代数学基础期末考试

2013年1月20日

1 对于域上 n 次多项式 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 (a_0 a_n \neq 0)$, 令

$$f^*(x) = x^n f(\frac{1}{x}).$$

(1) 证明 $f(x)$ 不可约当且仅当 $f^*(x)$ 不可约.

(2) 证明 $3x^5 + 6x^4 + 3x^2 + 1$ 在 $\mathbb{Z}[x]$ 中不可约.

(3) 设 $x_1, x_2, \ldots, x_n$ 为 $f(x)$ 的 n 的根, 使用 $f(x)$ 的系数表示

$$(x_1 + \cdots + x_n)(\frac{1}{x_1} + \cdots + \frac{1}{x_n}).$$

2 写出 S_4 中所有的 2 阶元, 写出 S_5 中阶最大的一个元素, 并简述理由.

3 (1) 设 X 为有限集, Y 与 Z 是 X 的子集且 $|Y| > \frac{|X|}{2}, |Z| > \frac{|X|}{2}$. 证明 $Y \cap Z$ 非空.

(2) 设 p 为奇素数, $a, b \in \mathbb{F}_p^\times, c \in \mathbb{F}_p$. 证明方程 $ax^2 + by^2 = c$ 在 $\mathbb{F}_p$ 中总有解.

4 计算 $x^4 + x^2 + x + 1$ 与 $x^5 + x^2 + x + 1$ 在 $\mathbb{F}_2[x]$ 和在 $\mathbb{Q}[x]$ 中的最大公因子.

5 证明 $x^2 + y^2 + z^2 = 1007$ 没有整数解.

6 (1) 试讨论 $\mathbb{Z}/n\mathbb{Z}$ 上置换 $x \mapsto -x$ 的奇偶性.

(2) 证明映射 $x \mapsto x^5$ 是 $\mathbb{F}_p^\times$ 上的同构当且仅当 p 不同余于 $1 \bmod 5$.

7 对所有素数 p, 讨论多项式 $x^2 - 6$ 在 $\mathbb{F}_p[x]$ 中是否可约.

8 设 $\alpha, \beta \in \mathbb{Z}[i]$ 且 $\beta \neq 0$. 证明存在 $\gamma, \delta \in \mathbb{Z}[i]$, 满足

$$\alpha = \beta\gamma + \delta, \quad 0 \leq |\delta| < |\beta|,$$

其中 $|z|$ 即复数 z 的模长.

代数学基础期中考试

2014年11月15日

1. 计算题:

(1) 求 953 和 657 的最大公因子 d, 并求 u, v 使得 $953u + 657v = d$.

(2) 试求

$$\sum_{i=1}^{n} i^3.$$

(3) 在有限域 $\mathbb{F}_{13}$ 中求 5 的乘法逆元.

(4) 求解同余方程组:

$$\begin{cases} 5x \equiv 4 \bmod 6, \\ 3x \equiv 2 \bmod 10. \end{cases}$$

2. 对于正整数 k, 设 $\mu_k = \{\zeta_k^i \mid 0 \leqslant i < k\}$(其中 $\zeta_k = \cos\frac{2\pi}{k} + i\sin\frac{2\pi}{k}$)是复数域 $\mathbb{C}$ 中 k 次单位根构成的乘法群. 对于正整数 m 和 n, 试证明:

(i) $\mu_m \cap \mu_n = \mu_{(m,n)}$.

(ii) 存在整数 a, b 使得 $\zeta_{[m,n]} = \zeta_m^a \zeta_n^b$.

3. 设 D 是固定无平方因子整数.

(i) 试问所有形如 $\begin{pmatrix} x & y \\ Dy & x \end{pmatrix}$(其中 $x, y \in \mathbb{Z}$)的矩阵集合在矩阵的加法和乘法意义下是否构成环?

(ii) 试问所有形如 $\frac{1}{2}\begin{pmatrix} x & y \\ Dy & x \end{pmatrix}$(其中 $x, y \in \mathbb{Z}$ 且 x, y 同奇偶)的矩阵集合在矩阵的加法和乘法意义下是否构成环?

4. 设 $X = [0, 1)$. 在 X 上定义加法 $\alpha \oplus \beta$ 为实数 $\alpha + \beta$ 的分数部分.

(i) 证明 $(X, \oplus)$ 为阿贝尔群.

(ii) 给出 X 到单位元 S^1 的群同构.

5. 设 a 为正有理数, k 为正整数. 证明: $\sqrt[k]{\alpha}$ 是有理数当且仅当对所有素数 p, $v_p(a) \equiv 0 \bmod k$. (注意 $v_p(a)$ 即 a 的因子分解中 p 的幂次)

6. (i) 设 p, q 为不同的奇素数, $m = pq$. 证明对于任意 $a \in \mathbb{Z}$, $(a, m) = 1$, $a^{\varphi(m)/2} \equiv 1 \bmod m$.

(ii) 求 $2^{500} \bmod 2014$.

试卷解答

2014年11月15日

1. 计算题:

(1) 求 953 和 657 的最大公因子 d, 并求 u, v 使得 $953u + 657v = d$.

解: 利用辗转相除法.

$$953 = 657 + 296, \quad 657 = 296 \times 2 + 65, \quad 296 = 65 \times 4 + 36,$$

$$65 = 36 + 29, \quad 36 = 29 + 7, \quad 29 = 7 \times 4 + 1,$$

因此 $(953, 657) = 1$, 且

$$\begin{aligned} 1 &= 29 - 7 \times 4 = 29 - (36 - 29) \times 4 = 29 \times 5 - 36 \times 4 \\ &= (65 - 36) \times 5 - 36 \times 4 = 65 \times 5 - 36 \times 9 \\ &= 65 \times 5 - (296 - 65 \times 4) \times 9 = 65 \times 41 - 296 \times 9 \\ &= (657 - 296 \times 2) \times 41 - 296 \times 9 = 657 \times 41 - 296 \times 91 \\ &= 657 \times 41 - (953 - 657) \times 91 = 657 \times 132 - 953 \times 91, \end{aligned}$$

因此特解为 $(u_0, v_0) = (-91, 132)$, 通解为 $(u, v) = (-91 - 657t, 132 + 953t), t \in \mathbb{Z}$.

(2) 试求

$$\sum_{i=1}^{n} i^3.$$

解1: 由于

$$(i+1)^4 - i^4 = 4i^3 + 6i^2 + 4i + 1,$$

$$(n+1)^4 - 1 = 4\sum_{i=1}^{n} i^3 + 6\sum_{i=1}^{n} i^2 + 4\sum_{i=1}^{n} i + n,$$

因此

$$\begin{aligned} \sum_{i=1}^{n} i^3 &= \frac{1}{4}\big((n+1)^4 - 1 - 6\sum i = 1^n i^2 - 4\sum_{i=1}^{n} i - n)\big) \\ &= \frac{1}{4}\big((n+1)^4 - 1 - 6\frac{n(n+1)(2n+1)}{6} - 4\frac{n(n+1)}{2} - n\big) \\ &= \frac{n^4 + 2n^3 + n^2}{4}. \end{aligned}$$

解2: 由于

$$i^2(i+1)^2 - (i-1)^2 i^2 = 4i^3,$$

因此

$$\sum_{i=1}^{n} i^3 = \frac{1}{4}\sum_{i=1}^{n}(i^2(i+1)^2 - (i-1)^2 i^2) = \frac{n^2(n+1)^2}{4}.$$

也可以利用数学归纳法.

(3) 在有限域 $\mathbb{F}_{13}$ 中求 5 的乘法逆元.

由于在 $\mathbb{F}_{13}$ 中, $5 \times 5 = 25 = -1$, 因此 $5^{-1} = -5 = 8$.

(4) 求解同余方程组:

$$\begin{cases} 5x \equiv 4 \bmod 6, \\ 3x \equiv 2 \bmod 10. \end{cases}$$

解: 原方程等价于

$$\begin{cases} 5x \equiv 4 \bmod 2, \\ 5x \equiv 4 \bmod 3, \\ 3x \equiv 2 \bmod 2, \\ 3x \equiv 2 \bmod 5 \end{cases}$$

即

$$\begin{cases} x \equiv 0 \bmod 2, \\ x \equiv 2 \bmod 3, \\ x \equiv -1 \bmod 5 \end{cases}$$

由中国剩余定理, $x \equiv 2 \times 10 - 1 \times 6 \equiv 14 \bmod 30$.

2. 对于正整数 k, 设 $\mu_k = \{\zeta_k^i \mid 0 \leqslant i < k\}$(其中 $\zeta_k = \cos\frac{2\pi}{k} + i\sin\frac{2\pi}{k}$)是复数域 $\mathbb{C}$ 中 k 次单位根构成的乘法群. 对于正整数 m 和 n, 试证明:

(1) $\mu_m \cap \mu_n = \mu_{(m,n)}$.

(2) 存在整数 a, b 使得 $\zeta_{[m,n]} = \zeta_m^a \zeta_n^b$.

证明: (1) 由 Bezout 等式, 存在正整数 $a, b \in \mathbb{Z}$ 使得 $an + bm = (m, n)$, 于是对任意 $x \in \mu_m \cap \mu_n$,

$$x^{(m,n)} = x^{an+bm} = (x^n)^a (x^m)^b = 1,$$

因此 $x \in \mu_{(m,n)}, \mu_m \cap \mu_n \subseteq \mu_{(m,n)}$. 反之, 对任意 $x \in \mu_{(m,n)}$, $x^{(m,n)} = 1$. 由 $(m,n) \mid m, n$ 知 $x^m = x^n = 1$, 因此 $\mu_{(m,n)} \subseteq \mu_m \cap \mu_n$.

(2) 由于 $(m,n)[m,n] = mn$, 因此

$$\frac{1}{[m,n]} = \frac{(m,n)}{mn} = \frac{an+bm}{mn} = \frac{a}{m} + \frac{b}{n},$$

于是

$$\zeta_{[m,n]} = e^{\frac{2\pi i}{[m,n]}} = e^{\frac{2\pi ia}{m} + \frac{2\pi ib}{n}} = \zeta_m^a \zeta_n^b.$$

3. 设 D 是固定无平方因子整数.

(1) 试问所有形如 $\begin{pmatrix} x & y \\ Dy & x \end{pmatrix}$(其中 $x, y \in \mathbb{Z}$)的矩阵集合在矩阵的加法和乘法意义下是否构成环?

(2) 试问所有形如 $\frac{1}{2}\begin{pmatrix} x & y \\ Dy & x \end{pmatrix}$(其中 $x, y \in \mathbb{Z}$ 且 x, y 同奇偶)的矩阵集合在矩阵的加法和乘法意义下是否构成环?

解1: (1) 构成. 设该集合为 S. 由于对任意 $x_1, y_1, x_2, y_2 \in \mathbb{Z}$,

$$\begin{pmatrix} x_1 & y_1 \\ Dy_1 & x_1 \end{pmatrix} - \begin{pmatrix} x_2 & y_2 \\ Dy_2 & x_2 \end{pmatrix} = \begin{pmatrix} x_1 - x_2 & y_1 - y_2 \\ D(y_1 - y_2) & x_1 - x_2 \end{pmatrix} \in S,$$

$$\begin{pmatrix} x_1 & y_1 \\ Dy_1 & x_1 \end{pmatrix} \begin{pmatrix} x_2 & y_2 \\ Dy_2 & x_2 \end{pmatrix} = \begin{pmatrix} x_1x_2 + Dy_1y_2 & x_1y_2 + x_2y_1 \\ D(x_1y_2 + x_2y_1) & Dy_1y_2 + x_1x_2 \end{pmatrix} \in S,$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in S,$$

因此 S 构成 $M_2(\mathbb{R})$ 的子环.

(2) 不一定. 设该集合为 T, 由(1)知 T 构成环等价于对任意 $x_1, y_1, x_2, y_2 \in \frac{1}{2}\mathbb{Z}, x_1 + y_1, x_2 + y_2 \in \mathbb{Z}$,

$$\begin{pmatrix} x_1x_2 + Dy_1y_2 & x_1y_2 + x_2y_1 \\ D(x_1y_2 + x_2y_1) & Dy_1y_2 + x_1x_2 \end{pmatrix} \in T,$$

即 $2(x_1x_2+Dy_1y_2), x_1x_2+Dy_1y_2+x_1y_2+y_1x_2\in\mathbb{Z}$. 而

$$x_1x_2+Dy_1y_2+x_1y_2+y_1x_2=(x_1+y_1)(x_2+y_2)+(D-1)y_1y_2,$$

因此 $D-1$ 是4的倍数, 且此时

$$2(x_1x_2+Dy_1y_2)=2x_2(x_1+y_1)+2y_1(x_2+y_2)-4x_2y_1+2(D-1)y_1y_2\in\mathbb{Z}.$$

故 T 是环当且仅当 $D\equiv 1 \bmod 4$.

解2: 设 $S=\mathbb{Z}+\mathbb{Z}\alpha, \alpha\in\mathbb{C}$ 满足 $\alpha^2=a\alpha+b$. 对任意 $x_1,y_1,x_2,y_2\in\mathbb{Z}$,

$$1\in S,$$

$$(x_1+y_1\alpha)-(x_2+y_2\alpha)=(x_1-x_2)+(y_1-y_2)\alpha\in S,$$

$$(x_1+y_1\alpha)(x_2+y_2\alpha)=(x_1x_2+by_1y_2)+(ay_1y_2+x_2y_1+x_1y_2)\alpha,$$

于是 S 是环等价于最后一个式子在 S 中, 即 $a,b\in\mathbb{Z}$.

由于

$$\begin{pmatrix}0 & 1\\ D & 0\end{pmatrix}^2=D\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},$$

(1) 中的集合一一对应于 $S=\mathbb{Z}+\mathbb{Z}\alpha, \alpha^2=D$, 且保持运算. 因此构成环.

由于

$$\begin{pmatrix}\frac{1}{2} & \frac{1}{2}\\ \frac{D}{2} & \frac{1}{2}\end{pmatrix}^2=\begin{pmatrix}\frac{1}{2} & \frac{1}{2}\\ \frac{D}{2} & \frac{1}{2}\end{pmatrix}^2+\frac{D-1}{4}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},$$

(2) 中的集合一一对应于 $S=\mathbb{Z}+\mathbb{Z}\alpha, \alpha^2-\alpha-\frac{D-1}{4}=0$, 且保持运算. 因此构成环当且仅当 $D\equiv 1 \bmod 4$.

4. 设 $X=[0,1)$. 在 X 上定义加法 $\alpha\oplus\beta$ 为实数 $\alpha+\beta$ 的分数部分.

(1) 证明 $(X,\oplus)$ 为阿贝尔群.

(2) 给出 X 到单位元 S^1 的群同构.

证明: (1) 封闭性显然. 对任意 $x,y,z\in X$,

$$0\oplus x=x\oplus 0=x,$$

$$0\oplus 0=0,\ x\oplus(1-x)=0 \text{ 如果 } x\neq 0,$$

$$\begin{aligned}(x\oplus y)\oplus z&=(x+y-[x+y])\oplus z\\ &=x+y+z-[x+y]-[x+y+z-[x+y]]\\ &=x+y+z-[x+y]-[x+y+z]+[x+y]\\ &=x+y+z-[x+y+z],\end{aligned}$$

同理 $x\oplus(y\oplus z)=x+y+z-[x+y+z]$, 这里 $[\ ]$ 表示取整. 因此 $(X,\oplus)$ 构成群.

(2) 设

$$\begin{aligned}\varphi: X&\to S^1\\ x&\mapsto e^{2\pi i x},\end{aligned}$$

则易见 φ 是双射. 又因为 $\varphi(x\oplus y)=e^{2\pi i(x+y-[x+y])}=e^{2\pi i(x+y)}=\varphi(x)\varphi(y)$, 因此 φ 是群同构.

5. 设 a 为正有理数, k 为正整数. 证明: $\sqrt[k]{a}$ 是有理数当且仅当对所有素数 p, $v_p(a)\equiv 0 \bmod k$. (注意 $v_p(a)$ 即 a 的因子分解中 p 的幂次)

证明: 由 $a\neq 0$ 知 $\sqrt[k]{a}\neq 0$. 若 $\sqrt[k]{a}$ 是有理数, 则可以设

$$\sqrt[k]{a}=\prod_p p^{m_p},$$

于是
$$a=\prod_p p^{km_p},$$
$v_p(a)=km_p\equiv 0 \bmod k$.

反之, 若对所有素数 p, $v_p(a)\equiv 0 \bmod k$, 则
$$\sqrt[k]{a}=\prod_p p^{v_p(a)/k}\in\mathbb{Q}.$$

6. (1) 设 p,q 为不同的奇素数, $m=pq$. 证明对于任意 $a\in\mathbb{Z}$, $(a,m)=1$, $a^{\varphi(m)/2}\equiv 1 \bmod m$.

(2) 求 $2^{500} \bmod 2014$.

解: (1) 由费马小定理,
$$a^{p-1}\equiv 1 \bmod p,\quad a^{q-1}\equiv 1 \bmod q,$$
由于 p,q 是奇数, $p-1,q-1$ 是偶数, 因此
$$a^{\frac{(p-1)(q-1)}{2}}\equiv 1 \bmod p,\quad a^{\frac{(p-1)(q-1)}{2}}\equiv 1 \bmod q,$$
由于 $(p,q)=1$, 因此 $a^{\varphi(m)/2}\equiv a^{\frac{(p-1)(q-1)}{2}}\equiv 1 \bmod m$.

(2) 首先 $2014=2\times 19\times 53, \varphi(19\times 53)=2\times 468$, 因此由(1)知
$$2^{468}\equiv 1 \bmod 19\times 53,$$
$$\begin{aligned}2^{500}&\equiv 2^32\equiv 1024\times 2048^2\equiv 1024\times 34^2\equiv 34\times 17\times 34\\&\equiv 1156\times 17\equiv 2312\times 8+1156\equiv 298\times 8+1156\equiv 1526 \bmod 2014.\end{aligned}$$

代数学基础期末考试

2015年1月27日

1 计算题(需简要说明理由)

(1) 确定 1 在多项式 $x^{2n} - nx^{n+1} + nx^{n-1} - 1$ 中的零点重数.

(2) 求置换$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 7 & 5 & 4 & 6 & 3 & 1 & 2 \end{pmatrix}$的阶.

(3) 求 S_{30} 中型为 $1^1 2^2 3^3 4^4$ 的置换的个数.

(4) 判断同余方程 $x^2 \equiv 137 \pmod{227}$ 是否有解.

(5) 若群 G 中元素 x 的阶为 21, 则 x^{14} 的阶是多少?

(6) 设 p 是奇素数, 则 $\mathbb{F}_p[x]$ 中形如 $x^2 + ax + b$ 的二次多项式中共有多少个不可约多项式?

2 求一个首项系数为1的三次多项式 $f(x) \in \mathbb{Q}[x]$, 使得它的根是多项式 $x^3 + 2x^2 + 3x - 2$ 的根的平方.

3. (i) 找出 $\mathbb{F}_2[x]$ 的所有二次不可约多项式.
(ii) 在 $\mathbb{F}_2[x]$ 中分解多项式 $x^5 - x - 1$.
(iii) 证明多项式 $x^5 - x - 1$ 在 $\mathbb{Q}[x]$ 中为不可约多项式.

4. 对于$n = 2, 3, 4$ 和 5, 分别判断命题

若群 G 和 H 满足 $|G| = |H| = n$, 则 G 与 H 是同构的群.

是否正确, 并证明你的结论.

5. 对于有限群 G, 设 $d(G)$ 是最小的正整数 s 使得对任意 $g \in G$, $g^s = 1$. 证明:
(i) $d(G)$ 是 $|G|$ 的因子, 它等于 G 中所有元素阶的最小公倍数.
(ii) 如果 G 是阿贝尔群, 则 G 中存在元素阶为 $d(G)$.
(iii) 有限阿贝尔群 G 为循环群当且仅当 $d(G) = |G|$.

中国科学技术大学

2014 - 2015学年第一学期期终考试试卷(B)

考试科目: 代数学基础　　　　得分:______________

姓名______ 学号______ 学生所在院系______

装 订 线

1 计算题（需简要说明理由）

(a) 【10分】 确定 1 在多项式 $x^{2n} - nx^{n+1} + nx^{n-1} - 1$ 中的零点重数。

(b) 【10分】 求置换$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 7 & 5 & 4 & 6 & 3 & 1 & 2 \end{pmatrix}$的阶。

(c) 【10分】 求 S_{20} 中型为 $1^4 2^3 3^2 4^1$ 的置换的个数。

(d) 【10分】 判断同余方程 $x^2 \equiv 286 \pmod{563}$ 是否有解。 (563 是素数)

(e) 【10分】 若群 G 中元素 x 的阶为 20，则 x^{14} 的阶是多少？

(f) 【10分】 设 p 是奇素数，则 $\mathbb{F}_p[x]$ 中形如 x^2+ax+b 的二次多项式中共有多少个不可约多项式？

2 【10分】 求一个首项系数为1的三次多项式 $f(x) \in \mathbb{Q}[x]$，使得它的根是多项式 x^3+2x^2+3x+2 的根的平方。

线

订

装

3 【10分】

(a) 找出 $\mathbb{F}_2[x]$ 的所有二次不可约多项式。

(b) 在 $\mathbb{F}_2[x]$ 中分解多项式 $x^5 - x + 1$。

(c) 证明多项式 $x^5 - x + 1$ 在 $\mathbb{Q}[x]$ 中为不可约多项式。

4 【10分】若 H 是 G 的子群，且 $(G:H)=2$，证明 H 是 G 的正规子群。（提示：可以研究 H 的陪集）

5【10分】对于有限群 G，设 $d(G)$ 是最小的正整数 s 使得对任意 $g \in G$，$g^s = 1$。证明：

(a) $d(G)$ 是 $|G|$ 的因子，它等于 G 中所有元素阶的最小公倍数。

(b) 如果 G 是阿贝尔群，则 G 中存在元素阶为 $d(G)$。

(c) 有限阿贝尔群 G 为循环群当且仅当 $d(G) = |G|$。

装 订 线