

# 线性代数

参考书: 《基础代数》(席南华)  
教材: 《线性代数讲义》(徐晓平)  
《代数学引论》(柯斯特利金)

## 第一章. 代数的起源

### §1.1~1.3 从代数起源到低阶行列式

$n \times n$  一般方程 ( $n \geq 5$ ) 没有根式解:

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 = 0$$

对角矩阵:

$$\begin{bmatrix} a_{11} & 0 & \dots & 0 \\ 0 & a_{22} & \dots & : \\ 0 & 0 & \dots & a_{nn} \end{bmatrix} = \text{diag}(a_{11}, \dots, a_{nn})$$

diagonal adj./n. 对角(线)

当  $a_{11} = a_{22} = \dots = a_{nn} = a$  时, 称为纯量矩阵

记为  $\text{diag}_n(a)$ . 矩阵  $\text{diag}_n(1)$  称为  $n$  阶单位矩阵, 记作  $E_n, E$ , 或  $I_n, I$ .

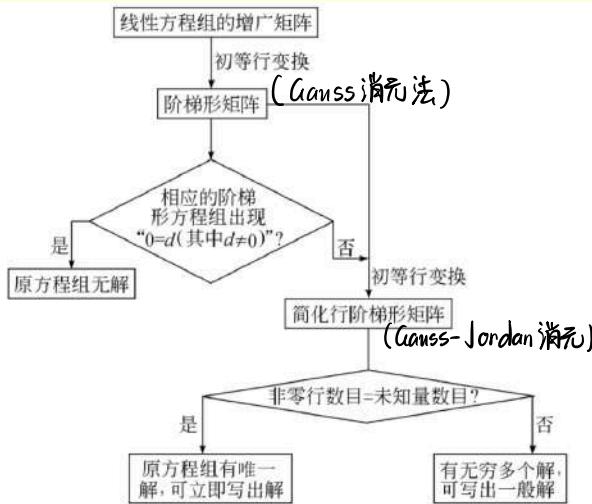
方程组 (a) 与 (b) 等价记作: (a)  $\sim$  (b)

相容	不确定	确定
恰 $b_i = \bar{b}_i$ , 且 $\bar{b}_i \neq 0$ 的方程	先相容, 再 $\text{row} < \text{unknown}$	先相容, 再 $\text{row} = \text{unknown}$ $\Leftrightarrow  \Lambda  \neq 0$

线性方程组的类型			
一般	齐次	$n > m$ 非齐次	$n > m$ 齐次
解的个数	0 1 $\infty$	1 $\infty$	0 $\infty$

高斯的运算次数为  $T_n = \frac{n^3}{3}$  (主要考虑乘法)

线性方程组的 Gauss-Jordan 消元法:



### §1.4 集合与映射

差集:  $X \setminus Y$  或  $X - Y$

$Y \subset X$ , 也称为  $Y$  对  $X$  的补集 (或  $Y$  在  $X$  中的补集)

笛卡尔积:  $X \times Y = \{(x, y) \mid x \in X, y \in Y\}$

$n$  阶笛卡尔积:  $X^n = \underbrace{X \times X \times \dots \times X}_{n \text{ 个相乘}}$

集合的基数(势):

设  $X, Y$  为两集合, 如果存在映射  $f: X \rightarrow Y$ , 则称  $X$  与  $Y$  等势或有相同的基数. 记作  $\text{card } X = \text{card } Y$  或  $X \sim Y$ .

运算:  $|X| = \text{card } X = n$ ,  $|Y| = \text{card } Y = m$

$$|X \times Y| = \text{card}(X \times Y) = n \cdot m$$

$$|X \cup Y| = n+m - |X \cap Y|$$

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

$$\Rightarrow |S_1 \cup S_2 \cup S_3| = |S_1| + |S_2| + |S_3| - |S_1 \cap S_2| - |S_1 \cap S_3| - |S_2 \cap S_3|$$

映射的像:

映射  $f$  的像 =  $f$  的值域 =  $\text{Im } f = \{f(x) \mid x \in X\} = f(X) \subset Y$

映射的原像:

映射  $f$  的原像 =  $f$  的定义域 =  $\{x \in X \mid f(x) \in Y\} = f^{-1}(Y)$

映射的收缩/扩张:

定义  $f: X \rightarrow Y$ ,  $g: X' \rightarrow Y'$

如果  $X \subset X'$ ,  $Y \subset Y'$ , 且  $\forall x \in X$ ,  $f(x) = g(x)$

则称  $f$  为  $g$  的收缩,  $g$  为  $f$  的扩张.

映射的逆:  $(f_1, f_2, \dots, f_n)^{-1} = f_n^{-1} \dots f_2^{-1} f_1^{-1}$

如果  $f$  的逆存在, 则一定唯一.

定理: 映射  $f$  存在逆  $\Leftrightarrow f$  为双射.

$\begin{cases} X \text{ 为有限集} \\ f: X \rightarrow X \text{ 为单射} \end{cases} \Rightarrow f \text{ 为满射}$

$\begin{cases} X \text{ 为有限集} \\ f: X \rightarrow X \text{ 为满射} \end{cases} \Rightarrow f \text{ 为单射}$

集合的并集: 若  $A \cap B = \emptyset$ , 则记  $A \cup B = A \sqcup B$

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  $P(X)$ .

# 8.1.5 等价关系与商映射

二元关系  $W = \{\text{如} <\}$

给定两个集合  $X, Y$ , 且  $W \subset X \times Y$ , 则  $W$  叫作  $X$  与  $Y$  之间的一个二元关系.

二元关系. 若  $(x, y) \in W$ , 则称  $x, y$  有关系  $W$ , 记作  $x \sim y$ .

e.g. 给定集合  $A = \{\text{喜羊羊, 灰太狼, 沸羊羊, 红太狼, 美羊羊}\}$ , 定义二元关系  $\sim = \{( \text{沸羊羊, 美羊羊}), (\text{灰太狼, 红太狼}), (\text{美羊羊, 喜羊羊})\}$

则  $\sim$  为集合  $A$  上的一个二元关系. 显然此二元关系  $\sim$  不满足的反性 " $x \sim x$ ",

不满足对称性 ( $\text{沸} \sim \text{美} \Rightarrow \text{美} \sim \text{沸}$ ), 亦不满足传递性 ( $\text{沸} \sim \text{美}, \text{美} \sim \text{喜} \Rightarrow \text{沸} \sim \text{喜}$ )

等价关系  $\sim$ : (等号 " $=$ " 的推广)

等价关系是一种特殊的二元关系  $W$ , 满足如下性质:

1. 反身性(自反性):  $x \sim x$

2. 对称性:  $x \sim y \Rightarrow y \sim x$

3. 传递性:  $x \sim y, y \sim z \Rightarrow x \sim z$

与等价关系相关知识:

1. 等价类: 设  $\sim$  是  $X$  上的一个等价关系, 对  $x \in X$ ,

定义  $X$  关于  $\sim$  的等价类:  $\bar{x} = \{x' \in X \mid x' \sim x\}$

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

3. 自然映射: 对于集合  $X$  中的一个元素  $x$ , 将  $x$  映射到  $\bar{x}$  的

映射  $g: g(x) = \bar{x}$  叫作从  $X$  到  $X/\sim$  的自然映射

4. 划分: 将集合  $X$  按某种依据划分为数个互不相交的新集合, 且有定理: 一个集合的等价关系(或商集)与它的划分一一对应

5. 映射的分解:  $f = \bar{f} \circ g$ :

$$\begin{array}{lll} f: X \rightarrow Y & g: X \rightarrow X/\sim & \bar{f}: X/\sim \rightarrow Y \\ \downarrow x \mapsto f(x) & \downarrow x \mapsto \bar{x} & \downarrow \bar{x} \rightarrow \bar{f}(\bar{x}) \\ \text{原映射} & \text{自然映射(满射)} & \text{诱导映射(单射)} \end{array}$$

偏序关系  $\leq$ : (小写等号 " $\leq$ " 的推广)

偏序关系是一种特殊的二元关系  $W$ , 满足如下性质:

1. 反身性(自反性):  $x \leq x$

2. 反对称性:  $x \leq y, y \leq x \Rightarrow x = y$

3. 传递性:  $x \leq y, y \leq z \Rightarrow x \leq z$

与偏序关系相关知识:

1. 可比:  $x, y \in A$ , 与可比  $\Leftrightarrow x \leq y \vee y \leq x$

2. 全序集: 若集合  $A$  上一个偏序关系  $\leq$  满足:  $\forall x, y \in A$ , 都有  $x, y$  可比. 也即  $\forall x, y \in A$ , 有  $x \leq y$  或  $y \leq x$ . 则称偏序关系  $\leq$  为全序, 同时称集合  $A$  为全序集

3. 覆盖:  $x, y \in A$  且  $x \neq y$ , 若  $\forall z \in A$  使  $x < z < y$ , 则称  $y$  覆盖  $x$ .

例如  $A = \{1, 2, 4, 9\}$  上的整数关系, 9 覆盖 1, 4 覆盖 2, 4 不覆盖 1.

4. 偏序集: 由集合  $A$  与  $A$  上的一个偏序关系构成的一个“类对”, 记作  $(A, \leq)$

如  $(\mathbb{N}, \leq)$  或  $(P(A), \subseteq)$  表示  $A$  的全体子集构成的一个集合.

5. 偏序图(哈塞图): 简化的偏序关系图.

如  $\{1, 2, 3, 4, 5, 6, 7\}$  整除的哈塞图:



## 8.1.6 置换

与“排列”的异曲同工  
n为X的元素个数

置换: 由  $X \rightarrow X$  的一个双射, 其中  $X$  为  $n$  元有限非空集合.

对称群:  $X$  的全体置换构成的集合  $S_X$ , 且  $|S_X| = \text{Card } S_X = n!$

每一个置换都是  $X$  上的一个等价关系, 对应  $X$  的一种划分.

对应一个  $X/n$

与置换相关知识点:

1. 置换的乘法(置换的复合): 满足结合律, 不一定满足交换律

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

$$\text{则 } \tau \nu = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

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

注意: 置换乘法从右向左计算 → 类似映射  $gfh$ , 从右向左计算

将置换看为映射, 如  $\tau = \begin{cases} \tau(1) = 2 \\ \tau(2) = 3 \\ \tau(3) = 1 \\ \tau(4) = 4 \end{cases}$

2. 循环:

每个置换  $\tau$  都对应一个循环, 如果  $\tau$  “移动”了  $X$  中的  $n$  个元素, 则称  $\tau$  为

$r$ -循环( $r$ -cycle). 记作  $\tau = (i_1, i_2, \dots, i_r)$ , 且可以用循环图表示:

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} = (1 2 3)$$

为 3-循环

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

为 5-循环

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

为 3-循环

特别地, 移动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-循环仅仅交换  $X$  中的一对元素, 旗称为对换. 为什么不是 0-循环

3. 循环的乘法(复合):

① 循环的乘法可按置换来做:

$$\text{常用这种 } (1 2)(13425) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix} = (1 3 4)(2 5)$$

② 或根据循环意义来做(记得从右向左):  $= (1 3 4)(2 5)$

从右向左算, 得到哪个数字就继续看其变化, 加得 "(14)" 下一步便看谁变成了谁, 直至形成闭环, 打上括号. 然后为了避免遗漏, 由小到大看是否未变换的数.

4. 置换相交/不相交:

定义: 两个置换  $\tau_1, \tau_2$ , 若  $\forall i \in \{1, 2, \dots, n\}$ ,  $i$  被且仅被  $\tau_1, \tau_2$  中的一个移动, 则称  $\tau_1$  与  $\tau_2$  不相交. 反之则称  $\tau_1$  与  $\tau_2$  相交.

$\tau_1$  与  $\tau_2$  不相交  $\Leftrightarrow \tau_1, \tau_2$  的循环没有都出现的数字  $\Leftrightarrow \tau_1 \tau_2 = \tau_2 \tau_1$

5. 置换的奇偶性:

若一个置换  $\tau$  可以写成奇数(偶数)个对换的乘积, 则称置换  $\tau$  为奇的(偶的)

并定义符号  $E_\tau = \begin{cases} -1, & \tau \text{ 奇} \\ 1, & \tau \text{ 偶} \end{cases}$ , 则有  $E_{\tau_1 \tau_2} = E_{\tau_1} E_{\tau_2}$ .

由循环的对换分解, 可得  $E_\tau = (-1)^{r-1}$ , 再由置换基本定理, 有  $E_\tau = (-1)^{\sum_{i=1}^{n(r-1)}}$

6. 置换作用于函数:

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

则有  $(\tau \circ f) = \tau(f \circ \tau)$

7. 对称函数:

若  $\forall \tau \in S_X$ , 有  $\tau f = f$ , 则称  $f$  为对称函数.

例如  $f(x_1, \dots, x_n) = \sum_{i=1}^n x_i^2, g(x_1, \dots, x_n) = \sum_{1 \leq i < j \leq n} x_i x_j$  都是对称函数.

8. 置换的逆: 略

## 9. 斜对称函数:

若  $f(x_1, \dots, x_i, x_{i+1}, \dots, x_n) = -f(x_1, \dots, x_{i+1}, x_i, x_n)$ , 则称  $f$  为斜对称.

函数  $f(x_1, \dots, x_n)$  可推得时任意斜对称函数  $f$  有:  $\tau \circ f = E_n f$

例如  $f(x_1, \dots, x_n) = \prod_{1 \leq i < j \leq n} (x_i - x_j)$  是一个斜对称函数.

## 10. 置换的阶

对于任意  $\tau \in S_n$ , 若  $\tau^p = e$ , 则称  $\tau$  为一个  $p$  阶置换

思考是否有  $\forall r$ -cycle  $\tau \in S_n$ , 有  $\tau^r = e$ ?

经查阅资料,  $\forall n$ -cycle  $\tau$ , 有  $\tau^n = e$ , 也即  $n$ -cycle 也是一个  $n$  阶置换

## 与置换相关的定理/推论:

### 1. 置换基本定理: → 自己类比取的名字 → 比较算术基本定理

每一个非恒等置换都可分解为数个不相交的循环之积, 且分解唯一.

即  $\forall \tau \in S_n$ , 存唯一互不相容的、不相交的  $\tau_1, \tau_2, \dots, \tau_m$ , 使  $\tau = \tau_1 \tau_2 \dots \tau_m$ .

### 2. 置换的对称分解:

对任意长度为  $r$  的循环  $\tau = (i_1 i_2 \dots i_r)$ ,  $\tau$  可写为  $(r-1)$  个对称之积:  $\tau = (i_1 i_r)(i_2 i_{r-1}) \dots (i_r i_2)$

特别地, 对恒等置换有  $\tau = (12)(12) = (13)(13) = \dots = (i_1 i_2)(i_1 i_2)$

3. 奇偶置换数量相等: 一个  $n$  元对称群  $S_n$  中全体奇置换  $\bar{A}_n$  与全体偶置换  $A_n$  的

数量相同. 即  $\text{card } \bar{A}_n = \text{card } A_n = \frac{n!}{2}$ .

### 4. 置换的共轭作用: (作业 5)

$\forall \tau, \nu \in S_n$ ,  $\nu = (i_1, i_2, \dots, i_n) \cdots (j_1, j_2, \dots, j_s)$

有  $\tau \nu \tau^{-1} = (\tau(i_1), \dots, \tau(i_n)) \cdots (\tau(j_1), \dots, \tau(j_s))$

## 8.1.7 整数的算术

与整数相关的定理/推论:

1. 算术基本定理:  $\forall n \in \mathbb{N}, n \geq 2$ , 存唯一的  $p_1, p_2, \dots, p_r$ , 其中  $p_i$  为素数, 使得  $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$

2. 欧几里得定理: 有无穷多个素数

3. 带余除法:  $\forall a, b \in \mathbb{N}$ ,  $\exists q, r \in \mathbb{N}$  使  $a = bq + r$  满足  $0 \leq r < b$ .

4. 欧几里得算法(辗转相除法):  $\forall a, b \in \mathbb{N}^*$  且  $b \neq 0$ , 令  $r_0 = a$ ,  $r_1 = b$ . 定义  $r_{i+1} = q_{i+1} r_{i+1} + r_{i+2}$ , 其中  $0 \leq r_{i+2} < r_{i+1}$ . 则  $\exists$  最小的整数  $n$  使得  $r_{n+2} = 0$ , 且有  $r_{n+1} = \text{gcd}(a, b)$

整除符号:  $b | a \Leftrightarrow r=0$  求余法:  $r = a \bmod b$

5. 定理:  $\text{gcd}(a, b, c) = \text{gcd}(a, \text{gcd}(b, c)) \quad \text{lcm}(a, b, c) = \text{lcm}(a, \text{lcm}(b, c))$

6. 置换的阶与分解: 将一个  $m$  阶置换分解为长度为  $l_1, l_2, \dots, l_s$  的  $s$  个互不相交的循环的积:

$\tau = v_1 v_2 \cdots v_s$ , 则有:  $m = \text{lcm}(l_1, l_2, \dots, l_s)$

由此可以确定  $S_n$  中元素的最大阶为  $m = \text{lcm}(1, 2, 3, \dots, n)$

经查阅资料,  $\text{lcm}(1, 2, \dots, n) = f(n)$ , 为 Landau's function, 渐近于  $e$

7.  $\forall m, n \in \mathbb{Z}, mn \neq 0$ ,  $\exists s, t \in \mathbb{Z}$ , 使  $\text{gcd}(m, n) = sm + tn$

8. 互质定理:  $(m, n \in \mathbb{Z}, mn \neq 0) \ LCM(m, n) \mid mn \Leftrightarrow \exists s, t \in \mathbb{Z}$ , 使  $sm + tn = 1$

注: 由欧几里得算法求  $s, t \in \mathbb{Z}$ , 使  $\text{g.c.d}(m, n) = sm + tn$  的步骤如下:

商数 以  $\text{g.c.d}(54, 20)$  为例, 作辗转相除有:

↓ 除数附录 ↓ 系数 ↓

$$2 | 54 - 40 = 14$$

$$1 | 20 - 14 = 6$$

$$2 | 14 - 12 = 2$$

$$3 | 12 - 6 = 6$$

$$(2) | 6 - 0 = 0$$

$$2 = 14 - 2 \times 6 \quad 20 = 14 \times 1 + 6$$

$$\Rightarrow 2 = 14 - 2 \times (20 - 14) = (-2) \times 20 + 3 \times 14$$

$$\Rightarrow 2 = (-2) \times 20 + 3 \times (54 - 2 \times 20) = (-3) \times 20 + 3 \times 54$$

$$\Rightarrow 2 = (-3) \times 20 + 3 \times 54 = 64$$

$$\Rightarrow \text{g.c.d}(54, 20) = 2$$

$$\Rightarrow 2 = 14 - 2 \times 6 \quad 20 = 14 \times 1 + 6$$

$$\Rightarrow 2 = 14 - 2 \times (20 - 14) = (-2) \times 20 + 3 \times 14$$

$$\Rightarrow 2 = (-2) \times 20 + 3 \times (54 - 2 \times 20) = (-3) \times 20 + 3 \times 54$$

$$\Rightarrow 2 = (-3) \times 20 + 3 \times 54 = 64$$

$$\Rightarrow \text{g.c.d}(54, 20) = 2$$

$$\Rightarrow 2 = 14 - 2 \times 6 \quad 20 = 14 \times 1 + 6$$

$$\Rightarrow 2 = 14 - 2 \times (20 - 14) = (-2) \times 20 + 3 \times 14$$

$$\Rightarrow 2 = (-2) \times 20 + 3 \times (54 - 2 \times 20) = (-3) \times 20 + 3 \times 54$$

$$\Rightarrow 2 = (-3) \times 20 + 3 \times 54 = 64$$

$$\Rightarrow \text{g.c.d}(54, 20) = 2$$

$$\Rightarrow 2 = 14 - 2 \times 6 \quad 20 = 14 \times 1 + 6$$

$$\Rightarrow 2 = 14 - 2 \times (20 - 14) = (-2) \times 20 + 3 \times 14$$

$$\Rightarrow 2 = (-2) \times 20 + 3 \times (54 - 2 \times 20) = (-3) \times 20 + 3 \times 54$$

$$\Rightarrow 2 = (-3) \times 20 + 3 \times 54 = 64$$

$$\Rightarrow \text{g.c.d}(54, 20) = 2$$

$$\Rightarrow 2 = 14 - 2 \times 6 \quad 20 = 14 \times 1 + 6$$

$$\Rightarrow 2 = 14 - 2 \times (20 - 14) = (-2) \times 20 + 3 \times 14$$

$$\Rightarrow 2 = (-2) \times 20 + 3 \times (54 - 2 \times 20) = (-3) \times 20 + 3 \times 54$$

$$\Rightarrow 2 = (-3) \times 20 + 3 \times 54 = 64$$

$$\Rightarrow \text{g.c.d}(54, 20) = 2$$

$$\Rightarrow 2 = 14 - 2 \times 6 \quad 20 = 14 \times 1 + 6$$

$$\Rightarrow 2 = 14 - 2 \times (20 - 14) = (-2) \times 20 + 3 \times 14$$

$$\Rightarrow 2 = (-2) \times 20 + 3 \times (54 - 2 \times 20) = (-3) \times 20 + 3 \times 54$$

$$\Rightarrow 2 = (-3) \times 20 + 3 \times 54 = 64$$

$$\Rightarrow \text{g.c.d}(54, 20) = 2$$

$$\Rightarrow 2 = 14 - 2 \times 6 \quad 20 = 14 \times 1 + 6$$

$$\Rightarrow 2 = 14 - 2 \times (20 - 14) = (-2) \times 20 + 3 \times 14$$

$$\Rightarrow 2 = (-2) \times 20 + 3 \times (54 - 2 \times 20) = (-3) \times 20 + 3 \times 54$$

$$\Rightarrow 2 = (-3) \times 20 + 3 \times 54 = 64$$

$$\Rightarrow \text{g.c.d}(54, 20) = 2$$

# 第二章. 矩阵

## §2.1 行和列的向量空间

与向量空间相关知识:

1.  $n$  维向量空间  $\mathbb{R}^n = \{\vec{x}_1, \vec{x}_2, \dots, \vec{x}_n \mid x_1, x_2, \dots, x_n \in \mathbb{R}\}$ , 对线性运算封闭.

和  $\mathbb{R}^2$ , 我们将向量与其坐标等同. 则  $\mathbb{R}^n$  是一个由向量组成的集合, 称为二维向量空间.

### 2. 子空间:

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

为  $\mathbb{R}^n$  的子空间. 容易证明,  $\forall n > 2$ ,  $\mathbb{R}^n$  有无数个子空间.

### 3. 线性张成:

设有限集  $S = \{\vec{a}_1, \vec{a}_2, \dots, \vec{a}_n\} \subset \mathbb{R}^n$ , 定义  $\text{Span } S = \{\alpha_1\vec{a}_1 + \alpha_2\vec{a}_2 + \dots + \alpha_n\vec{a}_n \mid \alpha_i \in \mathbb{R}\}$

为  $S$  张成的线性空间, 则  $\text{Span } S$  是  $\mathbb{R}^n$  的一个子空间. 特别地, 有  $\mathbb{R}^n = \text{Span } \{\vec{e}_1, \vec{e}_2, \dots, \vec{e}_n\}$

其中  $\vec{e}_i = (0, \dots, 0, 1, 0, \dots, 0) \in \mathbb{R}^n$ .

推论:  $\mathbb{R}^n$  中任意两个子空间  $H, V$ ,  $H \cap V$  也是  $\mathbb{R}^n$  的子空间而  $H \cup V$  不一定.

### 4. 线性方程组、 $\mathbb{R}^n$ 、行列式间的联系.

$m$  行  $n$  列齐次线性方程组的解构成  $\mathbb{R}^n$  的一个子空间.  $\text{Span } \{\vec{a}_1, \vec{a}_2, \dots, \vec{a}_n\}$  是  $\mathbb{R}^n$  的子空间

$m$  行  $n$  列线性方程组有解  $\Leftrightarrow \vec{b} \in \text{Span } \{\vec{a}_1, \vec{a}_2, \dots, \vec{a}_n\}$ , 其中

$\vec{b} = (b_1, b_2, \dots, b_m)$ ,  $\vec{a}_i = (a_{i1}, a_{i2}, \dots, a_{in}) \in M_m$ ,  $i=1, 2, \dots, n$

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = b_1, \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = b_2, \\ \dots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = b_m. \end{cases} \quad (\text{I})$$

若行列式  $\begin{vmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{vmatrix} \neq 0$ , 则对  $\vec{b} \in \mathbb{R}^n$ ,  $n$  元线性方程组  $A\vec{x} = \vec{b}$  有唯一解.  $\Leftrightarrow \text{Span } \{\vec{a}_1, \vec{a}_2, \dots, \vec{a}_n\} = M_m \Leftrightarrow \{\vec{a}_1, \vec{a}_2, \dots, \vec{a}_n\}$  非线性相关.

### 5. 线性相关:

向量组  $A = \{\vec{a}_1, \vec{a}_2, \dots, \vec{a}_n\}$ , 若存在不全为零的常数  $a_1, a_2, \dots, a_n \in \mathbb{R}$ , 使得  $a_1\vec{a}_1 + a_2\vec{a}_2 + \dots + a_n\vec{a}_n = \vec{0}$ , 则称  $\{\vec{a}_1, \vec{a}_2, \dots, \vec{a}_n\}$  线性相关.

$\Leftrightarrow \exists \vec{a}_i \in A$ , 使  $\vec{a}_i \in \text{Span } \{\vec{a}_1, \dots, \vec{a}_{i-1}, \vec{a}_{i+1}, \dots, \vec{a}_n\}$

$\Leftrightarrow$  齐次线性方程组 (I) 存在非零解  $\Leftrightarrow$  非齐次线性方程组 (II) 存在无数解

特别地, 如果  $m < n$ , 则  $\{\vec{a}_1, \vec{a}_2, \dots, \vec{a}_n\} \subset \mathbb{R}^m$  必线性相关.

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = 0 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = 0 \\ \dots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = 0 \end{cases} \quad (\text{II})$$

### 6. 维数与秩:

$\dim V =$  子空间  $V$  的一组基的元素个数, 称为维数

设  $\{\vec{a}_1, \vec{a}_2, \dots, \vec{a}_s\}$  为  $A = \{\vec{a}_1, \vec{a}_2, \dots, \vec{a}_n\}$  的一个极大线性无关组, 则:

向量组  $A$  的秩  $s = \dim \text{Span } A$

### 求 $A$ 的极大线性无关组: 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. 在向量组中选取第一个非零向量为  $\vec{a}^1$ , 然后取向量组中第一个不属  $\text{Span } \{\vec{a}^1\}$  的向量为  $\vec{a}^2$ , 再取向量组中第一个不属  $\text{Span } \{\vec{a}^1, \vec{a}^2\}$  的向量为  $\vec{a}^3$ , 如此下去, 最终得到一个极大线性无关子集  $\{\vec{a}^1, \dots, \vec{a}^s\}$ . 此方法只对某些特别的向量组有效.

### 7. 对任意 $V_1, V_2$ 为 $\mathbb{R}^n$ 的子空间, 有结论:

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

### 7. 矩阵的行空间、列空间:

对  $m \times n$  矩阵:  $A = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{bmatrix}$  可看作  $n$  个  $m$  维列向量

记其行向量为  $\vec{a}_{ij} = [a_{j1}, a_{j2}, \dots, a_{jn}]$ ,  $j \in \{1, 2, \dots, m\}$

记其列向量为  $\vec{a}^{(j)} = \begin{bmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{bmatrix}$ ,  $j \in \{1, 2, \dots, n\}$

$\rightarrow m \times n$  维向量

则有  $A$  的行空间  $V_r(A) = \text{Span} \{\vec{a}_{11}, \vec{a}_{12}, \dots, \vec{a}_{1n}\} \subseteq \mathbb{R}^n$

$A$  的列空间  $V_c(A) = \text{Span} \{\vec{a}^{(1)}, \vec{a}^{(2)}, \dots, \vec{a}^{(n)}\} \subseteq \mathbb{R}^m$

行秩  $r_{r(A)} = \dim V_r(A)$ , 列秩  $r_c(A) = \dim V_c(A)$  这里角标相反, 且

写作  $\equiv$  “等于”, 因为每一个列向量  $\vec{a}_{ij}$  都是  $M_{m \times 1}$  中的一个元素, 列空间也是  $M_m$  的一个子空间.

### 与向量空间相关的定理/推论:

#### 1. 基定理:

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

#### 2. 基扩充定理:

设  $V$  是  $m$  维子空间  $U$  上的一个  $n$  维子空间,  $\{\vec{v}_1, \dots, \vec{v}_r\}$  是  $V$  的一组基. 则在  $U$  中一定可以找到  $m-r$  个向量  $\vec{u}_1, \dots, \vec{u}_{m-r}$ , 使  $\{\vec{v}_1, \dots, \vec{v}_r, \vec{u}_1, \dots, \vec{u}_{m-r}\}$  是  $U$  的一组基.

#### 3. 矩阵的秩:

$\forall m \times n$  矩阵  $A$ , 都有  $r_c(A) = r_r(A)$ , 称为矩阵的秩, 记为  $\text{rank } A$ .

#### 4. 秩与方程组的解:

线性方程组 (I) 有解  $\Leftrightarrow \text{rank } A = \text{rank } A'$ ,  $A'$  为系数矩阵,  $A$  为增广矩阵.

#### 5. 和的维度:

设  $U, V$  为  $\mathbb{R}^n$  的子空间, 其 和为  $U+V = \{\vec{u}+\vec{v} \mid \vec{u} \in U, \vec{v} \in V\}$ .

且  $\dim(U+V) + \dim(U \cap V) = \dim U + \dim V$

注: 和  $U+V$  与并集不同. 可以证明,  $M_n(\mathbb{R})$  既是一个  $n^2$  维向量空间, 也是一个环.

#### 6. 矩阵空间(结合环):

全体  $n$  阶实矩阵的集合称为  $n$  阶矩阵空间, 记为  $M_n(\mathbb{R})$  或  $M_n$

### 线性方程组解集情况的补充:

#### 1. 判断有无解:

$A\vec{x} = \vec{b}$  有解  $\Leftrightarrow \vec{b} \in \text{Span } A$

#### 2. 有解时, 判断唯一/无穷解:

$\dim(\ker A) + \text{rank } A = n$  (当  $\text{rank } A = n$  时,  $\dim(\ker A) = 0$  为一点, 有唯一解)

#### 3. 由齐次解的结构得到非齐次解的结构:

详见 §2.2 “线性方程组中的向量空间”

### 线性方程组与向量空间联系的补充:

利用行列式可以判断数域  $K$  上  $n$  个方程的  $n$  元线性方程组有没有唯一解, 并且可以给出这个唯一解的公式表示, 但是无法分辨无解和有无穷多个解的情形. 因此需要进一步研究一般的线性方程组如何直接从它的系数和常数项判断它有没有解, 有多少解, 以及有无穷多个解时, 其解集的结构.

为了寻找解决上述问题的途径, 想法之一是: 在利用阶梯形方程组判断原线性方程组有没有解、有多少解时, 需要对线性方程组的增广矩阵施行初等行变换. 1"型等价变换把矩阵的一行的倍数加到另一行上, 这里“一行的倍数”是将这一行的每个元素乘以这个数, 由此引出一个数乘一个有序数组的运算: “加到另一行上”引出了两个有序数组的加法运算. 由此受到启发, 应当在所有  $n$  元有序数组组成的集合中规定加法运算和数乘有序数组(称为数量乘法)运算. 这样  $n$  元有序数组的集合就像几何中所有向量组成的集合那样, 有加法和数量乘法两种运算. 借用几何的语言, 数域  $K$  上所有  $n$  元有序数组组成的集合(记作  $K^n$ ), 连同定义在它上面的加法运算和数量乘法运算, 及其满足的加法交换律、结合律等 8 条运算法则一起, 称为数域  $K$  上的  $n$  维向量空间, 把  $K^n$  的元素称为  $n$  维向量.

想法之二是: 二元齐次线性方程  $2x+y=0$  的解集是平面内过原点的一条直线  $L$ . 在  $L$  上取一个非零向量  $\vec{a}$ , 那么  $L$  上每一个向量都可表示成  $k\vec{a}$ , 其中  $k$  是某个实数. 这表明  $2x+y=0$  的无穷多个解可以通过一个解  $\vec{a}$  表示出来. 由此受到启发, 为了研究数域  $K$  上线性方程组有无穷多个解时解集的结构, 我们应当研究  $n$  维向量空间  $K^n$  中, 向量之间的关系.

## 线性相关与线性无关的补充:

线性相关与线性无关是线性代数中最基本的概念之一。可以从几个角度来考查线性相关的向量组与线性无关的向量组的本质区别:

(1) 从线性组合看:

- 向量组  $\alpha_1, \dots, \alpha_s$  ( $s \geq 1$ ) 线性相关  
 $\iff$  它们有系数不全为 0 的线性组合等于零向量;
- 向量组  $\alpha_1, \dots, \alpha_s$  ( $s \geq 1$ ) 线性无关  
 $\iff$  它们只有系数全为 0 的线性组合才会等于零向量。

(2) 从线性表看出:

- 向量组  $\alpha_1, \alpha_2, \dots, \alpha_s$  ( $s \geq 2$ ) 线性相关  
 $\iff$  其中至少有一个向量可以由其余向量线性表出。

(3) 从齐次线性方程组看:

- 列向量组  $\alpha_1, \dots, \alpha_s$  ( $s \geq 1$ ) 线性相关  
 $\iff$  齐次线性方程组  $x_1\alpha_1 + \dots + x_s\alpha_s = 0$  有非零解:  $\iff$  齐次方程有无数解;
- 列向量组  $\alpha_1, \dots, \alpha_s$  ( $s \geq 1$ ) 线性无关  
 $\iff$  齐次线性方程组  $x_1\alpha_1 + \dots + x_s\alpha_s = 0$  只有零解。

(4) 从行列式看:

- $n$  个  $n$  维列(行)向量  $\alpha_1, \alpha_2, \dots, \alpha_n$  线性相关  
 $\iff$  以  $\alpha_1, \alpha_2, \dots, \alpha_n$  为列(行)向量组的矩阵的行列式等于零;
- $n$  个  $n$  维列(行)向量组  $\alpha_1, \alpha_2, \dots, \alpha_n$  线性无关  
 $\iff$  以  $\alpha_1, \alpha_2, \dots, \alpha_n$  为列(行)向量组的矩阵的行列式不等于零。

(5) 从向量组线性表出一个向量的方式看:

- 设向量  $\beta$  可以由向量组  $\alpha_1, \dots, \alpha_s$  线性表出, 则向量组  $\alpha_1, \dots, \alpha_s$  线性无关  
 $\iff$  表出方式唯一。(证明见本节典型例题的例 6)。
- 向量组  $\alpha_1, \dots, \alpha_s$  线性相关  
 $\iff$  表出方式有无穷多种。

(6) 从向量组与它的部分组的关系看:

- 如果向量组的一个部分组线性相关, 那么整个向量组也线性相关。
- 如果向量组线性无关, 那么它的任何一个部分组也线性无关。

(7) 从向量组与它的延伸组或缩短组的关系看:

- 如果向量组线性无关, 那么把每个向量添上  $m$  个分量(所添分量的位置对于每个向量都一样)得到的延伸组也线性无关。

## 与矩阵有关的一些基本性质/推论:

1. 可逆乘法秩序:

$\forall A \in M_{m \times n}(R)$ , 左乘或右乘一个可逆矩阵, 矩阵的秩不变。

2. 矩阵等价与商集:

$\forall A \in M_{m \times n}(R)$ , 定义  $A_1 \sim A_2$  为  $\exists$  可逆矩阵  $B_{m \times m}, C_{n \times n}$  使  $A_1 = BA_2C$ , 则  $M_{m \times n}(R)/\sim$

有  $+m \times n$  个元素 (即  $+m \times n$  个等价类)

3. 矩阵与核:

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

4. 矩阵的秩:

$\forall A \in M_{m \times n}(R)$ ,  $\text{rank } A \leq \min\{m, n\}$ , 当且仅当  $A$  为线性无关组时取等。 $\iff A$  为列满秩或行满秩。

## 矩阵乘法:

1. 定义: 跳

$$\text{可推出 } \text{rank } A = \text{rank} \begin{bmatrix} A \\ 0 \end{bmatrix} = \text{rank} \begin{bmatrix} A & 0 \end{bmatrix}$$

2. 运算: 跳

3. 秩相关结论:

- ①  $\text{rank } A + \text{rank } B - s \leq \text{rank } AB \leq \text{rank } B$
- ②  $\text{rank } A + \text{rank } B \geq \text{rank } [A, B] = \text{rank} \begin{bmatrix} A \\ B \end{bmatrix} \geq \begin{cases} \text{rank } A \\ \text{rank } B \end{cases}$
- ③  $\text{rank } \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix} = \text{rank } A + \text{rank } B$
- ④  $\text{rank } A + \text{rank } B + \text{rank } C \geq \text{rank } \begin{bmatrix} A & 0 \\ C & B \end{bmatrix} \geq \text{rank } A + \text{rank } B$

## 3.2.2 线性映射和矩阵运算

与线性映射有关的知识点:

1. 线性映射:  $V$  和  $U$  为 vector space  $\rightarrow$  特别地, 当  $\dim V = \dim U$  时,

一个由  $V \rightarrow U$  的映射  $f$  称为线性的, 如果  $f$  满足: 称  $f$  为线性变换  
 $\forall \lambda, \mu \in R, u, v \in V$ , 有  $f(\lambda u + \mu v) = \lambda f(u) + \mu f(v)$

且定义两个线性映射  $f, g$  的线性运算:

$$(f + \mu g)(u) = \lambda f(u) + \mu g(u), \lambda, \mu \in R, u \in V$$

此时  $(\lambda f + \mu g)$  也是一个由  $V \rightarrow U$  的线性映射。

2. 线性映射在基下的矩阵: 线性映射的线性组合仍是一个线性映射

线性映射在基  $\{\bar{e}_1, \bar{e}_2, \dots, \bar{e}_n\}$  下的矩阵为:

$$A = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ a_{21} & \dots & a_{2n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{bmatrix}, \text{ 其中 } \bar{e}_i \in R, q_A(\bar{e}_i) = \begin{bmatrix} a_{1i} \\ a_{2i} \\ \vdots \\ a_{mi} \end{bmatrix}$$

可以理解为, 给定每一个  $q_A(\bar{e}_i)$ ,  $i=1, 2, \dots, n$ , 则线性映射  $q_A$  唯一确定。

这相当于给出  $q_A$  在基  $\{\bar{e}_1, \bar{e}_2, \dots, \bar{e}_n\}$  下的一个矩阵:  
 $A = [q_A(\bar{e}^{(1)}) \ q_A(\bar{e}^{(2)}) \ \dots \ q_A(\bar{e}^{(n)})] = [\bar{a}^{(1)} \ \bar{a}^{(2)} \ \dots \ \bar{a}^{(n)}] = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ a_{21} & \dots & a_{2n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{bmatrix}$

而一般情况下, 我们默认 "R" 的基为标准基,

这时便可以说 " $q_A$  就是矩阵  $A$ , 矩阵  $A$  就是线性映射  $q_A$ "。

4. 线性映射与矩阵具有等同性:

任何一个线性映射都可以用矩阵表示, 任何一个矩阵都对应唯一的线性映射。

与矩阵运算有关的知识点:

1. 矩阵线性运算:

$$A = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ a_{21} & \dots & a_{2n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{bmatrix}, B = \begin{bmatrix} b_{11} & \dots & b_{1n} \\ b_{21} & \dots & b_{2n} \\ \vdots & \ddots & \vdots \\ b_{m1} & \dots & b_{mn} \end{bmatrix}, \text{ 则由 } q_C = \lambda q_A + \mu q_B \text{ 可定义:}$$

$$\bar{c}^{(i)} = \bar{a}^{(i)} + \bar{b}^{(i)}, \text{ 若 } C = \lambda A + \mu B = \begin{bmatrix} c_{11} & \dots & c_{1n} \\ c_{21} & \dots & c_{2n} \\ \vdots & \ddots & \vdots \\ c_{m1} & \dots & c_{mn} \end{bmatrix} = \begin{bmatrix} \lambda a_{11} + \mu b_{11} & \dots & \lambda a_{1n} + \mu b_{1n} \\ \lambda a_{21} + \mu b_{21} & \dots & \lambda a_{2n} + \mu b_{2n} \\ \vdots & \ddots & \vdots \\ \lambda a_{m1} + \mu b_{m1} & \dots & \lambda a_{mn} + \mu b_{mn} \end{bmatrix}$$

2. 矩阵乘法:

$$\text{设 } \bar{a} = a_1\bar{e}^{(1)} + \dots + a_n\bar{e}^{(n)}, A = [\bar{a}^{(1)} \ \bar{a}^{(2)} \ \dots \ \bar{a}^{(n)}] = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ a_{21} & \dots & a_{2n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{bmatrix}$$

$$\text{则 } q_A(\bar{a}) = A\bar{a} = a_1\bar{a}^{(1)} + \dots + a_n\bar{a}^{(n)}, \text{ 写为矩阵有:}$$

$$A\bar{a} = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ a_{21} & \dots & a_{2n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} c_{11} \\ c_{21} \\ \vdots \\ c_{m1} \end{bmatrix}, \text{ 其中 } c_{ij} = [a_{11} \ a_{12} \ \dots \ a_{1n}] \begin{bmatrix} a_i \\ a_2 \\ \vdots \\ a_n \end{bmatrix} = \sum_{j=1}^n a_{1j}a_{ij}$$

类似地, 对  $A_{m \times s}, B_{s \times n}$ , 有:

$$AB = \begin{bmatrix} a_{11} & \dots & a_{1s} \\ a_{21} & \dots & a_{2s} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{ms} \end{bmatrix} \begin{bmatrix} b_{11} & \dots & b_{1n} \\ b_{21} & \dots & b_{2n} \\ \vdots & \ddots & \vdots \\ b_{s1} & \dots & b_{sn} \end{bmatrix} = \begin{bmatrix} c_{11} & \dots & c_{1n} \\ c_{21} & \dots & c_{2n} \\ \vdots & \ddots & \vdots \\ c_{s1} & \dots & c_{sn} \end{bmatrix}$$

$$\text{其中 } c_{ij} = [a_{11} \ a_{12} \ \dots \ a_{1s}] \begin{bmatrix} b_{i1} & b_{i2} & \dots & b_{in} \end{bmatrix} = \sum_{k=1}^s a_{1k}b_{ik}$$

且矩阵的乘积满足:  $\forall A \in M_{m \times s}, B \in M_{s \times n}$ , 有

$$\min\{\text{rank } A, \text{rank } B\} \geq \text{rank } AB \geq \text{rank } A + \text{rank } B - s$$

$\text{rank } ABC \geq \text{rank } AB + \text{rank } BC - \text{rank } B, \text{rank } (A+B) \leq \text{rank } A + \text{rank } B$

3. 矩阵乘法满足结合律、分配律, 不一定满足交换律。这是矩阵加减法不是直和

4. 矩阵的转置:

$$(A^T)^T = A, (A+B)^T = A^T + B^T, (\lambda A)^T = \lambda(A^T), (AB)^T = B^T A^T$$

$$\text{rank } A^T = \text{rank } A = \text{rank } AA^T = \text{rank } A^T A$$

## 5. 矩阵的等价:

$A, B \in M_{m \times n}$ ,  $A \sim B := \exists P \in M_{m \times m}, Q \in M_{n \times n}$  使  $A = PBQ$

思考: 是否有  $A \sim B \Leftrightarrow \text{rank } A = \text{rank } B$ . 答: 是的.

且  $\forall A \in M_{m \times n}$ ,  $\text{rank } A \leq \min\{m, n\}$ , 由此可得  $M_{m \times n}(R)$  中共有  $(\lfloor \frac{m}{n} \rfloor)$  个等价类.

## 6. 矩阵的幂:

$$A^1 = A, A^2 = AA, A^{i+1} = AA^i$$

注意是定义为左乘.

## 特殊矩阵:

### 1. 对角矩阵 (diagonal matrices): $\text{diag}\{d_1, d_2, \dots, d_n\}$

用一个对角矩阵左(右)乘一个矩阵  $A$ , 就相当于用对角矩阵的主对角元分别去乘  $A$  的相应的行(列).

左行右列原则, 如:

$$\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ 2c & 2d \end{bmatrix}, \quad \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} a & 2b \\ c & 2d \end{bmatrix}$$

定理: 纯量矩阵交换性: 设  $A \in M_{n \times n}(R)$ , 有结论:

$$\forall B \in M_{n \times n}(R), AB = BA \Leftrightarrow A = \text{diag}_n(\lambda), \lambda \in R$$

### 2. 初等矩阵 (elementary matrices):

由  $I_n$  经过一次初等行变换得到的矩阵称为初等矩阵, 常记为下, 例如:

$F_{i,j}$  = 将  $I_n$  第  $i, j$  行互换所得矩阵  $\Leftrightarrow$  左右乘  $A$  时将  $A$  第  $i, j$  行(列)互换. 其它类似:

①  $F_{s,t}$  —— 将矩阵的第  $s$  和  $t$  行(列)交换位置,

②  $F_{s,t}(\lambda)$  —— 将矩阵的第  $t$  行(列)乘以  $\lambda$  加到第  $s$  行(列)

③  $F_s(\lambda)$  —— 将矩阵的第  $s$  行(列)乘以  $\lambda$ .

特别地有:  $(F_{i,j})^T = F_{i,j}$ ,  $F_{i,j}^{-1} = F_{i,j}$ ,  注:  $F_{s,t}$  与  $F_{s,t}(\lambda)$  不同, 不能混淆

$$F_{i,j}^{-1}(\alpha) = F_{i,j}(-\alpha), \quad F_{i,j}^{-1} = F_i(\frac{1}{\alpha})$$

$F_{i,j}(\lambda)A =$  将  $\lambda$  乘  $j$  行加到  $i$  行上,  $AF_{i,j}(\lambda) =$  将  $\lambda$  乘  $j$  列加到  $i$  列上.

### 3. 可逆矩阵:

给定方阵  $A \in M_{n \times n}$ , 若  $\exists B \in M_{n \times n}$ , 使  $AB = E = BA$ , 则称  $A$  为可逆矩阵(也称非退化的), 同时记  $B = A^{-1}$ . 且有结论:

$A \in M_{n \times n}$  可逆  $\Leftrightarrow \text{rank } A = n \Leftrightarrow \dim \ker A = 0 \Leftrightarrow$

$A\vec{x} = \vec{0}$  仅有零解  $\Leftrightarrow \det A = 0 \Leftrightarrow A = (I_n)^{-1}$

定理: 对一个给定矩阵  $A$ , 左乘或右乘可逆矩阵不改变  $A$  的秩.

### 4. 三角矩阵 (triangular matrices): 腑

### 5. 对称矩阵 (symmetric matrices):

若  $A, B$  为对称矩阵, 则:  $AB$  为对称矩阵  $\Leftrightarrow AB = BA$

### 6. 退化/非退化:

$A \in M_n(R)$ , 若它的各行(列)线性无关, 即  $\text{rank } A = n$ , 则称  $A$  为非退化的. 否则, 称其为退化的.

### 7. 反射、投影、旋转矩阵, 置换矩阵(正交矩阵的一种)

### 8. 索等矩阵: $A \in M_{n \times n}$ , $A^2 = A$ (索等价于 $\forall k \in N^*, A^k = A$ )

### 9. 正交矩阵:

设  $A \in M_n(R)$ , 若  $A^T A = I$ , 则称  $A$  为正交矩阵. 且有推论:

$A$  是  $R$  上的正交矩阵  $\Leftrightarrow A A^T = I \Leftrightarrow A^T A = I \Leftrightarrow A^T = A^{-1}$

$\Rightarrow |A| = 1$  或  $-1 \Leftrightarrow A$  的向量组是  $R^n$  的一组标准基

## 线性方程组中的向量空间:

### 1. 解空间(零空间) $\text{ker } A (\ker A)$ :

齐次线性方程组的规范基础解系张成的  $R^n$  的子空间.

如  $A\vec{x} = \vec{0}$ , 其中  $A = \begin{bmatrix} 1 & -3 & 4 & -3 & 2 & 5 \\ 3 & -7 & 8 & -5 & 8 & 9 \\ 0 & 3 & -6 & 6 & 4 & -5 \\ 1 & 0 & -2 & 3 & 6 & 0 \\ 1 & -2 & 2 & -1 & 3 & 2 \end{bmatrix}$ . 可以这样理解:

$A$  为一个列向量组  $\rightarrow$  6个三维列向量,  $\vec{x}$  指这6个列向量的一种线性组合方式, 组合的结果为了  $\vec{0}$ , 求这些组合方式.

由 Gauss-Jordan 消元可得:

$$\vec{x} = \begin{bmatrix} 2x_3 - 3x_4 + 2x_5 \\ 2x_3 - 2x_4 + 7x_5 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix}, \text{ 这表明 } \vec{x} \text{ 可视为 } R^5 \text{ 中 } 5 \text{ 个 } 3 \text{ 维列向量的}$$

线性组合,  $n$  表示自由变量的个数, 此处  $n=3$ , 也即:

$$\vec{x} = x_3 \begin{bmatrix} 2 \\ 2 \\ 1 \\ 0 \\ 0 \end{bmatrix} + x_4 \begin{bmatrix} -3 \\ -2 \\ 0 \\ 1 \\ 0 \end{bmatrix} + x_5 \begin{bmatrix} 2 \\ 7 \\ 0 \\ -4 \\ 1 \end{bmatrix} \text{ 则解空间 } \text{ker } A = \text{span} \left\{ \begin{bmatrix} 2 \\ 2 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} -3 \\ -2 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 2 \\ 7 \\ 0 \\ -4 \\ 1 \end{bmatrix} \right\} \text{ 是 } R^5 \text{ 的一个子空间.}$$

且有定理:

① 对  $\forall A \in M_{m \times n}(R)$ , 都有  $\text{rank } A + \dim(\ker A) = n$

② 对  $\forall A \in M_{m \times n}(R), B \in M_{n \times n}(R)$ , 有:

$\ker B \subset \ker AB$ , 若还满足  $AB = BA$ , 则有  $\ker A \subset \ker AB$   
 $\Rightarrow \ker A \cup \ker B \subset \ker AB$

③ 对  $\forall A, B \in M_{n \times n}(R)$ , 且  $AB = BA$ , 有:

$\ker A + \ker B \subset \ker AB$

④ 对  $R^n$  的任意子空间  $V_1, V_2$ , 有:

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

⑤  $\forall A \in M_{m \times n}(R), \ker A^T A = \ker A A^T = \ker A$

2. 由齐次方程求非齐次方程:  $\rightarrow$  一般令阶梯形矩阵中所有自由变量为 0 即得.

设  $\vec{x}$  是  $A\vec{x} = \vec{b}$  的一个特解 ( $\vec{b} \neq \vec{0}$ ), 则:

$$A(\vec{x} - \vec{x}) = \vec{b} - \vec{b} = \vec{0} \Rightarrow \vec{x} - \vec{x} \in \ker A$$

$\Rightarrow A\vec{x} = \vec{b}$  的解集为  $\{\vec{x} + \vec{w} \mid \vec{w} \in \ker A\}$ .

3. 若  $A$  为实数域上的方阵, 也即  $A \in M_{n \times n}(R)$ , 则有:

$$\ker(A^T A) = \ker(A) \Leftrightarrow \text{rank}(A^T A) = \text{rank}(A)$$

补充: 线性空间

思考: 求下列矩阵的逆矩阵

$$A = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ x_{2,1} & 1 & 0 & \cdots & 0 \\ x_{3,1} & x_{3,2} & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ x_{n,1} & x_{n,2} & \cdots & x_{n,n-1} & 1 \end{bmatrix}$$

且有推论:

$A$  为幂等矩阵  $\Leftrightarrow \text{rank } A + \text{rank}(I_n - A) = n$

理解矩阵是一种线性映射  $\varphi: \mathbb{R}^n \rightarrow \mathbb{R}^m$

1.  $A \in M_{m \times n}$ ,  $m=n$ : 行数等于列数  $n=2$

$$A = \begin{bmatrix} * \\ * \end{bmatrix}$$

$$= A \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} * \\ * \end{bmatrix}$$

=  $A[\vec{e}_1, \vec{e}_2] \begin{bmatrix} * \\ * \end{bmatrix}$  分块矩阵

=  $(A[\vec{e}_1, \vec{e}_2]) \begin{bmatrix} * \\ * \end{bmatrix}$  矩阵乘法结合律

=  $[A\vec{e}_1, A\vec{e}_2] \begin{bmatrix} * \\ * \end{bmatrix}$  与  $[A\vec{e}_1, A\vec{e}_2] \begin{bmatrix} * \\ * \end{bmatrix}$  对比, 含义为: 基向量

$\vec{e}_1, \vec{e}_2$  变为  $A\vec{e}_1, A\vec{e}_2$ , 也即  $\varphi_A(\vec{e}_1), \varphi_A(\vec{e}_2)$ .

第二种理解

左右两列步步对应:

$$A[\vec{e}_1, \vec{e}_2] \begin{bmatrix} * \\ * \end{bmatrix}$$

$$\varphi_A[\vec{e}_1, \vec{e}_2] \begin{bmatrix} * \\ * \end{bmatrix}$$

加法

$$= A(x\vec{e}_1 + y\vec{e}_2)$$

$$\varphi_A(x\vec{e}_1 + y\vec{e}_2)$$

=  $Ax\vec{e}_1 + Ay\vec{e}_2$  (分配律) =  $\varphi_A(x\vec{e}_1) + \varphi_A(y\vec{e}_2)$  线性映射性质①

=  $xA\vec{e}_1 + yA\vec{e}_2$  (数乘可交换) =  $x\varphi_A(\vec{e}_1) + y\varphi_A(\vec{e}_2)$  线性映射性质②

=  $x(A\vec{e}_1) + y(A\vec{e}_2)$  (结合律) =  $x\varphi_A(\vec{e}_1) + y\varphi_A(\vec{e}_2)$  数乘

令  $A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ , 则  $A\vec{e}_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ ,  $A\vec{e}_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

对比如下:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$A = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$$

$\varphi_A$  是一个  $\mathbb{R}^2 \rightarrow \mathbb{R}^2$  的线性映射

2.  $A \in M_{m \times n}$ ,  $m < n$ : 行数少于列数  $n=3$

$$A\vec{e} = A \begin{bmatrix} * \\ * \\ * \end{bmatrix} = A \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} * \\ * \\ * \end{bmatrix}$$

$$= A[\vec{e}_1, \vec{e}_2, \vec{e}_3] \begin{bmatrix} * \\ * \\ * \end{bmatrix} = A(x\vec{e}_1 + y\vec{e}_2 + z\vec{e}_3)$$

$$= x(A\vec{e}_1) + y(A\vec{e}_2) + z(A\vec{e}_3)$$

$$= x\vec{e}'_1 + y\vec{e}'_2 + z\vec{e}'_3.$$

设  $A = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \end{bmatrix}$ , 则  $\vec{e}'_1 = A\vec{e}_1 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$

$\vec{e}'_2 = \begin{bmatrix} 1 \\ 2 \end{bmatrix}$ ,  $\vec{e}'_3 = \begin{bmatrix} 1 \\ 3 \end{bmatrix}$ , 也即  $A = [\vec{e}'_1, \vec{e}'_2, \vec{e}'_3]$

对比如下:

$$I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$A = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \end{bmatrix}$$

$\varphi_A$  是一个  $\mathbb{R}^3 \rightarrow \mathbb{R}^3$  的线性映射.

3.  $A \in M_{m \times n}$ ,  $m > n$ :

$$\text{设 } A = \begin{bmatrix} 1 & 1 \\ 2 & 3 \\ 3 & 1 \end{bmatrix}, \text{ 此时 } n=2, m=3$$

将  $\mathbb{R}^2$  中的向量  $x\vec{e}_1 + y\vec{e}_2 = x\begin{bmatrix} 1 \\ 0 \end{bmatrix} + y\begin{bmatrix} 0 \\ 1 \end{bmatrix}$

映到  $\mathbb{R}^3$  中:  $x\vec{e}'_1 + y\vec{e}'_2 = x\begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} + y\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$

对比如下:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$A = \begin{bmatrix} 1 & 1 \\ 1 & 2 \\ 1 & 3 \end{bmatrix}$$

$\varphi_A$  是一个  $\mathbb{R}^2 \rightarrow \mathbb{R}^3$  的线性映射.

分块矩阵的性质:

1. 线性等式:

$$\text{① } \text{rank}(AB) \leq \min(\text{rank}(A), \text{rank}(B)), \text{ rank}(AB) \geq \text{rank}(A) + \text{rank}(B) - s$$

$$\text{② } |\text{rank}(A) - \text{rank}(B)| \leq \text{rank}(A \pm B) \leq \text{rank}(A) + \text{rank}(B)$$

$$\text{③ } r(A) + r(B) \geq r(A \pm B) = r(\overset{\Delta}{B}) \geq \min(r(A), r(B))$$

$$\text{④ } A \text{ 为实数域上矩阵, 则 } r(AB) = r(A)$$

$$\text{⑤ } A \in M_{m \times s}, B \in M_{s \times n}, \text{ 则 } r(A) + r(B) \leq s$$

$$\text{⑥ } r(\overset{\Delta}{AB}) = r(A) + r(B), r(\overset{\Delta}{AC}) \geq r(A) + r(B)$$

$A \in M_{m \times s}, B \in M_{s \times n}$

利用 B 的列是 ker A 的元素证明.

2. 左乘列满秩, 右乘行满秩, 等不变: 对一般的矩阵 A, 进行

$F_{i,j}(A), F_{i,j}(B)$  时:

$$A \text{ 列满秩} \Rightarrow r(B) = r(AB)$$

$$A \text{ 行满秩} \Rightarrow r(B) = r(BA)$$

3. 列满秩有左消去律, 行满秩有右消去律:

$$A \text{ 列满秩}, AB = AC \Rightarrow B = C$$

$$A \text{ 行满秩}, BA = CA \Rightarrow B = C$$

$A \in M_{m \times n}$ ,  $\text{rank}(A) = r$ , 则 可逆矩阵  $P, Q$  使:

$$A = P \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}_{m \times n} Q$$

$$= P \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix} Q$$

思考:

Q1.  $AB = BA$  可交换等价于什么?

答: 等价于  $\exists$  矩阵 C 与多项式 f, g, 使  $A = f(C), B = g(C)$  也有其它不同角度.

Q2.  $A \in M_{m \times n}(\mathbb{R})$ ,  $m \neq n$ , A 的左逆、右逆?

答: 广义矩阵逆.

草稿纸上求矩阵逆过程的书写：黑笔+绿笔

$$(1) \text{ 求 } \begin{bmatrix} 2 & 1 & -2 \\ 1 & 2 & 2 \\ 2 & -2 & 1 \end{bmatrix}^{-1}$$

$$\begin{array}{c|ccc} & 2 & 1 & -2 \\ \hline 2 & 1 & 2 & 2 \\ 1 & 2 & 2 & 0 \\ 2 & -2 & 1 & 0 \end{array} \quad \begin{array}{c|ccc} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}$$

$$\begin{array}{c|ccc} & -2 & -4 & -4 \\ \hline ① & 2 & 2 & 2 \\ ② & 2 & 1 & -2 \\ 2 & -2 & 1 & 0 \end{array} \quad \begin{array}{c|ccc} 0 & -2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}$$

$$\begin{array}{c|ccc} & 0 & -2 & -4 \\ \hline ③ & 1 & 2 & 2 \\ ② & 0 & -3 & -6 \\ 2 & 0 & -6 & -3 \\ 0 & 6 & 12 & 0 \end{array} \quad \begin{array}{c|ccc} \frac{2}{3} & -\frac{4}{3} & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}$$

$$\begin{array}{c|ccc} & 1 & 0 & -2 \\ \hline ④ & 0 & -3 & -6 \\ ⑤ & 0 & 0 & 9 \\ ⑥ & 0 & 0 & 1 \end{array} \quad \begin{array}{c|ccc} \frac{2}{3} & -\frac{1}{3} & 0 \\ 1 & -2 & 0 \\ -2 & 2 & 1 \\ -\frac{4}{9} & \frac{4}{9} & \frac{2}{9} \end{array}$$

$$\begin{array}{c|ccc} & 0 & 0 & 2 \\ \hline ⑦ & 1 & 0 & -2 \\ ⑧ & 0 & 0 & 6 \\ ⑨ & 0 & -3 & -6 \\ ⑩ & 0 & 0 & 1 \end{array} \quad \begin{array}{c|ccc} \frac{2}{3} & -\frac{1}{3} & 0 \\ -\frac{12}{9} & \frac{12}{9} & \frac{6}{9} \\ 1 & -2 & 0 \\ -\frac{2}{9} & \frac{2}{9} & \frac{1}{9} \end{array}$$

$$\begin{array}{c|ccc} & 1 & 0 & 0 \\ \hline ⑪ & 0 & -3 & 0 \\ ⑫ & 0 & 0 & 1 \\ ⑬ & 0 & 0 & 1 \end{array} \quad \begin{array}{c|ccc} \frac{2}{9} & \frac{1}{9} & \frac{2}{9} \\ -\frac{3}{9} & -\frac{6}{9} & \frac{6}{9} \\ -\frac{2}{9} & \frac{2}{9} & \frac{1}{9} \end{array}$$

$$\begin{array}{c|ccc} & 1 & 0 & 0 \\ \hline ⑭ & 0 & 1 & 0 \\ ⑮ & 0 & 0 & 1 \\ ⑯ & 0 & 0 & 1 \end{array} \quad \begin{array}{c|ccc} \frac{2}{9} & \frac{1}{9} & \frac{2}{9} \\ \frac{1}{9} & \frac{2}{9} & -\frac{2}{9} \\ -\frac{2}{9} & \frac{2}{9} & \frac{1}{9} \end{array}$$

$$\begin{array}{c|ccc} & 1 & 0 & 0 \\ \hline ⑰ & 0 & 1 & 0 \\ ⑱ & 0 & 0 & 1 \\ ⑲ & 0 & 0 & 1 \end{array} \quad \begin{array}{c|ccc} \frac{2}{9} & \frac{1}{9} & \frac{2}{9} \\ \frac{1}{9} & \frac{2}{9} & -\frac{2}{9} \\ -\frac{2}{9} & \frac{2}{9} & \frac{1}{9} \end{array}$$

$$\begin{array}{c|ccc} & 1 & 0 & 0 \\ \hline ⑳ & 0 & 1 & 0 \\ ㉑ & 0 & 0 & 1 \\ ㉒ & 0 & 0 & 1 \end{array} \quad \begin{array}{c|ccc} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}$$

$$(2) \text{ 求 } \begin{bmatrix} 2 & 5 & 7 \\ 5 & -2 & -3 \\ 6 & 3 & 4 \end{bmatrix}^{-1}$$

$$\begin{array}{c|ccc} & 5 & 7 & 1 \\ \hline ① & 2 & -2 & -3 \\ ② & 6 & 3 & 4 \\ ③ & 5 & -2 & -3 \\ ④ & 6 & 3 & 4 \end{array} \quad \begin{array}{c|ccc} 1 & 0 & 0 \\ -\frac{5}{2} & 0 & 0 \\ 0 & 1 & 0 \\ -3 & 0 & 0 \\ 0 & 0 & 1 \end{array}$$

$$\begin{array}{c|ccc} & 2 & 5 & 7 \\ \hline ⑤ & 0 & \frac{-29}{2} & \frac{-41}{2} \\ ⑥ & 0 & -12 & -17 \end{array} \quad \begin{array}{c|ccc} 1 & 0 & 0 \\ -\frac{5}{2} & 1 & 0 \\ -3 & 0 & 1 \end{array}$$

$$\begin{array}{c|ccc} & 0 & -5 & -205 \\ \hline ⑦ & 2 & 5 & 7 \\ ⑧ & 0 & 29 & 41 \\ ⑨ & 0 & -12 & -17 \end{array} \quad \begin{array}{c|ccc} \frac{-25}{29} & \frac{10}{29} & 0 \\ 5 & -2 & 0 \\ -3 & 0 & 1 \end{array}$$

$$\begin{array}{c|ccc} & 0 & 12 & 12 \times 41 \\ \hline ⑩ & 29 & 12 & 29 \\ ⑪ & 62 & -24 & 0 \end{array} \quad \begin{array}{c|ccc} \frac{62}{29} & \frac{-24}{29} & 0 \\ 0 & 0 & 1 \end{array}$$

$$\begin{array}{c|ccc} & 2 & 0 & -\frac{2}{29} \\ \hline ⑫ & 0 & 29 & 41 \\ ⑬ & 0 & -2 & 0 \end{array} \quad \begin{array}{c|ccc} \frac{4}{29} & \frac{10}{29} & 0 \\ 5 & -2 & 0 \end{array}$$

$$\begin{array}{c|ccc} & 0 & 0 & \frac{-1}{29} \\ \hline ⑭ & 29 & 0 & 1 \\ ⑮ & 0 & 27 & 41 \end{array} \quad \begin{array}{c|ccc} -\frac{27}{29} & -\frac{24}{29} & 1 \\ 54 & 48 & -58 \end{array}$$

$$\begin{array}{c|ccc} & 0 & 0 & -2 \\ \hline ⑯ & 29 & 0 & 1 \\ ⑰ & 0 & -41 & 1 \\ ⑱ & 0 & 0 & 1 \end{array} \quad \begin{array}{c|ccc} 4 & 10 & 0 \\ 5 & -2 & 0 \\ 27 & 24 & -29 \end{array}$$

$$\begin{array}{c|ccc} & 58 & 0 & 0 \\ \hline ⑲ & 0 & 29 & 0 \\ ⑳ & 0 & 0 & 1 \end{array} \quad \begin{array}{c|ccc} 58 & 58 & -58 \\ -1102 & -986 & 41 \times 29 \end{array}$$

$$\begin{array}{c|ccc} & 0 & 0 & 1 \\ \hline ㉑ & 27 & 24 & -29 \end{array}$$

$$\begin{array}{c|ccc} & 1 & 1 & -1 \\ \hline ㉒ & 0 & 1 & 0 \\ ㉓ & 0 & 0 & 1 \end{array} \quad \begin{array}{c|ccc} 1 & 1 & -1 \\ -38 & -34 & 41 \\ 27 & 24 & -29 \end{array}$$

# 第三章. 行列式

## §3.1 行列式的构造和刻画

线性、双线性、多重线性映射:

### 1. 线性:

对定义域为  $R^n$  的一元映射  $f$ , 若对变量满足加法、数乘, 则称其为线性映射  
也即:  $\forall \vec{u}, \vec{v} \in R^n, f(\vec{u} + \vec{v}) = f(\vec{u}) + f(\vec{v})$  (加法) (I)

$\forall \vec{u} \in R^n, a \in R, f(a\vec{u}) = af(\vec{u})$  (数乘) (II)

此时, 我们称映射  $f$  为线性的.  $\forall f(x) = kx + b$  为  $R^1 \rightarrow R^1$  的线映  
 $\nwarrow x \in R^1$ . 也即  $\vec{x}$

并且(I)(II)可等价地、简洁地写为:

$\forall \vec{u}, \vec{v} \in R^n, a, b \in R, f(a\vec{u} + b\vec{v}) = af(\vec{u}) + bf(\vec{v})$  (线性) (III)

也即 (I) and (II)  $\Leftrightarrow$  (III)

### 2. 双线性:

对定义域为  $(R^n)^2 = R^n \times R^n$  的二元映射  $f$ , 若其对两个变量都是线性的, 则称  $f$  是双线性的, 也即  $f$  是双线性映射. 也即:

(I) 对第一个变量  $u$  线性:

$\forall \vec{u}, \vec{v}_1, \vec{v}_2 \in R^n, a, b \in R, f(a\vec{u}_1 + b\vec{u}_2, \vec{v}) = af(\vec{u}_1, \vec{v}) + bf(\vec{u}_2, \vec{v})$

(II) 对第二个变量  $v$  线性:

$\forall \vec{u}, \vec{v}_1, \vec{v}_2 \in R^n, a, b \in R, f(\vec{u}, a\vec{v}_1 + b\vec{v}_2) = af(\vec{u}, \vec{v}_1) + bf(\vec{u}, \vec{v}_2)$

(I) and (II) 同样可以等价地写为:

$\forall \vec{u}_1, \vec{u}_2, \vec{v}_1, \vec{v}_2 \in R^n, a, b, c, d \in R$ , 有  $f(a\vec{u}_1 + b\vec{u}_2, c\vec{v}_1 + d\vec{v}_2) = acf(\vec{u}_1, \vec{v}_1) + bcf(\vec{u}_2, \vec{v}_1) + adf(\vec{u}_1, \vec{v}_2) + bdf(\vec{u}_2, \vec{v}_2)$  (III) 双线性

### 3. 多重线性:

与①②类似, 定义在  $(R^n)^m$  上的  $m$  元映射  $f$ , 若其对每个变量都是线性的 (一共  $m$  个), 则称  $f$  为  $m$  重线性映射, 可写为:

$\forall \vec{u}_{11}, \vec{u}_{12} \in R^n, i \in N^* (i \neq n), a, b \in R$ , 有:

$f(\vec{u}_1, \dots, a\vec{u}_{11} + b\vec{u}_{12}, \dots, \vec{u}_n)$

$= af(\vec{u}_1, \vec{u}_2, \dots, \vec{u}_{11}, \dots, \vec{u}_n) + bf(\vec{u}_1, \vec{u}_2, \dots, \vec{u}_{12}, \dots, \vec{u}_n)$

### 4. 线性映射的线性组合:

设线性映射  $g_1, g_2: R^n \rightarrow R^m$ , 定义线性映射的线性组合:

$\forall a, b \in R, (ag_1 + bg_2)(x) = ag_1(x) + bg_2(x)$

这样, 容易验证线性映射的线性组合仍是线性映射, 其它也类似.

对称/斜对称函数:

### 1. 对称函数:

一个  $n$  元函数  $f$  被称为对称的, 如果  $\forall u_i \in I$ , 有

$f(u_1, u_2, \dots, u_s, \dots, u_r, \dots, u_n) = f(u_1, u_2, \dots, u_r, \dots, u_s, \dots, u_n)$

即: 任意交换两变量位置, 函数值不变.

### 2. 斜对称函数:

一个  $n$  元函数  $f$  被称为斜对称的, 如果  $\forall u_i \in I$ , 有

$f(u_1, u_2, \dots, u_s, \dots, u_r, \dots, u_n) = -f(u_1, u_2, \dots, u_r, \dots, u_s, \dots, u_n)$

即: 任意交换两变量位置, 函数值相反.

推论:  $\forall$  斜对称函数  $f$ ,  $\tau \in S_n$ , 有

$\tau f = f(\tau(u_1), \tau(u_2), \dots, \tau(u_n)) = \epsilon_\tau f(u_1, \dots, u_n)$

行列式的定义:

这里的  $g$  不一定  $\det$  运算  $\nearrow d(F)$  不是  $\det(F)$

定义  $d(F_{i,j}) = -1, d(F_{i,j}(a)) = 1, d(F_{i,j}(a)) = a^{-1}$ , 则有定理:

对任意  $(R^n)^n$  上的斜对称多重线性函数  $g$ , 有  $g(A) = d(F)g(FA), A \in (R^n)^n$

特别地, 若存在  $g$  的自变量  $\vec{u}_i = \vec{u}_j$ , 由  $A = F_{i,j}A$ , 得到:

$g(A) = d(F_{i,j})g(F_{i,j}A) = -g(A) \Rightarrow g(A) = 0$ . 若存在  $\vec{u}_i = \vec{0}$ , 由  $A = F_{i,i}A$

可得  $g(A) = d(F_{i,i}(a))g(F_{i,i}(a)A) = \frac{1}{a}g(A) \Rightarrow g(A) = 0$ .

### 2. 斜对称多重线性函数的基本:

设  $(R^n)^n$  上的所有斜对称多重线性函数构成集合  $C$ , 则存在双射  $H$ :

$g(I_n) \longmapsto g$ . 也即  $g$  由  $g(I_n)$  唯一确定. (对于行列式:  $g(I_n) = 1$ )

3.  $n$  阶行列式:  $\nearrow R^n$  的  $n$  重笛卡尔积  $\{\vec{u}_1, \dots, \vec{u}_n\} \vec{u}_1, \dots, \vec{u}_n \in R^n$

$n$  阶行列式是  $(R^n)^n$  到  $R$  的一个映射, 也可视为是  $R^n$  上的一个  $n$  元函数  $f(\vec{u}_1, \dots, \vec{u}_n)$ , 每一个变量  $\vec{u}_i \in R^n$ , 共  $n$  个向量, 并且容易验证行列式  $f$  是一个多重线性映射、斜对称函数. 其计算定义有多种:

#### ① 逆序数求和计算:

$$f(A) = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{vmatrix} = \sum (-1)^{\sigma} (a_{1p_1} a_{2p_2} \dots a_{np_n}), \text{共 } n!$$

#### ② 按行/列展开计算:

$$f(A) = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{vmatrix} = \begin{cases} \sum_{i=1}^n (-1)^{i+s} A[i] A[s], \text{按第 } s \text{ 行展开} \\ \sum_{i=1}^n (-1)^{i+s} A[s] A[i], \text{按第 } s \text{ 列展开} \end{cases}$$

#### ③ $n$ 元时称辞计算:

$$f(A) = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{vmatrix} = \sum_{\tau \in S_n} \epsilon_\tau a_{1\tau(1)} a_{2\tau(2)} \dots a_{n\tau(n)}$$

### 常规行列式的计算:

低阶 (1, 2, 3) 时用角线法计算, 不再阐述.

1. 初等行变换化为上三角: (高斯消元)  $\forall A, B \in M_{n \times n}, |AB| = |A||B| = |BA|$

当  $f$  表示行列式时, 易证  $f(F) = \frac{1}{d(F)}$ , 也即

$$\det(A) = \frac{\det(FA)}{\det(F)} \iff \det(FA) = \det(F) \det(A)$$

特别地, 当  $A$  可逆时, 我们有  $\det(A^{-1}) \det(A) = \det(A^{-1}A) = 1$

### 2. 按行/列展开: (中阶优势)

记  $A[j]$  为  $A$  中划去第  $j$  行、第  $j$  列所剩下的  $(n-1) \times (n-1)$  行列式, 记条子式  $M_{ij} = A[j]$ ,

代数余子式  $A_{ij} = (-1)^{i+j} M_{ij} = (-1)^{i+j} A[j]$ , 则有结论:

$$f(A) = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{vmatrix} = \begin{cases} \sum_{i=1}^n (-1)^{i+s} a_{si} A[s], \text{按第 } s \text{ 行展开} \\ \sum_{i=1}^n (-1)^{i+s} a_{is} A[s], \text{按第 } s \text{ 列展开} \end{cases}$$

### 3. 斜对称式:

矩阵  $A$  称为斜对称的, 如果  $A^\top = -A$ . 又容易证明  $\det(A) = \det(A^\top)$ ,

$\Rightarrow \forall$  斜对称矩阵  $A \in M_{n \times n}, n$  为奇数, 有  $\det(A) = 0$

## §3.2 行列式的性质

特殊行列式：行列式的计算常常先找递推公式，再求通项。

1. 上下三角式：

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_{nn} \end{vmatrix} = a_{11} a_{22} \cdots a_{nn}, \quad \begin{vmatrix} 0 & \cdots & 0 & a_{1,n} \\ \vdots & \ddots & \vdots & \vdots \\ 0 & a_{n-1,2} & \cdots & a_{n-1,n} \\ a_{n,1} a_{n,2} \cdots a_{n,n} \end{vmatrix} = (-1)^{\frac{n(n-1)}{2}} a_{1n} \cdots a_{nn}$$

2. 范德蒙德行列式：

$$\Delta(x_1, x_2, \dots, x_n) = \begin{vmatrix} x_1^n & x_2^n & \cdots & x_n^n \\ x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ x_1^1 & x_2^1 & \cdots & x_n^1 \end{vmatrix} = \prod_{i=1}^{n-1} \prod_{j=i+1}^n (x_j - x_i) = \prod_{1 \leq i < j \leq n} (x_j - x_i)$$

$$\Delta(x_1, x_2, x_3, \dots, x_n) \leftarrow \text{过程如下} \\ = \det [F_{21}(-x_1) F_{32}(-x_1) \cdots F_{n(n-1)}(-x_1)] \Delta(x_1, x_2, x_3, \dots, x_n)$$

$$= \begin{vmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & x_2 - x_1 & x_3 - x_1 & \cdots & x_n - x_1 \\ 0 & x_2(x_2 - x_1) & x_3(x_3 - x_1) & \cdots & x_n(x_n - x_1) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & x_2^{n-2}(x_2 - x_1) & x_3^{n-2}(x_3 - x_1) & \cdots & x_n^{n-2}(x_n - x_1) \end{vmatrix}$$

$$\text{按列1展开} \quad \begin{vmatrix} x_2 - x_1 & x_3 - x_1 & \cdots & x_n - x_1 \\ x_2(x_2 - x_1) & x_3(x_3 - x_1) & \cdots & x_n(x_n - x_1) \\ \vdots & \vdots & \ddots & \vdots \\ x_2^{n-2}(x_2 - x_1) & x_3^{n-2}(x_3 - x_1) & \cdots & x_n^{n-2}(x_n - x_1) \end{vmatrix} \\ = (x_2 - x_1)(x_3 - x_1) \cdots (x_n - x_1) \begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_2 & x_3 & \cdots & x_n \\ \vdots & \vdots & \ddots & \vdots \\ x_2^{n-2} & x_3^{n-2} & \cdots & x_n^{n-2} \end{vmatrix}$$

$$\Rightarrow \Delta(x_1, x_2, \dots, x_n) = (x_2 - x_1)(x_3 - x_1) \cdots (x_n - x_1) \Delta(x_2, \dots, x_n) \\ = \prod_{i=2}^n (x_i - x_1) \Delta(x_2, \dots, x_n) \Rightarrow \text{注意 } j-i$$

$$\Delta(x_1, x_2, \dots, x_n) = \prod_{i=1}^{n-1} \prod_{j=i+1}^n (x_j - x_i) = \prod_{1 \leq i < j \leq n} (x_j - x_i)$$

由此可以知道  $\Delta(x_1, x_2, \dots, x_n)$  是  $\mathbb{R}^n$  上的非线性对称函数

3. 对角分块式（双三角型）：

$$D_n = \begin{vmatrix} a & b & b & \cdots & b \\ c & a & b & \cdots & b \\ c & c & a & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & b \\ c & \cdots & c & a & \end{vmatrix} = \frac{b(a-c)^n - c(a-b)^n}{b-c}$$

特别地，当  $b=c$  时，由于  $D_n(b)$  在  $U(c, \delta)$  上连续，可得：

$$b=c \text{ 时, } D_n = \lim_{b \rightarrow c} D_n(b) \frac{b-a}{c-a} (a-c)^n + nc(a-c)^{n-1} = (a-c)^{n-1}(a-c+nc)$$

求解过程如下：

解 矩阵  $A_n$  的特点是主对角线上的元素都是  $a$ ，严格上三角元素都是  $b$  而严格下三角元素都是  $c$ 。注意第一行  $(a, b, b, \dots, b) = (a-b, 0, 0, \dots, 0) + (b, b, b, \dots, b)$ 。

根据行列式的多重线性。

$$\begin{aligned} D_n &= \begin{vmatrix} a-b & 0 & 0 & \cdots & 0 \\ c & a & b & \cdots & b \\ c & c & a & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & b \\ c & \cdots & c & a & \end{vmatrix} + \begin{vmatrix} b & b & b & \cdots & b \\ c & a & b & \cdots & b \\ c & c & a & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & b \\ c & \cdots & c & a & \end{vmatrix} \\ &= (a-b) \begin{vmatrix} 0 & 0 & 0 & \cdots & 0 \\ c & a-c & b-c & \cdots & b-c \\ c & 0 & a-c & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & b-c \\ c & 0 & 0 & \cdots & 0 \end{vmatrix} \\ &= (a-b) D_{n-1} + b \begin{vmatrix} a-c & b-c & \cdots & b-c \\ 0 & a-c & \ddots & \vdots \\ \vdots & \ddots & \ddots & b-c \\ 0 & 0 & \cdots & 0 \end{vmatrix} \\ &= (a-b) D_{n-1} + b(a-c)^{n-1}, \end{aligned}$$

即我们有递推公式  $D_n = (a-b) D_{n-1} + b(a-c)^{n-1}$ 。  
也可以通过得到

注意  $A_n$  可以从  $A_{n-1}$  中交换  $b$  和  $c$  得到。故  $D_n = {}^t A_n = (a-c) D_{n-1} + c(a-b)^{n-1}$ 。

当  $b \neq c$  时，从上述两个等式解  $D_n$  得  $D_n = \frac{b(a-c)^n - c(a-b)^n}{b-c}$ 。

由伴随矩阵求矩阵的逆：

1. 代数余子式：

记  $A[\frac{i}{j}]$  为从  $A$  中划去第  $i$  行、第  $j$  列剩下的  $(n-1) \times (n-1)$  方阵的行列式。  
称  $M_{ij} = A[\frac{i}{j}]$  为第  $i$  行、第  $j$  列的余子式，而  $A_{ij} = (-1)^{i+j} M_{ij}$  称为  $A$  中  $a_{ij}$  的代数余子式，也即  $A_{ij} = (-1)^{i+j} A[\frac{i}{j}]$

2. 伴随矩阵：

伴随矩阵  $A^*$ （或  $A^Y$ ）为代数余子式矩阵的转置，也即：

$$A^* = \begin{bmatrix} A_{11} & A_{12} & \cdots & A_{1n} \\ A_{21} & A_{22} & \cdots & A_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ A_{n1} & A_{n2} & \cdots & A_{nn} \end{bmatrix}^T \quad \text{勿忘 transpose !!}$$

3. 用伴随矩阵求矩阵的逆： $A^{-1} = \frac{A^*}{|A|}$

4. 伴随矩阵的行列式： $|A^*| = |A|^{n-1}$

斜对称多重线性函数的重要性质

1. 重要性质：

对任意的斜对称多重线性函数  $g$ ，我们有：

$$g(\bar{x}_1, \dots, \bar{x}_n) = g(\bar{e}_1, \dots, \bar{e}_n) \cdot \det(\bar{x}_1, \dots, \bar{x}_n) \quad (*)$$

此式常用于各种矩阵的行列式计算。

$$\text{也即 } g(A) = g(I_n) \det(A)$$

Example 1:

证明： $\forall A, B \in M_{n \times n}$ ,  $|AB| = |A||B| = |BA|$

$\downarrow$  一次验证了  $g(I_n)$  与  $g$  是一一对应的

只证左等号，如下：

对任意固定的  $A$ ，定义  $g(B) = \det(AB)$ ，则  $g(B)$  是  $B$  的列向量的  $n$  元斜对称多重线性函数，由  $(*)$  式得  $g(B) = g(I_n) \det(B)$ ，也即

$$\det(AB) = \det(AI_n) \det(B) = \det(A) \det(B)$$

Example 2:

证明： $\forall A \in M_{n \times n}$ ,  $B \in M_{m \times m}$ ,  $C \in M_{n \times m}$ ,  $\det \begin{bmatrix} A & C \\ 0 & B \end{bmatrix} = \det(A) \det(B)$

对任意固定的  $A, C$ ，定义  $g(B) = \det \begin{bmatrix} A & C \\ 0 & B \end{bmatrix}$ ，则  $g(B)$  是  $B$  的行向量的  $n$  元斜对称多重线性函数，由  $(*)$  式得  $g(B) = g(I_m) \det(B)$ ，也即

$$\det \begin{bmatrix} A & C \\ 0 & B \end{bmatrix} = \det \begin{bmatrix} A & C \\ 0 & I_m \end{bmatrix} \cdot \det(B)$$

类似地，令  $h(A) = \det \begin{bmatrix} A & B \\ 0 & C \end{bmatrix}$ ，可得  $\det \begin{bmatrix} A & C \\ 0 & I_m \end{bmatrix} = \det \begin{bmatrix} I_n & C \\ 0 & I_m \end{bmatrix} \cdot \det(A) = \det(A) \Rightarrow$

$$\det \begin{bmatrix} A & C \\ 0 & B \end{bmatrix} = \det(A) \det(B)$$

分块矩阵行列式不显然

其它性质：

1. 上/下三角矩阵组的  $\det$ ：

$$\det \begin{bmatrix} A_{11} & A_{12} \\ 0 & A_{22} \end{bmatrix} = \det(A_{11}) \cdot \det(A_{22}), \quad \det \begin{bmatrix} A & B \\ C & D \end{bmatrix} = \det(AD - ACA^{-1}B)$$

$$\det \begin{bmatrix} A_{11} & A_{12} & \cdots & A_{1n} \\ 0 & A_{22} & \cdots & A_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_{nn} \end{bmatrix} = \det(A_{11}) \cdots \det(A_{nn})$$

2. 矩阵\实数乘积的  $\det$ ：

$$\forall A, B \in M_{n \times n}, |AB| = |BA| = |A||B|$$

$$\text{由此可以得到: } \begin{vmatrix} KA & KB \\ C & D \end{vmatrix} = \begin{vmatrix} K & 0 \\ 0 & I_n \end{vmatrix} \begin{vmatrix} A & B \\ C & D \end{vmatrix} = \begin{vmatrix} K & 0 \\ 0 & I_n \end{vmatrix} \cdot \begin{vmatrix} A & B \\ C & D \end{vmatrix}$$

$$\Rightarrow \begin{vmatrix} KA & KB \\ C & D \end{vmatrix} = |K| \cdot \begin{vmatrix} A & B \\ C & D \end{vmatrix}$$

另外，对  $\forall a \in \mathbb{R}$ ，我们有： $|aA| = a^n |A|$

### 3. 行列式的几何意义:

对矩阵  $A \in M_{n \times n}$ ,  $\det(A)$  几何上就是以  $A$  的列/行向量为邻边的平行多面体的广义体积.

### 4. 矩阵的子式与矩阵的秩:

子式: 设  $A \in M_{m \times n}(\mathbb{R})$  且  $r \in \mathbb{N}$  满足  $1 \leq r \leq \min\{m, n\}$ , 对行指标  $1 \leq i_1 < i_2 < \dots < i_r \leq m$ , 和列指标  $1 \leq j_1 < j_2 < \dots < j_r \leq n$ , 我们用  $A(i_1, i_2, \dots, i_r | j_1, j_2, \dots, j_r)$  表示由  $A$  中处于第  $i_1, i_2, \dots, i_r$  行和第  $j_1, j_2, \dots, j_r$  列的  $r \times r$  个元素构成的  $r \times r$  矩阵. 如:

设  $A = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \end{bmatrix}$ , 则

$$A(1, 3 | 2, 4) = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \end{bmatrix} = \begin{bmatrix} a_{12} & a_{14} \\ a_{32} & a_{34} \end{bmatrix}$$

同时记行列式  $\det(A(1, 3 | 2, 4)) = A(1, 3 | 2, 4)$  为  $A$  的一个子式, 并有定理:  $\text{rank}(A) = \text{非零子式的最高阶}$ .

注1: 是留下交叉处的元素, 而非按行/列展开时那样划去.

注2: 我们有两个“子式”概念, 一个是余子式  $M_{ij}$ , 另一个矩阵的秩中的子式  $A(i_1, i_2, \dots, i_r | j_1, j_2, \dots, j_r)$ , 两者不同, 但都是行列式.

### §3.3 伴随矩阵和 Cramer's rule

#### 1. 定义:

伴随矩阵  $A^*$  (或  $A^T$ ) 为代数余式矩阵的转置, 也即:

$$A^* = \begin{bmatrix} A_{11} & A_{12} & \dots & A_{1n} \\ A_{21} & A_{22} & \dots & A_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ A_{n1} & A_{n2} & \dots & A_{nn} \end{bmatrix}^T$$

勿忘 transpose!!

#### 2. 定理:

① 对任意的方阵  $A$ :  $AA^T = |A|I_n \Rightarrow A^{-1}|A| = A^T$

再利用  $|AA^T| = |A||A^T| \Rightarrow A^T = \frac{A^{-1}}{|A|} (|A||A^{-1}| \neq 0)$

这表明  $A^{-1}$  与  $A^T$  紧密联系. 这表明  $|A^{-1}| = |A|^{-1} = \frac{1}{|A|}$

②  $\det(A^T) = [\det(A)]^{n-1}$

③  $(A^T)^T = |A|^{n-2} A$

#### 3. Cramer's Rule:

对可逆的矩阵  $A_{n \times n}$ , 方程组  $A\vec{x} = \vec{b}$  有唯一解

$\vec{x} = A^{-1}\vec{b}$ :  $x_1 = \frac{|A_{11}|}{|A|}, x_2 = \frac{|A_{21}|}{|A|}, \dots, x_n = \frac{|A_{n1}|}{|A|}$   
其中  $|A_{ij}|$  表示将  $|A|$  的第  $i$  列替换为  $\vec{b}$  所得行列式, 也即:

$$|A_{ij}| = \begin{vmatrix} a_{11} & \dots & a_{1(i-1)} & b_1 & a_{1(i+1)} & \dots & a_{1n} \\ a_{21} & \dots & a_{2(i-1)} & b_2 & a_{2(i+1)} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{n1} & \dots & a_{n(i-1)} & b_n & a_{n(i+1)} & \dots & a_{nn} \end{vmatrix}$$

### §3.4 Laplace expansion 与 Binet-Cauchy theorem

拉普拉斯展开

比内-柯西定理

#### Laplace expansion:

##### 1. 余子式:

$A \in M_{n \times n}$ , 记  $A \begin{bmatrix} i_1 & i_2 & \dots & i_n \\ j_1 & j_2 & \dots & j_n \end{bmatrix}$  为划去  $A$  第  $i_1, \dots, i_r$  行和  $j_1, \dots, j_r$  列的  $(n-r) \times (n-r)$  行列式, 称为余子式 (不是代数余子式)

##### 2. 定理 Laplace expansion: 行列式 $A$ 将第 $i_1, \dots, i_r$ 行展开有

$$\det(A) = \sum_{1 \leq i_1 < i_2 < \dots < i_r \leq n} (-1)^{\sum_{k=1}^r (i_k + j_k)} A \begin{bmatrix} i_1 & \dots & i_r \\ j_1 & \dots & j_r \end{bmatrix}$$

$r$  值求和, 如  $r=2, n=4$ , 按第1、2行展开时, 右边即为:

$$\begin{aligned} & \sum_{j_1=1}^3 \sum_{j_2=j_1+1}^4 (-1)^{\sum_{k=1}^2 (i_k + j_k)} A \begin{bmatrix} 1 & 2 \\ j_1 & j_2 \end{bmatrix} \cdot A \begin{bmatrix} 1 & 2 \\ j_1 & j_2 \end{bmatrix} \\ &= \sum_{j_1=2}^4 (-1)^{\sum_{k=1}^2 (i_k + j_k)} A \begin{bmatrix} 1 & 2 \\ j_1 & j_2 \end{bmatrix} \cdot A \begin{bmatrix} 1 & 2 \\ j_1 & j_2 \end{bmatrix} \\ &+ \sum_{j_1=3}^4 (-1)^{\sum_{k=1}^2 (i_k + j_k)} A \begin{bmatrix} 1 & 2 \\ j_1 & j_2 \end{bmatrix} \cdot A \begin{bmatrix} 1 & 2 \\ j_1 & j_2 \end{bmatrix} \\ &+ \sum_{j_1=4}^4 (-1)^{\sum_{k=1}^2 (i_k + j_k)} A \begin{bmatrix} 1 & 2 \\ j_1 & j_2 \end{bmatrix} \cdot A \begin{bmatrix} 1 & 2 \\ j_1 & j_2 \end{bmatrix} \\ &= \begin{vmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{vmatrix} \end{aligned}$$

Example: 求  $\begin{vmatrix} 1 & 1 & 3 & 4 \\ 2 & 0 & 0 & 8 \\ 3 & 0 & 0 & 2 \\ 4 & 4 & 7 & 5 \end{vmatrix}$

按第2、3行展开有:

$$T = 0 + 0 + \begin{vmatrix} 2 & 8 & | & 1 & 3 \\ 3 & 2 & | & 4 & 7 \end{vmatrix} + 0 + 0 + 0 = 100.$$

#### Binet - Cauchy theorem:

1. 由来: 我们知道对两个  $n \times n$  矩阵  $A, B$ ,  $|AB| = |A||B|$ , 那么  $|A_{mn}B_{nxm}| \neq 0$ ? 这就是 Binet - Cauchy theorem 做的事情

##### 2. Binet - Cauchy theorem:

$$\forall A \in M_{m \times n}, B \in M_{n \times m} \quad \det(AB) = \sum_{1 \leq i_1 < i_2 < \dots < i_m \leq n} A \begin{bmatrix} i_1 & i_2 & \dots & i_m \\ i_1 & i_2 & \dots & i_m \end{bmatrix} B \begin{bmatrix} i_1 & i_2 & \dots & i_m \\ 1 & 2 & \dots & m \end{bmatrix}$$

特别地, 当  $m=2 < n$  时所得 Cauchy 恒等式:

$$\left( \sum_{r=1}^n a_{1r}b_{r1} \right) \left( \sum_{s=1}^n a_{2s}b_{s2} \right) - \left( \sum_{r=1}^n a_{1r}b_{r2} \right) \left( \sum_{s=1}^n a_{2s}b_{s1} \right) = \sum_{1 \leq r < s \leq n} (a_{1r}a_{2s} - a_{1s}a_{2r})(b_{r1}b_{s2} - b_{r2}b_{s1}).$$

并且我们注意到,  $m < n$  时  $|A_{mn}B_{nxm}| \neq 0$  不一定等于  $|B_{nxm}A_{mn}|$

这是因为  $n$  阶方阵的秩  $r(BA) \leq \min\{r(B), r(A)\} \leq m < n$   
 $\Rightarrow |B_{nxm}A_{mn}| \equiv 0$ , 故  $|A_{mn}B_{nxm}| = |B_{nxm}A_{mn}| \Leftrightarrow |A_{mn}B_{nxm}| = 0$ .

Binet - Cauchy theorem 可通过行列式的多重线性证明, 谈贝讲义

“子式”剖析:

$A(\quad) \rightarrow$  子阵

子式: 留下,  $A \begin{bmatrix} i_1 & \dots & i_n \\ j_1 & \dots & j_r \end{bmatrix}$  任意矩阵都有  $\rightarrow$  秩

余子式: 别掉,  $A \begin{bmatrix} i_1 & \dots & i_n \\ j_1 & \dots & j_r \end{bmatrix}$  方阵才有  $\rightarrow$  排行、列展开

代数余子式:  $(-1)^{\sum_{k=1}^r (i_k + j_k)} A \begin{bmatrix} i_1 & \dots & i_n \\ j_1 & \dots & j_r \end{bmatrix}$

都是行列式

### §3.5 八大常见行列式及其解法：

一、三对角线行列式：递推 + 特征根 + 对称

$$D_n = \begin{vmatrix} a & b & & & \\ c & a & b & & \\ & c & a & b & \\ & & c & \ddots & \\ & & & a & b \\ & & & c & a \\ 0 & & & c & a \end{vmatrix}_{n \times n}$$

，依次按第n列、第n-1行展开，可得

$$D_n = a D_{n-1} - b c D_{n-2} \text{，解特征方程}$$

$$x^2 = ax - bc \Rightarrow x_1 = ? , x_2 = ?$$

$$\text{则得 } (D_n - x_1 D_{n-1}) = x_2 (D_{n-1} - x_1 D_{n-2})$$

$$\Rightarrow D_{n+1} - x_1 D_n = (D_2 - x_1 D_1) \cdot x_2^{n-1}$$

$$\text{这样 } x_1, x_2 \text{ 得: } D_{n+1} - x_2 D_n = (D_2 - x_2 D_1) \cdot x_1^{n-1}$$

①  $x_1 \neq x_2$  时：相减得：

$$D_n = \frac{x_1 x_2^{n-1} - x_2 x_1^{n-1}}{x_1 - x_2} \cdot D_1 + \frac{x_1^{n-1} - x_2^{n-1}}{x_1 - x_2} \cdot D_2$$

这是一般的规律。特别地，此题中有  $D_1 = x_1 + x_2 = a$ ， $D_2 = (x_1 + x_2)^2 - x_1 x_2 = a^2 - bc$ ，代入化简得  $D_n = \frac{x_1^{n+1} - x_2^{n+1}}{x_1 - x_2}$ 。

②  $x_1 = x_2$  时：记为  $x_0$ ，我们有事实：

$$D_n = \frac{x_0^{n+1} - x_2^{n+1}}{x_0 - x_2} = (n+1)x_0^n.$$

③  $x_1, x_2$  不存在：则  $\{D_n\}$  为循环数列。  
是否有一定？有待探讨

二、箭型行列式：消加到第1列

(空白处都为0)

$$D_n = \begin{vmatrix} x_1 & a & a & a & \cdots & a \\ a & x_2 & & & & \\ a & & x_3 & & & \\ a & & & x_4 & & \\ \vdots & & & & \ddots & \\ a & & & & & x_n \end{vmatrix} = a^2 \begin{vmatrix} \frac{x_1}{a^2} & 1 & 1 & 1 & \cdots & 1 \\ 1 & x_2 & & & & \\ & 1 & x_3 & & & \\ & & 1 & x_4 & & \\ & & & \vdots & \ddots & \\ & & & & & x_n \end{vmatrix}$$

依次将第i列的  $\frac{-1}{x_i}$  倍加到第一列， $i=2, 3, \dots, n$

$$D_n = a^2 \begin{vmatrix} \left( \frac{x_1}{a^2} - \frac{1}{x_2} - \cdots - \frac{1}{x_n} \right) & 1 & 1 & \cdots & 1 \\ 0 & x_2 & & & \\ 0 & & x_3 & & \\ \vdots & & & \ddots & \\ 0 & & & & x_n \end{vmatrix}$$

$$= a^2 \left( \frac{x_1}{a^2} - \sum_{i=2}^n \frac{1}{x_i} \right) \prod_{i=2}^n x_i$$

$$= (x_1 - a^2 \sum_{i=2}^n \frac{1}{x_i}) \prod_{i=2}^n x_i$$

上三角行列式

三、双三角形行列式（对角切割式）：拆行+对称

$$D_n = \begin{vmatrix} x_1 & a & a & \cdots & a \\ b & x_2 & a & \cdots & a \\ b & b & x_3 & \cdots & a \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b & b & b & \cdots & x_n \end{vmatrix} = \begin{vmatrix} x_1 & a & a & \cdots & a+b \\ b & x_2 & a & \cdots & a+b \\ b & b & x_3 & \cdots & a+b \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b & b & b & \cdots & x_n+b \end{vmatrix}$$

$$= \begin{vmatrix} x_1 & a & a & \cdots & a \\ b & x_2 & a & \cdots & a \\ b & b & x_3 & \cdots & a \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b & b & b & \cdots & b \end{vmatrix} + \begin{vmatrix} x_1 & a & a & \cdots & a \\ b & x_2 & a & \cdots & a \\ b & b & x_3 & \cdots & a \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b & b & b & \cdots & b \end{vmatrix}$$

剩下的内容详见知乎“八大常见类型的行列式及其解法”。

# 第四章. 群、环、域

## 9.4.1 群的概念与类型

具有代数运算的集合——“群”：

### 1. 二元运算：

从  $X \times X$  到  $X$  的一个映射  $f: X^2 \rightarrow X$  叫作  $X$  上的一个二元代数运算，常引入特殊的符号 +, ., \*, 或 - 等，将  $f(a, b)$  表示为  $a \cdot b$ ，如  $a+b$ 。

### 2. 代数结构(代数系统)：

在集合  $X$  上，我们可以定义多种不同的运算，选取其中的一种 \*，并用记号  $(X, *)$  表示：\* 定义了  $X$  上的一种代数结构，或称  $(X, *)$  是一个代数结构/代数系统。

### 3. 结合律：定义在 $X$ 上的二元运算 \* 称为结合的如果

$$\forall a, b, c \in X, (a * b) * c = a * (b * c)$$

### 4. 交换律：定义在 $X$ 上的二元运算 \* 称为交换的如果

$$\forall a, b \in X, a * b = b * a$$

### 5. 单位元： $\oplus(R, +)$ 的单位元是 0， $(M_{mn}, \cdot)$ 的单位元是 $I_n$

一个代数结构  $(X, *)$  最多有一个单位元  $e \in X$  满足

$$\forall x \in X, e * x = x * e = x$$

### 6. 半群：

一个代数结构  $(X, *)$  称为一个半群如果 \* 满足结合律。

特别地，当半群  $(X, *)$  拥有单位元时，称其为么半群。

### 7. 可逆元素：

么半群  $(X, *)$  中的一个元素  $a$  称为可逆的如果  $\exists b \in X$  使得  $a * b = b * a = e$ 。此时记  $b$  为  $a^{-1}$

### 8. 群：每个元素都可逆的么半群称为群。

### 9. 交换群(abelian group)：如 $(\mathbb{Z}, +)$ $(\mathbb{Q}^*, \cdot)$ 都为交换群

任意两个元素都可交换的群称为交换群，或阿贝尔群。

### 10. 子群：

$$\Omega = \mathbb{Q} \setminus \{0\}$$

记群  $G = (X, *)$ ,  $H$  为  $X$  的一个非空子集，则

设  $H \subseteq G$ ,  $(H, *)$  称为  $G$  的一个子群如果  $\forall a, b \in H, a * b^{-1} \in H$ , 则  $H \subseteq G$

$\hookrightarrow$  记为  $H \leq G$ . 这等价于  $H$  对取逆映射  $x \rightarrow x^{-1}$  和运算 \* 封闭

$\forall a, b \in H$ , 特别地,  $([e], *)$  称为平凡子群, 若  $H \neq [e]$  或  $X$ , 则

称  $(H, *)$  为  $G$  的真子群. 且易证, 子群的交仍是子群.

和  $(m\mathbb{Z}, +)$  是  $(\mathbb{Z}, +)$  的一个子群。

$S_n$  中的全体偶置换  $S_n$  关于 \* 构成一个子群，称为交错群。

### 11. 群的基数：即为集合 $X$ 的基数，等价符号有 $\text{card } G$ , $|G|$ , $[G : \langle e \rangle]$

### 12. 由子集生成子群：

群  $G = (X, *)$ , 设  $S \subseteq X$ , 并记  $S^{-1} = \{a^{-1} | a \in S\}$ , 记

$$\langle S \rangle = \{a_1 * \dots * a_n | n \in \mathbb{N}, a_i \in S \cup S^{-1}\}$$

一个子群。此时称  $\langle S \rangle, *$  为由  $S$  生成的子群(不称作由  $\langle S \rangle$  生成)。

例如置换群  $S_n$  即为由  $\{\tau_1, \dots, \tau_n\}$  生成的群，其中  $\tau_i = (1 i)$ .

特别地，当  $S$  中有且仅有-一个元素  $a$  时，称  $S$  生成的群为循环群。

若  $\exists k \in \mathbb{N}_+$  使得  $a^k = e$ ，称为  $k$  阶循环群，否则称为无限阶循环群。

### 13. 循环群：

$\rightarrow$   $k$  为负数时，约定  $-n \tau a$  表示  $n \tau a^{-1}$

一个群  $(X, *)$  称为循环群如果  $\exists a \in X$ , 使得

$X = \{a * a * \dots * a | k \in \mathbb{Z}\}$ , 并称  $a$  为生成元。也可称  $(X, \cdot)$  是带有生成元  $a$  的循环群，或由元素  $a$  生成的循环群。

### 一些特殊的群：

#### 1. 一般线性群 (general linear group):

记  $\mathbb{R}$  上的  $n \times n$  可逆矩阵全体为  $GL_n(\mathbb{R}) = \{A \in M_{n \times n}(\mathbb{R}) | \det(A) \neq 0\}$ ,

则  $(GL, \cdot)$  构成一个无限连续群，称为一般线性群。

#### 2. 正交群：

$$\text{记 } O_n(\mathbb{R}) = \{A \in M_{n \times n}(\mathbb{R}) | A^T A = I_n \text{ (即 } A^{-1} = A^T)\}$$

$(O_n(\mathbb{R}), \cdot)$  构成  $(GL_n(\mathbb{R}), \cdot)$  的子群

#### 3. 特殊线性群 (special linear group):

$$\text{记 } SL_n(\mathbb{R}) = \{A \in M_{n \times n}(\mathbb{R}) | \det(A) = 1\} \Leftrightarrow A \cdot A = I_n$$

则  $(SL_n(\mathbb{R}), \cdot)$  构成  $(GL_n(\mathbb{R}), \cdot)$  的子群。

#### 4. 旋转群：

$$SO_n(\mathbb{R}) = O_n(\mathbb{R}) \cap SL_n(\mathbb{R})$$
 是  $\mathbb{R}^n$  中旋转变换全体所对应的群。

#### 5. 模群 (modular group):

$$\text{记 } SL_2(\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\} \text{ 由于}$$

$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \in SL_2(\mathbb{Z}) \subset SL_2(\mathbb{R})$ , 因此  $(SL_2(\mathbb{Z}), \cdot)$  构成  $(SL_2(\mathbb{R}), \cdot)$  的一个子群。特别地, 令  $T = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ , 则  $T^n = \begin{bmatrix} 0 & n \\ n & 0 \end{bmatrix}$  为无限阶循环群。

再令  $S = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}, S^2 = -I_2 \Rightarrow S^6 = I_2$  为四阶, 且有定理:  $SL_2(\mathbb{Z}) = \langle S, T \rangle$

#### 6. 交错群：置换群 $S_n$ 中的全体偶置换构成一个群，称为交错群。

#### 7. 整数加法群：

$(\mathbb{Z}, +)$  构成一个以 1 为生成元的循环群，所有元素都是 1 的“乘方”，也即对于加法  $\langle 1 \rangle = \mathbb{Z}$

#### 8. dihedral 群：

$$D_{2n} = \{A \in O_2(\mathbb{R}) \mid A(\mathbb{Z}_n) = \mathbb{Z}_n\}, \mathbb{Z}_n \text{ 指平面上重心在原点及有一条对称轴在 } y \text{ 轴上的正 } n \text{ 边形。}$$

#### 9. 模 $n$ 剩余类加法群 $\mathbb{Z}_n$ :

定义模  $n$  运算下的  $\bar{i} = \{i + kn \mid k \in \mathbb{Z}\}$ , 例如  $n=3$  时 (模 3), 有

$$\bar{4} = \bar{1} = \{1 + kn \mid k \in \mathbb{Z}\}, \text{ 令 } \mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \bar{n-1}\}$$

容易证明  $\mathbb{Z}_n$  构成一个加法群，称为模  $n$  剩余类群，且有  $\langle 1 \rangle = \mathbb{Z}_n$ 。

$$\bar{i} = \{i + kn \mid k \in \mathbb{Z}\}, \mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$$

### 与群有关的定理/推论：

#### 1. 左单位元 + 左可逆(左同理):

如果一个半群  $(X, \cdot)$  含左单位元  $e$  且每个元素关于  $e$  左可逆，也即  $\forall a \in X, \exists b \in X$  使得  $b \cdot a = e$ , 则  $(X, \cdot)$  构成一个群。

#### 2. 等价模群:

$$\text{记 } S = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \text{ 则有定理: } SL_2(\mathbb{Z}) = \langle S, T \rangle$$

#### 3. 元素的阶:

$\forall a \in G$  (这里  $G$  是任意的群),  $a$  的阶等于  $\text{card} \langle a \rangle$

## §4.2 群同态

通常来讲，我们可以用乘法群的运算类似地表示其它运算。因此之后的情形一般都用乘法群来表示。

### 陪集与 Lagrange:

1. 左商空间：等价于  $g_1^{-1}g_2 = h \in H$

设  $H$  是  $G$  的一个子群，我们在  $G$  中定义关系： $g_1 \sim_H g_2$  如果  $\exists h \in H$  使得  $g_1 = g_2 * h$  ( $g_1, g_2 \in G$ )，容易证明此关系是一个等价关系，其等价类即为左陪集，且  $G$  是关于  $\sim_H$  的等价类的并集。

对  $\forall g \in G$ ，定义左陪集： $gH = \{gh \mid h \in H\}$ ，则可以证明：

$$\begin{aligned} g_1 \sim_H g_2 &\iff g_1, g_2 \text{ 属于同一个左陪集} \\ &\iff g_1, g_2^{-1} \in H \end{aligned}$$

$G/\sim_H = \{gH \mid g \in G\}$  记为  $G/H$ ，称其为  $G$  关于子群  $H$  的左商空间，也即  $G$  关于  $H$  的全部左陪集构成的集合。

### 2. 群乘法：

对群  $X, Y$ ，定义群的乘法： $X \cdot Y = \{xy \mid x \in X, y \in Y\}$ ，有以下结论：

- ① 若  $g_1H, g_2H$  都是左陪集，则  $g_1H \cdot g_2H = g_1g_2H$
- ② 若  $H, K$  是  $G$  的子群，则  $HK$  是  $G$  的子群  $\iff HK = KH$

### 3. 群阶与 Lagrange theorem:

群阶：即群集合的元素个数  $|G|$

指标： $G/H$  的元素个数（不同陪集个数） $|G/H|$  称为  $H$  在  $G$  中的指标，

记为  $[G : H]$ ，如  $[S_n : A_n] = 2$  置换群 交错群

Lagrange theorem:  $|G| = [G : H] \cdot |H|$  也即  $|G/H| = \frac{|G|}{|H|}$

当  $G$  是有限群时， $|H|$  整除  $|G|$ ，并且  $\forall a \in G$ ， $a$  的阶整除群的阶  $|G|$ 。

并且有推论：

① 设  $G$  为有限群，且  $K \leq H, H \leq G$ ，则  $[G : K] = [G : H][H : K]$

② 设  $K \leq G, H \leq G$ ，且  $|K| < \infty, |H| < \infty$ ，则  $|HK| = \frac{|H||K|}{|H \cap K|}$

### 4. 应加莱定理：

这里并不要求  $HK$  是群 子群的交还是子群

如果有有限多个子群的指标都是有限数，则它们的交的指标也是有限数。)

即  $[G : H_1], [G : H_2] < \infty \Rightarrow [G : H_1 \cap H_2] < \infty$  正规子群的交也是正规

### 正规子群：

#### 1. 定义：

① 设  $H$  是  $G$  的子群，若  $\forall a \in G, h \in H$ ，有  $aha^{-1} \in H$ ，即  $aHa^{-1} \subseteq H$ ，则称  $H$  是  $G$  的正规子群。记为  $H \trianglelefteq G$

② 设  $H$  是  $G$  的子群，若  $\forall a \in G$ ，有  $H = aHa^{-1}$ ，则称  $H$  是  $G$  的一个正规子群，记为  $H \trianglelefteq G$ 。

③ 设  $H \trianglelefteq G$ ，若  $\forall g \in G, gh = hg$ ，则称  $H$  为  $G$  的正规子群

注：上述三系定义等价。

群  $G$  关于正规子集的左右陪集相等，统称陪集。

#### 2. 共轭

设  $a, b \in G$ ，我们称  $a$  和  $b$  是共轭的如果  $\exists g \in G$  使得  $a = gbg^{-1}$ ，也即  $ag = gb$ 。集合的共轭也是类似的： $K = gHg^{-1}$ 。

由此我们可以发现，正规子群定义描述的是“对称性”。

意一个正规子群的元素，它的共轭元素也在群里。”

#### 3. 性质：

① 正规子群的交  $H \cap K$  仍是正规子群。

② 正规子群的积  $HK$  仍是正规子群。

③  $H$  是  $G$  的正规子群  $\iff$  任意两个左(右)陪集的积仍是左陪集。

④  $H \trianglelefteq G$  且  $[G : H] = 2 \Rightarrow H \trianglelefteq G$

⑤ 一个交换群的任意子群是正规子群。

#### 4. 商群：

$H$  是  $G$  的一个正规子群，则  $G/H = \{aH \mid a \in G\}$  关于陪集的乘法构成群，这个群称为  $G$  关于  $H$  的商群，或  $G$  模  $H$  的商群。

因为对任意的群  $G, G^2 = G$ ，和子群的乘积

$aH \cdot bH = abH$ ，故  $\langle aH \rangle = \{a^kH \mid k \in \mathbb{N}\}$

### 群同态/群同构：

#### 1. 群同态：

$G \rightarrow G'$  的映射  $\varphi$  称为同态如果  $\forall a, b \in G$ ，有  $\varphi(ab) = \varphi(a) \cdot \varphi(b)$

#### 2. 性质：

①  $\varphi(e)$  是  $G'$  的单位元， $\varphi(a)$  和  $\varphi(a^{-1})$  互为逆元。

② 若  $H$  是  $G$  的子群，则  $\varphi(H)$  是  $G'$  的子群。特别地，令  $H = G$ ，可得  $\varphi(G)$  是  $G'$  的子群。

③  $\exists$  双射  $\varphi$  使  $G/\ker(\varphi) \cong \text{Im}(\varphi) = \varphi(G) \rightarrow$  同态基本定理 (第一同构定理)

#### 3. 同态核/同态像

群同态  $\varphi$  的值域称为同态像  $\text{Im}(\varphi)$ ，也即  $\text{Im}(\varphi) = \varphi(G) = \{\varphi(g) \mid g \in G\}$ 。

另外， $\varphi$  把  $G$  中的一些元素映成了  $G'$  的单位元，称这些元素为同态核  $\ker(\varphi)$ ，也即  $\ker(\varphi) = \{g \mid \varphi(g) = e' \in G'\}$ 。并且可以证明： $\ker(\varphi)$  是  $G$  的正规子群，并且  $\varphi$  是单射  $\iff \ker(\varphi) = \{e\}$

#### 4. 自然同态：

设  $H \trianglelefteq G$ ，同态  $\varphi: a \mapsto aH$  称为从  $G$  到  $G/H$  的自然同态。

#### 5. 群同构：

当  $\varphi$  是双射时，称  $\varphi$  是  $G$  到  $G'$  的同构。记为  $G \cong G'$ 。同构的两个群可以看成同一群的不同体现。

#### 6. 定理：

设  $G$  是一个有限群，若  $a, b \in G$  是不交换的两个二阶元，则子群  $\langle a, b \rangle$  同构于一个 dihedral 群。

#### 7. 无限群可以与其子群同构

如  $\varphi: n \mapsto 2n$  是从正到2正的群同构。

#### 8. 自同构群 $\text{Aut}(G)$ ：

群  $G$  到其自身的同构称为自同构。

群  $G$  的全体自同构  $\text{Aut}(G)$  关于映射乘积构成一个群，称为  $G$  的自同构群。

如给定  $g \in G$ ，定义  $I_g: a \mapsto gag^{-1}$ ，其中  $a \in G$ ，则  $I_g$  是一个自同构，称为内自同构。

9. 内自同构群  $\text{Inn}(G)$ ：

可以证明： $G/\text{Inn}(G) \cong \text{Inn}(G)$

证明详见 goodnotes “群论基础” P46.

$\forall g \in G$ ，定义从  $G$  到  $G$  的映射  $I_g: a \mapsto gag^{-1}$ ，则  $I_g$  构成  $G$  的自同构，称为内自同构。全体内自同构构成  $\text{Aut}(G)$  的正规子群，记为  $\text{Inn}(G)$ ，即  $\text{Inn}(G) = \{I_g \mid g \in G\}$ 。且  $(I_g)^{-1} = I_{g^{-1}}$ 。

#### 10. 定理：

设  $G$  是一个有限群，若  $G$  有一个二阶自同构  $\varphi$  满足  $I_g \circ I_g = I_{g \cdot g}$ 。

$\varphi(a) = a \Rightarrow a = e$ ，则  $G$  是一个交错群。

### §4.3 群作用在集合上

群在集合上的作用及其推论

#### 1. 群作用在集合上

群  $G$  在集合  $X$  上的作用是一个  $G \times X$  到  $X$  的映射:  $(g, x) \mapsto g \cdot x$

且映射满足:  $e(x) = x$ ,  $(g_1 g_2)(x) = g_1(g_2(x))$ ,  $g_1, g_2 \in G$ ,  $x \in X$

#### 2. 变换:

对任意给定的  $g \in G$ , 定义  $X$  上的变换:  $\varphi_g(x) = g \cdot x$ ,  $x \in X$

则商式等价于  $\varphi_e = e_x$ ,  $\varphi_{g_1 g_2} = \varphi_{g_1} \circ \varphi_{g_2}$ , 且  $\varphi: G \rightarrow S_X$  是一个

群同态. 反之, 给定一个群同态  $\varphi: G \rightarrow S_X$ , 映射  $(g, x) \mapsto \varphi(g)(x)$

$= g \cdot x$  给出了群  $G$  在  $X$  上的作用.

例如  $G = GL_n(\mathbb{R})$ , 对任意  $A \in GL_n(\mathbb{R})$ , 线性变换  $\varphi_A: \mathbb{R}^n \rightarrow \mathbb{R}^m$

是群同态, 它定义了群  $G$  在  $\mathbb{R}^n$  上的作用:  $\varphi_A(\vec{x}) = A\vec{x}$

#### 3. 左乘变换:

设  $|G| = n < \infty$ , 对任意给定  $g \in G$ , 定义  $G$  上的左乘变换:

$L_g(a) = ga$ ,  $a \in G$ , 则有  $L_g(e) = g$  和  $L_{g_1 g_2}(a) =$

$L_{g_1}(L_{g_2}(a))$ , 故映射  $g \mapsto L_g$  是  $G$  到  $S_G \cong S_n$  的一个单同态 (同态且单射).

#### 4. Cayley theorem: 所有 $n$ 阶群同构于对称群 $S_n$ 的某个子群.

#### 5. 轨道 $O_x$ :

对任意固定的  $x \in X$ , 集合  $O_x = \{g \cdot x = g_1 \cdot x \mid g \in G\}$ , 称为  $x$  在  $G$  作用下的轨道, 简称  $x$  的  $G$  轨道. 这里的  $g$  是一个映射, 也即  $g \cdot x = g_1 \cdot x$ , 一般也写作  $g \cdot x$ . 至于映射  $g$  具体是怎样映射的, 我们和矩阵  $A$  代表线性变换无关, 它可以是多样的.

#### 6. 稳定化子 (stabilizer) $C_x$ :

设群  $G$  作用在  $X$  上,  $x \in X$ , 称  $C_x = \{g \in G \mid g \cdot x = x\}$  为  $G$  关于  $x$  的稳定化子, 它构成  $G$  的子群, 几何上称为迷向子群.

#### 7. 推论:

$k | C_x | = |G|$  形成了一个等价类

假设轨道  $O_x$  中两元素相等  $g_1 \cdot x = g_2 \cdot x \Leftrightarrow g_1^{-1} g_2 \cdot x = x \Leftrightarrow g_1^{-1} g_2 \in C_x \Leftrightarrow g_1 \in g_2 C_x$

于是映射  $j_{C_x}: O_x \rightarrow g_2 C_x$  给出了从商空间  $G/G_x$  到  $O_x$  的同构.

$j_{C_x} \in G/G_x$ ,  $j_{C_x} \in O_x$ , 且每个  $j_{C_x}$  与  $j_{C_y}$  一一对应 (集合  $O_x$  元素的非同性).

如果  $O_x$  是个有限集, 那么  $|O_x| = [G : C_x] = |G/G_x|$ .

另外, 如果两个轨道有交, 即  $\exists w = g_1 \cdot x = g_2 \cdot y$  使得  $w \in O_x \cap O_y$ , 那么

推得  $O_x = O_y$ , 因此有结论: 不同的轨道互不相交. 对于不同的  $x \in X$ ,

$O_x$  给出了  $X$  的一个划分 (不交并).

#### 8. 中心 $C(G)$ : 这个符号是 $G$ 的花体, 也即 $G$ 与所有元素交换

$G$  的子集  $C(G) = \{c \in G \mid \forall g \in G, cg = gc\}$  构成一个灰换子群, 称为  $G$  的中心. 且有结论:  $C(G) \trianglelefteq G$  等价  $\forall g \in G, x = gxg^{-1}$

若  $C(G) = \{e\}$ , 称  $G$  为无中心群, 否则称  $G$  有非平凡的中心.

#### 9. $p$ 群

$p$  为一个素数, 群  $G$  称为一个  $p$  群如果  $|G| = p^n$ ,  $n \in \mathbb{N}_+$ . 且有

定理 8: 若  $G$  是一个  $p$  群, 则  $|C(G)|$  是  $p$  的倍数.

#### 10. Sylow 第一原理:

设  $G$  为阶  $n = mp^r$  的有限群, 其中  $m, r \in \mathbb{N}$  且  $\text{g.c.d}(m, p) = 1$ ,

则  $\forall s \in \mathbb{N}, s \leq r$ ,  $G$  含有所  $p^s$  的子群. 特别地, 令  $s=1$ , 即得到

Cauchy theorem:

如果素数  $p$  整除有限群  $G$  的阶  $|G|$ , 则  $G$  含有所  $p$  的子群.

Sylow 第一原理中,  $G$  的  $p^r$  阶子群称为  $G$  的 Sylow- $p$  子群.

#### 11. Sylow 第二原理:

设  $G$  为阶  $n = mp^r$  的有限群, 其中  $m, r \in \mathbb{N}$  且  $\text{g.c.d}(m, p) = 1$ , 设  $G$  的一个  $p^r$  阶子群为  $H$ , Sylow- $p$  子群为  $P$ , 则存在  $g \in G$ , 使  $gHg^{-1} \subseteq P$ , 特别地, 当  $s=r$  时有  $gP_1g^{-1} = P_2$ , 即  $G$  的任意两个 Sylow- $p$  子群共轭.

#### 12. Sylow 第三原理:

设  $G$  为阶  $n = mp^r$  的有限群, 其中  $m, r \in \mathbb{N}$  且  $\text{g.c.d}(m, p) = 1$ , 记以为  $G$  的 Sylow- $p$  子群个数, 则  $k \mid m$  且  $p \mid (k-1)$ . 特别地, 我们有  $k = 1 \Leftrightarrow$  Sylow- $p$  子群为正规子群.

### §4.4 有限群的一些结构

有限群的结构与定理:

#### 1. 直积

在笛卡尔积  $G_1 \times G_2$  上定义乘积:  $(a_1, a_2) \cdot (b_1, b_2) = (a_1 b_1, a_2 b_2)$  其中  $a_1, b_1 \in G_1$ ,  $a_2, b_2 \in G_2$ . 则  $(G_1 \times G_2, \cdot)$  构成一个群, 我们称群  $G_1 \times G_2$  为  $G_1$  和  $G_2$  的直积, 类似地可定义多个群的直积.

#### 2. 定理 12:

若  $p$  为素数且  $G$  为  $p^r$  阶群, 则  $G \cong \mathbb{Z}_{p^r}$  或  $G \cong \mathbb{Z}_p \times \mathbb{Z}_{p^{r-1}}$

#### 3. 半直积 $\rtimes$ :

给定群  $H, K$  和群同态  $\varphi: H \rightarrow \text{Aut } K$ , 在  $K \times H$  上定义运算:  $(a_1, b_1) \cdot (a_2, b_2) = (a_1 \cdot \varphi_{b_1}(a_2), b_1 \cdot b_2)$ ,  $a_1, a_2 \in K, b_1, b_2 \in H$  则  $K \times H$  关于上述运算构成群, 称为群  $K$  和  $H$  关于  $\varphi$  的半直积 (semidirect product), 记为  $K \rtimes H$ . 若  $K, H$  都是交换群, 则  $K \rtimes H$  是交换群  $\Leftrightarrow \varphi(H) = \{e\}$

#### 4. 模 $n$ 乘法群 $\mathbb{Z}_n^*$ :

定义模  $n$  乘算下的  $\bar{n} = \{i + kn \mid k \in \mathbb{Z}\}$

如  $n=5$  时,  $\bar{1} = \bar{1} = 1, \bar{2} = \bar{3}$ .

易推得  $\bar{i} \cdot \bar{j} = (\bar{i} \cdot j)$ , 称之为元素  $\bar{i}$  的乘法, 有结论:

$\mathbb{Z}_n^*$  的元素  $\bar{i}$  关于乘法可逆  $\Leftrightarrow g.c.d(i, n) = 1$

如  $n=6$  时,  $g.c.d(6, 5) = 1 \Rightarrow \bar{5}$  可逆

由此得  $\mathbb{Z}_n^* = \{\bar{i} \mid i \in \{1, \dots, n-1\}, g.c.d(i, n) = 1\}$ , 特别地, 当  $n$  为素数  $p$  时,  $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{\bar{0}\}$

这里是差集, 不是商集

#### 5. 定理 13:

设  $K$  是群  $G$  的  $m$  阶子群,  $H$  是  $G$  的  $n$  阶子群, 且  $\text{g.c.d}(m, n) = 1$  有结论  $|KH| = |K| \cdot |H|$ , 特别地, 如果  $K \trianglelefteq G$ , 还有  $KH \cong K \times H$ .

#### 6. 定理 14:

设  $p, q$  为素数且  $p > q$ , 有结论:

$\begin{cases} q \nmid (p-1) \text{ 时: 任意 } p^q \text{ 阶群与 } \mathbb{Z}_{p^q} \text{ 同构} \\ q \mid (p-1) \text{ 时: 有且仅有 } p^q \text{ 阶群 } \mathbb{Z}_p \times \mathbb{Z}_{p^{q-1}} \text{ 与 } \mathbb{Z}_{p^q} \text{ 同构} \end{cases}$

#### 7. 有限交换群结构定理:

若  $G$  是一个有限交换群, 则存在正整数  $n_1, n_2, \dots, n_s$  满足  $n_i \mid n_j$ , 使得  $G \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \dots \times \mathbb{Z}_{n_s}$

#### 8. 有限群的柯西定理:

$\text{Sylow I} + p$  阶群必循环

若  $\exists$  素数  $p$  使  $p \mid |G|$ , 则  $G$  一定含有  $p$  阶元.

## 9. 单群:

群  $G$  称为一个单群如果  $G$  的所有正规子群是  $G, \{e\}$ ,  
也即  $G$  没有非平凡正规子群.

$G$  是素数阶循环群

10. 设  $G$  是交换群, 则:  $G$  是单群  $\Leftrightarrow G$  是素数阶群

11. 群的乘积:

设  $H, K$  是群, 则  $HK := \{hk \mid h \in H, k \in K\}$

三大同构定理:

1. 第一同构定理(同态基本定理):

设  $\varphi: G \rightarrow G'$  是群同态, 则  $\ker(\varphi) \trianglelefteq G$ ,  $\varphi(G) \leq G'$ , 且

$$G/\ker(\varphi) \cong \text{Im}(\varphi) = \varphi(G)$$

证明详见“作业12”第2题.

2. 第二同构定理

若  $H \trianglelefteq G$ ,  $K \trianglelefteq G$ , 则  $H \cap K \trianglelefteq H$ ,  $K \trianglelefteq HK$  且

$$H/(H \cap K) \cong HK/K$$

证明详见“作业12”第2题.  $\Downarrow$

3. 第三同构定理

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$$

若  $\ker(\varphi) \subseteq H \trianglelefteq G$ , 则  $G/H \cong \varphi(G)/\varphi(H)$ ,

考虑到  $G$  的每一个正规子群都是某个同态的核, 我们有: 若  $N \trianglelefteq G$ ,  $H \trianglelefteq G$  且  $N \leq H \leq G$ ,

则  $G/H = (G/N)/(H/N)$ . 证明详见 goodnotes “群论基础” P39.

其它常用结论:

1. (正规)子群的交:

子群的交仍是子群, 正规子群的交仍是正规子群.

2. 子群的积是否仍为子群:

设  $H \trianglelefteq G$ ,  $K \trianglelefteq G$ , 有结论:

$$HK \trianglelefteq G \Leftrightarrow HK = KH \Leftrightarrow K \trianglelefteq G$$

3. 陪集的性质:  $\rightarrow$  两个左陪集要么交要么相同.

设  $H \trianglelefteq G$ ,  $a, b \in G$ , 有结论:  $\nearrow$  逆在左边

$$aH = bH \Leftrightarrow b^{-1}a \in H, Ha = Hb \Leftrightarrow ab^{-1} \in H$$

特别地, 令  $b = e$ , 得  $aH = H \Leftrightarrow a \in H \Leftrightarrow Ha = H$

4. 群同态的单射判定:

设群同态  $\varphi: G \rightarrow G'$ ,  $e$  为  $G$  的幺元, 则有结论:

$$\varphi \text{ 为单射} \Leftrightarrow \ker(\varphi) = \{e\} \quad \ker(\varphi) = \{g \in G \mid \varphi(g) = e'\} \subseteq G$$

5. 循环群的生成元:

设  $G$  为一个循环群, 则有结论:

$\begin{cases} |\varphi(G)|, |G| < \infty \end{cases} ??$   
 $G$  生成元的个数为  $\begin{cases} 1, & \text{若 } |G|=2 \\ 2, & \text{若 } |G|=\infty \end{cases}$   $\rightarrow$  有且仅有  $g, g^{-1}$  两个.  
 $\downarrow$   $q(n)$  为欧拉函数:  $q(n) =$  小于  $n$  的与  $n$  互素的正整数个数. 如  $q(8) = 4$ .

6. 中心群的等价条件与  $n$  互素的正整数个数. 如  $q(8) = 4$ .

设  $G$  的中心群  $\ell(G) = \{x \in G \mid \forall g \in G, xg = gx\}$ , 有结论:

$$x \in \ell(G) \Leftrightarrow \forall g \in G, x = gxg^{-1}$$

7. 群元素的阶:

群  $G$  中,  $a \in G$ , 设  $|a| = n$ , 则有:

$$\forall k \in \mathbb{N}, |a^k| = \frac{n}{\text{g.c.d}(n, k)}, \text{ 且 } |a^k| \text{ 为 } \text{g.c.d}(n, k)$$

## B. 奇数阶群可开方:

若  $|G|$  为奇数, 则  $\forall g \in G, \exists a \in G$  使  $a^2 = g$ .

9.  $[G:H] = 2 \Rightarrow H \trianglelefteq G$  具有传递性

10.  $N \trianglelefteq H, H \trianglelefteq G \Rightarrow N \trianglelefteq G$  其中  $|g| = 2k+1$

11. 定理 13:

$K \leq G, H \leq G$ , 且  $\text{g.c.d}(|K|, |H|) = 1$ , 则

$$|KH| = |K| \cdot |H|. \text{ 若 } K \trianglelefteq G, \text{ 则 } KH \leq G \text{ 且}$$

$$KH \cong K \times H$$

12.

13.  $60$  所以下的单群:

设  $|G| < 60$ , 则  $G$  是单群  $\Leftrightarrow |G|$  是素数.  $\Rightarrow G$  是循环群

14. 几个典型正规子群:

①  $G$  的 Sylow-P 子群个数为 1 时, 它是  $G$  的正规子群

② 指数为 2 的子群是正规子群

③ 中心  $\ell(G) \trianglelefteq G$

④  $\ker(\varphi) \trianglelefteq G$

15. 素数阶群一定是循环群.  $\rightarrow$  素数阶群

16.  $\mathbb{Z}_p^*$  构成循环群(关于乘法)

17. 有限半群  $G$  满足消去律  $\Rightarrow G$  为域群

证明: 设  $|G| = n$ , 并设  $G = \{g_1, g_2, \dots, g_n\}$ , 考虑集合  $J: G = \{g_1, g_2, \dots, g_{n!}\}$ , 作假设  $\{g_1, g_2, \dots, g_{n!}\}$  中有相同元素, 即  $g_i, g_j = g_1, g_j \stackrel{\text{消去律}}{\Rightarrow} g_i = g_j$  ( $i \neq j$ ), 这与  $g_i \neq g_j$  矛盾, 因此  $|J| = n \Rightarrow J \cdot G = G$ , 再假设  $g_i, g_j = g_{\pi(i)} = g_{\pi(j)}$ ,  $\pi \in S_n$ , 由  $|J| \mid |S_n| = n!$ , 可得  $(g^{n!})_{j \in J} = g_{\pi^{-1}(j)} = g_{\pi(j)} = g_j$ , 右乘同理, 因此  $\exists e = g_1^{n!} \in G$ , 并且  $g \cdot G = G \Leftrightarrow \forall g \in G, \exists g_2 \in G$  使  $g \cdot g_2 = g$ , 令  $g = e$ , 则  $g \cdot g_2 = e$ , 左乘同理, 因此  $g_2^{-1} = g_2$ , 由  $g$  任意性,  $G$  中所有元素可逆, 构成群, 证毕.

18. 交换群的单性:

设  $G$  是交换群, 则:  $G$  是单群  $\Leftrightarrow |G|$  为素数  $\Rightarrow G$  是循环群

## §4.6 群论思维导图

$H$ 是 $G$ 的子群，设 $[G:H] = r$

则 $G$ 是关于 $H$ 的左(右)陪集的并：

$G = H \cup a_1H \cup \dots \cup a_{r-1}H$ ,  $\{e, a_1, \dots, a_{r-1}\}$ 称  
为左陪集代表系

推论:  
 $|G| < 60$ , 则  $G$  为单群  
 $\Leftrightarrow |G|$  为素数.

Lagrange Theorem:  $|G| = |G/H| \cdot |H|$

单群  
正根子群  $H \trianglelefteq G$

$$\forall g \in G, gh = hg \Leftrightarrow H = ghg^{-1}$$

商群  $G/H$   
生成群

$H$  正根

商空间  $G/H = \{gH \mid g \in G\}$   
子群  $H \leq G$

$$\forall a, b \in H, ab^{-1} \in H \Leftrightarrow H \trianglelefteq G, H \neq G$$

子群  $H \trianglelefteq G$   
 $\forall g \in G, gH = Hg \Leftrightarrow g \in H$   
 $gH = H \Leftrightarrow g \in H$

Sylow- $p$  子群

Abel 群

Sylow 第一定理

Sylow 第二定理

Sylow 第三定理

群的阶

正根分子  $N_G(H)$

子群  $H \trianglelefteq G$

群的阶

商空间  $G/H = \{gH \mid g \in G\}$

群在集合上的作用

第二同构定理:

$\varphi: G \rightarrow G'$

群  $G$ : 封+结+单+逆

商空间  $G/H = \{gH \mid g \in G\}$

稳定化子  $C_{x_0}$

轨道  $O_x$

自然同态

同态映射  $\varphi: G \rightarrow G'$

群同构

同态像  $\text{Im}(\varphi)$

第三同构定理:

同态基本定理(第一同构定理):  
 $\varphi: G \rightarrow G'$ ,  $\text{Im}(\varphi) \cong \text{Im}(\varphi)$

内自动构群  $I_m(G)$

同构群  $\text{Aut}(G)$

## 9.4.5 环和域

即 ① 加法交换群 ② 乘法半群 ③ 分配律

环的相关概念：

1. 环的定义：环的本质是一个加法交换群。

环R是带有两个二元运算“加法+”和“乘法·”的非空集合，且

$(R, +)$ 构成一个交换群， $(R, \cdot)$ 构成一个半群，并且乘法与加法的分配律成立： $\begin{cases} (a+b) \cdot c = a \cdot c + b \cdot c & (\text{右分配}) \\ a \cdot (b+c) = a \cdot b + a \cdot c & (\text{左分配}) \end{cases}$

如果 $(R, \cdot)$ 是个么半群，我们称R为有单位元的环，其单位元记为 $1_R$ （或简记为1）。称 $(R, +)$ 为R的加法群， $(R, \cdot)$ 为R的乘法半群。如果 $(R, \cdot)$ 是交换的，则R称为交换环。

2. 子环：

若环R的子集L构成一个环，则称L是R的子环。这等价于 $(L, +)$ 是 $(R, +)$ 的子交换群且 $(L, \cdot)$ 是 $(R, \cdot)$ 的子半群。

3. 零因子：

若 $\exists a, b \in R$  且 $a, b \neq 0_R$  满足 $a \cdot b = 0_R$ ，则称a为左零因子，称b为右零因子。上面的“ $0_R$ ”指交换群 $(R, +)$ 中的单位元 $0_R$ 。如二阶矩阵环 $M_{2x2}(R)$ 中， $\begin{bmatrix} 1 & 1 \\ 2 & 2 \end{bmatrix} \begin{bmatrix} 3 & 4 \\ -3 & -4 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

4. 零元素：

环R的元素a称为零元素如果 $\exists n \in \mathbb{N}_+$ 使得 $a^n = 0_R$ 。

如四阶矩阵环 $M_{4x4}(R)$ 中，令 $M = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$ ，则 $M^4 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$

5. 整环：

一个环R称为整环如果只是有单位元 $1_R \neq 0_R$ 的交换环且R没有零因子。

6. 环同态：

设 $R, R'$ 是两个环，映射 $\varphi: R \rightarrow R'$ 称为环同态如果：

$$\forall a, b \in R, \varphi(a+b) = \varphi(a) +_2 \varphi(b), \varphi(a \cdot b) = \varphi(a) \cdot_2 \varphi(b)$$

例如映射 $\varphi: \mathbb{Z} \rightarrow \mathbb{Z}$ 是整数环到剩余类环 $\mathbb{Z}_n$ 的同态。

映射 $\varphi: a_i \mapsto \bar{a}_i$ 是 $\mathbb{Z}_{[n]}$ 到 $\mathbb{Z}_{[n]}$ 的环同态。

8. 理想 I：

设I是R的一个子环，且 $\forall i \in I, r \in R$ , 有 $ri \in I$ （等价于

理想在环中的地位 $rI = I$ ），则称I是一个左理想。（ $ir \in I$ 时为右理想）

类似正规子群在群中的地位并记为 $I \trianglelefteq R$ 。 $\Rightarrow \{0\}$ 和 $\{R\}$ 称为R的平凡理想

理想和正规子群的区别：若R无其它理想，称为单环。

$$\text{正规子群: } gH = Hg \Leftrightarrow gh^{-1} \in H \quad \text{理想: } rI, I_r \subseteq I \Leftrightarrow ri, ir \in I$$

9. 环的同态核  $\ker(\varphi)$ ：

设 $\varphi$ 是R到R'的环同态，定义环的同态核：

$$\ker(\varphi) = \{a \in R \mid \varphi(a) = 0_{R'}\} \quad \text{注意: } 0_{R'} \text{是环 } R' \text{ 的加法单位元, 与群同态核不同, 要注意区分。}$$

容易证明， $\ker(\varphi) \trianglelefteq R$

10. 环关于理想的商环：

类比群论中的商群， $R/I = \{r+I \mid r \in R\}$ ，定义 $R/I$ 上的乘法：

$$(a+I) \cdot (b+I) = ab + I, a, b \in R, \text{ 则 } R/I \text{ 构成一个环。}$$

称为R关于I的商环。

11. 自然环同态：

构造R到 $R/I$ 的映射 $\varphi: r \mapsto r+I$ ，则 $\varphi$ 构成一个环同态，

称为自然环同态。

12. 生成子环：

设 $S \subseteq R$ 且非空，记R的所有包含S的子环构成的集合为J，即 $J = \{L \leq R \mid S \subseteq L\}$ ，则 $\bigcap_{L \in J} L$ 是R的含有S的最小子环，称为R的由S生成的子环，记为 $\langle S \rangle$ ，即 $\langle S \rangle = \bigcap_{L \in J} L$ 。

13. 生成理想：

设 $S \subseteq R$ 且非空，记R的所有包含S的理想构成的集合为I，即 $I = \{I \trianglelefteq R \mid S \subseteq I\}$ ，则 $\bigcap_{I \in I} I$ 是R的含有S的最小理想，称为R关于S的生成理想，记为 $\langle S \rangle$ ，即 $\langle S \rangle = \bigcap_{I \in I} I$ 。

14. 主理想：

则称为主理想， $Rc = \{rc \mid r \in R\}$ ，若 $Rc$ 构成R的理想，设R是一个环，给定 $c \in R$ ，并定义集合 $Cr = \{cr \mid r \in R\}$ ，因为 $\forall r \in Cr, r' \in R$ ，有 $r'r \in Cr$

ChatGPT说：

- 环的主理想是由一个元素生成的理想，这个元素称为主元。主理想的所有元素都可以表示为主元与环中任意元素的乘积的形式。这个性质使得主理想在环的理论中非常最重要。
- 主理想在环的研究中有着广泛的应用，例如在模运算中，模 $\$n\$$ 的所有倍数生成一个主理想，称为模 $\$n\$$ 的主理想。主理想可以帮助我们更好地理解环的结构和性质。
- 对于一个环 $\$R\$$ 和一个元素 $\$a \in R\$$ ，我们可以定义一个主理想 $\$(a) = \{ra \mid r \in R\}$ ，它由 $\$a\$$ 生成。这个主理想包含了所有 $\$a\$$ 的倍数，并且是一个环的理想。如果 $\$R\$$ 是一个交换环，那么 $\$(a)\$$ 是一个主理想。

14. 环的“陪集”：

对带有 $1_R$ 的交换环R的任意乘法不可逆元b，集合 $Rb = \{ab \mid a \in R\}$ 构成R的一个理想，即 $Rb \trianglelefteq R$ ，且 $Rb \neq R$ 。

15. 环同构：

一个环同态称为环同构如果它是双射。例如，设环同态 $\varphi: R \rightarrow R'$ ，则映射 $\bar{\varphi}: a + \ker(\varphi) \mapsto \varphi(a)$ ,  $a \in R$ , 是从 $R/\ker(\varphi)$ 到 $I_{\varphi}(R)$ 的一个同构。

有关环的结论：

环同态基零同态

1. 理想 I 与 乘法单位元  $1_R$  : // 设 R 为环，则有：

$$1_R \in I \iff I = R \quad \text{环的本质是加法群, 一定有的单位元是 } 0_R.$$

2. 理想的和、交：

设  $I_1 \trianglelefteq R, I_2 \trianglelefteq R$ , 则  $(I_1 + I_2) \trianglelefteq R, (I_1 \cap I_2) \trianglelefteq R$ .

即理想的和仍是理想，理想的交仍是理想。

3. 设 R 是环, 则  $|R| = p$  为素数  $\Rightarrow R$  为加法循环群  $\Rightarrow R$  乘法交换。

4. 设  $R_1, R_2$  是环, 则  $R_1 + R_2$  也构成环。

注意这里是加法而非乘法，这是因为环的基本运算是加法（加法交换群+乘法半群+分配律）

即 $(a+b) \cdot c = a \cdot c + b \cdot c$ ， $a, b, c \in R$ 。

即 $a \cdot (b+c) = a \cdot b + a \cdot c$ ， $a, b, c \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot (b+c) = a \cdot b + a \cdot c$ ， $a, b, c \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

即 $a \cdot b = b \cdot a$ ， $a, b \in R$ 。

# 一些特殊的环：

## 1. 半群环 $R[G]$ ：

设  $G$  是一个有限半群，将  $G$  到  $\mathbb{R}$  的全体映射（函数）记为  $\mathbb{R}[G]$ ，

则  $(\mathbb{R}[G], +, \cdot)$  构成一个环，称为半群环。当  $G$  是群时，称

$\mathbb{R}[G]$  为群代数 (group algebra)。

## 2. $n$ 阶实数矩阵环 $M_{n \times n}(\mathbb{R})$ ：

$M_{n \times n}(\mathbb{R})$  关于矩阵加法和矩阵乘法构成一个幺环，称为矩阵环。

## 3. 剩余类环 $\mathbb{Z}_n$ ：

$\mathbb{Z}_n = \{0, 1, \dots, n-1\}$  构成一个幺环，称为剩余类环。

## 4. 多项式环 $R[x]$ ：

$R$  为环，对给定  $n \in \mathbb{N}$ ，定义  $R[x] = \{a_n x^n + \dots + a_1 x + a_0 \mid a_i \in R\}$ ，

则  $R[x]$  构成一个幺交换环，称为多项式环。

## 5. 整数环 $\mathbb{Z}$ ：

$\mathbb{Z} = \{0, 1, -1, 2, -2, \dots\}$  构成一个幺环，且有结论：

$\forall k \in \mathbb{Z}, k \mathbb{Z} \trianglelefteq \mathbb{Z}$ 。

# 域：

即：①  $R$  是环，②  $R^*$  构成乘法交换群。

## 1. 域的概念：

若一个交换环  $R$  中所有非  $0_R$  的元素关于乘法可逆，则称为一个域，记为  $F$ 。

例如， $\mathbb{Q}$  和  $\mathbb{R}$  是域，当  $p$  为素数时，剩余类环  $\mathbb{Z}_p$  是域，记

$\mathbb{Q}[F] = \{a + b\sqrt{-1} \mid a, b \in \mathbb{Q}\}$ ，则  $\mathbb{Q}[F]$  是域，记

$\hat{C} = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \mid a, b \in \mathbb{R} \right\}$ ，则  $\hat{C}$  是域

域一定是整环，但整环不一定是域。如  $\mathbb{Z}$  是整环但不是域。

## 2. 域的特征 $\text{char}(F)$ ：

设  $1_F$  为域  $F$  的乘法单位元，则映射  $\psi: n \mapsto n \cdot 1_F, n \in \mathbb{Z}$  是从  $\mathbb{Z}$  到  $F$  的同态，若  $\ker(\psi) = \{0\}$ ，我们称域  $F$  的

特征为 0。此时， $\forall 0 \neq n \in \mathbb{Z}, 0_F \neq a \in F$ ，我们有：

$$n \cdot 1_F \neq 0 \Rightarrow na = n \cdot 1_F \cdot a \neq 0$$

当  $\ker(\psi) \neq \{0\}$  时，它是  $\mathbb{Z}$  的非零理想，且由素数  $p \in \mathbb{Z}$  使得  $\ker(\psi) = p\mathbb{Z}$ ，这表明  $\mathbb{Z}$  的理想都是素理想，故  $\mathbb{Z}/\ker(\psi) \cong \psi(\mathbb{Z})$ 。

这时，我们称  $F$  的特征为  $p$ ，记为  $\text{char}(F) = p$ ，或  $\text{char } F = p$ 。

$\text{char } F$  说：

定义：域的特征是一个非负整数，它描述了在该域内进行加法操作时元素的周期性。更准确地说，域  $F$  的特征是最小的正整数  $n$ （如果存在的话），使得对于域中的每个元素  $a$ ，我们有  $n$  个  $a$  的和等于加法单位元（即零元素）：

$$\underbrace{a + a + \dots + a}_{[n \text{ text}(\{ \})]} = 0$$

如果这样的  $n$  不存在，那么我们说域的特征是 0。这意味着无论你把元素自身加多少次，都不可能得到 0（除非元素本身就是 0）。

理解域的特征：要理解域的特征，你可以将其视为一种度量，它告诉我们在域内进行加法操作时元素如何重复。如果一个域的特征是 0，那么它在某种意义上与我们熟悉的有理数、实数或复数域相似。这些域的元素可以无限地相加而不会循环回到起点。如果一个域的特征是一个正整数  $n$ ，那么它与我们熟悉的整数运算不同，因为在这样的域中，加法变得有界限，循环发生在  $n$  的倍数上。

举例：

1. 特征为 0 的域：有理数域  $(\mathbb{Q})$ 、实数域  $(\mathbb{R})$  和复数域  $(\mathbb{C})$  的特征都是 0。在这些域中，任何非零元素的有限加法都不会产生 0。

2. 特征为正整数的域：考虑有限域  $\mathbb{F}_{p^n}$ ，其中  $p$  是一个素数。这个域由模  $p$  算术构成，也就是说，它包含了从 0 到  $p-1$  的整数，并且所有的加法和乘法都是模  $p$  的。在  $\mathbb{F}_{p^n}$  中...

$\underbrace{1 + 1 + \dots + 1}_{[p \text{ text}(\{ \})]} \equiv 0 \pmod{p}$

这意味着当你把 1 加到自己  $p$  次时，你会回到 0。

有关域的结论：

1.  $\mathbb{Z}_n$  构成一个域  $\Leftrightarrow n$  为素数

2. 对任意有限域  $F$ ， $F^* = F \setminus \{0_F\}$  构成乘法循环群

3. 设  $F$  是域， $C$  是  $F^*$  的有限乘法子群，则  $C$  构成循环群

证明：设  $|C| = n$ ， $C$  中最大元素的阶是  $m$ ，由于  $C$  是交换的， $\forall a \in C$ ，  
 $a^m = e \Rightarrow a$  是  $x^m - e = 0$  的根，根的个数  $= n \leq m$ ， $\exists m \leq n$ 。  
因此  $n = m$ . 证毕。

4. 有限整环构成一个域

5. 有限无零因子环是除环  $(R^* = R \setminus \{0_F\}$  中元素都可逆)

证明： $\forall r \in R$ , 考虑  $a^1, a^2, \dots, R$  有限  $\Rightarrow \exists m, n \in \mathbb{N}_+$ ，  
使  $a^m = a^n \Rightarrow a^n(a^{m-n}-1) = 0$ ， $\because R$  无零因子， $\therefore a^n \neq 0$   
 $\Rightarrow a^{m-n} - 1 = 0 \Rightarrow a^{m-n} = 1$ ，因此  $a$  可逆，由  $a$  任意性。  
 $R^*$  中元素都可逆。  
R 存在性如何？

6. 有限无零因子环构成域（证明交换性无初等方法）

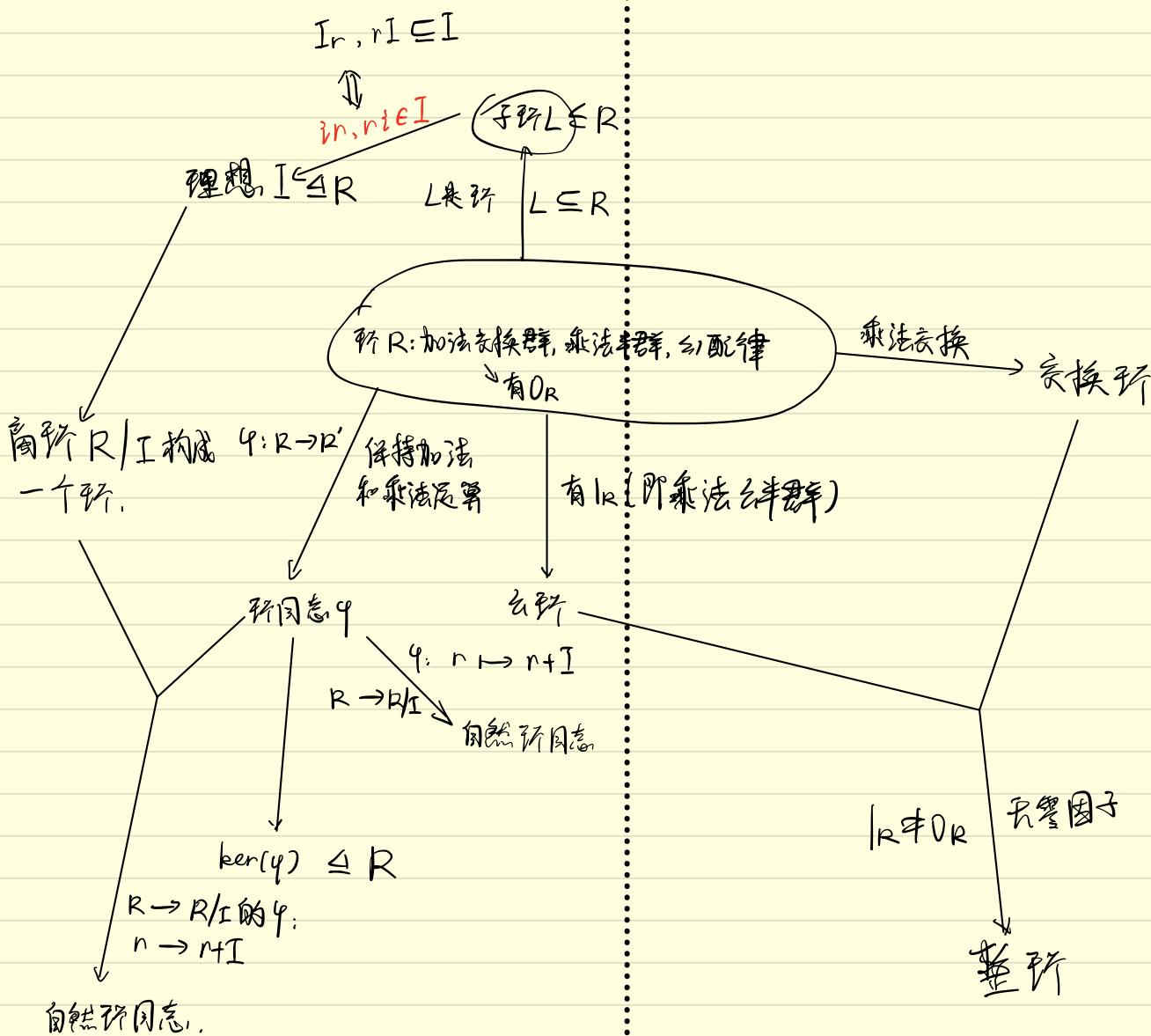
7. Wedderburn Theorem：有限除环构成域

8. 设  $f, g \in F[x]$ , 且  $f, g$  首一，则  $f(x)g(x) = g.c.d(f, g) \cdot l.c.m(f, g)$

9. 有限域的特征是素数  $p$

## §4.6 环思维导图

## §4.7 域思维导图



## §4.8 群环域中一些辨析/深入

群模子群  $G/H = \{gH \mid g \in G\}$

### 1. 封闭性?

设  $G$  为群,  $H \leq G$ , 此时定义  $G$  关于  $H$  的全体左陪集为  $G/H = \{gH \mid g \in G\}$ . 一般来说, 集合  $G/H$  中的元素对乘法不一定封闭, 即  $aH, bH \in G/H$  时,  $(aH) \cdot (bH)$  不一定仍为左陪集 ( $\nexists H' \in G/H$  使得  $aH \cdot bH = H'$ ).

### 2. 但是, 当 $H \trianglelefteq G$ 时:

由于  $\forall g \in G$ , 有  $gH = Hg$ , 因此  $aH \cdot bH = aHHb = aHb = abH \in G/H$ , 且容易验证,  $G/H$  关于集合乘法构成一个群, 称为  $G$  模  $H$  的商群 (quotient group), 其单位元是  $eH = H$ ,  $(aH)^{-1} = a^{-1}H$ .

### 3. 另外, 当 $H \trianglelefteq G$ 时:

由于  $gH = Hg$ , 因此  $G/H = \{Hg \mid g \in G\}$ , 也即全体左陪集构成的集合等价于全体右陪集构成的集合.

类似的有子环、理想的传递性、交、积, 见后文子群/正规子群的传递性、交、积:

### 1. 子群:

① 可传递性 ( $\vee$ ):  $K \trianglelefteq H, H \trianglelefteq G \Rightarrow K \trianglelefteq G$

② 对“ $\cap$ ”封闭 ( $\vee$ ):  $K \trianglelefteq G, H \trianglelefteq G \Rightarrow K \cap H \trianglelefteq G$

③ 对乘法封闭 ( $\times$ ):  $K \trianglelefteq G, H \trianglelefteq G \Rightarrow KH \trianglelefteq G$

### 2. 正规子群:

① 可传递性 ( $\times$ ):  $K \trianglelefteq H, H \trianglelefteq G \Rightarrow K \trianglelefteq G$ .

② 对“ $\cap$ ”封闭 ( $\vee$ ):  $K \trianglelefteq G, H \trianglelefteq G \Rightarrow K \cap H \trianglelefteq G$

③ 对乘法封闭 ( $\vee$ ):  $K \trianglelefteq G, H \trianglelefteq G \Rightarrow KH \trianglelefteq G \Leftrightarrow KH = HK$

## 群、环、域同态:

### 1. 群同态:

① 定义: 设  $\varphi: G \rightarrow G'$  是一个群同态, 则  $\forall g_1, g_2 \in G$ , 有  $\varphi(a \cdot b) = \varphi(a) \varphi(b)$

② 性质:  $\varphi(1_G) = 1_{G'}$ ;  $\varphi(g) \in G'$ ;  $\ker \varphi \trianglelefteq G$ ;

$\varphi$  是单射  $\Leftrightarrow \ker \varphi = \{e\}$ ;

第一同构:  $G/\ker(\varphi) \cong \varphi(G) = \text{Im}(\varphi)$

第二同构:

使用 Sylow 时的验证  $\text{g.c.d}(m, p) = 1$

利用 Sylow Theorem 证明某个群不是单群

### 1. 体型 I:

利用 Sylow、Lagrange 比较元素个数即可证明.

证明 56 阶群非单:

$56 = 2^3 \cdot 7$ , 由 Sylow III,  $G$  含有 8 阶 Sylow-2 子群, 个数  $k \in \{1, 7\}$ , 含有 7 阶 Sylow-7 子群, 个数  $k' \in \{1, 8\}$ ,  $k=1$  ( $k'=1$ ) 时, Sylow-2 (Sylow-7) 正规,  $G$  非单, 下面考虑,

$(k-1)(k'-1) \neq 0$ . 记 8 阶子群为  $H_1, \dots, H_7$ , 7 阶子群为  $K_1, \dots, K_8$ ,

子群的交仍为子群, 注意到  $\text{g.c.d}(8, 7) = 1$ , 由 Lagrange,  $\forall i, j$ ,

有  $H_i \cap K_j = \{e\}$  (阶只能为 1)  $\Rightarrow (\bigcup_{i=1}^7 H_i) \cap (\bigcup_{j=1}^8 K_j) = \{e\}$ .

再考察  $|\bigcup_{i=1}^7 H_i|$  和  $|\bigcup_{j=1}^8 K_j|$ , 对于前者, 考虑  $H_1$  与  $H_2$ , 由 Lagrange  $|H_1 \cup H_2| = 8 + 8 - |H_1 \cap H_2| \geq 16 - 4 = 12 \Rightarrow |\bigcup_{i=1}^7 H_i| \geq |H_1 \cup H_2| = 12$ , 对后者, 因为 7 是素数, 所以由 Lagrange,  $K_i$  与  $K_j$  要么相同要么为  $\{e\}$  (构成底子群, 只能是 7 或 1), 故  $K_i \cap K_j = \{e\}, i \neq j \Rightarrow |\bigcup_{j=1}^8 K_j| = 6 \times 8 + 1 = 49$ , 故  $|G| \geq |\bigcup_{i=1}^7 H_i| + |\bigcup_{j=1}^8 K_j| - 1 = 49 + |\bigcup_{i=1}^7 H_i| - 1 \geq 49 + 12 - 1 = 60 > 56$ , 矛盾!

故  $(k-1)(k'-1) = 0$ ,  $G$  非单, 证毕.

类似的例子还有: 证明 72 阶群非单

2. 体型 II:

在 Sylow II 的基础上, 得到了群构成的集合  $X$ , 并构造  $G$  到  $S_X$  的同态  $\psi$ , 由同态基本定理 + Lagrange, 利用 Sylow II 的共轭导出矛盾.

证明: 72 阶群非单

$72 = 3^2 \times 2^3 = 9 \times 2^3 = 8 \times 3^2$ , 由 Sylow I,  $G$  的 8 阶 Sylow-2 子群个数  $k_2 \in \{1, 3, 9\}$ , 9 阶 Sylow-3 子群个数  $k_3 \in \{1, 4\}$ . 考虑  $(k_2-1)(k_3-1) \neq 0$  的情况: 则  $k_3 = 4$ ,  $k_2 = 3$  或 9.  $k_3 = 9$  时, 由体型 I 的思路, 下限为  $60 < 72$ , 无法得到矛盾,  $k_3 = 3$  时也不行, 因此考虑群作用: 由  $k_3 = 4$ , 记这四个群构成  $X = \{P_1, P_2, P_3, P_4\}$ ,  $S_X$  是作用在  $X$  上的全体排列 (想想  $S_n$  作用在  $\{1, \dots, n\}$  上). 构造  $G$  到  $S_X$  的映射  $\psi: g \mapsto \psi_g$ ,  $\psi_g$  定义为  $\psi_g(P_i) = gP_i g^{-1}$ , 则  $\psi$  构成一个群同态, 由同态基本定理,  $\ker(\psi) \trianglelefteq G$ ,  $\psi(G) \subseteq G'$ , 且  $G/\ker(\psi) \cong \psi(G)$ . 故  $[G : \ker(\psi)] = |\psi(G)| \mid |S_X| = |S_4| = 24 \Rightarrow \frac{72}{|\ker(\psi)|} \mid 24 \Rightarrow 3 \leq |\ker(\psi)| \leq 72$ , 又由 Sylow II,  $\exists g \in G, g \neq e$  使  $P_1 = gP_2g^{-1}$ , 因此  $g \notin \ker(\psi) \Rightarrow |\ker(\psi)| < 72$ , 也即  $3 \leq |\ker(\psi)| \leq 71 < |G| = 72$ , 故  $\ker(\psi)$  是  $G$  的非平凡正规子群,  $G$  非单. 证毕.

类似的例子还有: 证明 48 阶群非单.

$48 = 16 \cdot 3^1 = 3 \cdot 2^4 \Rightarrow 3$  阶 Sylow-3 子群  $k_3 \in \{1, 4, 16\}$ , 16 阶 Sylow-2 子群  $k_{16} \in \{1, 3\}$ , 只需考虑  $k_{16}$  而无需在意  $k_3$ . 当  $k_{16} = 3$  时: 记三个子群构成集合  $X = \{P_1, P_2, P_3\}$ , 构造  $G$  到  $S_X$  的映射  $\psi: g \mapsto \psi_g$ , 则  $\psi$  构成同态, 有  $G/\ker(\psi) \cong \psi(G) \Rightarrow \frac{|G|}{|\ker(\psi)|} = |\psi(G)| \mid |S_X| = 3! = 6 \Rightarrow 8 \leq |\ker(\psi)| \leq 48$ , 又  $\exists g \in G, g \neq e$  使  $P_1 = gP_2g^{-1}$ , 因此  $g \notin \ker(\psi) \Rightarrow |\ker(\psi)| < |G|$ , 故  $\ker(\psi)$  是  $G$  的非平凡正规子群,  $G$  非单. 当  $k_{16} = 1$  时, 此 Sylow-2 子群正规,  $G$  非单. 证毕.

## 群、环、域同态:

### 1. 同态的本质:

同态是指一个代数结构到另一个同型代数结构, 并保持其运算的一种映射.

2. 群环域同态:  $\psi: R \xrightarrow{\sim} R'$   $\downarrow$   $\psi(0_R) \neq 0_{R'}$   $\downarrow$   $\psi(1_R) \neq 1_{R'}$   $\downarrow$   $\psi(0_R) \neq 0_{R'} \Rightarrow \psi(1_R) \neq 1_{R'}$

① 群:  $\psi: G \rightarrow G'$ , 且  $\psi(g_1 \cdot g_2) = \psi(g_1) \psi(g_2)$ , 必有  $\psi(e) = e'$ .

② 环:  $\psi: R \rightarrow R'$ , 且  $\psi(g_1 \cdot g_2) = \psi(g_1) \psi(g_2)$ ,  $\psi(g_1 + g_2) = \psi(g_1) + \psi(g_2)$ ,

必有  $\psi(0_R) = 0_{R'}$ , 不一定有  $\psi(1_R) = 1_{R'}$   $\downarrow$   $\psi(0_R) \neq 0_{R'} \Rightarrow \psi(1_R) \neq 1_{R'}$

③ 域:  $\psi: F \rightarrow F'$ , 且  $\psi(g_1 \cdot g_2) = \psi(g_1) \psi(g_2)$ ,  $\psi(g_1 + g_2) = \psi(g_1) + \psi(g_2)$ ,

必有  $\psi(0_F) = 0_{F'}$ , 必有  $\psi(1_F) = 1_{F'}$

可以注意到: 对于一个(乘法或加法)单位元  $e$ , 判断是否  $\psi(e) = e'$

(注意 $\varphi(x)$ 的单位元可能不等于 $e'$ )  
判断 $\varphi(x)$ 是否一定含 $e'$ . 例如对于环同态 $\varphi$ , 定义 $\forall r \in R$ ,

$\varphi(r) = 0_{R'}$ , 显然 $\varphi$ 是同态, 但 $I_R \notin \varphi(I) = \{0_{R'}\}$ , 因此 $\varphi(I_R) \neq I_{R'}$  (无论 $R'$ 是否含 $0$ ). 此时 $\varphi(I)$ 是具有乘法、加法单位元的都是 $0_{R'}$ .

### 3. 三大同构定理:

同构定理不仅可以用子描述群, 也能用于描述环(域较少见), 这也是为什么我们引入了“理想”(为了建立与正规子群类似的概念).

设 $\varphi: G \rightarrow G'$ 为同态, 则三大同构定理:

I:  $\ker(\varphi) \trianglelefteq G$ ,  $\varphi(G) \trianglelefteq G'$  且  $G/\ker(\varphi) \cong \varphi(G)$

II: 若  $H \trianglelefteq G$ ,  $K \trianglelefteq G$ , 则  $H \cap K \trianglelefteq H$ ,  $K \trianglelefteq HK$  且

$$(H/(H \cap K)) \cong HK/K \quad \text{这是因为群的基本运算是乘法, 而环的基本运算是加法.}$$

对称:  $H/(H \cap K) \cong (H+K)/K$

III: 若集合 $H$ 满足  $\ker(\varphi) \leq H \trianglelefteq G$ , 则:

$$C/H \cong \varphi(G)/\varphi(H) \quad \text{令 } H = \ker(\varphi) \text{ 即得 I}$$

另一形式为: 若  $N \trianglelefteq C$ ,  $H \trianglelefteq C$  且  $N \leq H$ , 则:  $\varphi(N) = gN$  得

$$C/H \cong (C/N)/(H/N) = \frac{C/N}{H/N} \quad \text{写为 } N \subseteq H \text{ 也可}$$

在群中, “ $\leq$ ”“ $\trianglelefteq$ ”表示子群、正规子群; 在环中, “ $\leq$ ”“ $\trianglelefteq$ ”表示子环、理想.

## 子环、理想的传递性、交、积:

### 1. 子环:

① 可传递性 ( $\vee$ ):  $J \trianglelefteq I$ ,  $I \trianglelefteq R \Rightarrow J \trianglelefteq R$

② 对“ $\cap$ ”封闭 ( $\vee$ ):  $J \trianglelefteq R$ ,  $I \trianglelefteq R \Rightarrow J \cap I \trianglelefteq R$

③ 对加法封闭 ( $\vee$ ):  $J \trianglelefteq R$ ,  $I \trianglelefteq R \Rightarrow (I+J) \trianglelefteq R$

④ 对乘法封闭 ( $\times$ ): 环乘法的定义不同于群乘法, 该 $R_1, R_2$ 是两个环,

定义  $R_1 R_2 = \left\{ \sum_{i=1}^n a_i b_i \mid a_i \in R_1, b_i \in R_2, i=1, 2, \dots, n \right\}$ , 特别地,

当  $R_1 = \{a\}$  时, 记  $R_1 R_2 = aR_2 = \{ar \mid r \in R_2\}$ . 与群类似, 不具

有传递性:  $J \trianglelefteq R$ ,  $I \trianglelefteq R \not\Rightarrow IJ \trianglelefteq R$ .

例如令  $S = \{0, 1, 2\}$ ,  $T = \{3, 4\}$ , 则  $ST = \{0, 3, 4, 6, 7, 8, 9, \dots\}$

这个定义的意思是,  $S$  中取一些元素(不限数目, 可以重复),  $T$  中取同样多的元素(不限数目, 可以重复), 把他们相乘再相加.

比如说,  $S$  中, 可以取  $1, 1, 1, 2, 2$ ,  $T$  中可以取  $3, 3, 4, 4, 4$ , 这样相乘再相加, 就可以得到  $1*3 + 1*3 + 1*4 + 2*4 + 2*4 = 26$

2. 理想:

① 可传递性 ( $\times$ ):  $J \trianglelefteq I$ ,  $I \trianglelefteq R \not\Rightarrow J \trianglelefteq R$

② 对“ $\cap$ ”封闭 ( $\vee$ ):  $J \trianglelefteq R$ ,  $I \trianglelefteq R \Rightarrow J \cap I \trianglelefteq R$

③ 对加法封闭 ( $\vee$ ):  $J \trianglelefteq R$ ,  $I \trianglelefteq R \Rightarrow (I+J) \trianglelefteq R$

④ 对乘法封闭 ( $\times$ ):  $J \trianglelefteq R$ ,  $I \trianglelefteq R \Rightarrow IJ \trianglelefteq R$

## 主理想的概念与表示:

### 1. 基本定义:

在 §4.5 中, 我们给出了生成理想的概念, 若  $S$  有且仅有一个元素  $a \in R$ , 即得到主理想, 如下: 设  $a \in R$ , 考虑全体包含  $a$  的理想构成的集合, 即定义:

$\langle a \rangle = \{I \mid I \trianglelefteq R, a \in I\}$ , 并考虑  $\langle a \rangle$  中所有元素的交, 定义  $\langle a \rangle = \bigcap_{I \in \langle a \rangle} I$ , 由于

理想的交仍是理想, 因此  $\langle a \rangle \trianglelefteq R$ , 称为由  $a$  生成的主理想, 且它是含  $a$  的最小理想(阶最低).

## 2. 多种形式:

① R 为环:  $\langle a \rangle = \left\{ \sum_{i=1}^n x_i a y_i + x a + a y + m a \mid x_i, y_i, x, y \in R, m \in \mathbb{Z} \right\}$

② R 含幺:  $\langle a \rangle = \left\{ \sum_{i=1}^n x_i a y_i \mid x_i, y_i \in R \right\}$

③ R 交换:  $\langle a \rangle = \{xa + ma \mid x \in R, m \in \mathbb{Z}\}$

④ R 含幺且交换:  $\langle a \rangle = ar = \{ar \mid r \in R\}$

## 从环过渡到域

### 1. 定义过渡

设  $R$  是一个环, 若  $R^*$  构成乘法交换群, 则  $R$  构成域. (有限时成立, 无限时不成立)

### 2. 有限无零因子环构成域 (证明交换时无初等方法)

### 3. 有限无零因子交换环构成域

① 证明  $R$  满足消去律:  $\forall r, r_1, r_2 \in R$ , 若  $rr_1 = rr_2$ , 则

$r(r_1 - r_2) = 0_R$ , 又  $R$  无零因子, 因此  $r_1 - r_2 = 0_R \Rightarrow r_1 = r_2$ , 右边得证.

② 证明  $R$  含  $I_R$ : 由于  $R$  有限, 因此可设  $R = \{r_1, r_2, \dots, r_n\}$ , 其中  $n = |R|$ .

考虑集合  $nR = \{r_1 r_1, r_1 r_2, \dots, r_1 r_n\}$ , 其中  $r_1 \neq 0_R$ , 由消去律,  $r_1 r_2 = r_1 r_j$

$\Rightarrow r_2 = r_j$ , 因此  $r_1 r_1, r_1 r_2, \dots, r_1 r_n$  为  $n$  个不同的元素  $\Rightarrow nR = R$ .

则  $\forall r_1, r_2 \in R, \exists r \in S_n$  使  $r_1 r_2 = r r(r)$ , 于是  $r_1^{-1} r_2 = r^{-1} r(r) = r_2$ .

同理可得  $r_1^{-1} r_1 = r_1$ , 因此  $r_1^{-1}$  为乘法单位元. 故  $r_1^{-1} r_1 = I_R$ ,  $R$  含幺.

③ 证明  $R^*$  构成乘法交换群: 只需说明可逆.  $\forall r \in R^*$ , 考虑元素  $r, r^2, r^3, \dots$ , 由于

$R^*$  有限,  $\exists m, n \in \mathbb{N}_{+(m < n)}$  使得  $r^m = r^n \Rightarrow r^m \cdot (r^{n-m} - I_R) = 0_R$ , 由于  $R$  无零

因子, 因此  $r^{n-m} = I_R \Rightarrow (r)^{-1} = r^{n-m-1}$ , 由上的任意性,  $R^*$  中元素可逆. 证毕.

### 4. 有限整环(无零因子、交换、幺)构成一个域

照搬上面证明中的③即可.

## P<sup>1</sup>群与P群/PQ群与P<sup>2</sup>群的性质

### 1. P<sup>2</sup>群:

#### ① 是 Abel 群

证明: 设  $|G| = p^2$ , 若  $G$  有  $p^2$  阶元, 则构成循环群, 自然交换; 若  $G$  不含  $p^2$

阶元, 较麻烦, 此外略. (这是群的直积, 构成群, 其运算定义)

② P<sup>2</sup>群  $\cong \mathbb{Z}_{p^2}$  或  $(\mathbb{Z}_p \times \mathbb{Z}_p)$

证明方法一(讲义中的方法): 设  $|G| = p^2$ , 由 Lagrange,  $\forall g \in G, |g| \in \{1, p, p^2\}$

(1) 若  $G$  含有  $p^2$  阶元  $a$ , 则  $\langle a \rangle = \{a^0, a^1, \dots, a^{p^2-1}\} \cong \mathbb{Z}_{p^2}$

(2) 若  $G$  不含  $p^2$  阶元, 则  $\forall e \neq a \in G, |a| = p$ , 取  $e \neq b \in \langle a \rangle, c \in G \setminus \langle b \rangle$ ,

则  $\langle b \rangle \cong \mathbb{Z}_p$ ,  $\langle c \rangle \cong \mathbb{Z}_p$ , 且  $bc = cb \Rightarrow b^i c^j = c^j b^i$ . 假设

$\exists 0 < i < p, 0 < j < p$  使  $b^i c^j = 1 \Leftrightarrow c^j = b^{-i} \in \langle b \rangle \cap \langle c \rangle$ , 而

$|\langle b \rangle| = |\langle c \rangle| = p$  为素数, 由 Lagrange,  $\langle b \rangle \cap \langle c \rangle = \{e\}$ , 因此

$b^{-i} c^j = 1 \Leftrightarrow c^j = b^i \in \langle b \rangle \cap \langle c \rangle = \{e\} \Leftrightarrow b^i = c^j = e$

于是  $b^i c^j = b^{i_2} c^{j_2} \Leftrightarrow b^{i_1-i_2} c^{j_1-j_2} = e \Leftrightarrow b^{i_1-i_2} = c^{j_1-j_2} = e$

$\Leftrightarrow b^{i_1} = b^{i_2}, c^{j_1} = c^{j_2}$ , 因此  $|\langle b, c \rangle| = p^2 = |G|$ , 且  $\langle b, c \rangle \subseteq G$ ,

可得  $G = \langle b, c \rangle = \{b^i c^j \mid i, j \in \mathbb{Z}\}$ . 因为  $b^i c^j = c^j b^i$ , 所以映射

$c: b^i c^j \mapsto (\bar{i}, \bar{j})$  是  $G$  到  $\mathbb{Z}_p \times \mathbb{Z}_p$  的同构.

证明方法二(利用性质①):

设  $|G| = p^2$ , 则  $G$  为交换群, 若  $G$  含  $p^2$  阶元, 同上, 若  $G$  不含  $p^2$  阶元, 考虑非单位元

$a, b$  且  $a \neq b$ , 令  $H = \langle a \rangle, K = \langle b \rangle$ , 由 Lagrange,  $|H| = \frac{|G|}{|H \cap K|} = \frac{|G|}{|H||K|} = p^2$

$$\Rightarrow G = HK = \{hk \mid h \in \langle a \rangle, k \in \langle b \rangle\} = \{a^i b^j \mid i, j \in \mathbb{Z}\} \cong \mathbb{Z}_p \times \mathbb{Z}_p.$$

因为  $b^i c^j = c^j b^i$ , 所以映射  $\varphi: b^i c^j \mapsto (\bar{i}, \bar{j})$  是  $G$  到  $\mathbb{Z}_p \times \mathbb{Z}_p$  的同构

## 2. $p^r$ 群 ( $|G| = p^r$ )

待定.

## 3. $pq$ 群 ( $p \neq q$ ):

$$\begin{matrix} p/(q-1) & p/(q-1) \\ \downarrow & \uparrow \\ n_p \in \{1, q\} & n_q \in \{1\} \end{matrix}$$

不妨令  $p < q$ ,  $|G| = q \cdot p^r = p \cdot q^r$ ,  $G$  总存在唯一的 Sylow- $q$  子群,  $G$  非单.

① 非单群. 存在唯一 Sylow- $q$  子群  $Q \trianglelefteq G$

②  $G = PQ = \{a^i b^j \mid 0 \leq i \leq p-1, 0 \leq j \leq q-1\}$ , 其中  $P = \{a^0, \dots, a^{p-1}\}$

为一个唯一的 Sylow- $p$  子群,  $Q = \{b^0, \dots, b^{q-1}\}$  为唯一的 Sylow- $q$  子群.

设  $a^i b^j = a^k b^l$ , 则  $a^{i-k} = b^{l-j} \in Q \cap P = \{e\} \Rightarrow \begin{cases} i=k \\ j=l \end{cases}$ , 故  $G = PQ$ .

更一般的结论是“若  $H \leq G$ ,  $K \leq G$  且  $H \cap K = \{e\}$ , 则  $G = HK = KH$ ”

③ 若  $p > q$ , 若  $q \nmid (p-1)$ , 则  $G \cong \mathbb{Z}_{pq}$

证明见讲义 P105.

## 4. $p^2q$ 群:

① 非单群: 存在唯一 Sylow- $q$  子群  $Q \trianglelefteq G$

# 第五章. 多项式

## §5.1 单变量多项式

单变量多项式的相关概念

### 1. R 上的全体映射 $F(R)$ :

设  $R$  是一个环, 记  $F(R)$  为  $R$  到  $R$  的全体映射(函数), 定义  $F(R)$  上的加法和乘法:  $(f+g)(a) = f(a)+g(a)$ ,  $(f \cdot g)(a) = f(a) \cdot g(a)$ ,  $f, g \in F(R)$ , 则  $F(R)$  构成一个带  $\text{I}_R$  的环.

### 2. 单变量多项式环 $R_{[x]}$ :

最高次项系数为首项 (leading term)

定义由  $R$  到  $R$  的映射  $f: x \mapsto a_n x^n + \dots + a_1 x^1 + a_0$ , 其中

$a_0, \dots, a_n \in R$ , 若  $a_n \neq 0_R$ , 则称为  $n$  次多项式, 记其次数为

$\deg f = n$ , 且定义  $\deg 0 = -\infty$ , 这里的 0 指零映射:  $x \mapsto 0$ .

当  $|R| < \infty$  时,  $f(x) = 0 \iff a_0 = \dots = a_n = 0_R$ . 我们将  $R$  上

的全体多项式函数记为  $R_{[x]}$ , 则  $R_{[x]}$  构成  $F(R)$  的带有  $\text{I}_R$  的子环,

称为  $R$  上的单变量多项式环.

推论: 若  $R$  是一个整环, 则  $R_{[x]}$  是一个整环.

### 3. 定理: 多项式带余除法

对  $f(x), g(x) \in F_{[x]}$  且  $g(x) \neq 0$ ,  $\exists! p_{(n)}, q_{(n)} \in F_{[x]}$  使得  $f(x) = p_{(n)}g(x) + q_{(n)}$ ,

其中  $\deg(q) < \deg(g)$ .

### 4. 定理: $F_{[x]}$ 的理想.

设  $I$  是  $F_{[x]}$  的一个理想, 即  $I \trianglelefteq F_{[x]}$ , 则  $\exists g \in F_{[x]}$  使得  $I = (g)F_{[x]}$

$= \{g(x)f(x) \mid f(x) \in F_{[x]}\}$ , 也即  $F_{[x]}$  的理想都是主理想, 即  $F_{[x]}$  是主理想环

且也是主理想环

## 整除与公因式:

### 1. 整除:

设  $f(x), g(x) \in F_{[x]}$ , 若  $\exists q(x) \in F_{[x]}$  使  $f(x) = g(x)q(x)$ , 则称  $g(x)$  整除  $f(x)$ , 记

为  $g(x) \mid f(x)$

### 2. 首一多项式 (monic polynomial) 与 $M_{F_{[x]}}$ :

一个非零多项式称为 monic polynomial 如果它的首项系数是 1. 记  $M_{F_{[x]}}$  为  $F_{[x]}$

中的全体 monic polynomial, 则  $M_{F_{[x]}}$  关于乘法构成  $F_{[x]}$  的子群. 定义  $M_{F_{[x]}}$

上的二元关系  $g_{(n)} \prec f_{(n)}$  如果  $g_{(n)} \mid f_{(n)}$ , 则  $\prec$  是一个偏序关系.

### 3. 公因式:

$h(x)$  称为  $f(x)$  和  $g(x)$  的公因式如果  $\begin{cases} h(x) \mid f(x) \\ h(x) \mid g(x) \end{cases}$ ,  $d(x)$  称为  $f(x), g(x)$  的最大公因

式如果  $\forall h(x)$  满足  $\begin{cases} h(x) \mid f(x) \\ h(x) \mid g(x) \end{cases}$ , 都有  $h(x) \mid d(x)$ .

### 4. 定理: 最大公因式

设  $f, g \in F_{[x]}$ , 则存在  $f(x)$  和  $g(x)$  的最大公因式  $d(x)$ ,  $\exists s, t \in F_{[x]}$  使得:

$$d(x) = s(x)f(x) + t(x)g(x)$$

### 5. 辗转相除法求 $g.c.d(f(x), g(x))$ :

我们记首项系数为 1 的最大公因式为  $g.c.d(f(x), g(x))$ , 且有辗转相除法:

令  $r_0(x) = f(x)$ ,  $r_1(x) = g(x)$  与归纳带余除法  $r_i(x) = q_{i+1}(x)r_{i+1}(x) + r_{i+2}(x)$ , 其中  $i \geq 0$

且  $\deg r_{i+1} > \deg r_{i+2}$ , 则  $\exists$  最小的整数  $n$  使得  $r_{n+2}(x) = 0$ , 且  $r_{n+1}(x) = g.c.d(f, g)$ .

先回顾整数的辗转相除: 求  $g.c.d(m, n) = s \cdot m + t \cdot n$ , 令  $\begin{cases} m=54 \\ n=20 \end{cases}$

辗转相除法: 求  $g.c.d(m, n)$  和  $s, t$

$$i=0, r_0 = q_1 r_1 + r_2 \quad ①$$

$$54 = 2 \times 20 + 14$$

$$i=1, r_1 = q_2 r_2 + r_3 \quad ②$$

$$20 = 1 \times 14 + 6$$

$$i=2, r_2 = q_3 r_3 + r_4 \quad ③$$

$$14 = 2 \times 6 + 2$$

$$i=3, r_3 = q_4 r_4 + r_5 \quad ④$$

$$6 = 3 \times 2 + 0$$

$\Rightarrow g.c.d(54, 20) = r_4 = 2$ , 再求  $s, t$ , 有:

由 ② 得系数为 1 的  $r_4$ :  $r_4 = r_2 - q_3 r_3$ , ① 改写为  $r_3 = r_1 - q_2 r_2$ ,

代入消去  $r_3$ , 得:  $r_4 = 3r_2 - 2r_1$ , ② 改写为  $r_2 = r_0 - q_1 r_1$ , 代

入消去  $r_2$ , 得:  $r_4 = 3r_0 - 8r_1 \Rightarrow s=3, t=-8$

再回到多项式的辗转相除:

$$\text{令 } f(x) = x^4 + 3x^3 - x^2 - 4x - 3, g(x) = 3x^3 + 10x^2 + 2x - 3.$$

$$i=0, r_0(x) = q_1(x)r_1(x) + r_2(x) \quad ①$$

$$q_1(x) = \frac{x}{3} - \frac{1}{9}, r_2(x) = -\frac{5}{9}x^2 - \frac{25}{9}x - \frac{10}{3}$$

$$i=1, r_1 = q_2 r_2 + r_3 \quad ②$$

$$q_2(x) = -\frac{27}{5}x + 9, r_3(x) = 9x + 27$$

$$i=2, r_2 = q_3 r_3 + r_4 \quad ③$$

$$q_3 = -\frac{5}{81}x - \frac{10}{27}, r_4 = 0$$

注意要将  $r_3(x)$  的首项系数转为 1, 才得  $g.c.d(f(x), g(x)) = x+3$ ,

再求  $s(x), t(x)$ :

将  $r_3$  系数变换后, ① 式变为  $9r_3 = r_1 - q_2 r_2$ , 将 ② 代入消  $r_2$ , 得:

$$9r_3 = (1 + 9q_2)r_1 - q_2 r_0 \Rightarrow r_3 = \frac{1 + 9q_2}{9} \cdot r_1 + \frac{-q_2}{9} \cdot r_0$$

$$\Rightarrow r_3 = \frac{1 + 9q_2}{9} = -\frac{1}{5}x^2 + \frac{2}{5}x, r_0 = -\frac{q_2}{9} = \frac{3}{5}x - 3. \text{ 解毕.}$$

### 6. 互素:

$f(x), g(x)$  称为互素的如果  $g.c.d(f(x), g(x)) = 1$ , 通常情况下  $\exists s(x), t(x) \in F_{[x]}$  使  $1 = s(x)f(x) + t(x)g(x)$ .

### 7. 定理:

① 设  $f, g, h \in F_{[x]}$ , 且  $f$  与  $g$  互素, 则:

$$f(x) \mid g(x), h(x) \Rightarrow f(x) \mid h(x)$$

② 设  $f, g, h \in F_{[x]}$ , 且  $f$  与  $g$  互素, 则:

$$\begin{cases} f(x) \mid h(x) \\ g(x) \mid h(x) \end{cases} \Rightarrow f(x), g(x) \mid h(x)$$

与整数的理论  
完全类似.

## 95.2 因式分解

因式分解的相关理论:

### 1. 不可约多项式:

设  $f \in \mathbb{F}[x]$ , 若  $f$  能写为  $\mathbb{F}$  中两个次数大于 0 (至少 1 次) 的多项式的积, 则称  $f$  为  $\mathbb{F}$  中的不可约多项式. 如  $\mathbb{F}$  中的一次多项式一定是不可约多项式.  $x^2 - 2$  和  $x^2 + 2$  是  $\mathbb{Q}$  中的不可约多项式.  $x^2 + 2$  是  $\mathbb{R}$  中的不可约多项式.

### 2. 定理 5:

设  $\mathcal{V}_{(n)}$  是  $\mathbb{F}[x]$  中的不可约多项式,  $I = \{v_{(n)} f(x) \mid f \in \mathbb{F}[x]\}$  由  $\mathcal{V}_{(n)}$  生成的主理想, 也即  $I = \mathcal{V}_{(n)}[\mathbb{F}]$ , 则:  $\mathbb{F}[x]/I$  构成一个域.

3. 定理 6:   
这是因为  $\mathbb{F}$  构成含幺乘环

设  $f, g, h \in \mathbb{F}[x]$ ,  $f | g \cdot h \Rightarrow f | g$  或  $f | h$ .

### 4. 定理 7: 算术基本定理

$\mathbb{F}$  中任意一个次数大于 0 的多项式可分解为不可约多项式的乘积, 不考虑常数倍和次序时, 这样的分解唯一.

### 5. 重因式:

设  $\vartheta$  是  $f$  的  $k$  重因式 ( $k \geq 2$ ), 则存在  $g \in \mathbb{F}[x]$  使  $f(x) = \vartheta^k \cdot g(x)$

### 6. 定理 8:

设  $\mathcal{V}, f \in \mathbb{F}[x]$ ,  $\mathcal{V}$  互可约, 且  $\mathbb{F}$  的特征为 0, 即  $\text{char}(\mathbb{F}) = 0$ , 则:  
 $\mathcal{V}_{(n)}$  是  $f(x)$  的重因式  $\Leftrightarrow \mathcal{V}_{(n)}$  是  $f(x)$  和  $f'(x)$  的因式

### 7. 本原多项式:

$a_i \in \mathbb{N}$

$f(x) = a_n x^n + \dots + a_1 x^1 + a_0$  称为本原多项式如果  $\text{g.c.d}(a_n, \dots, a_0) = 1$

### 8. 高斯定理:

本原多项式的积还是本原多项式

### 9. 定理 10:

$\forall 0 \neq f \in \mathbb{Q}[x]$ ,  $\exists! a \in \mathbb{Q}$  和正首项系数的本原多项式  $g \in \mathbb{Q}[x]$  使得  $f(x) = a g(x)$

### 10. Eisenstein 判别法:

延伸:   
若  $f(x)$  是整系数多项式, 若  $\exists$  整数  $p$  使  $p \nmid a_n, p \mid a_{n-1}, \dots, p \mid a_0$  且  $p^2 \nmid a_0$ , 则  $f$  是  $\mathbb{Q}$  上的不可约多项式.  $= f(x) + g(x) \in \mathbb{F}[x]$

### 11. $\mathbb{F}$ 中的 $\overline{f(x)}$ : 也即 $\overline{f(x)} = \{f(x) + h(x)g(x) \mid h(x) \in \mathbb{F}[x]\}$

设  $f \in \mathbb{F}[x]$ , 在模  $g(x)$  的情况下, 定义  $\overline{f(x)} = f(x) + I_g$ , 其中

$I_g = \{h(x)g(x) \mid h(x) \in \mathbb{F}[x]\}$  为由  $g$  生成的主理想.

### 12. 推论:

$\mathbb{R}$  中的不可约多项式有且仅有两种形式:  $x-a$  或  $(x-a)^2+b^2$ , 其中  $a, b \in \mathbb{R}$  且  $b \neq 0$ .

### 13. 定理 13:

设  $f \in \mathbb{R}[x]$  且  $\forall x \in \mathbb{R}, f(x) > 0$ , 则  $\exists f_1, f_2 \in \mathbb{R}[x]$  使  $f(x) = f_1^2(x) + f_2^2(x)$

### 14. 求有理根的定理 14:

设  $f(x)$  是整系数多项式, 且  $\frac{r}{s}$  满足  $\text{g.c.d}(r, s) = 1$  是  $f(x)$  的一个有理根,

则  $r | a_0$  且  $s | a_n$ .

### 15. 定理 10 与推论 11:

定理 10: 设  $f(x) \in \mathbb{Q}[x]$ , 则  $\exists$  唯一的  $a \in \mathbb{Q}$  和正首项本原多项式  $f_1(x)$  使  $f(x) = a f_1(x)$  (或写为  $f_1(x) = a f(x)$ )

推论 11: 若  $f \in \mathbb{Q}[x]$  在  $\mathbb{Q}$  上可约, 则  $\exists$  整系数多项式  $f_1, f_2$  使  $f(x) = f_1(x) f_2(x)$

## 95.3 多项式的根

多项式根的相关理论:

### 1. 多项式的根:

设  $f \in \mathbb{F}[x]$ , 则  $\forall b \in \mathbb{F}$ ,  $b$  是  $f(x)$  根  $\Leftrightarrow (x-b) \mid f(x)$

2. 代数基本定理: 次数大于 0 的复系数在复数域中至少有一个根  $\Rightarrow$  数域上有且仅有 n 个根

### 3. 定理 13:

设  $f \in \mathbb{R}[x]$  且  $\forall a \in \mathbb{R}, f(a) > 0$ , 则  $\exists f_1, f_2 \in \mathbb{R}[x]$  使  $f(x) = f_1^2(x) + f_2^2(x)$

### 4. 定理 14:

设  $f(x) = a_n x^n + \dots + a_1 x^1 + a_0$  是整系数多项式,  $\frac{r}{s}$  是  $f(x)$  的一个有理根, 且

$\text{g.c.d}(r, s) = 1$ , 则:  $r | a_0$  且  $s | a_n$

### 5. 对称对称多项式:

对任意  $n \in \mathbb{N}$ ,  $n \leq n$ , 定义 n 元多项式  $\tau: \tau(x_1, \dots, x_n) = \sum_{i_1, i_2, \dots, i_n} x_{i_1} x_{i_2} \cdots x_{i_n}$

其中  $x_1, \dots, x_n \in \mathbb{F}$ , 则  $\tau(x_1, \dots, x_n)$  是一个对称多项式 (若  $\mathbb{F}$  为无限域, 则为对称函数), 称为初等对称多项式.

$\therefore \tau(x_1, \dots, x_n) = x_1 + \dots + x_n, \tau_n(x_1, \dots, x_n) = x_1 x_2 \cdots x_n$

### 6. 华达定理:

对  $n$  个根分别取为  $c_1, \dots, c_n$

设  $f(x) = x^n + a_{n-1} x^{n-1} + \dots + a_0 = (x - c_1) \cdots (x - c_n) \in \mathbb{F}[x]$ , 则有:

$x^n + \sum_{m=1}^n (-1)^m \tau_m(c_1, \dots, c_n) x^{n-m}$ , 也即  $a_{n-m} = (-1)^m \tau_m(c_1, \dots, c_n)$ ,  $m=1, \dots, n$

### 7. Wilson 定理:

设  $p > 2$  是一个素数, 则  $p | [(p-1)! + 1]$

### 8. 拉格朗日插值定理 (Lagrange's Interpolation Theorem)

设  $n \in \mathbb{N}$  且  $n \geq 2$ ,  $a_1, \dots, a_n \in \mathbb{F}$  是  $n$  个不同的元素, 则:

不完全相同

$\forall b_1, \dots, b_n \in \mathbb{F}$ ,  $\exists$  唯一的、 $\deg \leq n-1$  的多项式  $f \in \mathbb{F}[x]$  使得  $f(a_i) = b_i$ ,

$i = 1, \dots, n$ . 并且此多项式为:

$$f(x) = b_1 \cdot \frac{(x-a_2) \cdots (x-a_n)}{(a_1-a_2) \cdots (a_1-a_n)} + \cdots + b_n \cdot \frac{(x-a_1) \cdots (x-a_{n-1})}{(a_n-a_1) \cdots (a_n-a_{n-1})} + \cdots + b_n \cdot \frac{(x-a_1) \cdots (x-a_{n-1})}{(a_n-a_1) \cdots (a_n-a_{n-1})}$$

以  $\mathbb{F} = \mathbb{R}$  为例, 给定  $\mathbb{R}$  平面上的  $n$  个点 (横坐标不能相同), 则一定存在唯一  $\deg \leq n-1$  的多项式函数  $f$  “穿过”这  $n$  个点.

纵坐标不完全相同

### 9. 结式 (resolvent) $R(f, g)$ :

设非零  $f, g \in \mathbb{F}[x]$ ,  $\deg f = n$ ,  $\deg g = m$ , 则:

$\text{g.c.d}(f, g) \neq 1 \iff$

非零  $h_1, h_2 \in \mathbb{F}[x]$  使得  $h_1(x)f(x) + h_2(x)g(x) = 0$

待定系数法

$$R(f, g) = \begin{vmatrix} a_n & \tau_{m+1} \\ a_{n-1} & a_n \\ a_{n-2} & a_{n-1} & \ddots \\ \vdots & a_{n-2} & \ddots & a_n \\ a_0 & \vdots & \ddots & a_{n-1} \\ a_0 & a_{n-2} & \ddots & a_0 \end{vmatrix} \begin{vmatrix} b_m & \tau_{n+1} \\ b_{m-1} & b_m \\ b_{m-2} & b_{m-1} & \ddots \\ \vdots & b_{m-2} & \ddots & b_m \\ b_0 & \vdots & \ddots & b_{m-1} \\ b_0 & b_{m-2} & \ddots & b_0 \\ \ddots & \vdots & \ddots & \vdots \\ a_0 & & & b_0 \end{vmatrix} = 0$$

其中  $f(x) = a_n x^n + \dots + a_1 x + a_0$ ,  $g(x) = b_m x^m + \dots + b_1 x + b_0$ .

特别地,  $f(x)$  有重根  $h(x) \Leftrightarrow \begin{vmatrix} h(x) & f(x) \\ h'(x) & f'(x) \end{vmatrix} \Leftrightarrow \text{g.c.d}(f, f') \neq 1 \Leftrightarrow R(f, f') = 0$

## 3.5.4 对称多项式

多元多项式环  $\mathbb{F}[x_1, \dots, x_n]$ :

### 1. 非负整数么半群 $\mathbb{N}_0$ :

记全体非负整数为  $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ , 则  $\mathbb{N}_0$  构成加法么半群.

### 2. 字典序 (lexical order):

在  $\mathbb{N}_0^n = \{\vec{a} = (a_1, \dots, a_n) \mid a_i \in \mathbb{N}_0\}$  上定义二元关系 " $<$ ":  $\vec{a} < \vec{b}$  如果

$(\vec{a} - \vec{b})$  的第一个非零坐标小于 0, 类似地可定义  $\vec{a} < \vec{0}$  和  $\vec{a} > \vec{b}$ . 容易证明以下性质:

① 自反:  $\vec{a} \leq \vec{a}$  ② 反对称:  $\vec{a} < \vec{b}, \vec{b} < \vec{a} \Rightarrow \vec{a} = \vec{b}$

③ 可传递性:  $\vec{a} \leq \vec{b}, \vec{b} \leq \vec{c} \Rightarrow \vec{a} \leq \vec{c}$ , 又  $\forall \vec{a}, \vec{b} \in \mathbb{N}_0^n$ , 都有  $\vec{a} \leq \vec{b}$  或

$\vec{b} \leq \vec{a}$  (即所有元素都“可比”), 因此 “ $\leq$ ” 构成一个全序, 称为字典序. 且易证  $\frac{\vec{a} - \vec{b}}{c - d} \leq 1$

$$\Rightarrow \vec{a} + \vec{c} < \vec{b} + \vec{a}.$$

### 3. 多元多项式:

设  $\mathbb{F}$  是一个无限整环,  $x_1, x_2, \dots, x_n$  为  $n$  个不定元 (变量), 记  
 $x^{\vec{a}} = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}, \vec{a} \in \mathbb{N}_0^n$ . 定义无限整环  $\mathbb{F}$  上的, 以  $x_1, x_2, \dots, x_n$  为变量的全体多元多项式为  $\mathbb{F}[x_1, \dots, x_n]$ , 容易验证它构成一个环, 称为多元多项式环. 例如令  $f(x_1, \dots, x_n) = \sum_{\vec{a}} a_{\vec{a}} x^{\vec{a}}$ , 其中  $a_{\vec{a}} \in \mathbb{F}$ , 显然  $f \in \mathbb{F}[x_1, \dots, x_n]$  且系数  $a_{\vec{a}_1}, a_{\vec{a}_2}, \dots$  只有有限个非零 (这是多项式定义要求, 否则称为级数).

在  $\mathbb{F}[x_1, \dots, x_n]$  上定义加法、乘法:

$$f(x_1, \dots, x_n) + g(x_1, \dots, x_n) = \sum_{\vec{a}} (a_{\vec{a}} + b_{\vec{a}}) x^{\vec{a}}$$

$$f(x_1, \dots, x_n) \cdot g(x_1, \dots, x_n) = \sum_{\vec{a}} \left[ \left( \sum_{\vec{a}_1 + \vec{a}_2 = \vec{a}} a_{\vec{a}_1} b_{\vec{a}_2} \right) \cdot x^{\vec{a}} \right]$$

### 4. 首项:

设  $f(x_1, \dots, x_n) = a_{\vec{a}} x^{\vec{a}} + a_{\vec{a}_1} x^{\vec{a}_1} + \cdots + a_{\vec{a}_m} x^{\vec{a}_m}$

单项式  $a_{\vec{a}} x^{\vec{a}}$  称为  $f(x_1, \dots, x_n)$  的首项如果  $a_{\vec{a}} \neq 0$  且  $\forall \vec{a}_i, i = 1, 2, \dots, m$  有  $\vec{a}_i > \vec{a}$ . 由此可以推出“首项的积还是首项”.  
类似一元多项式.

### 5. 次数 (degree):

若  $f(x_1, \dots, x_n) = \sum_{\vec{a}} a_{\vec{a}} x^{\vec{a}}$ , 定义  $f$  的次数为:

$$\deg f = \max \left\{ \sum_{i=1}^n a_i \mid a_i \neq 0, \vec{a} = (a_1, \dots, a_n) \in \mathbb{N}_0^n \right\}, \text{ 也记为 } \deg(f).$$

对称多项式:

为

### 1. 非零对称多项式的首项:

若  $a_{\vec{a}} x^{\vec{a}}$  是对称多项式  $f(x_1, x_2, \dots, x_n)$  的首项, 则  $\tau_1 \geq \tau_2 \geq \cdots \geq \tau_n$

### 2. 对称多项式基本定理:

$\forall$  对称多项式  $f(x_1, \dots, x_n) \in \mathbb{F}[x_1, \dots, x_n]$ , 存在唯一的  $q(x_1, \dots, x_n) \in \mathbb{F}[x_1, \dots, x_n]$

使得  $f(x_1, x_2, \dots, x_n) = q(\tau_1(x_1, \dots, x_n), \tau_2(x_1, \dots, x_n), \dots, \tau_n(x_1, \dots, x_n))$ .

也即  $f(x_1, x_2, \dots, x_n) = q(\tau_1, \tau_2, \dots, \tau_n)$

### 3. 支配项:

记  $\Lambda^+ = \{\vec{a} \in \mathbb{N}_0^n \mid \tau_1 \geq \tau_2 \geq \cdots \geq \tau_n\}$ , 对于对称多项式  $f$ , 若  $\exists \vec{a} \in \Lambda^+$  使  $a_{\vec{a}} \neq 0$ , 则称  $a_{\vec{a}} x^{\vec{a}}$  为  $f$  的支配项.

并且可以证明:

没有支配项的多项式为零多项式

### 4. 对称多项式的符号分解:

$\forall$  对称多项式  $f$ ,  $\exists \vec{a}_1, \vec{a}_2, \dots, \vec{a}_k \in \Lambda^+$  使得  $f(x_1, \dots, x_n) = \sum_{i=1}^k a_{\vec{a}_i} \text{Sym}(x^{\vec{a}_i})$

其中多项式  $\text{Sym}(x^{\vec{a}}) = x^{\vec{a}_1} + \cdots + x^{\vec{a}_k}$  为对称多项式

定义轨道  $S_n(x^{\vec{a}}) = \{x^{\vec{a}_{\sigma(1)}}, x^{\vec{a}_{\sigma(2)}}, \dots, x^{\vec{a}_{\sigma(n)}} \mid \sigma \in S_n\} = \{x^{\vec{a}_1}, x^{\vec{a}_2}, \dots, x^{\vec{a}_k}\}$

由此可以得到:

① 一个多元对称多项式由其支配项完全确定

② 设  $k \leq n$ , 多元对称多项式  $f(x_1, \dots, x_n)$  的支配项都在  $\mathbb{F}[x_1, \dots, x_k]$  中如果  $\deg f \leq k$

5. 牛顿公式:

$$\forall k \in \mathbb{N}_+, \sum_{i=0}^k (-1)^i \tau_i S_{k-i} = 0 = S_k + (-1) \tau_1 S_{k-1} + \cdots + (-1)^k \tau_k$$

$$\text{也可写为 } (-1)^k S_k = \sum_{i=0}^{k-1} (-1)^i \tau_{k-i} S_i$$

其中  $S_m(x_1, x_2, \dots, x_n) = \text{Sym}(x^m) = x_1^m + \cdots + x_n^m$  为一重猜测的对称多项式

特别地,  $\forall k > n$ , 定义  $\tau_k = 0$ , 另外定义  $\tau_0 = 1, S_0 = k$

$$S_n = \begin{vmatrix} \tau_1 & 2\tau_2 & 3\tau_3 & \cdots & (n-1)\tau_{n-1} & n\tau_n \\ 1 & \tau_1 & \tau_2 & \cdots & \tau_{n-2} & \tau_{n-1} \\ 0 & 1 & \tau_1 & \cdots & \tau_{n-3} & \tau_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \tau_1 & \tau_2 \\ 0 & 0 & 0 & \cdots & 1 & \tau_1 \end{vmatrix}$$

$R$  是  $I_R \neq 0$  的环,  $a, b \in R$ , 且  $(1-ab)$  可逆, 证明:  $1-ba$  也可逆

$$b(1-ab) = b - bab = (1-ba)b \Rightarrow b = (1-ba)b(1-ab)^{-1}$$

$$(1-ab)a = a - aba = a(1-ba) \Rightarrow a = (1-ab)^{-1}a(1-ba)$$

取  $d = 1 + b(1-ab)^{-1}a$ , 则  $(1-ba)d = d(1-ba) = 1$

$$\begin{aligned} & (1-ba)d \\ &= (1-ba) + (1-ba)b(1-ab)^{-1} \\ &= (1-ba) + ba = 1 \end{aligned}$$

$$d(1-ba)$$

$$= (1-ba) + b(1-ab)^{-1}a(1-ab)$$

$$= (1-ba) + ba = 1$$

# 判别某多项式是否有根/是否可约的方法

1. 对于根的问题：

① 几个基本事实

在  $\mathbb{Q}$  上有根  $\Rightarrow$  在  $\mathbb{Q}$  上可约      在  $\mathbb{Q}$  上没有根  $\Rightarrow$  在  $\mathbb{Q}$  上不可约

在  $\mathbb{R}$  上有根  $\Rightarrow$  在  $\mathbb{R}$  上可约      在  $\mathbb{R}$  上没有根  $\Rightarrow$  在  $\mathbb{R}$  上不可约

② 判断是否存在有理根，如果存在，求出：

如  $f(x) = x^4 + 2x^2 + 1$  在  $\mathbb{R}$  上无根，但在  $\mathbb{Q}$  上可约

假设  $\exists \frac{p}{q} \in \mathbb{Q}$ , 由  $s|a_n$  和  $r|a_0$  导出矛盾或解出有理根。

2. 对于约的问题：

1. 在  $\mathbb{Q}$  上：

① 证明其不可约

如  $f(x) = x^4 + 2x^2 + 1$  在  $\mathbb{Q}$  上无根，但在  $\mathbb{Q}$  上可约

↓

期末：

行列式

三大因式定理

Sylvan 三定理

Eisenstein 判别法（将  $f(x)$  与  $f(x+1)$  互换后运用判别法）

Lagrange 插值