

Contents

1	抽象代数	3
1.1	群的定义问题集(MA2008)	4

Chapter 1

抽象代数

定理 1.0.1

同类置换有相同的循环结构.

解. $P, Q, T \in S_n$ 且 $Q = TPT^{-1}$, Q, P 属同类, 则 Q, P 有相同的循环结构.

$P(v) = (1^{v_1} 2^{v_2} \cdots m^{v_m})$, $P = C_1 C_2 \cdots C_r$, $r = \sum_i v_i$, $n = \sum_i i v_i$. $Q = TPT^{-1} = \prod_i T C_i T^{-1} = \prod_i C'_i$.
 T 是一一映射, $(C'_i)_i$ 两两不交, 因 $(C_i)_i$ 两两不交, C'_i 与 C_i 同阶, 所以 $Q(v) = P(v)$. □

问题 1.0.1

在环 R 中, 对于任意的 $x \in R$, 都存在 $n \in \mathbb{N}_+$, 使得 $x = x^{n+1}$, 证明: 对于任意的 $y \in R$, $yx^n = x^n y$.

解. 先证 x^n 是幂等的, $(x^n)^2 = x^n$.

再证, 若 $ab = 0$, 则 $ba = (ba)^{n+1} = b(ab)^n a = 0$.

再证, $x = x^{n+1}$, 则 $yx^n = yx^{2n}$, 所以 $(y - yx^n)x^n = 0$, 所以 $x^n(y - yx^n) = 0$, 即 $x^n y = x^n y x^n$.

最后, 同上面的做法, 由 $x^n y = x^{2n} y$, 有 $yx^n = x^n y x^n$, 所以 $x^n y = y x^n$. □

问题 1.0.2: AMM, E.C.Johnsen, D.L. Outcalt and Adil Yaqub, An Elementary Commutativity Theorem For Rings, Vol. 75, No. 3, 288-289

有么元的非结合环 R 中, 若对于任意的 $x, y \in R$, 有 $(xy)^2 = x^2 y^2$, 则 R 是交换环.

解. 由 $(xy)^2 = x^2 y^2$, $(x(y+1))^2 = x^2 y^2 + 2x^2 y + x^2$, 而 $(x(y+1))^2 = (xy+x)^2 = (xy)^2 + (xy)x + x(xy) + x^2$, 所以 $xyx + xxy + 2x^2 y$, 将 $x+1$ 代换 x 的位置, 有 $xyx + yx + xxy = 2x^2 y + xy$, 即得 $xy = yx$.

注. 含么性不可省, $R = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in \mathbb{Z} \right\}$, 或 $\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \right\} \leq \text{GF}(2)$ 有左么元.

注2. $(xy)^k = x^k y^k$ 在 $k > 2$ 时有反例, $k \geq 3$ 固定, p 素且满足: k 奇时, $p \mid k$, k 偶时, $p \mid \frac{k}{2}$.

$$R = \left\{ \begin{pmatrix} a & b & c \\ 0 & a & d \\ 0 & 0 & a \end{pmatrix} : a, b, cd \in \text{GF}(p) \right\} \leq \text{GF}(p),$$

这里的 R 不可交换. □

问题 1.0.3

R 是含么环, 若对于任意的 $x, y \in R$, 存在 $m, n \in \mathbb{N}$, 使得 $x^{m+1} y^{n+1} = x^m y x y^n$, 则 R 是交换环.

解. $x^m(xy - yx)y^n = 0$, $x^l(xy - yx)(y+1)^k = 0$, 定义 $r = \max\{m, l\}$, 则

$$x^r(xy - yx)y^n = 0, \quad x^r(xy - yx)(y+1)^k = 0, \quad (y, y+1) = 1 \implies (y^n, (y+1)^k) = 1.$$

所以 $(y^{2n-1}, (y+1)^k y^{n-1}) = y^{n-1}$, 所以存在 $A(y), B(y)$ 使得 $Ay^{2n-1} + B(y+1)^k y^{n-1} = y^{n-1}$, 所以 $x^r(xy - yx)y^{n-1} = 0$, 注意到红色部分的 y^n 得到了降次, 所以存在 s 满足 $x^s(xy - yx) = 0$.

再设 $(x+1)^t(xy - yx) = 0$, 同样辗转相除得到 $xy - yx = 0$, 即 R 可交换. □

1.1 群的定义问题集(MA2008)

问题 1.1.1

Prove that the set

$$G = \{3^k/2^{2k}; k \in \mathbb{Z}\}$$

forms a group with respect to multiplication. You may assume that multiplication is associative.

问题 1.1.2

Consider the following group of congruence classes of integers modulo 14 with respect to multiplication:

$$G = \{[1]_{14}, [3]_{14}, [5]_{14}, [9]_{14}, [11]_{14}, [13]_{14}\}$$

Given that $[1]_{14}$ is the identity of the group, find (a) the order of $[13]_{14}$, (b) the order of $[3]_{14}$, (c) the inverse of $[9]_{14}$.

问题 1.1.3

Suppose that G is a group, $x \in G$ is an element of order 3 and $y \in G$ is an element of order N . Prove that

$$(x^2yx)^N = 1$$

问题 1.1.4

Let $G = \{1, a, a^2, b, b^2, ab, ab^2, a^2b, a^2b^2\}$ be a group where $a^3 = b^3 = 1$ and $ab = ba$. (a) Find $\langle b^2 \rangle$, the subgroup of G generated by b^2 . (b) It is given that $H = \{1, ab, a^2b^2\}$ is a subgroup of G . Find the distinct right cosets of H .

问题 1.1.5

Suppose G is an abelian group with its binary operation written as multiplication. Show that the mapping $\theta : G \rightarrow G$ defined by $g\theta = g^{-1}$ is a homomorphism.

问题 1.1.6

Prove that the set of vectors

$$\left\{ \begin{pmatrix} a+b \\ a-b \\ a \end{pmatrix} : a, b \in \mathbb{R} \right\}$$

is a vector subspace of \mathbb{R}^3 . Calculate a basis and the dimension of this subspace.

问题 1.1.7

Reduce the matrix $A = \begin{pmatrix} 2 & 0 & 1 & 1 \\ 1 & 0 & -1 & 0 \\ 3 & 0 & 0 & 1 \\ 3 & 0 & -3 & 0 \end{pmatrix}$ to row-echelon form. Give a basis for the row-space of A .

问题 1.1.8

Prove that the following vector subspaces V and W of \mathbb{R}^3 are equal:

$$V = \text{span} \left(\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix} \right), \quad W = \text{span} \left(\begin{pmatrix} 0 \\ 2 \\ 4 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}, \begin{pmatrix} 5 \\ 7 \\ 9 \end{pmatrix} \right)$$

问题 1.1.9

Explain carefully which of the following functions define homomorphisms of vector spaces:

- (a) $f: \mathbb{R} \rightarrow \mathbb{R}$ defined by $f(a) = a + 1$,
 (b) $f: \mathbb{R}^2 \rightarrow \mathbb{R}$ defined by $f\begin{pmatrix} a \\ b \end{pmatrix} = a + b$,
 (c) $f: \mathcal{P}_2 \rightarrow \mathcal{P}_5$ defined by $f(a + bx + cx^2) = (1 - 3x^2 + 7x^3)(a + bx + cx^2)$.

问题 1.1.10

State the rank-nullity theorem for a homomorphism of finite-dimensional vector spaces. For any linear map $f: M_{2 \times 2}(\mathbb{R}) \rightarrow \mathbb{R}^2$, prove there are at least two linearly independent matrices $A \in M_{2 \times 2}(\mathbb{R})$ which satisfy $f(A) = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$.

问题 1.1.11

- (a) Suppose G is a finite group and g is an element of G . Define the terms i. order of G , ii. order of g .
 (b) Use Lagrange's theorem to prove the following. If G is a finite group and $g \in G$ then the order of g divides the order of G .
 (c) Now suppose that G is an abelian group and let

$$H_k = \{x \in G : x^k = 1_G\}$$

where k is a positive integer. Show that H_k is a subgroup of G .

- (d) Let G be the group with the following operation table.

	1	a	a^2	a^3	b	ab	a^2b	a^3b	b^2	ab^2	a^2b^2	a^3b^2
1	1	a	a^2	a^3	b	ab	a^2b	a^3b	b^2	ab^2	a^2b^2	a^3b^2
a	a	a^2	a^3	1	ab	a^2b	a^3b	b	ab^2	a^2b^2	a^3b^2	b^2
a^2	a^2	a^3	1	a	a^2b	a^3b	b	ab	a^2b^2	a^3b^2	b^2	ab^2
a^3	a^3	1	a	a^2	a^3b	b	ab	a^2b	a^3b^2	b^2	ab^2	a^2b^2
b	b	ab^2	a^2b	a^3b^2	b^2	a	a^2b^2	a^3	1	ab	a^2	a^3b
ab	ab	a^2b^2	a^3b	b^2	ab^2	a^2	a^3b^2	1	a	a^2b	a^3	b
a^2b	a^2b	a^3b^2	b	ab^2	a^2b^2	a^3	b^2	a	a^2	a^3b	1	ab
a^3b	a^3b	b^2	ab	a^2b^2	a^3b^2	1	ab^2	a^2	a^3	b	a	a^2b
b^2	b^2	ab	a^2b^2	a^3b	1	ab^2	a^2	a^3b^2	b	a	a^2b	a^3
ab^2	ab^2	a^2b	a^3b^2	b	a	a^2b^2	a^3	b^2	ab	a^2	a^3b	1
a^2b^2	a^2b^2	a^3b	b^2	ab	a^2	a^3b^2	1	ab^2	a^2b	a^3	b	a
a^3b^2	a^3b^2	b	ab^2	a^2b	a^3	b^2	a	a^2b^2	a^3b	1	ab	a^2

- i. Write down the elements of $H_4 = \{x \in G : x^4 = 1_G\}$.
 ii. Is H_k always a subgroup of G , even if G is not abelian? Explain your answer.

解. $H_4 = \{1, a, a^2, a^3, b, ab, a^3b, ab^2, a^3b^2\}$. 其中 $(ab)^4 = (a^2)^2 = 1$, $(a^3b)^4 = (a^2)^2 = 1$, $(ab^2)^4 = (a^2)^2 = 1$, $(a^3b^2)^4 = a^2 = 1$. \square

问题 1.1.12

(a) Suppose that

$$G = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}$$

where

$$a^4 = 1, \quad a^2 = b^2, \quad ba = a^3b$$

and

$$G' = \{1, c, c^2, c^3, d, cd, c^2d, c^3d\}$$

where

$$c^4 = d^2 = 1 \text{ and } dc = cd.$$

Construct a non-trivial homomorphism $\theta : G \rightarrow G'$. Find the image and kernel of your homomorphism.

(b) Consider the linear map $f : \mathcal{P}_2 \rightarrow \mathcal{P}_2$ defined by

$$f(a + bx + cx^2) = (a + b) + (2b + c)x + 3cx^2.$$

Find three eigenvectors of f which form a basis \mathcal{B} of \mathcal{P}_2 . Write down the following matrices and the relation between them:

- The change of basis matrix P , from \mathcal{B} to the standard basis $\{1, x, x^2\}$.
- The matrix C which represents f with respect to the standard basis.
- The matrix D which represents f with respect to the basis \mathcal{B} .

问题 1.1.13

Consider the function

$$f : \mathcal{P}_2 \longrightarrow M_{2 \times 2}(\mathbb{R})$$

defined by

$$f(a + bx + cx^2) = \begin{pmatrix} a + b & 0 \\ a - c & b + c \end{pmatrix}$$

- (a) Prove that the nullspace of f has dimension one, and give a basis $\{v\}$ for it.
- (b) Prove that the matrices $f(x)$ and $f(x^2)$ form a basis for the image of f .
- (c) Find the matrix A which represents the linear map f with respect to the standard bases for \mathcal{P}_2 and $M_{2 \times 2}(\mathbb{R})$. Using part (b), write down a basis for the column-space of this matrix.
- (d) Extend the set $\{f(x), f(x^2)\}$ to a basis \mathcal{B} for $M_{2 \times 2}(\mathbb{R})$. Write down:
 - i. the change of basis matrix P from the basis \mathcal{B} to the standard basis for $M_{2 \times 2}(\mathbb{R})$,
 - ii. The change of basis matrix Q from the basis $\{v, x, x^2\}$, where v is the polynomial you gave in part (a), to the standard basis for \mathcal{P}_2 . Show that

$$AQ = P \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Chapter 2

定理集

定理 2.0.1: 勾股定理

若 $(\alpha, \beta) = 0$, 则

$$|\alpha + \beta|^2 = |\alpha|^2 + |\beta|^2.$$

进一步的, 若向量 $\alpha_1, \alpha_2, \dots, \alpha_m$ 两两正交, 则

$$|\alpha_1 + \alpha_2 + \dots + \alpha_m|^2 = |\alpha_1|^2 + |\alpha_2|^2 + \dots + |\alpha_m|^2.$$

定理 2.0.2

若 $\alpha_1, \alpha_2, \dots, \alpha_m$ 两两正交, 则 $\alpha_1, \alpha_2, \dots, \alpha_m$ 线性无关.

定理 2.0.3: 标准正交基的存在性

在任何有限维欧式空间中, 都有标准正交基. 有限维欧式空间 V 中的任何非零正交向量组都可以扩充为 V 的一个正交基.

定理 2.0.4

两个有限维欧式空间同构的充要条件是它们的维数相同.
任何 n 维欧式空间都与欧式空间 \mathbb{R}^n 同构.

定理 2.0.5

若欧式空间 V 的子空间 V_1, V_2, \dots, V_s 两两正交, 则它们的和是直和.
反之, 子空间的和为直和时, 子空间之间不一定正交.

定理 2.0.6

设 W 是欧式空间 V 的子空间. 则 $W^\perp = \{\gamma \mid \gamma \in V, \gamma \perp W\}$ 是 V 的子空间; 当 W 是有限维时, $V = W \oplus W^\perp$, $(W^\perp)^\perp = W$.

V_1, V_2 是欧式空间 V (不一定有限维) 的两个子空间. 证明:

$$(V_1 + V_2)^\perp = V_1^\perp \cap V_2^\perp.$$

定理 2.0.7

设 T 是 n 维欧式空间 V 的一个线性变换. 则 T 是正交变换的充要条件是, T 把标准正交基变成标准正交基.

定理 2.0.8

设 s_1, s_2, \dots, s_n 是 n 维欧式空间 V 的一个标准正交基, A 是一个 n 阶实方阵, 且 $(\eta_1, \eta_2, \dots, \eta_n) = (s_1, s_2, \dots, s_n)A$. 则 $\eta_1, \eta_2, \dots, \eta_n$ 是标准正交基的充要条件是, A 为正交方阵.

定理 2.0.9

设 T 是 n 维欧式空间 V 的一个线性变换. 则 T 是正交变换的充要条件是, T 在标准正交基下的矩阵是正交矩阵. 有限维欧式空间 V 的正交变换有逆变换, 而且是 V 到 V 的同构映射. 其中充分性部分, 标准正交性的条件不可省去.

定理 2.0.10

实数域上有限维空间(不要求是欧式空间)的每一个线性变换, 都有一维或二维的不变子空间.

解. 证明分实特征根和复特征根两种情况, 复的情况对特征向量分离实虚部, 得到不变子空间的基. □

定理 2.0.11

设 T 是有限维欧式空间 V 的一个正交变换. 若子空间 W 对 T 不变, 则 W^\perp 对 T 也不变. 设 T 是有限维欧式空间 V 的一个正交变换, 则 V 可分解成对 T 不变的一维或二维子空间的直和.

定理 2.0.12

欧式空间中正交变换的特征值为 ± 1 . 正交方阵的特征根的模为 1.

定理 2.0.13

设 T 是二维欧式空间 V 的一个正交变换, 且无特征值, 则 T 在标准正交基下的矩阵具有形状

$$\begin{pmatrix} \cos \varphi & -\sin \varphi \\ \sin \varphi & \cos \varphi \end{pmatrix}.$$

定理 2.0.14

设 T 是 n 维欧式空间 V 的一个正交变换, 则存在标准正交基, 使 T 在此基下的矩阵成下面形状:

$$\begin{pmatrix} 1 & & & & & & & \\ & \ddots & & & & & & \\ & & 1 & & & & & \\ & & & -1 & & & & \\ & & & & \ddots & & & \\ & & & & & -1 & & \\ & & & & & & S_1 & \\ & & & & & & & \ddots \\ & & & & & & & & S_r \end{pmatrix}$$

其中

$$S_i = \begin{pmatrix} \cos \varphi_i & -\sin \varphi_i \\ \sin \varphi_i & \cos \varphi_i \end{pmatrix}, \quad i = 1, 2, \dots, r.$$

对于任何 n 阶正交方阵 A , 都存在正交方阵 U , 使 $U^{-1}AU$ 为上面方阵的形式.

定理 2.0.15

设 T 是 n 维欧氏空间 V 的一个线性变换. 则 T 是对称变换的充要条件是, T 在标准正交基下的矩阵为对称方阵.

定理 2.0.16

实对称方阵的特征根全是实数.

定理 2.0.17

设 T 是 n 维欧氏空间 V 的对称变换, 则 T 的属于不同特征值的特征向量相互正交.

定理 2.0.18

设 T 是 n 维欧氏空间 V 的一个对称变换, W 是对 T 不变的非零子空间, 则 W 中有关于 T 的特征向量.

如果 α 是它的一个特征向量, 则与 α 正交的全体向量是 T 的 $n-1$ 维不变子空间.

对 V 的每个对称变换 T , 都存在标准正交基, 使 T 在此基下的矩阵为对角矩阵.

对每个实对称方阵 A , 都存在正交方阵 U , 使 $U^{-1}AU$ 为对角矩阵.

任何实二次型

$$f(x_1, x_2, \dots, x_n) = X'AX$$

都可经过正交线性代换 $X = UY$ 化成

$$\lambda_1 y_1^2 + \lambda_2 y_2^2 + \dots + \lambda_n y_n^2.$$

实对称方阵 A 是正定的充要条件是, A 的特征根全是正的.

2.1 数学分析

定理 2.1.1: 关于有界, 无界的充分条件

- (1) $\lim_{x \rightarrow x_0^-} f(x)$ 存在, 则 $\exists \delta > 0$, 当 $-\delta < x - x_0 < 0$ 时, $f(x)$ 有界; 对 $x \rightarrow x_0^+$, $x \rightarrow x_0$ 有类似结论.
- (2) $\lim_{x \rightarrow \infty} f(x)$ 存在, 则存在 $X > 0$, 当 $|x| > X$ 时, $f(x)$ 有界. $x \rightarrow \pm\infty$ 有类似结论.
- (3) $f(x) \in C[a, b]$, 则 $f(x)$ 在 $[a, b]$ 上有界.
- (4) $f(x)$ 在集 U 上有最大(小)值, 则 $f(x)$ 在 U 上有上(下)界.
- (5) 有界函数间的和, 积运算封闭.
- (6) $\lim_{x \rightarrow \square} f(x) = \infty$, 则 $f(x)$ 在 \square 的空心邻域内无界. \square 可为 $x_0, x_0^-, x_0^+, \infty, \pm\infty$.

定理 2.1.2: Stolz定理

证明: 若

- (a) $y_{n+1} > y_n (n \in \mathbb{N}_+)$;
- (b) $\lim_{n \rightarrow \infty} y_n = +\infty$;
- (c) $\lim_{n \rightarrow \infty} \frac{x_{n+1} - x_n}{y_{n+1} - y_n}$ 存在.

则

$$\lim_{n \rightarrow \infty} \frac{x_n}{y_n} = \lim_{n \rightarrow \infty} \frac{x_{n+1} - x_n}{y_{n+1} - y_n}.$$

定理 2.1.3: Cauchy定理

若函数 $f(x)$ 定义于区间 $(a, +\infty)$, 并且在每一个有限区间 (a, b) 内是有界的, 则

- (a) $\lim_{x \rightarrow +\infty} \frac{f(x)}{x} = \lim_{x \rightarrow +\infty} [f(x+1) - f(x)]$;
 (b) $\lim_{x \rightarrow +\infty} [f(x)]^{1/x} = \lim_{x \rightarrow +\infty} \frac{f(x+1)}{f(x)}, (f(x) \geq C > 0)$,

假定等是右端的极限都存在且可为 $\pm\infty$.

问题: 对于上下极限是否仍有类似结论?.

定理 2.1.4

假设 $f_n : [a, b] \rightarrow \mathbb{R}$, 每个在 $[a, b]$ 上均可积, 且 $f_n(x) \rightrightarrows f(x), n \rightarrow \infty$. 则 $f(x)$ 可积, 且

$$\int_a^b f \, dx = \lim_{n \rightarrow \infty} \int_a^b f_n \, dx.$$

解. 类似??

□

定理 2.1.5: (一致收敛级数)逐项积分

$u_k : [a, b] \rightarrow \mathbb{R}$, 对每个 $k \in \mathbb{N}_+$ 均可积, $\sum_{k=1}^{\infty} u_k(x)$ 在 $[a, b]$ 上一致收敛. 则 $f(x) = \sum_{k=1}^{\infty} u_k(x)$ 可积, 且

$$\int_a^b f(x) \, dx = \sum_{k=1}^{\infty} \int_a^b u_k(x) \, dx.$$

解. 让 $S_n(x) = \sum_{k=1}^n u_k(x)$ 并用??

□

定理 2.1.6: 逐项微分

设 $u_k : [a, b] \rightarrow \mathbb{R}, k \in \mathbb{N}_+$, 每项均有连续导数(端点处单边可微), 若有:

- (i) $\sum_{k=1}^{\infty} u_k(x_0)$ 在某些点 $x_0 \in [a, b]$ 收敛.
 (ii) $\sum_{k=1}^{\infty} u'_k(x)$ 在 $[a, b]$ 上一致收敛到 $f(x)$.

则

- (1) $\sum_{k=1}^{\infty} u_k(x)$ 在 $[a, b]$ 上收敛且和函数 $F(x) = \sum_{k=1}^{\infty} u_k(x)$ 在 $[a, b]$ 上可微且 $F'(x) = f(x)$.
 (2) $\sum_{k=1}^{\infty} u_k(x) \rightrightarrows F(x)$.

解. (1). u'_k 连续($k \in \mathbb{N}_+$), $\sum_{k=1}^{\infty} u'_k \rightrightarrows f$, 则 $f \in C[a, b]$, 所以 f 在 $[a, b]$ 上可积. 让 $x \in [a, b]$, 对 u'_k 和 f 在区间 $[x_0, x]$ 上使用??, (或 $[x, x_0]$, 如果 $x < x_0$), 则有

$$\sum_{k=1}^{\infty} \int_{x_0}^x u'_k(x) \, dx = \int_{x_0}^x f(x) \, dx = \lim_{n \rightarrow \infty} \sum_{k=1}^n (u_k(x) - u_k(x_0)).$$

由假设(i), $\sum_{k=1}^{\infty} u_k(x_0)$ 收敛, 所以级数 $F(x) = \lim_{n \rightarrow \infty} \sum_{k=1}^n u_k(x)$ 对任意 $x \in [a, b]$ 均收敛, 所以 $F : [a, b] \rightarrow \mathbb{R}$ 是良定义的, 于是 $F(x) - F(x_0) = \int_{x_0}^x f(x) \, dx$, 由 f 连续, 两边求导, 便有 $F'(x) = f(x)$.

(2). Cauchy判别法, 取 $\varepsilon > 0$, 则 $\exists N_1$ 使任意 $n \geq m \geq N_1$ 有

$$\left| \sum_{k=m}^n u_k(x_0) \right| < \frac{\varepsilon}{2}$$

存在 N_2 使任意 $n \geq m \geq N_2$ 有

$$\left| \sum_{k=m}^n u'_k(x) \right| < \frac{\varepsilon}{2(b-a)}, \quad x \in [a, b]$$

故可取 $N = \max\{N_1, N_2\}$, $g(x) = \sum_{k=m}^n u_k(x)$, 则 $g(x) - g(x_0) = g'(\xi)(x - x_0)$. 于是

$$|g(x)| \leq |g(x_0)| + |g(x) - g(x_0)| \leq \frac{\varepsilon}{2} + |g'(\xi)| \cdot |x - x_0| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2(b-a)} \cdot (b-a) = \varepsilon.$$

故由Cauchy判别法, $\sum_{k=1}^{\infty} u_k(x)$ 一致收敛. □

定理 2.1.7: 求导与极限的交换

函数列 $f_n : [a, b] \rightarrow \mathbb{R}$, $n \in \mathbb{N}_+$, 在 $[a, b]$ 上连续可微, $f_n(x) \rightarrow f(x)$, $x \in [a, b]$. $f'_n(x) \Rightarrow \varphi(x)$, $x \in [a, b]$, 则 f 可微且 $f'(x) = \varphi(x)$, 从而 $f_n \Rightarrow f$.

解. 取 $u_1 = f_1$, $u_n = f_n - f_{n-1}$, $n > 1$, 并用??. □

2.2 微分方程

定理 2.2.1: 伯努力方程

$\frac{dy}{dx} = p(x)y + q(x)y^n$, 其中 $p(x)$, $q(x)$ 是所考虑区域上的连续函数, $n(\neq 0, 1)$ 是常数.

解.

- (1) 当 $n > 0$ 时, $y = 0$ 是方程的解.
- (2) 当 $y \neq 0$ 时, 两边同除以 y^n , 令 $z = y^{1-n}$, 即得一阶线性方程.

□

定理 2.2.2

设 $y_1(x)$ 和 $y_2(x)$ 是方程

$$y'' + P(x)y' + Q(x)y = 0$$

的两个线性无关解, 齐次边值问题

$$\begin{cases} y'' + P(x)y' + Q(x)y = 0; \\ \alpha_1 y(a) + \beta_1 y'(a) = 0; \\ \alpha_2 y(b) + \beta_2 y'(b) = 0 \end{cases}$$

存在非平凡解(即不恒等于零的解)当且仅当

$$\begin{vmatrix} \alpha_1 y_1(a) + \beta_1 y_1'(a) & \alpha_1 y_2(a) + \beta_1 y_2'(a) \\ \alpha_2 y_1(b) + \beta_2 y_1'(b) & \alpha_2 y_2(b) + \beta_2 y_2'(b) \end{vmatrix} = 0$$

2.3 泛函分析

定理 2.3.1: Arzela-Ascoli定理

设 $\{f_n\}$ 是 $[0, 1]$ 上一致有界, 等度连续函数族, 则存在某一子序列 $\{f_{n(i)}\}$ 在 $[0, 1]$ 上一致收敛.

定理 2.3.2: Hahn-Banach, \mathbb{R} -version

设 \mathcal{X} 是定义在 \mathbb{R} 上的向量空间, $q: \mathcal{X} \rightarrow \mathbb{R}$ 是拟半范数. 若给定线性子空间 $\mathcal{Y} \subset \mathcal{X}$ 和其上的线性映射 $\phi: \mathcal{Y} \rightarrow \mathbb{R}$, 使得

$$\phi(y) \leq q(y), \forall y \in \mathcal{Y}.$$

则存在线性映射 $\varphi: \mathcal{X} \rightarrow \mathbb{R}$ 满足

- (i) $\varphi|_{\mathcal{Y}} = \phi$;
- (ii) $\varphi(x) \leq q(x), \forall x \in \mathcal{X}$.

解. 先证 $\mathcal{X}/\mathcal{Y} = 1$ 的情况. 即有 $x_0 \in \mathcal{X}$ 使得

$$\mathcal{X} = \{y + sx_0 : y \in \mathcal{Y}, s \in \mathbb{R}\}.$$

于是只需找到 $\alpha \in \mathbb{R}$ 使得映射 $\varphi(y + sx_0) = \phi(y) + s\alpha, \forall y \in \mathcal{Y}, s \in \mathbb{R}$ 满足条件(ii), 于是 $s > 0$ 时有

$$\alpha \leq q(z + x_0) - \phi(z), \forall z \in \mathcal{Y}, z = s^{-1}y, s > 0$$

对于 $s < 0$ 时有

$$\alpha \geq \phi(w) - q(w - x_0), \forall w \in \mathcal{Y}, w = t^{-1}y, s < 0$$

然而 $\phi(w) - q(w - x_0) \leq q(z + x_0) - \phi(z), \forall w, z \in \mathcal{Y}$ 恒成立. 然后用Zorn引理. □

未知 2.3.1: Hahn-Banach定理, \mathbb{C} -version

设 \mathcal{X} 是复数域 \mathbb{C} 上的向量空间, $q: \mathcal{X} \rightarrow \mathbb{R}$ 是 \mathcal{X} 上的拟半范数, 给定线性子空间 $\mathcal{Y} \subset \mathcal{X}$ 和 \mathcal{Y} 上的线性映射 $\phi: \mathcal{Y} \rightarrow \mathbb{C}$ 使得

$$\operatorname{Re}\phi(y) \leq q(y), \quad \forall y \in \mathcal{Y}.$$

则存在线性映射 $\psi: \mathcal{X} \rightarrow \mathbb{C}$ 满足:

- (i) $\psi|_{\mathcal{Y}} = \phi$;
- (ii) $\operatorname{Re}\psi(x) \leq q(x), \forall x \in \mathcal{X}$.

解. 设 $\phi_1 = \operatorname{Re}\phi$, 因 ϕ_1 是 $(\mathcal{Y}, \mathbb{R})$ 上的线性映射且被拟半范数 q 控制, 则由 \mathbb{R} -Hahn Banach定理, ϕ_1 可延拓到 $(\mathcal{X}, \mathbb{R})$ 上的实线性映射 ψ_1 且满足

- (i') $\psi_1|_{\mathcal{Y}} = \phi_1$;
- (ii') $\psi_1(x) \leq q(x), \forall x \in \mathcal{X}$.

但注意这里用的是实的Hahn Banach定理, 所延拓的 ψ_1 是针对实向量空间 $(\mathcal{X}, \mathbb{R})$ 的, 要得到复向量空间的 ψ_1 , 则在 $(\mathcal{Y}, \mathbb{C})$ 上考虑 $\psi_1(y) = \phi_1(y)$, 但新定义的 ψ_1 是实域上的线性映射, 而不是复域上的线性映射, 显然所求线性映射 ψ 的实部 $\operatorname{Re}\psi$ 在实线性空间中满足以上两条件. 若取 $\operatorname{Re}\psi = \psi_1$, 则 ψ 在实的情况已满足条件(ii). 而 $\operatorname{Im}\psi(y) = \operatorname{Re}(-i\psi(y)) = \operatorname{Re}\psi(-iy) = \psi_1(-iy)$, 于是 $\psi(y) = \psi_1(y) + i\psi_1(-iy)$, 要证 $\psi|_{\mathcal{Y}} = \phi$, 只需证 $\operatorname{Im}\psi(y) = \operatorname{Im}\phi(y), \forall y \in \mathcal{Y}$, 然而

$$\operatorname{Im}\phi(y) = \operatorname{Re}(-i\phi(y)) = \operatorname{Re}(\phi(-iy)) = \phi_1(-iy) = \psi_1(-iy) = \operatorname{Im}\psi(y).$$

最后证明线性映射 $\psi(x) = \psi_1(x) + i\psi_1(-ix)$ 在复域上满足(ii), 注意这里的 $\psi_1(-ix)$ 是怎么定义的? □

2.4 拓扑

定理 2.4.1: 杨忠道定理

证明: 拓扑空间中的每一子集的导集为闭集的充分必要条件是此空间中的每一个单点集的导集为闭集.

解. 只证充分性. 设拓扑空间 X 的每一个单点集的导集为闭集, 任意 $A \subset X$, 设 $x \in d(d(A))$, 对 x 的任意开邻域 U , 有 $U \cap (d(A) \setminus \{x\}) \neq \emptyset$, 因 $d(\{x\})$ 是闭集, 且 $x \notin d(\{x\})$, 令 $V = U \setminus d(\{x\})$, V 是 x 的开邻域, 从而有

$$y \in V \cap (d(A) \setminus \{x\}).$$

由 $y \in V$, $y \notin d(\{x\})$, 且 $y \neq x$, 于是存在 $W \in \mathcal{U}_y$, 使得 $x \notin W$, 因 $V \in \mathcal{U}_y$, 令 $K = W \cap V$, $K \in \mathcal{U}_y$, 由 $y \in d(A)$, 存在 $z \in K \cap (A \setminus \{y\}) \neq \emptyset$. 由 $z \in K \subset W$, $z \neq x$, 因此 $z \in U \cap (A \setminus \{x\})$, 故 $U \cap (A \setminus \{x\}) \neq \emptyset$, 即 $x \in d(A)$, 所以 $d(d(A)) \subset d(A)$, $d(A)$ 为闭集. \square

2.5 数论

定理 2.5.1: 恒等定理

设 $f(x), g(x) \in D[x]$, 若有无穷多个 $\alpha \in D$ 使 $f(\alpha) = g(\alpha)$, 则 $f(x) = g(x)$.

定理 2.5.2: 拉格朗日定理

设 $f(x)$ 是整系数多项式, 模 p 的次数为 n , 则同余方程

$$f(x) \equiv 0 \pmod{p} \quad (2.1)$$

至多有 n 个互不相同的解.

解. $n = 1$ 时结论显然成立, 对 n 归纳. 假设 $n - 1$ 时已正确, 当 f 的次数是 n 时, 若同余方程无解, 则无需证明. 若 $x = a$ 是一个解, 用 $(x - a)$ 除 $f(x)$ 得 $f(x) = g(x)(x - a) + A$, ($A \in \mathbb{Z}$), 若同余方程 $(?)$ 除 $x \equiv a \pmod{p}$ 外无解, 则证毕, 否则设 $x = b$ 是 $(?)$ 的另一个解, 且 $a \not\equiv b \pmod{p}$, 则

$$0 \equiv f(b) = g(b)(b - a) + A \pmod{p}, \text{ 又由 } 0 \equiv f(a) = g(a)(a - a) + A = A \pmod{p}.$$

所以 $g(b) \equiv 0 \pmod{p}$, 这表明 $(?)$ 的解除 $x \equiv a \pmod{p}$ 之外, 其余的解均是 $g(x) \equiv 0 \pmod{p}$ 的解, 但 $g(x)$ 模 p 的次数显然是 $n - 1$, 由归纳假设, $g(x) \equiv 0 \pmod{p}$, 至多有 $n - 1$ 个互不同余的解, 从而同余方程 $(?)$ 至多有 n 个解. \square

定理 2.5.3: 整系数多项式的有理根

$f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$, $n \geq 1$, $a_n a_0 \neq 0$ 且 $(a_n, \cdots, a_0) = 1$, 若 $\frac{b}{c}$ 是 $f(x)$ 的一个有理根 $(b, c) = 1$, 则 $c \mid a_n$, $b \mid a_0$. 特别地, 首项系数为 ± 1 的整系数多项式的有理根必是整数.

解. 由 $f(\frac{b}{c}) = 0$, 得 $a_n b^n + \cdots + a_1 b c^{n-1} + a_0 c^n = 0$, 所以 $a_0 \mid b$, $a_n \mid c$.

一种证明有理数是整数的证明途径: 证复数是整数, 先证其是有理数, 且找到作为零点的首一多项式. \square

定理 2.5.4: Gauss引理

$\mathbb{Z}[x]$ 中两个本原多项式的乘积仍是一个本原多项式.

解. 反证法, $f(x) = a_n x^n + \cdots + a_0$, $g(x) = b_m x^m + \cdots + b_0$, 若 $f(x)g(x)$ 不是本原多项式, 则有素数 p 整除 $f(x)g(x)$ 的所有系数. 设 r 是 a_i 不被 p 整除的最小角标, s 是 b_i 不被 p 整除的最小角标, 则 $f(x)g(x)$ 的 x^{r+s} 项系数不能被 p 整除. \square

定理 2.5.5: 艾森斯坦判别法

设 $f(x) = a_n x^n + \cdots + a_0$ 是一个整系数多项式, 其中 $n \geq 1$. 若存在一个素数 p , 使得 $p \nmid a_n$, $p \mid a_i (i = 0, 1, \cdots, n - 1)$, 但 $p^2 \nmid a_0$, 则 $f(x)$ 在 \mathbb{Z} 上不可约.

定理 2.5.6: 科恩定理

设 $p = \overline{a_n \cdots a_1 a_0}$ 是一个十进制素数, $0 \leq a_i \leq 9 (i = 0, 1, \cdots, n), a_n \neq 0$. 则多项式

$$f(x) = a_n x^n + \cdots + a_1 x + a_0.$$

在 \mathbb{Z} 上不可约.

解. 先用??, 再用??. □

定理 2.5.7

Every nonzero integer can be written as a product of primes.

解. Assume that there is an integer that cannot be written as a product of primes. Let N be the smallest positive integer with this property. Since N cannot itself be prime we must have $N = mn$, where $1 < m, n < N$. However, since m and n are positive and smaller than N they must each be a product of primes. But then so is $N = mn$. This is a contradiction.

The proof can be given in a more positive way by using mathematical induction. It is enough to prove the result for all positive integers. 2 is a prime. Suppose that $2 < N$ and that we have proved the result for all numbers m such that $2 \leq m < N$. We wish to show that N is a product of primes. If N is a prime, there is nothing to do. If N is not a prime, then $N = mn$, where $2 \leq m, n < N$. By induction both m and n are products of primes and thus so is N . □

定理 2.5.8: m 进(m-adic)表示

正整数 $m \geq 2, \forall a \in \mathbb{N}_+$, 有表示 $a = a_0 + a_1 m + \cdots + a_s m^s$.

定理 2.5.9: Bézout's identity (贝祖等式)

任意两整数 $a, b (b \neq 0)$ 的正最大公因子 $d = (a, b)$ 唯一存在, 而且存在整数 u, v 使得 $ua + vb = d$, u, v 称为 Bézout 系数, Bézout 系数不唯一, 若设 $a' = \frac{a}{d}, b' = \frac{b}{d}$, 则恰有两系数对满足 $|u| < |b'|, |v| < |a'|$.

解. 若 $a > b, a = bq + r$, 则 $(a, b) = (r, b)$, 于是由辗转相除法的逆过程可得 u, v . □

解. 不用辗转相除法. $M = \{ax + by \mid x, y \in \mathbb{Z}\}$, d 是 M 中的最小正整数 (自然数良序性). 则若 $d = ax_0 + by_0$ 知 $(a, b) \mid d$, 所以只需证 $d \mid (a, b)$. 若 $d \nmid a$, 取 $a = dq + r$, 则 $r = ax_0 + by_0 - dq < d$ 与 d 的选取矛盾. □

推论 2.5.1

a, b 互素等价于: 存在整数 u, v 使 $ua + vb = 1$.

$a, b \in \mathbb{Z}$, 则:

$$\begin{aligned} (a, b) = d &\Rightarrow \{am + bn \mid m, n \in \mathbb{Z}\} = \{dk \mid k \in \mathbb{Z}\} \\ &\Rightarrow a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z} \\ &\Rightarrow (a, b) = (d) \end{aligned}$$

推论 2.5.2: Bézout 等式

任 s 个非零整数 a_1, \cdots, a_s 的最大公因子 $d = (a_1, \cdots, a_s)$ 存在唯一, 且 $(a_1, \cdots, a_{s-1}, a_s) = ((a_1, \cdots, a_{s-1}), a_s)$, 且存在整数 u_1, \cdots, u_s 使 $u_1 a_1 + \cdots + u_s a_s = d$.

定理 2.5.10

$v_p(n)$ 使得 $p^k \parallel n$ 的整数 k . 则

$$v_p(n!) = \sum_k \left[\frac{n}{p^k} \right].$$

定理 2.5.11: 威尔逊定理

p 是素数, 则有 $(p-1)! \equiv -1 \pmod{p}$.

解. 当 $p = 2$ 时, 命题显然. 若 $p \geq 3$, 由于对每个与 p 互素的 a 在模 p 下均有逆 a^{-1} . 故可得 $1, 2, \dots, p-1$ 的每个与其逆配对, 而特别的当 $a = a^{-1}$ 时是例外. 此时对应 $a^2 \equiv 1 \pmod{p}$ 有解 $a = 1$ 或 $a = p-1$, 而 $2, \dots, p-2$ 可两两配对使积为 1. 所以 $(p-1)! \equiv 1 \cdot (p-1) \equiv -1 \pmod{p}$. \square

解. 用 Euler 恒等式

$$\sum_{i=0}^m (-1)^i \binom{m}{i} i^n = \begin{cases} 0, n < m \\ (-1)^n n!, n = m \end{cases}$$

取 $m = n = p-1$, 当 $p > 2$ 时及 Fermat 小定理有

$$(-1)^{p-1} \cdot (p-1)! \equiv \sum_{i=0}^{p-1} (-1)^i \binom{p-1}{i} i^{p-1} \equiv \sum_{i=0}^{p-1} (-1)^i \binom{p-1}{i} \equiv -1 \pmod{p}.$$

 \square

解. 当 $p \geq 3$ 时, 由 Fermat 小定理 $p-2$ 次同余方程

$$f(x) = (x-1)(x-2)\cdots(x-p+1) - x^{p-1} + 1 \equiv 0 \pmod{p}$$

有 $p-1$ 个不同得解, 所以 $f(x)$ 的系数模 p 余零, 所以常数项 $(p-1)! + 1 \equiv 0 \pmod{p}$. \square

2.6 不等式

定理 2.6.1: Generalized Schur Inequality

设六个非负实数 a, b, c, x, y, z 满足 (a, b, c) 和 (x, y, z) 均单调, 则

$$\sum_{cyc} x(a-b)(b-c) \geq 0.$$

解. 不妨设 $a \geq b \geq c$, 分 $x \geq y \geq z$ 与 $x \leq y \leq z$ 两种情况分别讨论. \square

推论 2.6.1

记 $S = \sum_{cyc} x(a-b)(a-c)$. 下面几条条件的任何一个均可证明 $S \geq 0$.

- (1) 当 $a \geq b \geq c \geq 0$, $x \geq y \geq 0$ 且 $z \geq 0$ 时.
- (2) 当 $a \geq b \geq c \geq 0$, $z \geq y \geq 0$ 且 $x \geq 0$ 时.
- (3) 当 $a \geq b \geq c \geq 0$, 且 $ax \geq by \geq 0$ 或者 $by \geq cz \geq 0$ 时.

解. (1)和(2)显然, 对于(3)有

$$\begin{aligned} & \frac{1}{abc} (x(a-b)(a-c) + y(b-a)(b-c) + z(c-a)(c-b)) \\ &= ax \left(\frac{1}{a} - \frac{1}{b} \right) \left(\frac{1}{a} - \frac{1}{c} \right) + by \left(\frac{1}{b} - \frac{1}{a} \right) \left(\frac{1}{b} - \frac{1}{c} \right) + cz \left(\frac{1}{c} - \frac{1}{a} \right) \left(\frac{1}{c} - \frac{1}{b} \right). \end{aligned}$$

便转化为前面的两种情况了. \square

定理 2.6.2: Cauchy不等式

对于欧式空间中任意向量 α, β 都有

$$|(\alpha, \beta)| \leq |\alpha||\beta|.$$

而且即当 α 与 β 线性相关时等号成立.

定理 2.6.3: 三角形不等式

对欧式空间中任意向量 α, β 有

$$|\alpha + \beta| \leq |\alpha| + |\beta|.$$

对欧式空间中任意向量 $\alpha_1, \alpha_2, \dots, \alpha_m$ 都有

$$|\alpha_1 + \alpha_2 + \dots + \alpha_m| \leq |\alpha_1| + |\alpha_2| + \dots + |\alpha_m|.$$

Bibliography

- [PH] The Man Who Loved Only Numbers, The Story of Paul Erdos and The Search for Mathematical Truth; Paul Hoffman; 1999.
- [YN] 数域的上同调; 尤尔根·诺伊基希, 亚历山大[德], 哈尔滨工业大学.
- [TH] Holder不等式及其应用; 田景峰, 哈明虎, 清华大学.
- [HKZ2013on] Hu, W., Kukavica, I., Ziane, M.: On the regularity for the Boussinesq equations in a bounded domain, J. Math. Phys. 54(8), 081507, 10 (2013)
- [T1997Inf] R. Temam, Infinite Dimensional Dynamical Systems in Mechanics and Physics, Applied Mathematical Sciences Vol. 68 (Springer, 1997).