec{a}_2,...,\vec{a}_n]$，向量组 $\hat{A}=\{\vec{a}_1,\vec{a}_2,...,\vec{a}_n\}$，则我们有推论：

$$\begin{aligned}&\hat{A}\text{ 线性相关}\\ \Longleftrightarrow\ &\exists\ \vec{a}_i\in\hat{A},\text{使得 }\vec{a}_i\in Span(\hat{A}\setminus\vec{a}_i)\\ \Longleftrightarrow\ &A\vec{x}=\vec{0}\text{ 存在非零解}\\ \Longleftrightarrow\ &A\vec{x}=\vec{0}\text{ 存在无数解}\end{aligned}$$

维数 (dimension) 与秩 (rank)：维数：设 V 是 $\mathbb{R}^n$ 的一个子空间，V 的一组基的元素个数称为 V 的维数，记为 $dim(V)$ 或 $dim\ V$。设 V_1，V_2 是 $\mathbb{R}^n$ 的两个子空间，定义子空间的和 $V_1+V_2=\{\vec{v}_1+\vec{v}_2\mid\vec{v}_1\in V_1,\vec{v}_1\in V_2\}$，则 V_1+V_2 构成一个子空间，且有推论：

$$dim(V_1+V_2)+dim(V_1\cap V_2)=dim\ V_1+dim\ V_2$$

秩：设矩阵 $A=[\vec{a}_1,\vec{a}_2,...,\vec{a}_n]$，其中 $\vec{a}_i\in\mathbb{R}^m$，向量组 $\hat{A}=\{\vec{a}_1,\vec{a}_2,...,\vec{a}_n\}$，我们定义矩阵 A 和向量组 $\hat{A}$ 的秩都为 $dim(Span\ \hat{A})$，记作 $rank\ A=rank\ \hat{A}=dim(Span\ \hat{A})$。并且可以证明：一个向量组的秩等于它的极大线性无关组的元素个数。

求向量组极大线性的方法：筛选迭代法

为求一个不全为零的向量组的极大线性无关子集，我们可以采取筛选法。在向量组中取第一个非零向量，记为 $\vec{a}_{i_1}$，然后取向量组中第一个不属于 $Span\{\vec{a}_{i_1}\}$ 的向量，记为 $\vec{a}_{i_2}$，再取 $\vec{a}_{i_3}$，如此重复下去，最终得到一个极大线性无关子集 $\{\vec{a}_{i_1},\vec{a}_{i_2},...,\vec{a}_{i_s}\}$，$s$ 即为这个向量组的秩。

注：此方法只对某些特别的向量组有效。

矩阵的行列空间：设矩阵 $A\in M_{m\times n}(\mathbb{R})$，则 A 既可以看作 m 个行向量，也可以看作 n 个列向量，由此引出行空间和列空间的概念：

行空间：记 A 的 m 个行向量为 $\vec{a}_1,...\vec{a}_m$，定义矩阵 A 的行空间 $V_{r(A)}:=Span\{\vec{a}_1,...\vec{a}_m\}$，并且容易验证，$V_{r(A)}$ 是 $\mathbb{R}^n$ 的子空间（每个行向量都属于 $\mathbb{R}^n$）。（$V_{r(A)}$ 中的字母 r 表示 row）

列空间：记 A 的 n 个列向量为 $\vec{a}^1,...\vec{a}^n$，定义矩阵 A 的列空间 $V_{c(A)}:=Span\{\vec{a}^1,...\vec{a}^n\}$，并且容易验证，$V_{c(A)}$ 是 $\mathbb{R}^m$ 的子空间（每个列向量都属于 $\mathbb{R}^m$）。（$V_{c(A)}$ 中的字母 c 表示 column）

行秩 $rank_r(A):=dim\ V_{r(A)}$，列秩 $rank_c(A):=dim\ V_{c(A)}$。

2.1.2 向量空间的定理/推论

基定理：若 V 是 $\mathbb{R}^n$ 的非零子空间，则 V 存在无数组基，且任意两组基的元素个数相同。

基扩充定理：设 U 是 $\mathbb{R}^n$ 的 m 维子空间，V 是 U 的 r 维子空间，$\{\vec{v}_1, \vec{v}_2, ..., \vec{v}_r\}$ 是 V 的一组基，则在 U 中一定可以找到 $m-r$ 个向量 $\vec{u}_1, \vec{u}_2, ..., \vec{u}_{m-r}$，使得 $\{\vec{v}_1, \vec{v}_2, ..., \vec{v}_r, \vec{u}_1, \vec{u}_2, ..., \vec{u}_{m-r}\}$ 是 U 的一组基，也即 $U = Span\{\vec{v}_1, \vec{v}_2, ..., \vec{v}_r, \vec{u}_1, \vec{u}_2, ..., \vec{u}_{m-r}\}$

矩阵行秩列秩相等：$\forall A \in M_{m\times n}(\mathbb{R})$，都有 $rank\ r(A) = rank\ c(A)$，统称为矩阵 A 的秩，记为 $rank\ A$，有的教材也记作 $r(A)$。

秩与方程组解的关系：设线性方程组 $A\vec{x} = \vec{b}$ 的增广矩阵为 C，则：$A\vec{x} = \vec{b}$ 有解 $\iff rank\ A = rank\ C$。

2.1.3 线性方程组的解集情况

1. 判断有解/无解：$A\vec{x} = \vec{b}$ 有解 $\Longleftarrow \vec{b} \in Span\ A$

2. 有解时，判断有唯一解还是无穷解：设 $A \in M_{m\times n}(R)$，定义 A 的核 $ker(A) = \{\vec{x} \mid A\vec{x} = \vec{0}\}$，也可记为 $ker\ A$，则有推论：

$$\forall\ A \in M_{m\times n}(R),\ dim(ker\ A) + rank(A) = n$$

并且，当且仅当 $rank(A) = n$ 时，方程组有唯一解。

3. 有无穷解时，由齐次解的结构得到非齐次解的结构：详见第 2.2 节。

2.1.4 线性方程组与向量空间的联系补充

2.1.5 线性相关与线性无关补充

2.1.6 分块矩阵

定义：略

运算：略

分块矩阵的秩：设 $A \in M_{m\times s}$，$B \in M_{s\times n}$，$C \in M_{s\times s}$，则有：

- $rank(A) + rank(B) - s \le rank(AB) \le \begin{matrix} rank(A) \\ rank(B) \end{matrix}$
- $\begin{matrix} rank(A) \\ rank(B) \end{matrix} \le rank(\begin{bmatrix} A \\ B \end{bmatrix}) \le rank(\begin{bmatrix} A, B \end{bmatrix}) \le rank(A) + rank(B)$
- $rank(\begin{bmatrix} A & O \\ O & B \end{bmatrix}) = rank(A) + rank(B)$
- $rank(A) + rank(B) \le rank(\begin{bmatrix} A & O \\ C & B \end{bmatrix}) \le rank(A) + rank(B) + rank(C)$

2.2 线性映射与矩阵运算

2.2.1 线性映射的基本概念

2.2.2 矩阵运算的基本概念

2.2.3 常见的特殊矩阵

2.2.4 线性方程组中的向量空间

2.2.5 理解矩阵是一种线性映射

2.3 第二章思考题

第 3 章　行列式 (determinant)

3.1　行列式的构造和刻画

3.1.1　线性、多重线性映射

3.1.2　对称、斜对称函数

3.1.3　行列式的定义

3.1.4　行列式基本计算方法

3.2　行列式的特性

3.2.1　常见的特殊行列式

3.2.2　由伴随矩阵求矩阵逆

3.2.3　斜对称多重线性函数的重要性质

3.2.4　行列式的性质

3.2.5　伴随矩阵和 Cramer’s Rule

3.3　Laplace Expansion 和 Binet-Cauthy Theorem

3.3.1　Laplace Expansion（拉普拉斯展开）

3.3.2　Binet-Cauthy Theorem（比内-柯西定理）

3.3.3　“子式”的辨析

3.4　八大常见行列式及其解法

3.5　第三章思考题

第 4 章　群 (group)、环 (ring)、域 (field)

4.1　群的概念与类型

4.1.1　群的基本概念

4.1.2　一些特殊的群

4.1.3　与群有关的定理/推论

4.2　群同态

你好你好

4.2.1 陪集与 Lagrange Theorem

4.2.2 正规子群

4.2.3 群同态与群同构

4.3 群作用在集合上

4.3.1 群对集合的作用及其推论

4.3.2 Sylow Theorem

4.4 有限群的结构特点

4.4.1 有限群的结构及其推论

4.4.2 三大同构定理

4.4.3 其它常用结论

4.5 群思维导图

4.6 环和域

4.6.1 环的相关概念

4.6.2 一些特殊的环

4.6.3 域的相关概念

4.6.4 一些特殊的域

4.7 环思维导图

4.8 群环域典型问题深入

你好你好

4.8.1 “模”与商空间

4.8.2 子群/正规子群的传递性、交、积

4.8.3 子环/理想的传递性、交、积

4.8.4 群、环、域同态

4.8.5 证明某个群非单

4.8.6 主理想的定义与表示

4.8.7 从环过渡到域

4.8.8 p^2 阶群、p 群、pq 群的性质

4.9 第四章思考题

第5章　多项式

5.1　一元多项式环

5.2　因式分解

5.3　上多项式的根

5.4　对称多项式

5.5　第五章思考题

参考文献

[1] 徐晓平. 线性代数 *I* 讲义. 中国科学院大学, 北京, 9 2023.

[2] A.I.Kostrikin. 代数学引论. 高等教育出版社, 北京, 12 2006.

[3] 丘维声. 抽象代数基础. 高等教育出版社, 北京, 8 2015.

[4] 丘维声. 高等代数. 上册. 清华大学出版社, 北京, 11 2018.