

章小明不会的题目

章小明

2025 年 3 月 1 日

目录

1 数学分析	1
1.1 裴礼文	1
1.2 于品	3
2 复分析	4
3 实变函数与泛函分析	5
4 线性代数	6
4.1 矩阵	6
4.2 行列式	9
4.2.1 结论	14
4.3 多项式	15
5 抽象代数	16
5.1 群	16
5.1.1 结论	18
5.2 环	18
6 概率论	20
6.0.1 结论	21
7 组合数学	22
8 数论	22

1 数学分析

1.1 裴礼文

题 1.1.

$$\lim_{n \rightarrow \infty} \left(\sqrt[n+1]{(n+1)!} - \sqrt[n]{n!} \right) = \frac{1}{e}$$

证明. 先证

$$\lim_{n \rightarrow \infty} \frac{n^{1/n}}{n} = \frac{1}{e} \text{ 或 } \lim_{n \rightarrow \infty} \frac{n}{n^{1/n}} = e$$

- 用 Stirling 公式: $n! \sim \sqrt{2\pi n} \left(\frac{n}{e}\right)^n$ 易证.

- 用 Stolz 公式: 即证 $\lim_{n \rightarrow \infty} \left(\ln n - \frac{\ln n!}{n} \right) = 1$. 有:

$$\lim_{n \rightarrow \infty} \left(\ln n - \frac{\ln n!}{n} \right) = \lim_{n \rightarrow \infty} \frac{1}{n} \left(n \ln n - \sum \ln k \right) \stackrel{\text{Stolz}}{=} \lim_{n \rightarrow \infty} n \ln \left(1 + \frac{1}{n} \right) = \lim_{n \rightarrow \infty} \ln \left(1 + \frac{1}{n} \right)^n = 1$$

- 使 $a_n = \left(1 + \frac{1}{n} \right)^n = \frac{(n+1)^n}{n^n}$, 有:

$$\prod a_n = \frac{2^1 3^2 4^3}{1^1 2^2 3^3} \cdot \frac{(n+1)^n}{n^n} = \frac{(n+1)^n}{n!} \implies \lim_{n \rightarrow \infty} \frac{n+1}{\sqrt[n]{n!}} = \lim_{n \rightarrow \infty} \left(\prod a_n \right)^{1/n} = \lim_{n \rightarrow \infty} a_n = e$$

最后

□

题 1.2. f 在 \mathbb{R} 上连续有界可微, 则

$$|f(x) - f'(x)| \leq 1 \implies |f(x)| \leq 1$$

证明. 在 $[x, +\infty)$ 上对 $(e^{-x} f(x))' = e^{-x} (f(x) - f'(x))$ 积分, 有

$$|e^{-x} f(x)| = \left| \int_x^{+\infty} e^{-t} |f(t) - f'(t)| dt \right| \leq \int_x^{+\infty} e^{-t} dt = e^{-x} \implies |f(x)| \leq 1$$

□

$$\ln \ln n \ll \ln n \ll n^a \ll n^k \ll a^n \ll n! \ll n^n$$

题 1.3. $\lim_{n \rightarrow \infty} a_n = a, \lim_{n \rightarrow \infty} b_n = b \implies \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=0}^n a_i b_{n-i} = ab$.

证明. 设 $\alpha_n = a_n - a, \beta_n = b_n - b$, 有

$$\frac{1}{n} \sum_{i=0}^n a_i b_{n-i} = \frac{1}{n} \sum_{i=0}^n (\alpha_n + a)(\beta_n + b) = ab + a \frac{\sum \beta_i}{n} + b \frac{\sum \alpha_i}{n} + \frac{\sum \alpha_i \beta_i}{n} \rightarrow ab$$

□

题 1.4. 在 \mathbb{R} 上的 $f(x)$ 有 (1) 介值性: $\forall \mu \in (f(x_1), f(x_2)) \exists \xi$ 在 x_1 和 x_2 间: $f(\xi) = \mu$; (2) $\forall r \in \mathbb{Q}: \{x | f(x) = r\}$ 闭. 求证 $f \in C(\mathbb{R})$.

证明. 首先, 由介值性 $f(x)$ 可以取遍 $\left(\inf_{x \in \mathbb{R}} f(x), \sup_{x \in \mathbb{R}} f(x) \right)$, 故 $\text{Im} f$ 在 \mathbb{R} 上单连通. 其次, 由介值性, 对任意的 $r \in \mathbb{Q} \cap \text{Im} f$ 都存在 x_0 使得 $f(x_0) = r$.

由题, 即 $\forall r \in \mathbb{Q}: \{x | f(x) \neq r\}$ 开, 故 $\forall \mathring{V}_{\mathbb{R}}(x_0): \{x | f(x) \neq r\} \cap \mathring{V}_{\mathbb{R}}(x_0)$ 有界开.

因此对任意的 $r \in \mathbb{Q} \cap \text{Im} f$ 的去心有界开邻域 $\mathring{U}_{\text{Im} f}(r)$, 任取 $\xi_1 \in (\inf U(r), r)$ 和 $\xi_2 \in (r, \sup U(r))$, 都存在 x_1, x_2 有 $\inf U(r) < f(x_1) = \xi_1 < r < \xi_2 < f(x_2) < \sup U(r)$. 因此存在去心有界开邻域 $\mathring{V}_{\mathbb{R}}(x_0) = (x_1, x_2) \setminus \{x_0\} \subset \{x | f(x) \neq r\}$ 使得 $f(\mathring{V}_{\mathbb{R}}(x_0)) \subset \mathring{U}_{\text{Im} f}(r)$.

□

思考: 是否能证明 f 在既开又闭的区间上连续?

题 1.5. $f \in C^{(2)}[-2, 2]; \forall x \in [-2, 2]: |f(x)| \leq 1; f^2(0) + f'^2(0) = 4$. 求证 $\exists \xi \in [-2, 2]:$

$$f(\xi) + f''(\xi) = 0$$

证明一. 取 $F(x) = f^2(x) + f'^2(x), F \in C^{(1)}[-2, 2]$, 故 $\exists \xi_1 \in (0, 2):$

$$f'(\xi_1) = \frac{f(2) - f(0)}{2} \implies |f'(\xi_1)| \leq 1 \implies F(\xi_1) \leq 2$$

由于 $F(0) = 4$, 因此 $\exists \eta_1 \in (0, \xi_1): F(\eta_1) = 3$.

使 $\delta_1 = \inf\{t | t > 0 \wedge F(t) = 3\}$, 可知 $F(\delta_1) = 3$, 且 $\forall x \in [0, \delta_1]: g(x) \geq 3$.

同理, 在 $[-2, 0]$ 上考虑相应的 ξ_2, η_2, δ_2 . 易知, $\exists \xi \in [\delta_2, \delta_1]: g'(\xi) = 0 \implies f'(\xi)(f(\xi) + f''(\xi)) = 0$.

由 $F(\xi) = f^2(\xi) + f'^2(\xi) = 3 > 1 = f^2(\xi) \implies f'(\xi) \neq 0$ 可知 $f(\xi) + f''(\xi) = 0$, 得证.

□

证明二. 由 $F'(x) = (f^2(x) + f'^2(x))' = 2f'(x)(f(x) + f''(x))$, 即证 $F(x) = f^2(x) + f'^2(x)$ 不单调¹, 否则必在 $[-2, 0)$ 或 $(0, 2]$ 中有 \square

1.2 于品

题 1.6. 一道 Putnam 竞赛题

证明. \square

题 1.7. $f \in C(\mathbb{R})$ 满足 $\forall \delta > 0$ 有 $\lim_{n \rightarrow +\infty} f(n\delta) = 0$, 求证 $\lim_{x \rightarrow +\infty} f(x) = 0$.

证明. 这是一道关于 Baire 纲定理的习题.

固定 $\varepsilon > 0$,

$$E_N = \{x : n \geq N \implies f(nx) \leq \varepsilon\} = \bigcap_{n \geq N} \{x : f(nx) \leq \varepsilon\} = \bigcap_{n \geq N} \frac{1}{n} f^{-1}((-\infty, \varepsilon])$$

是闭集. 另一方面, 由于

$$\forall x > 0 : (\forall \varepsilon \exists N_x \forall n > N_x : |f(nx)| < \varepsilon) \implies x \in E_{N_x}$$

因此 $\mathbb{R}_{>0} = \bigcup_{n \in \mathbb{N}} E_n$. 而 Baire 纲定理指出, 至少有一个集合 E_N 含开区间 (a, b) . 因此 $\forall n \geq N \forall t \in (na, nb) \subset E_N : f(t) < \varepsilon$.

取 $M \geq \max\left\{N, \frac{a}{b-a}\right\}$, 有 $(Ma, +\infty) = \bigcup_{n \geq M} (na, nb)$. 故 $\forall t > Ma : f(t) < \varepsilon$, 即 $\lim_{t \rightarrow +\infty} f(t) = 0$. \square

题 1.8. $\varphi \in C(\mathbb{R})$ 满足 (1) $\lim_{x \rightarrow +\infty} \varphi(x) - x = +\infty$ (2) 不动点集 $\{x \in \mathbb{R} : \varphi(x) = x\}$ 非空有限.

求证: 若有 $f \in C(\mathbb{R})$ 满足 $f \circ \varphi = f$, 则 f 一定是常值函数. @Unsolved

证明. \square

题 1.9. $f \in C(\mathbb{R}_{\geq 0})$ 满足 $\lim_{x \rightarrow +\infty} \frac{f(x)}{x} = 0$. 若非负实数数列 $\{a_n\}$ 满足 $\left\{\frac{a_n}{n}\right\}$ 有界, 求证 $\lim_{n \rightarrow +\infty} \frac{f(a_n)}{n} = 0$.

证明. 首先有: (1) $\exists A : \left|\frac{a_n}{n}\right| < A (\forall n \in \mathbb{N})$; (2) $\forall \varepsilon \exists B \forall x > B : \left|\frac{f(x)}{x}\right| < \frac{\varepsilon}{A}$.

又取 $C = \sup_{x \in [0, B]} f(x)$, $N = \left\lceil \frac{C}{\varepsilon} \right\rceil$, 则

$$\forall \varepsilon \exists N \forall n > N : \left|\frac{f(a_n)}{n}\right| = \begin{cases} \left|\frac{f(a_n)}{n}\right| < \frac{C}{n} < \varepsilon & a_n \in (0, B) \\ \left|\frac{f(a_n)}{a_n}\right| \left|\frac{a_n}{n}\right| < \frac{\varepsilon}{A} \cdot A = \varepsilon & a_n \geq B \end{cases}$$

题 1.10. A theorem about Cesàro mean, related to Stolz-Cesàro theorem

$\{a_n\}_{n \geq 1} \subset \mathbb{C}$, $\sigma_n = \frac{\sum_{k=1}^n a_k}{n}$, $b_n = a_{n+1} - a_n$, $|nb_n| \leq M < \infty$, $\lim_{n \rightarrow \infty} \sigma_n = \sigma$, 求证 $\lim_{n \rightarrow \infty} a_n = \sigma$.

证明. 设 $m < n$, 注意到

$$\sum_{k=m+1}^n a_k = \sum_{k=1}^m a_k - \sum_{k=1}^n a_k = n\sigma_n - m\sigma_m.$$

因此

$$\sum_{k=m+1}^n (a_n - a_k) = (n-m)a_n - (n\sigma_n - m\sigma_m) = (n-m)(a_n - \sigma_n) - m(\sigma_n - \sigma_m)$$

¹而且在 $f'(x) = 0$ 处同样不单调

因此

$$a_n - \sigma_n = \frac{m}{n-m}(\sigma_n - \sigma_m) + \frac{1}{n-m} \sum_{k=m+1}^n (a_n - a_k)$$

而

$$|a_n - a_k| = \left| \sum_{i=k}^{n-1} b_i \right| \leq \sum_{i=k}^{n-1} \frac{M}{i} \leq M \frac{n-k}{k} < M \frac{n-m-1}{m+1}$$

$$\frac{1}{n-m} \left| \sum_{k=m+1}^n (a_n - a_k) \right| < M \frac{n-m-1}{m+1} = M \left(\frac{n}{m+1} - 1 \right)$$

固定 ε , 任取 n , 取 m 满足 $m \leq \frac{n}{1+\varepsilon} < m+1$,

$$|a_n - \sigma_n| < \frac{m}{n-m} |\sigma_n - \sigma_m| + M \left(\frac{n}{m+1} - 1 \right) < \frac{|\sigma_n - \sigma_m|}{\varepsilon} + M\varepsilon$$

因此 $n \rightarrow \infty$ 时, $|a_n - \sigma_n| \rightarrow M\varepsilon$. 最后由 ε 任意性, $|a_n - \sigma_n| \rightarrow 0$. 由于 $\sigma_n \rightarrow \sigma$, 因此 $a_n \rightarrow \sigma$. □

2 复分析

题 2.1. $f \in H(B \cup \{1\})$, $f(B) \subset B$, $f(1) = 1$, 证明 $f'(1) \geq 0$.

证明. 对 $\theta \in \left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$, $r \in (0, 2 \cos \theta)$, 有 $1 - re^{i\theta} \in B$. 而 $f'(1) = \lim_{r \rightarrow 0} \frac{f(1 - re^{i\theta}) - 1}{-re^{i\theta}}$, 即 $f(1 - re^{i\theta}) = 1 - f'(1)re^{i\theta} + o(r)$. 而 $|f| < 1$, 故复数 $f'(1)e^{i\theta}$ 在虚轴右侧, 即 $\operatorname{Re}(f'(1)e^{i\theta}) \geq 0$. 再设 $f'(1) = re^{it}$, 有 $\operatorname{Re} e^{i(t+\theta)} \geq 0$, $t + \theta \in \left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$, 因此 $t = 0$, 即 $f'(1) \geq 0$. □

题 2.2. $f \in H(B)$, 若有 $z_0 \in B - \{0\}$, $f(z_0) \neq 0$, $f'(z_0) \neq 0$, $|f(z_0)| = \max_{|z| \leq |z_0|} |f(z)|$, 则 $\frac{z_0 f'(z_0)}{f(z_0)} > 0$.

geelaw 的证明. 令 $\frac{z_0 f'(z_0)}{f(z_0)} = x + iy$, $x, y \in \mathbb{R}$. 由 $f(z_0 e^{i\theta}) = f(z_0) + f'(z_0)z_0(e^{i\theta} - 1) + o(z_0 e^{i\theta} - z_0)$, 因此

$$\frac{f(z_0 e^{i\theta})}{f(z_0)} = 1 + \frac{z_0 f'(z_0)}{f(z_0)}(e^{i\theta} - 1) + z_0 o(e^{i\theta} - 1) = 1 + (x + iy)i\theta + o(\theta),$$

因此

$$1 \geq \left| \frac{f(z_0 e^{i\theta})}{f(z_0)} \right|^2 = 1 - 2y\theta + (x^2 + y^2)\theta^2 + o(\theta) = 1 - 2y\theta + o(\theta).$$

因此 $y\theta \geq 0$, 而 θ 可正可负, 因此 $y = 0$.

同理考虑 $f(z_0(1 + \delta))$, $\delta < 0$, 有

$$\frac{f(z_0(1 + \delta))}{f(z_0)} = 1 + (x + iy)\delta + o(\delta), \quad 1 \geq \left| \frac{f(z_0(1 + \delta))}{f(z_0)} \right|^2 = 1 + 2x\delta + o(\delta).$$

因此 $x \geq 0$. 最后由于所给限制条件, $x > 0$, 故得证. □

陈施毅的证明. 注意到 $F \in C^1(B)$ 时 $F(x_0, y_0) = \max_{|z| \leq r < 1} F(x, y)$ 有

$$\left(x \frac{\partial F}{\partial y} - y \frac{\partial F}{\partial x} \right) (x_0, y_0) = 0, \quad \left(x \frac{\partial F}{\partial x} + y \frac{\partial F}{\partial y} \right) (x_0, y_0) \geq 0$$

对于 $f = u + iv$, $F(x, y) = u(x, y)^2 + v(x, y)^2$. 我们有

$$\begin{aligned} z f'(z) \overline{f(z)} &= (x + iy) \left(\frac{\partial u}{\partial x} + i \frac{\partial v}{\partial x} \right) (u - iv) = (x + iy) \left(u \frac{\partial u}{\partial x} + v \frac{\partial v}{\partial y} + iu \frac{\partial v}{\partial x} - iv \frac{\partial u}{\partial y} \right) \\ &= \frac{1}{2} (x + iy) \left(\frac{\partial F}{\partial x} - i \frac{\partial F}{\partial y} \right) = \frac{1}{2} \left(\left(x \frac{\partial F}{\partial x} + y \frac{\partial F}{\partial y} \right) + i \left(y \frac{\partial F}{\partial x} - x \frac{\partial F}{\partial y} \right) \right) \geq 0 \end{aligned}$$

因此得证. □

严仲谨的证明. 注意到在圆周 $\gamma: |z| = |z_0|$ 上 z_0 处的切线的辐角为 $\arg z_0 \pm \frac{\pi}{2}$, 其在 f 作用下 $f(\gamma)$ 上 $f(z_0)$ 处的切线的辐角为 $\arg f(z_0) \pm \frac{\pi}{2}$, 而两者之差 $\left(\arg f(z_0) \pm \frac{\pi}{2}\right) - \left(\arg z_0 \pm \frac{\pi}{2}\right) = \arg f'(z_0)$, 因此 $\arg \frac{z_0 f'(z_0)}{f(z_0)} = 0$ 或 $\pm\pi$.

(To be continued...)

□

题 2.3. 设 $D = \{z \in \mathbb{C} : \theta_0 < \arg(z - a) < \theta_0 + \alpha\}$, $f \in C(\overline{D} - \{a\})$, 有:

(1) $\lim_{\substack{z \rightarrow a \\ z \in \overline{D} - \{a\}}} (z - a)f(z) = A$, 则 $\lim_{r \rightarrow 0} \int_{|z-a|=r} f(z)dz = i\alpha A$. (2) $\lim_{\substack{z \rightarrow \infty \\ z \in \overline{D} - \{a\}}} (z - a)f(z) = B$, 则 $\lim_{R \rightarrow \infty} \int_{|z-a|=R} f(z)dz = i\alpha B$.

证明. (1)

$$\begin{aligned} \left| \int_{|z-a|=r} f(z)dz - i\alpha A \right| &= \left| \int_{|z-a|=r} \left(f(z) - \frac{A}{z-a} \right) dz \right| \leq \int_{|z-a|=r} \frac{|(z-a)f(z) - A|}{|z-a|} |dz| \\ &\leq \frac{r\alpha}{r} \sup_{\substack{|z-a|=r \\ z \in \overline{D}}} |(z-a)f(z) - A| \rightarrow 0 \end{aligned}$$

□

题 2.4. $f \in C^1(D)$, 则 $f \in H(D) \iff \forall a \in D : \lim_{r \rightarrow 0} \frac{1}{\pi r^2} \int_{|z-a|=r} f(z)dz = 0$.

3 实变函数与泛函分析

题 3.1. E 是 $[0, 1]$ 的可测子集, 若 $m(E) > 0, m(E^c) > 0$, 则 $\exists p \in [0, 1] \forall O(p) \subset [0, 1] : m(E \cap O) > 0, m(E^c \cap O) > 0$.

证明. 令 $S_1 = \{x \in [0, 1] : \exists O(x) \subset [0, 1] : m(E^c \cap O) = 0\}$, $S_2 = \{x \in [0, 1] : \exists O(x) \subset [0, 1] : m(E \cap O) = 0\}$.

因此 $p \in S_1^c \cap S_2^c = (S_1 \cup S_2)^c$. 而显然 $S_1 \cap S_2 = \emptyset$, 因为若否, 则 $0 = m((O \cap E) \cup (O \cap E^c)) = m(O \cap (E \cup E^c)) = m(O)$, 矛盾.

下证 S_1 是开集, S_2 同理. $\forall x \in S_1 \exists O(x) : m(E^c \cap O) = 0$, 因此 $\forall y \in O(x) \exists O(y) \subset O(x) : m(E^c \cap O(y)) = 0$, 因此 $y \in S_1, O(x) \subset S_1$, 因此 S_1 开.

最后, 若 p 不存在, 则 $S_1 \cup S_2 = [0, 1]$, 但两者为不交开集, 而 $[0, 1]$ 是连通的, 矛盾. 因此 p 存在.

□

题 3.2. 请教一道 Lebesgue 积分的证明 $f \in L^1(\mathbb{R})$, 证明 $f\left(x - \frac{1}{x}\right) \in L^1(\mathbb{R})$ 且 $\int_{\mathbb{R}} f(x)dx = \int_{\mathbb{R}} f\left(x - \frac{1}{x}\right)dx$.

HINT: 顺序: 区间 \rightarrow 开集 \rightarrow 一般测度有限测集特征函数 \rightarrow 简单函数 \rightarrow 非负可测函数 $\rightarrow L^1$ 函数

证明. 1. $I = [a, b] \subset \mathbb{R}$, 令 $I_1 \cup I_2 = \left\{x \in \mathbb{R} : x - \frac{1}{x} \in [a, b]\right\}$, 其中

$$I_1 = \left[\frac{a + \sqrt{a^2 + 4}}{2}, \frac{b + \sqrt{b^2 + 4}}{2} \right], \quad I_2 = \left[\frac{a - \sqrt{a^2 + 4}}{2}, \frac{b - \sqrt{b^2 + 4}}{2} \right]$$

且 $m(I) = m(I_1) + m(I_2) = b - a$. 因此 $f = c1_{[a,b]}$ 时

$$\int_{\mathbb{R}} f(x)dx = \int_{\mathbb{R}} f\left(x - \frac{1}{x}\right)dx = c(b - a)$$

因此 f 是有界区间上的阶梯函数时, 结论成立.

2. 若 f 是紧支集连续函数, 设 $\text{supp}(f) \subset [a, b]$. 由一致连续性, 可作 $[a, b]$ 的分割 $T: a = x_0 < x_1 < \dots < x_N = b$, 使 $\lambda(T) = \max |\Delta x_i| < \delta, |f(x_k) - f(x_{k+1})| < \varepsilon$. 取 $c_k \in \left[\min_{[x_{k-1}, x_k]} f(x), \max_{[x_{k-1}, x_k]} f(x) \right], |c_k| = \min_{[x_{k-1}, x_k]} |f(x)|$, 作

$$\varphi(x) = \sum_{k=1}^N c_k 1_{I_k}(x), \quad I_k = [x_{k-1}, x_k], I_N = [x_{N-1}, x_N]$$

有 $\forall x \in [a, b] : |\varphi(x) - f(x)| < \varepsilon, |\varphi(x)| \leq |f(x)|$. 取 $\varepsilon = \frac{1}{n}$, 可得阶梯函数列 $\{\varphi_n(x)\}$, 使得 $\varphi(x) \nearrow f(x)$.

(To be continued...)

□

题 3.3. 网页链接 $L^2(\mathbb{R})$ 中可测函数列 $f_n \rightarrow f$ a.e., 若 $\|f_n\|_{L^2} \rightarrow \|f\|_{L^2}$, 证明 $\|f_n - f\|_{L^2} \rightarrow 0$.

证明. 由 $L^2(\mathbb{R})$ 是 Hilbert 空间, 且 $\|f_n\|_{L^2} \rightarrow \|f\|_{L^2}$, 因此仅需证明 f_n 弱收敛于 f , 即对

$$\forall g \in L^2(\mathbb{R}) : \lim \int_{\mathbb{R}} f_n g = \int_{\mathbb{R}} f g$$

由此可得到强收敛.

首先对 $g \in L^2(\mathbb{R})$ 必然有 $\int_{|x|>R} |g|^2 < \varepsilon^2$. 另外由 $\int g$ 的绝对连续性也有 $\int_E |g|^2 < \varepsilon^2$, 其中 $m(E) < \delta$. 由 Egorov 定理, 可取 $E_\delta \subset (-R, R)$ 且 $m((-R, R) - E_\delta) < \delta$, 使其上有 $f_n \xrightarrow{\text{uni.}} f$. 因此对充分大的 n 和任一点 $x \in E_\delta$ 可取 $|f_n - f| < \frac{\varepsilon}{\sqrt{2R}}$.

设 $M = \|g\|_{L^2} + \|f\|_{L^2} + \sup \|f_n\|_{L^2}$, 则对充分大的 n 有 $\int_E |f - f_n|^2 = \int_E f^2 + \int_E f_n^2 - 2 \int_E f f_n < M^2 + M^2 = 2M^2$,

$$\begin{aligned} \int_{\mathbb{R}} |f_n - f| |g| &= \left(\int_{E_\delta} + \int_{(-R, R) - E_\delta} + \int_{|x|>R} \right) |f_n - f| |g| \\ &\leq \left(\int_{E_\delta} |f - f_n|^2 \int_{E_\delta} |g|^2 \right)^{\frac{1}{2}} + \left(\int_{(-R, R) - E_\delta} |f - f_n|^2 \int_{(-R, R) - E_\delta} |g|^2 \right)^{\frac{1}{2}} + \left(\int_{|x|>R} |f - f_n|^2 \int_{|x|>R} |g|^2 \right)^{\frac{1}{2}} \\ &< \left(\frac{\varepsilon^2}{2R} \cdot 2R \cdot M^2 \right)^{\frac{1}{2}} + (2M^2 \cdot \varepsilon^2)^{\frac{1}{2}} + (2M^2 \cdot \varepsilon^2)^{\frac{1}{2}} = (M + 2\sqrt{2}M)\varepsilon \end{aligned}$$

故得证. □

4 线性代数

4.1 矩阵

题 4.1. q 元域 \mathbb{F}_q 上的 n 维向量空间 V 中有多少个 $k \in [n]$ 维子空间?

证明. 这一题其实用的是组合思想, 即:

$$k\text{维子空间数量} = \frac{\text{能张成不同空间的}k\text{维基底个数}}{k\text{维空间中可选取}k\text{维基底个数}} = \frac{n\text{维空间中可选取}k\text{维基底个数}}{k\text{维空间中可选取}k\text{维基底个数}}$$

换个思路, (每个) k 维空间中可选取 k 维基底个数 = 多少个 k 维基底对应一个 (不同的) k 维空间.

在此之前我一直以为 \mathbb{R}^n 中 k 维子空间的个数是 $\binom{n}{k}$ 个, 但实际上应当是无穷多个, 因为我一直只在标准正交系中找子空间.

考虑 n 维空间 $V_{\mathbb{F}_q}$ 中, 若首先要选择一个基底, 则有 $|V - \{0\}| = q^n - 1$ 个选择. 设选到的为 $v_1, V_1 = \langle v_1 \rangle$, 则第二个基底有 $|V - V_1| = q^n - q$ 个选择. 因此类推, 第 $k \in [n]$ 个基底有 $q^n - q^{k-1}$ 种选择. 因此在 \mathbb{F}_q^n 上的 n 维空间中可选取 k 维基底的个数是 $\frac{1}{k!} \prod_{i \in [k]} (q^n - q^{i-1})$, 因此在 k 维空间中可选取的基底的个数为 $\frac{1}{k!} \prod_{i \in [k]} (q^k - q^{i-1})$, 故 (不同) k 维子空间数量为

$$\prod_{i \in [k]} \frac{q^n - q^{i-1}}{q^k - q^{i-1}} = \prod_{i \in [k]} \frac{q^{n-i+1} - 1}{q^{k-i+1} - 1}$$

□

题 4.2. 求 \mathbb{Q} 上的 n 阶半幻方 $\text{SMag}_n(\mathbb{Q})$ 和幻方 $\text{Mag}_n(\mathbb{Q})$ 的维数, 并证明

$$\text{SMag}_n(\mathbb{Q}) = \text{Mag}_n(\mathbb{Q}) \oplus \mathbb{Q}I_n \oplus \mathbb{Q}D_n$$

其中 D_n 是 $a_{i, n+1-i} = 1$ 的 n 阶矩阵.

证明. 首先考察 $\text{SMag}_n(\mathbb{Q})$ 的维度, 若已知它的行列和 $\sigma(A)$, 则遮住一行一列的话, 剩下 $n-1$ 阶矩阵的数字可以任意选取, 即有 $(n-1)^2 + 1 = n^2 - 2n + 2$ 维.

另一个思路来说, 实际上可以认为 n 行 n 列的和都等于同一个数, 这就给出了 $2n$ 个线性方程和一个自由变量, 但有 n^2 个未知数. 实际上这 $2n$ 个线性方程可以从约去一个, 还剩 $2n-1$ 个线性无关的, 故最终维数为 $n^2 - (2n-1) + 1 = n^2 - 2n + 2$.

又由等式可知, $\dim \text{Mag}_n(\mathbb{Q}) = n^2 - 2n$. 下证等式.

首先显然 $\text{Mag}_n(\mathbb{Q}) \cap \mathbb{Q}I_n \cap \mathbb{Q}D_n = \{0\}$, 因此

$$\text{Mag}_n(\mathbb{Q}) + \mathbb{Q}I_n + \mathbb{Q}D_n = \text{Mag}_n(\mathbb{Q}) \oplus \mathbb{Q}I_n \oplus \mathbb{Q}D_n$$

其次, 设 $\forall S \in \text{SMag}_n(\mathbb{Q})$ 存在分解

$$\exists p, q, r \in \mathbb{Q}, S = pM + qI_n + rD_n$$

其中 $M \in \text{Mag}_n(\mathbb{Q})$, 则分别计算 S 的行列和 σ_1 、主对角线和 $\sigma_2 = \text{tr } S$ 和副对角线和 σ_3 如下:

$$Ap = \begin{pmatrix} \sigma(M) & 1 & 1 \\ \sigma(M) & n & \delta \\ \sigma(M) & \delta & n \end{pmatrix} \begin{pmatrix} p \\ q \\ r \end{pmatrix} = \begin{pmatrix} \sigma_1 \\ \sigma_2 \\ \sigma_3 \end{pmatrix} = \sigma$$

其中 $\delta = \text{OddQ}(n)$, 当 n 为奇数是 $\delta = 1$, 否则为 0.

通过化简可知 $\text{rank } A = 3$, 故 $A: \mathbb{Q}^3 \rightarrow \mathbb{Q}^3$ 是双射, 故

$$\dim_{\mathbb{Q}} \text{SMag}_n(\mathbb{Q}) = \dim_{\mathbb{Q}} \text{Mag}_n(\mathbb{Q}) + \dim_{\mathbb{Q}} \mathbb{Q}I_n + \dim_{\mathbb{Q}} \mathbb{Q}D_n$$

故等式得证.

另, 继续计算可得:

$$A^{-1}\sigma = \frac{1}{\det A} \begin{pmatrix} n^2 - \delta^2 & n - \delta & n - \delta \\ \sigma(n - \delta) & \sigma(n - 1) & \sigma(1 - \delta) \\ \sigma(n - \delta) & \sigma(1 - \delta) & \sigma(n - 1) \end{pmatrix} \begin{pmatrix} \sigma_1 \\ \sigma_2 \\ \sigma_3 \end{pmatrix} = \begin{pmatrix} p \\ q \\ r \end{pmatrix} = p$$

其中 $\det A = \sigma((n-1)^2 - (1-\delta)^2)$.

下分别给出 $\delta = 0$ 和 $\delta = 1$ 时的 A^{-1} :

$$A^{-1}_{\delta=0} = \frac{1}{2-n} \begin{pmatrix} \frac{n}{\sigma} & \frac{1}{\sigma} & \frac{1}{\sigma} \\ 1 & \frac{1-\sigma}{n} & \frac{1}{n} \\ 1 & \frac{1}{n} & \frac{1-n}{n} \end{pmatrix} \quad A^{-1}_{\delta=1} = \frac{1}{1-n} \begin{pmatrix} \frac{1+n}{\sigma} & \frac{1}{\sigma} & \frac{1}{\sigma} \\ 1 & -1 & 0 \\ 1 & 0 & -1 \end{pmatrix}$$

□

题 4.3. $\{V_i\}_{i \in [m]}$ 是 n 维空间 V 中的一组子空间, 若 $\sum_{i \in [m]} \dim V_i > n(m-1)$, 求证 $\bigcap V_i \neq \{0\}$.

证明. 首先, 若公式成立则 $V_i \neq \{0\}$, 因为若有 $\dim V_k = 0$, 则

$$\sum \dim V_i = \sum_{i \in [m]-k} \dim V_i + \dim V_k = \sum_{i \in [m]-k} \dim V_i \leq n(m-1)$$

$m=1$ 时公式显然成立, $m=2$ 时 $\dim V_1 + \dim V_2 > n$ 可知 $\dim V_1 \cap V_2 > 0$, 故也成立.

假设 $m=k$ 时公式成立, 则 $m=k+1$ 时, 假设 $\sum_{i \in [k+1]} \dim V_i > nk$. 若 $\bigcap V_i = \{0\}$, 则 $[k+1]$ 中存在 k 元指标集

J 有 $\bigcap_{j \in J} V_j = \{0\}$, 故 $\sum_{j \in J} \dim V_j \leq n(k-1)$. 设 $[k+1] - J = \{k+1\}$, 则

$$\dim V_{k+1} = \sum_{i \in [k+1]} \dim V_i - \sum_{j \in J} \dim V_j > nk - n(k-1) = n$$

矛盾, 故 $\bigcap V_i \neq \{0\}$.

□

题 4.4. 用平面上 n 条直线集合的几何性质给出

$$A = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix}, \quad B = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \\ c_1 & c_2 & \cdots & c_n \end{pmatrix}$$

有相等秩的条件. @Unsolved

证明. □

题 4.5 (秩的不等式). 1. Sylvester 秩不等式: $\forall A \in \mathbb{F}^{m \times k}, B \in \mathbb{F}^{k \times n} : \text{rank } A + \text{rank } B - k \leq \text{rank } AB$

2. Frobenius 秩不等式: $\forall A \in \mathbb{F}^{m \times s}, B \in \mathbb{F}^{s \times t}, C \in \mathbb{F}^{t \times n} : \text{rank } AB + \text{rank } BC \leq \text{rank } B + \text{rank } ABC$

3. $\forall A, B, C \in M_n(\mathbb{F})$, 若 $ABC = O$, 则 $\text{rank } A + \text{rank } B + \text{rank } C \leq 2n$

证明. (1) 证法 1: 考虑分块矩阵, 有

$$\begin{pmatrix} I_m & A_{m \times k} \\ O_{k \times m} & I_k \end{pmatrix} \begin{pmatrix} A_{m \times k} & O_{m \times n} \\ -I_k & B_{k \times n} \end{pmatrix} = \begin{pmatrix} O_{m \times k} & AB_{m \times n} \\ -I_k & B_{k \times n} \end{pmatrix}$$

因此

$$\text{rank } A + \text{rank } B \leq \text{rank} \begin{pmatrix} A & O \\ -I & B \end{pmatrix} = \text{rank} \begin{pmatrix} O & AB \\ -I & B \end{pmatrix} = \text{rank } AB + k$$

证法 2: 由于 A 可被化为等价标准型 $A' = I_r \oplus 0$, 即 $A = PA'Q$, 其中 P, Q 为可逆方阵, 我们可以化不等式为

$$\text{rank } A + \text{rank } B = r + \text{rank } QB \leq \text{rank } PA'QB + k = \text{rank } A'QB + k$$

令 $B' = QB$, 即证明 $\text{rank } A' + \text{rank } B' \leq \text{rank } A'B' + k$.

$$\begin{aligned} \text{rank } A' + \text{rank } B' &= \text{rank } A' + \text{rank}(A'B' + (I - A')B') \\ &\leq \text{rank } A' + \text{rank}(A'B') + \text{rank}((I - A')B') \\ &\leq r + \text{rank}(A'B') + (n - r) \\ &= \text{rank } A'B' + n \end{aligned}$$

证法 3: 即证 $\dim \ker AB \leq \dim \ker A + \dim \ker B$.

由于 $\ker B \subseteq \ker AB$, 考虑 $\bar{B} = B|_{\ker AB}$, 显然 $\ker B = \ker \bar{B}$, 而 $\text{Im } \bar{B} \subseteq \ker A$, 因此 $\text{rank } \bar{B} \leq \dim \ker A$, 即

$$\dim \ker AB = \dim \ker B + \text{rank } \bar{B} \leq \dim \ker B + \dim \ker A$$

(2) 证法 1: 考虑 $C : \ker(ABC) / \ker(BC) \rightarrow \ker(AB) / \ker B$, 这是一个映射且是一个单射.

首先, $x + \ker(BC) \mapsto Cx + C(\ker(BC))$, 显然 $x \in \ker(ABC) \implies Cx \in \ker(AB), C(\ker(BC)) = \ker(B)$ (互相包含), 因此

$$x + \ker(BC) = y + \ker(BC) \implies Cx + \ker(B) = Cy + \ker(B), C(x - y) \in \ker B$$

故这是一个映射. 而又有 $a \in \ker C, ABCa = 0$, 即 $a \in \ker(BC), Ca \in \ker B$, 故 C 是单射.

证法 2: 运用 Sylvester 不等式. 若 $\text{rank } B = r$, 则 B 有满秩分解 $B_{s \times t} = P_{s \times r} Q_{r \times t}$, 使得

$$\begin{aligned} \text{rank}(ABC) &= \text{rank}(APQC) \geq \text{rank}(AP) + \text{rank}(QC) - r \\ &= \text{rank}(APQ) + \text{rank}(PQC) - r \\ &= \text{rank}(AB) + \text{rank}(BC) - \text{rank } B \end{aligned}$$

证法 3: 注意到 $\text{Im } B = \text{Im}(AB) \oplus (\text{Im } B \cap \ker A)$, 因此

$$\text{rank}(AB) = \text{rank } B - \dim(\text{Im } B \cap \ker A)$$

类似也有

$$\text{rank}(ABC) = \text{rank}(BC) - \dim(\text{Im}(BC) \cap \ker A)$$

又有

$$\text{Im } BC \cap \ker A \subseteq \text{Im } B \cap \ker A$$

因此

$$\begin{aligned} \text{rank } AB + \text{rank } BC &= \text{rank } B + \text{rank } ABC \\ &\quad + \dim(\text{Im } BC \cap \ker A) - \dim(\text{Im } B \cap \ker A) \\ &\leq \text{rank } B + \text{rank } ABC \end{aligned}$$

(3) 证法 1: 运用两次 Sylvester 不等式:

$$0 = \text{rank } ABC \geq \text{rank } AB + \text{rank } C - n \geq \text{rank } A + \text{rank } B + \text{rank } C - 2n$$

证法 2: 首先注意到 $\text{Im } BC \subseteq \ker A$, 因此 $n = \text{rank } A + \dim \ker A \geq \text{rank } A + \text{rank } BC$. 其次, 注意到 $\text{Im } C = \text{Im } BC \oplus (\ker B \cap \text{Im } C)$, 因此有

$$\begin{aligned} n &\geq \text{rank } A + \text{rank } BC \\ &= \text{rank } A + \text{rank } C - \dim(\ker B \cap \text{Im } C) \\ &\geq \text{rank } A + \text{rank } C - \dim \ker B \\ &= \text{rank } A + \text{rank } C + \text{rank } C - n \end{aligned}$$

因此得证. □

题 4.6. 对 $\forall A \in M_2(\mathbb{R}), \forall k \in \mathbb{N}_+$, 若 $A^k = O$, 则 $A^2 = O$. @Unsolved

证明. □

题 4.7. 记 A^\vee 为 $A \in M_n(\mathbb{F})$ 的伴随矩阵, 则有

$$\text{rank } A^\vee = \begin{cases} n & \text{if } \text{rank } A = n \\ 1 & \text{if } \text{rank } A = n - 1 \\ 0 & \text{if } \text{rank } A < n - 1 \end{cases}$$

证明. $\text{rank } A < n - 1$ 时, A 的 $n - 1$ 阶子式均为 0, 即 $A^\vee = O$.

$\text{rank } A = n - 1$ 时, A 存在 $n - 1$ 阶子式非零, 此时运用 Sylvester 不等式有 $\text{rank } A + \text{rank } A^\vee \leq \text{rank}(AA^\vee) + n = n$, $\text{rank } A^\vee \leq 1$. 而 $A^\vee \neq O$, 因此 $\text{rank } A^\vee = 1$. □

4.2 行列式

题 4.8. 求证任意阶的斜对称矩阵 A 的行列式 $\det A \geq 0$. 特别的, 奇数阶时 $\det A = 0$.

证明. 首先对于奇数阶的情况有

$$\det A = \det A^T = \det(-A) = (-1)^n \det A = -\det A \implies \det A = 0$$

对偶数阶的情况:

证法 1: 由于 $\text{tr } A = 0$, 因此若 λ 是其本征值, 则 $-\lambda$ 也是. 有进一步的结论 $\Re(\lambda) = 0$, 即 λ 是纯虚数. 而 $\det A = \prod_{\text{本征值}} \lambda_i = \prod \lambda_i^2$, 得证.

证法 2: 对 $n = 2k$ 作归纳证明. 首先已知 $n = 2$ 时 $\det A = a_{12}^2$, 情况成立. 假设对 $n = 2k$ 成立, 则只需证 $n = 2k + 2$ 的情况, 此时

$$\det A_{2k+2} = \det \begin{pmatrix} 0 & a_{12} & \cdots \\ -a_{12} & 0 & \cdots \\ \vdots & \vdots & A_{2k} \end{pmatrix} \stackrel{\text{初等变换}}{=} \det \begin{pmatrix} 0 & a_{12} & O \\ -a_{12} & 0 & O \\ O & O & A'_{2k} \end{pmatrix} = a_{12}^2 \det A'_{2k}$$

而 $\det A'_{2k}$ 实际上也是 $2k$ 阶斜对称矩阵 (因为初等行列变换是对应的, 两个变换的结果相互抵消), 因此得证. □

题 4.9. 对元素 $a_{ij} = b_i^2 - b_j^2$ 的 n 阶斜对称矩阵, 求证其行列式总为零.

证明. 可以证明元素形如 $a_{ij} = x_i + y_j$ 的矩阵的秩至多为 2, 但也可以这样想: 这个斜对称矩阵是两个秩 1 矩阵的差, 即 $a_{ij} = b_i^2$ 和 $a_{ij} = b_j^2$ 的两个矩阵, 故矩阵的秩至多为 2. \square

题 4.10. 证明

$$\Delta_n(k_1, x_1; k_2, x_2; \cdots; k_m, x_m) = \det \begin{pmatrix} M_{k_1}^n(x_1) \\ M_{k_2}^n(x_2) \\ \vdots \\ M_{k_m}^n(x_m) \end{pmatrix} = \prod_{1 \leq j < i \leq m} (x_i - x_j)^{k_i k_j}$$

其中 $M_k^n(x)$ 是 $k \times n$ 阶矩阵:

$$M_k^n(x) = \begin{pmatrix} \binom{0}{0} x^0 & \binom{1}{0} x^1 & \binom{2}{0} x^2 & \cdots & \binom{n-1}{0} x^{n-1} \\ 0 & \binom{1}{1} x^0 & \binom{2}{1} x & \cdots & \binom{n-1}{1} x^{n-2} \\ 0 & 0 & \binom{2}{0} x^0 & \cdots & \binom{n-1}{2} x^{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \binom{n-1}{k-1} x^{n-k} \end{pmatrix}$$

即 $a_{ij} = \binom{j-1}{i-1} x^{j-i}$, 且 $\sum_{i \in [m]} k_i = n$.

特别的, $k_i = 1$, 即 $m = n$ 时化为 Vandermonde 行列式.

证明. 一篇 1983 年的国内论文 [Vandermonde 行列式推广及其在控制理论中的应用](#) 专门讨论了这个行列式, 摘录如下. 只需证明

$$\Delta_n(k_1, x_1; k_2, x_2; \cdots; k_m, x_m) = \Delta_n(k_1 - 1, x_1; k_2, x_2; \cdots; k_m, x_m) \prod_{i=2}^m (x_i - x_1)^{k_i}$$

这是因为

$$\begin{aligned} \text{LHS} &= \Delta_n(k_1 - 1, x_1; k_2, x_2; \cdots; k_m, x_m) \prod_{i=2}^m (x_i - x_1)^{k_i} = \Delta_n(k_2, x_2; \cdots; k_m, x_m) \prod_{i=2}^m (x_i - x_1)^{k_1 k_i} \\ &= \prod_{j=1}^m \left(\prod_{i=j+1}^m (x_i - x_j)^{k_i} \right)^{k_j} = \text{RHS} \end{aligned}$$

第一步: 仿照 Vandermonde 行列式的求法, 将第 $i \in [m-1]$ 列乘上 $-x_1$ 加到第 $i+1$ 列上, 得到

$$\text{LHS} = \begin{vmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & \binom{2}{1} x_1 - x_1 & \cdots & \binom{n-1}{1} x_1^{n-2} - \binom{n-2}{1} x_1^{n-2} \\ 0 & 0 & 1 & \cdots & \binom{n-1}{2} x_1^{n-3} - \binom{n-2}{2} x_1^{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \binom{n-1}{k_1-1} x_1^{n-k_1} - \binom{n-2}{k_1-1} x_1^{n-k_1} \\ 1 & x_2 - x_1 & x_2^2 - x_2 x_1 & \cdots & x_2^{n-1} - x_2^{n-2} x_1 \\ 0 & 1 & \binom{2}{1} x_2 - x_1 & \cdots & \binom{n-1}{1} x_2^{n-2} - \binom{n-2}{1} x_2^{n-3} x_1 \\ 0 & 0 & 1 & \cdots & \binom{n-1}{2} x_2^{n-3} - \binom{n-2}{2} x_2^{n-4} x_1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \binom{n-1}{k_2-1} x_2^{n-k_2} - \binom{n-2}{k_2-1} x_2^{n-k_2-1} x_1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \end{vmatrix} = \text{RHS}_1$$

第二步: 对第一行展开, 再运用组合恒等式 $\binom{n+1}{k+1} = \binom{n}{k+1} + \binom{n}{k}$ 化简前 $k_1 - 1$ 行, 并对第 k_1 行提取公因式 $(x_2 - x_1)$, 最终得到:

$$\text{RHS}_1 = (x_2 - x_1) \begin{vmatrix} 1 & x_1 & \cdots & x_1^{n-2} \\ 0 & 1 & \cdots & \binom{n-2}{1} x_1^{n-3} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \binom{n-2}{k_1-2} x_1^{n-k_1} \\ 1 & x_2 & \cdots & x_2^{n-2} \\ 1 & \binom{2}{1} x_2 - x_1 & \cdots & \binom{n-1}{1} x_2^{n-2} - \binom{n-2}{1} x_2^{n-3} x_1 \\ 0 & 1 & \cdots & \binom{n-1}{2} x_2^{n-3} - \binom{n-2}{2} x_2^{n-4} x_1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \binom{n-1}{k_2-1} x_2^{n-k_2} - \binom{n-2}{k_2-1} x_2^{n-k_2-1} x_1 \\ \vdots & \vdots & \vdots & \vdots \end{vmatrix} = (x_2 - x_1) \text{RHS}_2$$

第三步: 对于 RHS_2 , 将第 $k_1 + 1$ 行减去第 k_1 行, 则第 $k_1 + 1$ 行变为

$$\begin{aligned} (\text{RHS}_2)_{(k_1+1)} &= \left(0, x_2 - x_1, \binom{2}{1} x_2(x_2 - x_1), \cdots, \binom{n-2}{1} x_2^{n-3}(x_2 - x_1) \right) \\ &= (x_2 - x_1) \left(0, 1, \binom{2}{1} x_2, \cdots, \binom{n-2}{1} x_2^{n-3} \right) \end{aligned}$$

再依次将第 $k_1 + i$ 行减去第 $k_1 + i - 1$ 行 ($i = 2, 3, \cdots, k_2 - 1$), 最终得到:

$$\text{RHS}_2 = (x_2 - x_1)^{k_2-1} \begin{vmatrix} 1 & x_1 & \cdots & x_1^{n-2} \\ 0 & 1 & \cdots & \binom{n-2}{1} x_1^{n-3} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \binom{n-2}{k_1-2} x_1^{n-k_1} \\ 1 & x_2 & \cdots & x_2^{n-2} \\ 0 & 1 & \cdots & \binom{n-2}{1} x_2^{n-3} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \binom{n-2}{k_2-1} x_2^{n-k_2-1} \\ 1 & \binom{2}{1} x_3 - x_1 & \cdots & \binom{n-1}{1} x_3^{n-2} - \binom{n-2}{2} x_3^{n-3} x_1 \\ \vdots & \vdots & \vdots & \vdots \end{vmatrix} = (x_2 - x_1)^{k_2-1} \text{RHS}_3$$

即 $\text{RHS}_1 = (x_2 - x_1)^{k_2} \text{RHS}_3$.

第四步: 将上面对第 k_1 行到第 $k_1 + k_2 - 1$ 行所做的依次施加直到最后一行, 得到

$$\text{LHS} = \text{RHS}_1 = \text{RHS}_4 \prod_{i=2}^m (x_i - x_1)^{k_i} = \text{RHS}$$

因此得证. □

题 4.11. 证明

$$\det B_n(s, t) = \prod_{k \in [t]} \frac{\binom{n+s-k}{n}}{\binom{n+t-k}{n}} = \prod_{k \in [t]} \frac{(n+s-k)!}{(s-k)!} \frac{(t-k)!}{(n+t-k)!}$$

其中

$$B_n(s, t) = \begin{pmatrix} \binom{s}{t} & \binom{s}{t+1} & \cdots & \binom{s}{t+n-1} \\ \binom{s+1}{t} & \binom{s+1}{t+1} & \cdots & \binom{s+1}{t+n-1} \\ \vdots & \vdots & \ddots & \vdots \\ \binom{s+n-1}{t} & \binom{s+n-1}{t+1} & \cdots & \binom{s+n-1}{t+n-1} \end{pmatrix} \in M_n(\mathbb{Z}), \quad a_{ij} = \binom{s+i-1}{t+j-1}$$

证明. 讨论 s 和 t 的大小关系: 若 $s < t$, 则 $B_n(s, t)$ 至少有一行全为零, 故 $\det B_n(s, t) = 0 = \text{RHS}$, 等式成立.

若 $s = t$, 则 $B_n(s, s)$ 右上角全为 0, 主对角线全为 1, 故 $\text{LHS} = 1 = \text{RHS}$, 等式成立.

若 $s > t$, 则对行列式做 t 步变换. 在第 k 步时, 对第 i 行提取 $s+i-k$, 再从第 j 列提取 $(t+j-k)^{-1}$, 此时矩阵的元素变为 $a_{ij}^{(k+1)} = \binom{s+i-1-k}{t+j-1-k}$, 提取得到

$$\prod_{i \in [n]} \frac{s+i-k}{t+i-k} = \frac{(s+n-k)!}{(s-k)!} \frac{(t-k)!}{(n+t-k)!}$$

最终得到

$$B_n^{(t+1)}(s, t) = C_n^m = \begin{pmatrix} 1 & \binom{m}{1} & \cdots & \binom{m}{n-1} \\ 1 & \binom{m+1}{1} & \cdots & \binom{m+1}{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \binom{m+n-1}{1} & \cdots & \binom{m+n-1}{n-1} \end{pmatrix}, m = s - t, c_{ij} = \binom{m+i-1}{j-1}$$

对 $\det C_n^m$ 将第 i 行减去第 $i-1$ 行, 得到

$$\det C_n^m = \begin{vmatrix} 1 & \binom{m}{1} & \cdots & \binom{m}{n-1} \\ 0 & \binom{m}{1} & \cdots & \binom{m}{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \binom{m+n-2}{1} & \cdots & \binom{m+n-2}{n-2} \end{vmatrix} = \begin{vmatrix} 1 & \binom{m}{1} & \cdots & \binom{m}{n-2} \\ 1 & \binom{m+1}{1} & \cdots & \binom{m+1}{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \binom{m+n-2}{1} & \cdots & \binom{m+n-2}{n-2} \end{vmatrix} = \det C_{n-1}^m$$

而 $\det C_1^m = \det C_2^m = 1$, 因此 $\det C_n^m = 1$. 结合所求系数, 有

$$\text{LHS} = \prod_{k \in [t]} \frac{(n+s-k)!}{(s-k)!} \frac{(t-k)!}{(n+t-k)!} \det C_n^m = \text{RHS}$$

□

题 4.12. $X \in \mathbb{F}^{n \times k}, Y \in \mathbb{F}^{k \times n}$, 则 $\det(I_n + XY) = \det(I_n + YX)$

证明. 由

$$\begin{pmatrix} I_k + YX & O \\ X & I_n \end{pmatrix} \begin{pmatrix} I_k & Y \\ O & I_n \end{pmatrix} = \begin{pmatrix} I_k & Y \\ O & I_n \end{pmatrix} \begin{pmatrix} I_k & O \\ X & I_n + XY \end{pmatrix}$$

即马上得证.

□

题 4.13. 对 $A \in M_n(\mathbb{R})$ 有 $\forall i \neq j: (n-1)|a_{ij}| < |a_{ii}|$, 则 $\det A \neq 0$.

证明. 若 $\det A = 0$, 则 $AX = 0$ 有非零解 $X^0 = (x_1^0, \dots, x_n^0)^\top$, 其中 x_k^0 的模最大, 因此

$$A_{(k)} X^0 = \sum_{i \in [n]} a_{ki} x_i^0 = a_{kk} x_k^0 + \sum_{i \neq k} a_{ki} x_i^0 = 0$$

故

$$(n-1)|a_{kk}||x_k^0| = (n-1)\left|\sum_{i \neq k} a_{ki}a_i^0\right| < (n-1)|a_{kk}||x_k^0|$$

得到矛盾. □

题 4.14. $A, B \in M_n(\mathbb{R})$, 证明 (1) $\overline{\det(A + iB)} = \det(A - iB)$; (2) $\det \begin{pmatrix} A & B \\ -B & A \end{pmatrix} = |\det(A + iB)|^2$

证明. (1)

$$\overline{\det(A + iB)} = \sum_{\pi \in S_n} \varepsilon_{\pi} \prod_{i \in [n]} \overline{(a_{i, \pi(i)} + ib_{i, \pi(i)})} = \sum_{\pi \in S_n} \varepsilon_{\pi} \prod_{i \in [n]} (a_{i, \pi(i)} - ib_{i, \pi(i)}) = \det(A - iB)$$

(2)

$$\begin{aligned} \det \begin{pmatrix} A & B \\ -B & A \end{pmatrix} &= \det \begin{pmatrix} A - iB & iA + B \\ -B & A \end{pmatrix} = \det \begin{pmatrix} A - iB & O \\ -B & A + iB \end{pmatrix} \\ &= \det(A - iB) \det(A + iB) = |\det(A + iB)|^2 \end{aligned}$$

□

题 4.15. 证明

$$\det A = \begin{vmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ a_n & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1} & a_n & a_1 & \cdots & a_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_2 & a_3 & a_4 & \cdots & a_1 \end{vmatrix} = \prod_{k=1}^n \sum_{i=1}^n \varepsilon_n^{k(i-1)} a_i$$

其中 $\varepsilon_n = e^{\frac{2\pi i}{n}} = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$.

证明. 构造

$$B = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \varepsilon_n & \varepsilon_n^2 & \cdots & \varepsilon_n^n \\ \vdots & \vdots & \ddots & \vdots \\ \varepsilon_n^{n-1} & \varepsilon_n^{2(n-1)} & \cdots & \varepsilon_n^{n(n-1)} \end{pmatrix}, \quad \det B \neq 0$$

令 $f(x) = \sum_{i=1}^n a_i x^{i-1}$, 有:

$$\begin{aligned} f(\varepsilon_n^k) &= a_1 + a_2 \varepsilon_n^k + \cdots + a_n \varepsilon_n^{k(n-1)} \\ \varepsilon_n^k f(\varepsilon_n^k) &= a_n + a_1 \varepsilon_n^k + \cdots + a_{n-1} \varepsilon_n^{k(n-1)} \\ \varepsilon_n^{2k} f(\varepsilon_n^k) &= a_{n-1} + a_n \varepsilon_n^k + \cdots + a_{n-2} \varepsilon_n^{k(n-1)} \\ &\vdots \\ \varepsilon_n^{(n-1)k} f(\varepsilon_n^k) &= a_2 + a_3 \varepsilon_n^k + \cdots + a_1 \varepsilon_n^{k(n-1)} \end{aligned}$$

因此

$$\begin{aligned} (\det A)(\det B) &= \det(AB) = \det \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_n & a_1 & \cdots & a_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_2 & a_3 & \cdots & a_1 \end{pmatrix} \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \varepsilon_n & \varepsilon_n^2 & \cdots & \varepsilon_n^n \\ \vdots & \vdots & \ddots & \vdots \\ \varepsilon_n^{n-1} & \varepsilon_n^{2(n-1)} & \cdots & \varepsilon_n^{n(n-1)} \end{pmatrix} \\ &= \begin{vmatrix} f(\varepsilon_n) & f(\varepsilon_n^2) & \cdots & f(\varepsilon_n^n) \\ \varepsilon_n f(\varepsilon_n) & \varepsilon_n^2 f(\varepsilon_n^2) & \cdots & \varepsilon_n^n f(\varepsilon_n^n) \\ \vdots & \vdots & \ddots & \vdots \\ \varepsilon_n^{n-1} f(\varepsilon_n) & \varepsilon_n^{2(n-1)} f(\varepsilon_n^2) & \cdots & \varepsilon_n^{n(n-1)} f(\varepsilon_n^n) \end{vmatrix} = (\det B) \prod_{i=1}^n f(\varepsilon_n^i) \end{aligned}$$

代入 $f(\varepsilon_n^k) = \sum_{i=1}^n a_i \varepsilon_n^{k(i-1)}$, 有 $\det A = \prod_{k=1}^n \sum_{i=1}^n a_i \varepsilon_n^{k(i-1)}$. □

题 4.16 (一个行列式的计算). 求证

$$\begin{vmatrix} 1 & 0 & 0 & \cdots & 0 & 1 & 0 & 0 & \cdots & 0 \\ x & x & x & \cdots & x & y & y & y & \cdots & y \\ x^2 & 2x^2 & 2^2x^2 & \cdots & 2^{m-1}x^2 & y^2 & 2y^2 & 2^2y^2 & \cdots & 2^{m-1}y^2 \\ x^3 & 3x^3 & 3^2x^3 & \cdots & 3^{m-1}x^3 & y^3 & 3y^3 & 3^2y^3 & \cdots & 3^{m-1}y^3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ x^n & nx^n & n^2x^n & \cdots & n^{m-1}x^n & y^n & ny^n & n^2y^n & \cdots & n^{m-1}y^n \end{vmatrix} = (x-y)^{m^2} (xy)^{\frac{m^2-m}{2}} \left(\prod_{i=0}^{m-1} i! \right)^2$$

其中 $n = 2m - 1$. @Unsolved

证明. □

4.2.1 结论

1. 对

$$C_n = \begin{pmatrix} a_1 & b_1 & 0 & \cdots & 0 & 0 \\ c_1 & a_2 & b_2 & \cdots & 0 & 0 \\ 0 & c_2 & a_3 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & c_{n-1} & a_n \end{pmatrix}$$

有 $\det C_n = a_n \det C_{n-1} - b_{n-1} c_{n-1} \det C_{n-2}$.

• $a_i = b_i = 1, c_i = -1$ 时有 $\det C_n = \det C_{n-1} + \det C_{n-2}$, 这是 $a_1 = a_2 = 1$ 的 Fibonacci 数列, 即

$$\det C_n = \frac{\varphi^n - (-\varphi)^{-n}}{\sqrt{5}}, \varphi = \frac{1 + \sqrt{5}}{2}$$

• $a_i = 2, b_i = c_i = \pm 1$ 时 $\det C_n = n + 1$.

2. 对 $A_n = D_n + \text{diag}(0, 1, 2, \dots, n-1)$, 其中 D_n 是全 1 的 n 阶方阵, 有 $\det A_n = (n-1)!$.

3. $\det \begin{pmatrix} A & B \\ B & A \end{pmatrix} = \det(A+B) \det(A-B)$, 由

$$\det \begin{pmatrix} A & B \\ B & A \end{pmatrix} = \det \begin{pmatrix} A+B & A+B \\ B & A \end{pmatrix} = \det \begin{pmatrix} A+B & O \\ B & A-B \end{pmatrix}$$

马上得到.

4. 若 $A \in M_n(\mathbb{R}), B \in M_m(\mathbb{R})$ 可逆, $C \in \mathbb{R}^{n \times m}$ 则 (列方程解)

$$\begin{pmatrix} A & C \\ O & B \end{pmatrix}^{-1} = \begin{pmatrix} A^{-1} & -A^{-1}CB^{-1} \\ O & B^{-1} \end{pmatrix}$$

5.

$$\begin{aligned} \det \begin{pmatrix} A & B \\ C & D \end{pmatrix} &= \begin{cases} (\det A) \det(D - CA^{-1}B) = \det(AD - ACA^{-1}B) & \text{if } \det A \neq 0 \\ (\det D) \det(A - CD^{-1}B) = \det(DA - DCD^{-1}B) & \text{if } \det D \neq 0 \end{cases} \\ &= \begin{cases} \det(AD - CB) & \text{if } AC = CA \\ \det(DA - CB) & \text{if } AB = BA \end{cases} \end{aligned}$$

6. 记 A^\vee 为 $A \in M_n(\mathbb{F})$ 的伴随矩阵, 则有

(a) 题4.7

(b) $AA^\vee = A^\vee A = (\det A)I_n$, 因此 $\det A^\vee = (\det A)^{n-1}$. $\det A \neq 0$ 时 $A^{-1} = \frac{A^\vee}{\det A}$.

(c) $(AB)^\vee = B^\vee A^\vee, (A^\top)^\vee = (A^\vee)^\top, (\lambda A)^\vee = \lambda^{n-1} A^\vee, (A^\vee)^\vee = (\det A)^{n-2} A$

最后一式分类讨论: $\det A = 0$ 时 $\text{RHS} = O$, 而 $\text{rank } A^\vee < n-1$, 因此 $\text{rank}(A^\vee)^\vee = 0, \text{LHS} = O$.

$\det A \neq 0$ 时, 有 $(A^\vee)^\vee A^\vee = A^\vee (A^\vee)^\vee = (\det A^\vee)I_n$, 因此

$$(A^\vee)^\vee = \left(\frac{A^\vee}{\det A^\vee} \right)^{-1} = (\det A^\vee)(A^\vee)^{-1} = (\det A^\vee) \frac{A}{\det A} = (\det A)^{n-2} A$$

4.3 多项式

题 4.17. $\zeta = \frac{2+i}{2-i}$ 不是 1 的 n 次根.

证明一 (by Kostrikin). 若 $\zeta^n = 1$, 则有 $(2-i)^n = (2+i)^n = (2-i+2i)^n = (2-i)^n + \sum_{k=1}^{n-1} (2-i)^k (2i)^{n-k} + (2i)^n$. 化简并提取公因式 $2-i$, 则 $(2i)^n$ 可以被表示为 $(2-i)(a+bi)$, 其中 $a, b \in \mathbb{Z}$. 两式取模, 得到 $5(a^2+b^2) = 2^{2n}, 5|2^{2n}$, 矛盾. \square

证明二 (by 江弘毅). 考虑整数数列 $a_{n+1} = 6a_n - 25a_{n-1}$, 在 $n \geq 1$ 时所有 a_n 模 5 同余, 解得 $a_n = C_1(3+4i)^n + C_2(3-4i)^n$. 注意到 $a_n = (3+4i)^n + (3-4i)^n$ 是数列的一个解, 此时 $a_n \bmod 5 = 1$, 因此 $a_n \neq 2 \cdot 5^n$, 即 $\zeta^n \neq 1$.

思路: 因为本来就是为了考察 e^{inx} 是不是 1, 于是想到归纳法, 于是想到数列递推关系. 就是考虑 $\cos(nx)$ 的通项公式 $a_{n+1} - 2\cos x a_n + a_{n-1} = 0$ (解得 $a_n = C_1 e^{inx} + C_2 e^{-inx}$), 然后假设 $\cos x \in \mathbb{Q}$ 时可以写成 $p^n a_n = b_n \in \mathbb{Z}$, 接下来考察 $b_n \bmod p$ 就能判断 a_n 能不能再次取到 1. \square

证明三 (by 瓶子). 由下题立得. \square

题 4.18 (Niven 定理). $(a \in \mathbb{Q} \wedge \cos(a\pi) \in \mathbb{Q}) \iff \cos(a\pi) = 0, \pm \frac{1}{2}, \pm 1 \iff a = 2k \pm (0, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, 1), k \in \mathbb{Z}$.

证明一. 由

$$\cos nx = \sum_{k=0}^{\lfloor n/2 \rfloor} (-1)^k \binom{n}{2k} \cos^{n-2k} x \sin^{2k} x = \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k} \cos^{n-2k} x (\cos^2 x - 1)^k$$

令 $x = a\pi = \frac{m\pi}{n} (m \perp n), t = \cos \frac{m\pi}{n}$, 即有方程

$$\cos(m\pi) = \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k} t^{n-2k} (t^2 - 1)^k$$

这是一个在 \mathbb{Q} 上的多项式, 其 $\text{LHS} = \pm 1$ 依赖 m 的奇偶性.

若其有有理根 $t = \frac{q}{p} (p \perp q, 0 < p \leq q)$, 则 $p|a_n, q|a_0$, 其中 $a_n = \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k} = 2^{n-1}$, 故 $p = 2^s (s \in [n-1]^*)$.

考虑 x 的二倍角 $t_2 = \cos 2x = \cos \frac{2m\pi}{n}$, 无论 $t = \frac{q}{2^s}$ 是方程在 $\text{LHS} = \pm 1$ 时的解, t_2, t_{2^2}, \dots 都是方程在 $\text{LHS} = \cos(2m\pi) = 1$ 时的解. 由于方程 n 次项不变, 故仍有形式

$$t_2 = \frac{q_2}{2^{s_2}}, \quad t_4 = 2t_2^2 - 1 = \frac{q_2^2 - 2^{2s_2-1}}{2^{2s_2-1}} = \frac{q_4}{2^{s_4}}, \quad (q_2, q_4 \in \mathbb{Z}, s_2, s_4 \in [n-1]^*)$$

又由于 $q_2 \perp 2^{s_2}$, 则有 $s_4 = 2s_2 - 1$.

若 $s_2 > 1$, 则 $1 < s_2 < 2s_2 - 1 = s_4, s_{2^k} = 2^{k-1}(s_2 - 1) + 1$. 因此必然有 $k < n$ 使得 $s_{2^k} \geq n-1$, 而这与 $s_{2^k} \in [n-1]^*$ 矛盾. 因此 $s_2 = 1$, 即 $s = 1, p = 2$.

此时 $t = \frac{q}{p}$ 仅有可能 $0, \pm \frac{1}{2}, \pm 1$, 容易验证此时的 $a \in \mathbb{Q}$ 为题上数值. \square

证明二. Niven 定理的证明 \square

证明三 (by 江弘毅). 若 $\cos \theta = q/p, p \perp q$, 考察 $a_n = \cos(nx)$, 有 $a_{n+1} - 2 \cos x a_n + a_{n-1} = 0$.

(1) 若 $p > 1$ 是奇数, 令 $b_n = p^n a_n, b_0 = 1, b_1 = q$, 则 $b_{n+1} = 2qb_n - p^2 b_{n-1} \equiv_p 2qb_n \equiv_p 2^n q^{n+1}$. 由于 $2 \perp p \perp q$, 因此 $2^{n-1} q^n \perp p, b_n = sp + 2^{n-1} q^n \perp p$, 故 $b_n/p^n \notin \mathbb{Z}, a_n \neq 1$.

(2) 若 $p = 2k, k > 1$, 则 $k \perp q$. 取 $b_n = 2k^n a_n, b_1 = q, b_{n+1} = qb_n - k^2 b_{n-1} \equiv_k q^{n+1}$, 由于 $k \perp q$, 因此 $b_n \perp k, b^n/k^n \notin \mathbb{Z}, a_n = \frac{b_n}{2k^n} \notin \mathbb{Z}$.

(3) 因此, $p = 1 \vee p = 2$, 即 $\cos \theta = 0, \pm 1/2, \pm 1$ 时存在 $\cos(n\theta) = 1$. \square

题 4.19. \mathbb{F} 是域, 环 $\mathbb{F}[X]$ 的使 $\varphi(\mathbb{F}) = \mathbb{F}$ 的自同构 $\varphi \in \text{Aut}(\mathbb{F})$ 构成的群同构于变换群 $X \mapsto aX + b, a, b \in \mathbb{F}, a \neq 0$. @Unsolved

证明. \square

题 4.20. $f, g \in \mathbb{Z}[X]$ 是首一多项式, 证明存在 $u, v \in \mathbb{Z}[X]$ 且 $\deg u < \deg g, \deg v < \deg f$ 使得 $\gcd(f, g) = fu + gv$.

证明. 若有 $u, v \in \mathbb{Z}[X]$ 使得 $\gcd(f, g) = fu + gv$, 则由 f, g 是首一的, 有

$$\deg fu = \deg f + \deg u = \deg gv = \deg g + \deg v \geq \deg \gcd(f, g)$$

若有 $\deg u \geq \deg g$ 或 $\deg v \geq \deg f$, 上式取 $>$. 此时考察首项系数有

$$f_{\deg f} u_{\deg u} + g_{\deg g} v_{\deg v} = u_{\deg u} + v_{\deg v} = 0$$

由于 $u' = u + kg, v' = v - kf$ 时 $\gcd(f, g) = fu' + gv'$ 仍成立, 其中 $k \in \mathbb{Z}[X]$ 且

$$\deg u = \deg kg = \deg k + \deg g$$

$$\deg v = \deg f + \deg u - \deg g = \deg f + \deg k$$

可以选取 k 使得首项系数有

$$u'_{\deg u} = u_{\deg u} + k_{\deg k} g_{\deg g} = u_{\deg u} + k_{\deg k} = 0$$

$$v'_{\deg v} = v_{\deg v} - k_{\deg k} f_{\deg f} = v_{\deg v} - k_{\deg k} = 0$$

这样就得到 $u', v' \in \mathbb{Z}[X]$ 使得 $\deg u' < \deg u, \deg v' < \deg v$. 反复操作, 可以得到 u, v 使 $\deg u < \deg g, \deg v < \deg f$ 满足. \square

5 抽象代数

题 5.1. 对二元运算 \oplus 若有 $\forall x, y \in X : (x \oplus y) \oplus y = x, x \oplus (x \oplus y) = y$, 则 \oplus 交换.

证明. 记 $z = x \oplus y$, 则 $y \oplus (x \oplus y) = y \oplus z = (x \oplus z) \oplus z = x$. 同理 $(x \oplus y) \oplus x = y$. 因此 $x \oplus y = (y \oplus (y \oplus x)) \oplus y = y \oplus x$. \square

5.1 群

本档中所有置换乘法均与函数复合相同, 属于从右到左的运算.

题 5.2. 有限群 G 有一个 2 阶自同构 $\varphi(\varphi^2 = 1)$, 其没有非平凡不动点 ($\varphi(a) = a \iff a = e$), 则 G 交换, 且 $|G|$ 是奇数.

证明. 考虑 $f : a \mapsto \varphi(a)a^{-1}$, 有

$$\varphi(a)a^{-1} = \varphi(b)b^{-1} \implies \varphi(b)^{-1}\varphi(a) = b^{-1}a \implies b^{-1}a = e \implies b = a$$

因此 f 是单射, 又由于 G 有限, 因此 f 是双射, 即 $\forall g \in G \exists a \in G : g = \varphi(a)a^{-1}$. 但

$$\varphi(g) = \varphi(\varphi(a)a^{-1}) = \varphi^2(a)\varphi(a)^{-1} = a\varphi(a)^{-1} = g^{-1}$$

因此 $\varphi : g \mapsto g^{-1}$.

因此 (1) $ab = \varphi(a^{-1})\varphi(b^{-1}) = \varphi(a^{-1}b^{-1}) = ba$, (2) 由于 $g = g^{-1} \iff g = e$, 因此 $G = \{e; g_1, g_1^{-1}, g_2, g_2^{-1}, \dots\}$, 即 $|G|$ 是奇数. \square

题 5.3. 若 $S \subset G = \langle S \rangle := \bigcap_{G_i \subset S \text{ 是群}} G_i$, 则 $\forall g \in G : g = t_1 t_2 \cdots t_n$, 其中 $t_i \in S$ 或 $t_i^{-1} \in S$.

证明. 即证明 $G' = \langle t_1 t_2 \cdots t_n | t_i \in S \vee t_i^{-1} \in S \rangle = \langle S \rangle$, 因为 $g \in G' \implies g = t_1 \cdots t_n$.

首先显然有 $S \subset \{t_1 t_2 \cdots t_n | t_i \in S \vee t_i^{-1} \in S\}$, 因此 $\langle S \rangle < G'$. 其次, 对含 S 的群 G_i 一定有 $t_i \in S \vee t_i^{-1} \in S \implies t_i \in G_i$, 因此 $t_i \in \bigcap_{G_i \subset S \text{ 是群}} G_i$, 即

$$\forall g' \in G' : g' = t_1 t_2 \cdots t_n \in \bigcap_{G_i \subset S \text{ 是群}} G_i \implies G' < \langle S \rangle$$

因此得证. □

题 5.4. S 张成的么半群 $M = \langle S \rangle_{\text{monoid}} := \bigcap_{M_i \subset S \text{ 是么半群}} M_i$ 中 $s \in S$ 在 M 中可逆, 则 M 是群.

证明. 易知 M 中所有可逆元成群 $\text{Inv}(M)$ 且 $S \subset \text{Inv}(M) \subset M$, 而 $\text{Inv}(M)$ 也是一个么半群, 故 $M \subset \text{Inv}(M)$, 因此 $M = \text{Inv}(M)$ 是一个群. □

题 5.5. 若对么半群 $G, \forall a, b \in G : ax = b, ya = b$ 均有唯一解, 则 G 为群.

证明. 取 $b = e$, 则记 $ax = e, ya = e$ 的解为 a_1^{-1}, a_2^{-1} , 显然两者相等, 即 a^{-1} . 由于 a 的任意性, 因此任意元素均有逆, 即得证. □

题 5.6. 交换群 G 中 $|a| = s, |b| = t$, 则 $|ab| = \gcd(s, t)$. 若群不交换则 $|ab|$ 可能无限.

证明. $(ab)^k = a^k b^k = e \implies s|k \wedge t|k$, 故 $k \in \{ns + mt | n, m \in \mathbb{Z}\}$, 而 $\gcd(s, t) = \min \{ns + mt | n, m \in \mathbb{Z}\} \cap \mathbb{N}_+ = |ab|$, 得证.

群不交换时考虑 ${}_2(\mathbb{Z})$ 中 $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$, 则 $AB = \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}, BA = \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix}, (AB)^n = (-1)^n \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}, (BA)^n = (-1)^n \begin{pmatrix} 1 & 0 \\ -n & 1 \end{pmatrix}$, 因此 $\langle AB \rangle$ 和 $\langle BA \rangle$ 都是无限循环群. □

题 5.7. $S_n = \langle (12), (13), \dots, (1n) \rangle = \langle (12), (12 \cdots n) \rangle$

证明. 首先, 已知任意置换 π 可以写成对换的乘积 $\pi = \prod \tau_i$, 而 $(ij) = (1i)(1j)(1i)$, 故置换可以写成形如 $(1k)$ 形式对换的乘积.

其次, $(i, i+1) = (12 \cdots n)^{i-1} (12) (12 \cdots n)^{1-i}, (12 \cdots n) = (1n)(1, n-1) \cdots (12)$, 即两者之间可互相表出, 得证. □

题 5.8. $A_n = \langle (123), (124), \dots, (12n) \rangle$ (若 $n \geq 3$)

证明. 由于 3-轮换是偶置换, 因此其生成的置换也是偶置换, 故 $\text{LHS} \supset \text{RHS}$, 即只需要证明任意偶置换可以被形如 $(12k)$ 的轮换表出. 又由于偶置换可以分解为偶数个对换的积, 由结合性可知只需讨论任意两对换的积可以被这样表出.

两对换的积 $(st)(mn) (s \neq t \wedge m \neq n)$ 有如下分类讨论:

1. s, t 中有 2 个数与 m, n 相同: 则 $(st)(mn) = (1)$
2. s, t 中仅有 1 个数与 m, n 相同: $(st)(mn)$ 可记作 $(st)(sm)$. 分类讨论 s, t, m 的大小关系, 有

$$\begin{aligned} (st)(sm) &= (ij)(ik) \vee (ik)(ij) \vee (ji)(jk) \vee (jk)(ji) \vee (ki)(kj) \vee (kj)(ki) \\ &= (ikj) \vee (ijk) \vee (jki) \vee (jik) \vee (kji) \vee (kij) \\ &= (ijk) \vee (ijk)^{-1} \end{aligned}$$

其中 $i < j < k$, 故 $(st)(sm)$ 可被 (ijk) 表示.

- (a) 若 $i = 1, j = 2$, 则 $(ijk) = (12k)$
- (b) 若 $i = 1, j > 2$, 则 $j, k > 2, (ijk) = (1jk) = (1k)(1j) = [(1k)(12)][(12)(1j)] = (12k)(12j)^{-1}$
- (c) 若 $i = 2$, 则 $j, k > 2, (ijk) = (2jk) = (2k)(2j) = (12k)^{-1}(12j)$

- (d) 若 $i > 2$, 则 $i, j, k > 2, (ijk) = (ik)(ij) = (1ki)(1ij) = (12i)(12k)^{-1}(12j)(12i)^{-1}$
3. s, t 与 m, n 完全不相同: 分类讨论四者的大小关系, 有 $(st)(mn) = (ij)(kl) \vee (ik)(jl)$, 其中 $i < j < \min\{k, l\}$.
- (a) 若 $i = 1, j = 2$, 则 $k, l > 2$
- i. $(ij)(kl) = (12)(kl) = (12k)^{-1}(1kl) = (12k)^{-1}(12l)(12k)^{-1}$
- ii. $(ik)(jl) = (1k)(2l) = (12k)(12l)$
- (b) 若 $i = 1, j > 2$, 则 $j, k, l > 2, (ij)(kl) = (1j)(kl) = (12j)(12)(kl) = (12j)(12k)^{-1}(12l)(12k)^{-1}, (ik)(jl)$ 同理
- (c) 若 $i = 2$, 则 $j, k, l > 2, (ij)(kl) = (2j)(kl) = (12j)^{-1}(12k)^{-1}(12l)(12k)^{-1}, (ik)(jl)$ 同理
- (d) 若 $i > 2$, 则 $i, j, k, l > 2, (ij)(kl) = (12)(ij)(12)(kl) = (12i)^{-1}(12j)(12i)^{-1}(12k)^{-1}(12l)(12k)^{-1}$

□

题 5.9. 对 $\pi = (12 \cdots n) \in S_n, \pi^k$ 是 $d = \gcd(n, k)$ 个不交循环的积, 且每个循环长度均为 $q = n/d$.

证明. 由于 $\pi^k : i \mapsto k + i, i \in [n], k \in [n]^*$ 在有限集上, 因此必然有 $s \in \mathbb{N}_+$ 使得 $(\pi^k)^s = e$, 而 $|\pi| = n$, 因此 $n|ks, |\pi^k| = \min\{s \in \mathbb{N}_+ : n|ks\} = \min\{ks \in \mathbb{N}_+ : n|ks, k|ks\} / k = \text{lcm}(n, k) / k = q$.

对 $\forall i \in [n]$, 其所属循环即 $i \mapsto k + i \mapsto \cdots \mapsto lk + i \equiv_n i$, 即 $n|lk$, 而循环的长度 $\min\{l : n|lk\} = q$. 由任意性可知共有 $n/q = d = \gcd(n, k)$ 个循环. □

题 5.10. $\pi \in S_n$ 有循环分解 $\pi = \prod \pi_k$, 则 $|\pi| = \text{lcm}\{|\pi_k| : k \in [d]\}$.

证明. 有 $\pi^{|\pi|} = \left(\prod \pi_k\right)^{|\pi|} = \prod \pi_k^{|\pi|} = e$, 因此 $\forall k \in [d] : |\pi_k| \mid |\pi|$, 即 $|\pi| \in \Pi = \{p \in \mathbb{N}_+ : \forall k \in [d], |\pi_k| \mid p\}$, 只需证 $|\pi| = \min\{p : p \in \Pi\} = \text{lcm}\{|\pi_k| : k \in [d]\}$. 若 $\exists p \in \Pi : p < |\pi|$, 则 $\pi^p = \prod \pi_k^p = e \implies |\pi| \leq p$, 矛盾. □

题 5.11. 举出例子: $A, B \in M_n(\mathbb{R}), \exists m \in \mathbb{Z} : (AB)^m = I_n \neq (BA)^m$. @Unsolved

证明. □

题 5.12. 4 阶群均交换, 且同构意义上仅有 V_4 和 \mathbb{Z}_4 .

证明. 记群为 G , 可知 $\forall g \in G : g^4 = e$, 故 $|x| \mid 4$.

若群中有元素 x 的阶为 4, 则 $G = \{e, x, x^2, x^3\} \cong \mathbb{Z}_4$, 这是一个交换群.

若群中没有元素的阶为 4, 即 $\forall a \in G : a^2 = e$ (因为不可能 $a^1 = e$ 或 $a^3 = e$), 则有

$$abab = e \implies ab = b^{-1}a^{-1} = b(b^{-1})^2(a^{-1})^2 = beea = ba$$

因此这也是交换群, 这就是 V_4 . □

5.1.1 结论

1. 偶数阶群必有 2 阶元
2. $\langle \mathbb{P} \rangle = (\mathbb{Q}_+, \cdot)$ 且没有有限生成集生成后者
3. 有限群可以 (通过 Caylay 定理) 嵌入 (即存在单同态) 仅有两个生成元的有限群

5.2 环

题 5.13. 证明 $(2^X, \triangle, \cap)$ 是一个含么交换环, 并求么.

证明. $A \triangle B = (A + B)(A^c + B^c) = AB^c + BA^c$, 因此

$$\begin{aligned} A \triangle (B \triangle C) &= (A(B \triangle C)^c) + ((B \triangle C)A^c) = (A[(BC^c) + (CB^c)]^c) + [(BC^c) + (CB^c)]A^c \\ &= (A(BC^c)^c(CB^c)^c) + (BC^cA^c) + (CB^cA^c) = (A(C + B^c)(B + C^c)) + (BC^cA^c) + (CB^cA^c) \\ &= ABC + AB^cC^c + A^cBC^c + A^cB^cC \\ (A \triangle B) \triangle C &= (A \triangle B)C^c + C(A \triangle B)^c = (AB^c + BA^c)C^c + C(AB^c + BA^c)^c \\ &= AB^cC^c + A^cBC^c + C(AB + A^cB^c) = ABC + AB^cC^c + A^cBC^c + A^cB^cC \end{aligned}$$

而交的结合和交换显然, 对称差的交换显然. 由 $A \triangle \emptyset = \emptyset \triangle A = AX = A$ 可知 \emptyset 是 $(2^X, \triangle)$ 的么元, 而 X 是 $(2^X, \cap)$ 的么元. \square

题 5.14. 若 $\forall x \in R: x^2 = x$, 求证环 R 交换, 并讨论 $x^3 = x$ 时的情况.

证明. (1) $x + y = (x + y)^2 = x^2 + y^2 + xy + yx = x + y + xy + yx \implies xy + yx = 0$. 而 $xy = xyxy = -xxyy = -xy \implies yx = -xy = xy$.

(2) $x^3 = x$ 时 $(x + y)^3 = x + y \implies xy^2 + x^2y + xyx + yx^2 + y^2x + yxy = 0, (x - y)^3 = x - y \implies xy^2 + y^2x + yxy = x^2y + yx^2 + xyx, @Unsolved$ \square

题 5.15. 证明或证伪 $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}(\sqrt{5})$.

证明. 若存在一个同构 $f: \mathbb{Q}(\sqrt{2}) \implies \mathbb{Q}(\sqrt{5})$, 则 $f(n \cdot a) = nf(a) = f(n)f(a) \implies n = f(n)$. 而 $2 = f(2) = f(\sqrt{2})^2$, 设 $f(\sqrt{2}) = a + b\sqrt{5}, a, b \in \mathbb{Q}$, 则有 $a^2 + 5b^2 + 2\sqrt{5}ab = 2$, 即 $ab = 0$ 且 $a^2 + 5b^2 = 2$. 由于 \mathbb{Q} 是域, 故 $ab = 0 \implies a = 0 \vee b = 0 \implies a^2 = 2 \vee b^2 = 2/5$, 最终归结为是否 $\exists a \in \mathbb{Q}: a^2 = 2$. 若存在则设 $a = m/n$ 其中 $m, n \in \mathbb{N}_+$ 互素, 有 $m^2 = 2n^2$, 故 m^2 是偶数, m 也是, 则 $2 \nmid n$, 但 $2^2 \mid m^2$, 故矛盾, 即不存在这样的有理数 a , 即不存在这样的同构. \square

题 5.16. 证明有限整环是域.

证明. 对 $\forall x \in R^* - \{1\}$ 考察 $\langle x \rangle \subset R^*$, 由 R^* 有限故一定有 $x^m = x^n (m > n > 0)$, 则 $x^{m-n}(x^n - 1) = 0, x^{m-n} = 0 \vee x^n = 1$. 而 $\langle x \rangle \subset R^*$, 故仅可能 $x^n = 1, x^{-1} = x^{n-1}$, 则 x 可逆, 即得证. \square

题 5.17. 含么交换环 R 中有 $\forall x \in R: p \cdot x = 0$, 证明 $(x + y)^q = x^q + y^q$, 其中 $q = p^m, m \in \mathbb{N}_+$.

证明. 即证明对 $m \in \mathbb{N}_+, i \in [p^m - 1], p \mid \binom{p^m}{i}$. 而 $\binom{p^m}{i} = \frac{p^m}{i} \binom{p^m - 1}{i - 1}$, 其中后者是整数, 而 $i \in [p^m - 1]$ 的 p 次项 (p 的重数) 必然 $< m$, 因此 $p \mid \frac{p^m}{i} \binom{p^m - 1}{i - 1} = \binom{p^m}{i}$, 得证. \square

题 5.18. 5 元环在同构意义下仅有 \mathbb{Z}_5 和零乘法环两个.

证明. 考虑环 R 的交换加法群 $(R, +, 0)$, 由其势为 5, 故其群同构于 \mathbb{Z}_5 , 记为 $\{0, a, 2a, 3a, 4a\}$. 因此有 $ma + na = (m + n \bmod 5)a, ma \cdot na = (mn \bmod 5)a^2$.

若 R 含么 $ka = 1$, 则 $k^2 \bmod 5 = k, a^2 = a$, 在 $[4]$ 中仅有 $k = 1$ 符合条件, $a = 1, R = \{0, 1, 2, 3, 4\}$, 且乘法与 \mathbb{Z}_5 的相同, 故 $R \cong \mathbb{Z}_5$. 若 R 不含么, 则有 $(ka)^2 = (k^2 \bmod 5)a^2 = 0$, 即 $a^2 = 0$, 故任意元素的积为零, 即零乘法环. \square

题 5.19. (1) 含么环 R 中 x 幂零, 则 $1 - x$ 可逆; (2) \mathbb{Z}_m 中有幂零元 $\iff \exists a \in \mathbb{N}_+ - \{1\}, a^2 \mid m$.

证明. (1) $(1 - x)^{-1} = 1 + x + \dots + x^{n-1}$, 容易验证.

(2) \Leftarrow : 若 $m = a^2s, s \in \mathbb{N}_+$, 则取 $as \in \mathbb{Z}_m, (as)^2 = a^2s^2 = ms = 0$.

\implies : 若有幂零元 $x^n = 0 \wedge a = x^{n-1} \neq 0$, 其中 $n \geq 2$, 有 $a^2 = x^{2n-2} = x^n x^{n-2} = 0$, 即 $a^2 \mid m$. \square

题 5.20. 无限含么环 R 中非零不可逆元有无限多个.

证明. 反证, 若仅有有限多个, 设其全体为 $N = \{a_1, \dots, a_n\}$, 取全体可逆元 $X = R - N - \{0\}$ 有 $\forall x \in X, \rho_x: N \implies N, a_i \mapsto xa_i$. 首先 $xa_i = xa_j \iff x^{-1}xa_i = x^{-1}xa_j = a_i = a_j, \forall a_i \in N \exists a_j = x^{-1}a_i \in N: \rho_x(a_j) = a_i$, 故 ρ_x 是在 N 上的双射, 即 $\{\rho_x: x \in X\}$ 到 S_n 有一个嵌入. 而前者是一个无限集, 故有无限多对不同的 $x_i, x_j \in X$ 使得 $\rho_{x_i} = \rho_{x_j}, \rho_{x_i - x_j} = 0$, 矛盾, 故 $x_i - x_j \in N$. 固定一个 x 任取 y 使得 $x - y \in N, y$ 在一个无穷集内取, 故 N 无限, 矛盾. \square

题 5.21. 含么环 R 中若有 $1 - ab$ 可逆则 $1 - ba$ 可逆, 且 $(1 - ba)^{-1} = 1 + b(1 - ab)^{-1}a, (1 - ab)^{-1} = 1 + a(1 - ba)^{-1}b$.

证明. 注意到 $a(1-ba) = (1-ab)a$, 因此考虑 $(1-ab)^{-1}a(1-ba) = a$, 即 $b(1-ab)^{-1}a(1-ba) = ba = 1 - (1-ba)$, 移项得到 $(1-b(1-ab)^{-1}a)(1-ba) = 1$. 直接验证:

$$\begin{aligned}(1-ba)(1-ba)^{-1} &= (1-ba)(1+b(1-ab)^{-1}a) \\ &= 1+b(1-ab)^{-1}a-bab(1-ab)^{-1}a-ba \\ &= 1-ba+b(1-ab)(1-ab)^{-1}a = 1\end{aligned}$$

调换 a, b 即得另一式. □

题 5.22. 证明 $GL(3^3) = \{a + bi : a, b \in \mathbb{Z}_3\}$ 构成 9 元域, 且 $GL(3^3)^*$ 是 8 阶循环群.

证明. 由于 $(GL(3^3), +, 0) \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3$, 故交换加法群得证. 可以验证 $a = 1+i$ 生成的循环群 $\langle a \rangle = \{1+i, 2i, 1+2i, 2, 2+2i, i, 2+i, 2+GL(3^3)^*$. 分配性易证. 下给出 $GL(3^3)^*$ 关于加法和乘法的 Caylay 表 (由于 0 的运算是平凡的).

另外应该注意到, $a + bi$ 到 $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ 有一个同构关系, 因此也可以写成 $M_2(\mathbb{Z}_3)$ 上的域.

实际上 $GL(9)$ 描述的是 $x^9 = x$ 的根之间的关系, 更换写法变成:

$$\begin{aligned}\{0, \varepsilon_8, \varepsilon_8^2, \dots, \varepsilon_8^8 = 1\} &= \left\{0, \frac{1+i}{\sqrt{2}}, i, -\frac{1-i}{\sqrt{2}}, -1, -\frac{1+i}{\sqrt{2}}, -i, \frac{1-i}{\sqrt{2}}, 1\right\} \\ &\cong \{0, 1+i, 2i, 1+2i, 2, 2+2i, i, 2+i, 1\}\end{aligned}$$

其中的加法和乘法也应当是原本在 \mathbb{C} 上的形式. □

6 概率论

题 6.1. 已知若独立变量 $\xi, \eta \sim N(0, 1)$, 则 $\rho = \sqrt{\xi^2 + \eta^2}$ 服从 Rayleigh Distribution (分布函数为 $R(r) = I_{[0, +\infty)}(r)re^{-\frac{r^2}{2}}$), $\phi \sim U[0, 2\pi]$.

证明. □

题 6.2 (Box-Muller 变换). 若有独立同分布 $U_1, U_2 \sim U[0, 1]$, 求证

$$\xi = \frac{\cos(2\pi U_2)}{\sqrt{-2 \ln U_1}} \sim N(0, 1) \quad \eta = \frac{\sin(2\pi U_2)}{\sqrt{-2 \ln U_1}} \sim N(0, 1)$$

且相互独立, 并说明 ξ 和 η 是如何构造的.

证明. 这是 **Box-Muller 变换**, 主要思路是将两个独立的正态分布在二维平面上作极坐标变换 $X = R \cos \theta, Y = R \sin \theta$, 即 $R^2 = X^2 + Y^2, \theta = \arctan \frac{Y}{X}$, 本质公式即为

$$\int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} \frac{1}{2\pi} \exp\left(-\frac{X^2 + Y^2}{2}\right) dX dY = \int_0^{2\pi} \frac{1}{2\pi} d\theta \int_0^{+\infty} e^{-R^2/2} R dR = 1$$

因此有分布函数 $\Pr\{R < r\} = \int_0^r e^{-R^2/2} R dR = 1 - e^{-r^2/2}, \Pr\{\theta < \phi\} = \frac{\phi}{2\pi}$, 其中 $r \in [0, +\infty), \theta \in [0, 2\pi]$. 因此可以取 $F_R(r) = 1 - e^{-r^2/2}, F_\theta(t) = \frac{t}{2\pi}$.

已知: 若随机变量 $\xi \sim F(x)$, 则对 C^1 函数 $g(\cdot)$, 在定义域内 $g(\xi) \sim F \circ g^{-1}(x)$.

由于 $R \sim F_R(x)$, 故 $U_0 = F_R(R) = 1 - e^{-R^2/2} \sim U[0, 1], R = \sqrt{-2 \ln(1 - U_0)}$, 再取 $U_1 = 1 - U_0$ 即有 $R = \sqrt{-2 \ln U_1}$. 再取 $U_2 = \frac{\theta}{2\pi}$, 代入变换即可. □

题 6.3. 求证 $\sum_{i=0}^N \binom{N+k}{k} 2^{-k} = 2^N$.

证明. 首先 $N = 1$ 时 $\binom{1}{0}2^0 + \binom{2}{1}2^{-1} = 2^1$, 等式成立. 再设等式在 $N = n$ 时成立, 求证 $N = n + 1$ 时是否成立.

$$\begin{aligned}\sum_{k=0}^{n+1} \binom{n+1+k}{k} 2^{-k} &= 1 + \sum_{k=1}^{n+1} \left(\binom{n+k}{k} + \binom{n+k}{k-1} \right) 2^{-k} \\ &= 1 + \sum_{k=0}^n \binom{n+k}{k} 2^{-k} - 1 + \binom{2n+1}{n+1} 2^{-n-1} + \sum_{k=1}^{n+1} \binom{n+k}{k-1} 2^{-k}\end{aligned}$$

应用假设条件 $\sum_{k=0}^n \binom{n+k}{k} 2^{-k} = 2^n$, 有

$$\sum_{k=0}^{n+1} \binom{n+1+k}{k} 2^{-k} = 2^n + \binom{2n+1}{n+1} 2^{-n-1} + \sum_{i=0}^n \binom{n+k+1}{k} 2^{-k-1}$$

注意到 $\binom{n+k+1}{k} 2^{-k-1} = \frac{1}{2} \binom{n+1+k}{k} 2^{-k}$, 以及

$$\sum_{k=0}^{n+1} \binom{n+1+k}{k} 2^{-k} = \sum_{k=0}^n \binom{n+1+k}{k} 2^{-k} + \binom{2n+2}{n+1} 2^{-n-1} = \sum_{k=0}^n \binom{n+1+k}{k} 2^{-k} + \frac{1}{2} \binom{2n+1}{n+1} 2^{-n-1}$$

则最终得到 $\frac{1}{2} \sum_{k=0}^{n+1} \binom{n+1+k}{k} 2^{-k} = 2^n$, 即 $\sum_{k=0}^{n+1} \binom{n+1+k}{k} 2^{-k} = 2^{n+1}$, 得证, 因此对 $\forall N \in \mathbb{N}^*$ 等式均成立. \square

题 6.4. 若某系统中每个元件正常工作概率为 $p \in [0, 1]$, 有半数元件正常则系统可工作, 求 p 在什么范围时 $2k + 1$ 个元件的系统比 $2k - 1$ 个的好. @Unsolved

证明. \square

题 6.5 (赌徒问题). 若甲乙各剩 n, m 局赢得赌局, 则应以 $p_{\text{甲}} : 1 - p_{\text{甲}}$ 的比例分赌注, 其中 $p_{\text{甲}}$ 为甲赢得赌局的概率. 设 p 为甲每局胜的概率, 记 $q = 1 - p$, 有:

1. 因甲最早在 n 局后赢, 最晚在 $n + m - 1$ 局后赢, 因此只需计算甲在 $n + k$ 局下赢 n 局的概率之和, 即

$$\sum_{k=0}^{m-1} f(n+k; n, p) = \sum_{k=0}^{m-1} \binom{n+k-1}{k} p^n q^k$$

2. 由于 $p_{\text{甲}} + p_{\text{乙}} = 1$, 因此同理可得 $1 - \sum_{k=0}^{n-1} f(m+k; m, q) = \sum_{k=n}^{\infty} \binom{m+k-1}{k} p^k q^m$

3. 由于后面 $n + m - 1$ 局一定可以决定胜负, 即只需在后 $n + m - 1$ 局中至少赢 n 局, 即

$$\sum_{k=n}^{n+m-1} f(n+m-1; k, p) = \sum_{k=n}^{n+m-1} \binom{n+m-1}{k} p^k q^{n+m-1-k}$$

求证上面三式相等. 其中 $f(k; r, p) = \binom{k-1}{r-1} p^{r-1} q^{k-r}$ 表示 Pascal 分布, 即 Bernoulli 试验中第 r 个成功发生在第 k 次试验时的概率. @Unsolved

证明. \square

6.0.1 结论

1. 随机变量 $\xi \sim \chi_m^2, \eta \sim \chi_n^2$ 相互独立, 求证 $\alpha = \xi + \eta \sim \chi_{m+n}^2, \beta = \frac{\xi/m}{\eta/n} \sim F(m, n)$ 且相互独立.
2. 若 $\xi = (\xi_1, \xi_2)^T$ 的密度函数为 $p(x_1, x_2)$, 而 $(\eta_1, \eta_2)^T = \eta = A\xi, A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, 则 η 的密度函数 $q(y_1, y_2)$ 为:

$$q(y_1, y_2) = \frac{p\left(\frac{dy_1 - by_2}{\det A}, \frac{-cy_1 + ay_2}{\det A}\right)}{|\det A|}$$

3. 若 $\xi = (\xi_1, \xi_2)^\top \sim N_2(\mu, \Sigma)$, 其中 $\mu = (0, 0)^\top, \Sigma = \begin{pmatrix} \sigma_1^2 & \rho\sigma_1\sigma_2 \\ \rho\sigma_1\sigma_2 & \sigma_2^2 \end{pmatrix}, |\Sigma| = \sigma_1^2\sigma_2^2(1 - \rho^2)$, 其密度函数为

$$p(x_1, x_2) = \frac{1}{2\pi\sqrt{|\Sigma|}} \exp\left(-\frac{x\Sigma^{-1}x^\top}{2|\Sigma|}\right) = \frac{1}{2\pi\sqrt{|\Sigma|}} \exp\left(-\frac{\sigma_2^2x_1^2 + \sigma_1^2x_2^2 - 2\rho\sigma_1\sigma_2x_1x_2}{2|\Sigma|}\right)$$

现有旋转矩阵 $A_\alpha = \begin{pmatrix} \cos \alpha & \sin \alpha \\ -\sin \alpha & \cos \alpha \end{pmatrix}$ 使 $(\eta_1, \eta_2)^\top = \eta = A_\alpha \xi$, 则使用上条结论, η 的密度函数为

$$q(y_1, y_2) = p(y_1 \cos \alpha - y_2 \sin \alpha, y_1 \sin \alpha + y_2 \cos \alpha) = \frac{1}{2\pi\sqrt{|\Sigma|}} \exp\left(-\frac{Ay_1^2 - 2By_1y_2 + Cy_2^2}{2|\Sigma|}\right)$$

其中

$$A = \sigma_2^2 \cos^2 \alpha - 2\rho\sigma_1\sigma_2 \cos \alpha \sin \alpha + \sigma_1^2 \sin^2 \alpha$$

$$B = \sigma_2^2 \cos \alpha \sin \alpha - \rho\sigma_1\sigma_2(\sin^2 \alpha - \cos^2 \alpha) - \sigma_1^2 \cos \alpha \sin \alpha$$

$$C = \sigma_2^2 \sin^2 \alpha + 2\rho\sigma_1\sigma_2 \cos \alpha \sin \alpha + \sigma_1^2 \cos^2 \alpha$$

进一步, 若选取 α 使得 $\tan(2\alpha) = \frac{2\rho\sigma_1\sigma_2}{\sigma_1^2 - \sigma_2^2}$, 则 $B = 0$, 即 η_1, η_2 独立.

7 组合数学

题 7.1 (Bernoulli 信封匹配问题). n 阶对称群 S_n 中, 对 $\forall k \in [n]$ 都没有 $k \mapsto k$ 的置换有多少个?

证明. 这其实是 **Bernoulli 信封匹配问题**, 即将 n 只信封和 n 封信匹配.

我们记 A_i 为事件第 i 封信送对 (从 S_n 中所选置换 $\pi: i \mapsto i$), 以 $N(\cdot)$ 记方案数, 则

$$N_1 = N(A_i) = (n-1)!, \quad N_2 = N(A_i A_j) = (n-2)!, \quad N_n = N\left(\bigcap_{i \in [n]} A_i\right) = 1.$$

而事件 “ $\forall k \in [n]$ 都没有 $k \mapsto k$ 的置换” 即 $\overline{\bigcup_{i \in [n]} A_i}$, 因此有

$$\begin{aligned} N\left(\overline{\bigcup_{i \in [n]} A_i}\right) &= n! - N\left(\bigcup_{i \in [n]} A_i\right) = n! - \sum_{i \in [n]} (-1)^{i+1} \binom{n}{i} N_i = n! \left(1 + \sum_{i \in [n]} \frac{(-1)^i}{i!}\right) = n! \sum_{i=0}^n \frac{(-1)^i}{i!} \\ &= \text{Round}\left(\frac{n!}{e}\right) \end{aligned}$$

□

8 数论

题 8.1. x 是数码互异的三位非零正整数, $D(x), I(x)$ 分别是将 x 的数码降序和升序排列得到的整数, 求 $y = D(x) - I(x) =: F(x)$ 的不动点.

- 在 n 位时?
- 求 x 的迭代次数?

证明一. 先取 $9 \geq a > b > c \geq 0$, 有 $(100a + 10b + c) - (100c + 10b + a) = 99(a - c) = x$, 因此 $99|x$, 其十位必为 9, $a = 9$. 由于 $x = 100(a - c) - (a - c) = 100(a - c - 1) + 90 + (10 - (a - c))$, 因此其百位 $a - c - 1 = 8 - c = c$, 个位 $10 - (a - c) = 1 + c = b$, 解得 $c = 4, b = 5$, 带入得 $x = 495$. □

证明二. 设数字的数码为 abc , 其中位数为 d . 由于只有三位, 因此所得 $F(x)$ 的中间一位被抵消了 (如上, 不含 b), 因此 $b = 0(a \geq c)$ 或 $9(a < c)$, 而前者不存在, 因此 $b = 9$. 其他证明同上, 或者也可以直接验算. □