1 说明

1. 本文档由陈恭亮教授最后一节课的内容整理而成
2. **本文档仅代表个人观点，不代表正确观点，仅供学习参考使用，不对与最终考试试题的偏差负责，使用前请仔细甄别。**
3. **本文档仅代表个人观点，不代表正确观点，仅供学习参考使用，不对与最终考试试题的偏差负责，使用前请仔细甄别。**
4. **本文档仅代表个人观点，不代表正确观点，仅供学习参考使用，不对与最终考试试题的偏差负责，使用前请仔细甄别。**
5. 文档不断更新中，请以最新版为准。

2 正文

1. 置换 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 2 & 1 & 3 \end{pmatrix}$，$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 4 & 2 & 3 & 1 \end{pmatrix}$，求 $\sigma^{-1}, \sigma\tau\sigma^{-1}, \sigma\tau$，并将 $\tau, \sigma\tau\sigma^{-1}$ 表示为一系列循环置换的乘积。

置换群 考察了简单概念，求逆就是交换行，列可以随意交换，阅读书 *p261-p263* 即可理解

Solution.

$$\sigma^{-1} \overset{\text{交换行}}{=} \begin{pmatrix} 6 & 5 & 4 & 2 & 1 & 3 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 6 & 3 & 2 & 1 \end{pmatrix}$$

$$\begin{aligned} \sigma\tau &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 4 & 2 & 3 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 5 & 6 & 4 & 2 & 3 & 1 \\ 1 & 3 & 2 & 5 & 4 & 6 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 4 & 2 & 3 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 2 & 5 & 4 & 6 \end{pmatrix} \end{aligned}$$

$$\sigma\tau\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 4 & 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 6 & 3 & 2 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} 3 & 2 & 1 & 4 & 6 & 5 \\ 4 & 5 & 6 & 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 5 & 4 & 6 & 3 & 2 & 1 \\ 3 & 2 & 1 & 4 & 6 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 6 & 3 & 2 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 2 & 3 & 1 \end{pmatrix}$$

将 $\tau, \sigma\tau\sigma^{-1}$ 表示为一系列循环置换的乘积：

$$\tau = (1, 5, 3, 4, 2, 6)$$
$$\sigma\tau\sigma^{-1} = (1, 4, 2, 5, 3, 6)$$

■

2. 设 $f(x) = x^3 + 2x^2 + 1$

(a) 证明：$f(x)$ 是 $\mathbb{F}_3$ 上的不可约多项式。

Solution.

$f(x)$ 的次数 $deg\ f = 3$，若 $f(x)$ 有次数最小的非常数因式 $p(x)$，可知 $deg\ p \leq \frac{deg\ f}{2}$，即 $deg\ p = 1$，即所有可能的 $p(x)$ 有这样的形式：$p(x) = x - a,\ a \in \mathbb{F}_3$，所以只需验证 $\forall a \in \mathbb{F}_3$，有 $f(a) \neq 0$，即可证明 $f(x)$ 是 $\mathbb{F}_3$ 上的不可约多项式。

$$\because f(0) = 1 \neq 0$$
$$f(1) = 4 = 1 \neq 0$$
$$f(2) = 17 = 2 \neq 0$$

所以 $f(x)$ 是 $\mathbb{F}_3$ 上的不可约多项式。 ■

(b) 证明：由 $f(x)$ 生成的（主）理想 $I = (f(x))$ 是多项式环 $\mathbb{F}_3[3]$ 中的极大理想。

Solution.

若存在 M 为 $\mathbb{F}_3[x]$ 的理想且 M 真包含 I 的情况下（即 $M \supsetneq I$），则必定存在一个不属于 I 的多项式 $g(x) \in M \backslash I$，使得 $f(x) \nmid g(x)$。

因为 $f(x)$ 为不可约多项式，所以有 $(f(x), g(x)) = 1$，由广义欧几里得除法以及广义 Bézout 定理可知：

$$\exists s(x), t(x) \in \mathbb{F}_3[x]\ s.t. \quad s(x)f(x) + t(x)g(x) = 1$$

由理想的定义可知，若 $f(x), g(x) \in M$ $s(x), t(x) \in \mathbb{F}_3[x]$，则 $s(x)f(x)+t(x)g(x) = 1 \in M$，故 $M = \mathbb{F}_3[x]$，即 I 与 $\mathbb{F}_3[x]$ 之间不存在中间理想，所以由 $f(x)$ 生成的（主）理想 $I = (f(x))$ 是多项式环 $\mathbb{F}_3[3]$ 中的极大理想。 ■

(c) 判断 $g(x) = x$ 是否为 $\mathbb{F}_{3^3} = \mathbb{F}_3[x]\backslash(f(x))$ 的生成元，即 $g(x)$ 满足条件：

$$\mathbb{F}_{3^3}^* = \mathbb{F}_{3^3}\backslash\{0\} =< g >= \{g, g^2, g^3, \ldots, g^{3^3-1} = 1\}$$

Solution.

若 $g(x) = x$ 为 $\mathbb{F}_{3^3} = \mathbb{F}_3[x]\backslash(f(x))$ 的生成元，则元素 $g(x)$ 的阶必定为循环群 $\mathbb{F}_{3^3}^*$ 元素的个数。

同时我们知道循环群任意元素的阶必定是循环群元素个数的因数，循环群 $\mathbb{F}_{3^3}^*$ 元素的个数为 $\mid \mathbb{F}_{3^3}^* \mid= p^n - 1 = 3^3 - 1 = 26 = 2 \times 13$。所以只需验证 $g^2 \neq 1, g^{13} \neq 1$ 即可证明 $g(x) = x$ 为 $\mathbb{F}_{3^3} = \mathbb{F}_3[x]\backslash(f(x))$ 的生成元。

$$\begin{aligned}
g &= x \\
g^2 &= x^2 \neq 1 \\
g^3 &= x^3 = -2x^2 - 1 = x^2 + 2 \\
g^4 &= x^3 + 2x = x^2 + 2x + 2 \\
g^7 &= g^3 \cdot g^4 = (x^2 + 2)(x^2 + 2x + 2) = x^2 + 1 \\
g^6 &= g^2 \cdot g^4 = x^2(x^2 + 2x + 2) = 2x^2 + 2x \\
g^{13} &= g^6 \cdot g^7 = (x^2 + 1)(2x^2 + 2x) = 2 \neq 1
\end{aligned}$$

所以 g 为生成元。 ■

3. 为最终证明如下的定理：$\mathbb{F}_{q^n}$ 在 $\mathbb{F}_q$ 上的自同构集是一个阶为 n 的循环群，其生成元为自同构 $\sigma_q(\alpha) = \alpha^p$，请依次完成以下四个小问的问题。

(a) 证明：Frobenins 映射 $\sigma_q : \alpha \mapsto \alpha^q$ 是 $\mathbb{F}_{q^n}$ 的 $\mathbb{F}_q$-自同构，其中 $\alpha \in \mathbb{F}_{q^n}, q = p^m$，$p$ 为素数。

知识点 素域及域的特征 *p272-273*，自同态、自同构，二项展开，映射

Solution.

取任意的 $\alpha, \beta \in \mathbb{F}_{q^n}$，有

$$\sigma_q(\alpha + \beta) = (\alpha + \beta)^q = \alpha^q + \beta^q + \sum_{k=1}^{q-1} \frac{q!}{k!(q-k)!}\alpha^k\beta^{q-k}$$

因为域 $\mathbb{F}_q=\mathbb{F}_{p^m}$ 由域 $\mathbb{F}_p$ 扩张得到，而域 $\mathbb{F}_{q^n}$ 由域 $\mathbb{F}_q$ 扩张得到，p 为素数，所以域 $\mathbb{F}_p$ 为域 $\mathbb{F}_{q^n}$ 的素域，域 $\mathbb{F}_{q^n}$ 的特征 $char(\mathbb{F}_{q^n})=p$，由域的特征的定义可知对 $\forall\gamma\in\mathbb{F}_{q^n}$：

$$p\cdot\gamma=0$$
$$\Rightarrow q\cdot\gamma=p^m\cdot\gamma=0$$

$\because 1\le k\le q-1,\ (q,k!(q-k)!)=1,\ \therefore q\sum\limits_{k=1}^{q-1}\frac{(q-1)!}{k!(q-k)!}\alpha^k\beta^{q-k}=0$，即

$$\sigma_q(\alpha+\beta)=\alpha^q+\beta^q+q\sum_{k=1}^{q-1}\frac{(q-1)!}{k!(q-k)!}\alpha^k\beta^{q-k}=\alpha^q+\beta^q=\sigma_q(\alpha)+\sigma_q(\beta)$$

所以映射 σ_q 保持加法。又因为

$$\sigma_q(\alpha\beta)=(\alpha\beta)^q=\alpha^q\beta^q=\sigma_q(\alpha)\sigma_q(\beta)$$

所以映射 σ_q 保持乘法。由同态的定义可知，σ_q 是 $\mathbb{F}_{q^n}$ 的自同态，要证明 σ_q 是 $\mathbb{F}_{q^n}$ 的自同构，只需证明 σ_q 为一一映射即可：

i. 先证明 σ_q 为单射，即证 $ker(\sigma_q)=\{0\}$，其中 0 为有限域 $\mathbb{F}_{q^n}$ 的加法零元，其中 $ker(\sigma_q)=\{a\in\mathbb{F}_{q^n}|\sigma_q(a)=0\}$，即被 σ_q 映射至加法零元的元素集合。$\because \sigma_q(a)=a^q=0\Rightarrow a=0,\ \therefore ker(\sigma_q)=0$，所以 σ_q 为单射。

ii. 再证 σ_q 为满射，由于 $\mathbb{F}_{q^n}$ 为有限域，只含有有限个元素，又 σ_q 是 $\mathbb{F}_{q^n}$ 自身到自身的映射，故 σ_q 单射必须是满的。

所以 σ_q 为 $\mathbb{F}_{q^n}$ 的自同构。因为有限域 $\mathbb{F}_q$ 中一共只有 q 个元素，其中元素的指数是 q 的因数，所以对 $\forall a\in\mathbb{F}_q,\ \sigma_q(a)=a^q=a$，所以 σ_q 为 $\mathbb{F}_{q^n}$ 的 $\mathbb{F}_q$-自同构，不动元是 $\mathbb{F}_q$。 ■

(b) 取 β 是 $\mathbb{F}_{q^n}$ 中的生成元，即 $\mathbb{F}_{q^n}=\{0\}\cup<\beta>$，证明：$\beta,\sigma_q(\beta),\dots,\sigma^{n-1}(\beta)$ 是 β 的共轭根。

Solution.
取 $f(x)$ 为生成元 β 的定义多项式，则 $f(x)$ 的形式可表示为 $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0,\ a_i\in\mathbb{F}_q$，当 $f(\beta)=\beta^n+a_{n-1}\beta^{n-1}+\cdots+a_1\beta+a_0=0$

时，有：

$$\begin{aligned}\sigma_q(f(\beta)) &= \sigma_q(\beta^n + a_{n-1}\beta^{n-1} + \cdots + a_1\beta + a_0) \\ &= \sigma_q(\beta^n) + \sigma_q(a_{n-1}\beta^{n-1}) + \cdots + \sigma_q(a_1\beta) + \sigma_q(a_0) \\ &= \sigma_q(\beta^n) + \sigma_q(a_{n-1})\sigma_q(\beta^{n-1}) + \cdots + \sigma_q(a_1)\sigma_q(\beta) + \sigma_q(a_0) \\ &= \sigma_q(\beta)^n + a_{n-1}\sigma_q(\beta)^{n-1} + \cdots + a_1\sigma_q(\beta) + a_0 \\ &= f(\sigma_q(\beta))\end{aligned}$$

因为 $\sigma_q(f(\beta)) = \sigma_q(0) = 0 = f(\sigma_q(\beta))$，所以 $\sigma_q(\beta)$ 也是定义多项式 $f(x)$ 的根。
归纳地可以得到：$\sigma_q^2(\beta), \sigma_q^3(\beta), \ldots, \sigma_q^{n-1}(\beta)$ 也都是定义多项式 $f(x)$ 的根。
由于 $f(x)$ 一共有 n 个根，所以 $\beta, \sigma_q(\beta), \ldots, \sigma^{n-1}(\beta)$ 是 β 的 $f(x)$ 的 n 个不同的根。 ■

(c) 证明：$\forall \tau \in G = Aut_{\mathbb{F}_q}\mathbb{F}_{q^n}$，存在 i 使得 $\tau(\beta) = \sigma_q^i(\beta),\ 0 \le i \le n-1$，其中 β 为域 $\mathbb{F}_{q^n}$ 的生成元。

Solution.
因为映射 τ 保持域 $\mathbb{F}_q$ 中的元素不动，所以有

$$\begin{aligned}f(\tau(\beta)) &= \tau(\beta)^n + a_{n-1}\tau(\beta)^{n-1} + \cdots + a_1\tau(\beta) + a_0 \\ &= \tau(\beta^n) + a_{n-1}\tau(\beta^{n-1}) + \cdots + a_1\tau(\beta) + a_0 \\ &= \tau(\beta^n) + \tau(a_{n-1})\tau(\beta^{n-1}) + \cdots + \tau(a_1)\tau(\beta) + \tau(a_0) \\ &= \tau(\beta^n) + \tau(a_{n-1}\beta^{n-1}) + \cdots + \tau(a_1\beta) + \tau(a_0) \\ &= \tau(\beta^n + a_{n-1}\beta^{n-1} + \cdots + a_1\beta + a_0) \\ &= \tau(f(\beta)) = \tau(0) = 0\end{aligned}$$

可见 $\tau(\beta)$ 也是 $f(x)$ 的根，又因为 $\beta, \sigma_q(\beta), \ldots, \sigma^{n-1}(\beta)$ 是 β 的 $f(x)$ 的所有 n 个不同的根，所以必然存在 i，使得 $\tau(\beta) = \sigma_q^i(\beta),\ 0 \le i \le n-1$。 ■

(d) 取定整数 d 使得 $d|n$，对所有满足条件 $\sigma^d(\alpha) = \alpha, \alpha \in \mathbb{F}_{q^n}$ 的 α，在正规基底 $[\beta, \sigma(\beta), \sigma^2(\beta), \ldots, \sigma^{n-1}(\beta)]$ 下写出元素 α 的坐标：$\alpha = a_0\beta + a_1\sigma(\beta) + a_2\sigma^2(\beta) + \cdots + a_{n-1}\sigma^{n-1}(\beta)$，其中 $a_0, a_1, a_2, \ldots, a_{n-1} \in \mathbb{F}_q$。请确定系数 $a_0, a_1, a_2, \ldots, a_{n-1}$ 之间的关系。

Solution.

$$
\begin{aligned}
\alpha &= a_0\beta + a_1\sigma(\beta) + a_2\sigma^2(\beta) + \cdots + a_{n-1}\sigma^{n-1}(\beta) \\
\sigma^d(\alpha) &= \sigma^d(a_0\beta + a_1\sigma(\beta) + a_2\sigma^2(\beta) + \cdots + a_{n-1}\sigma^{n-1}(\beta)) \\
&= \sigma^d(a_0\beta) + \sigma^d(a_1\sigma(\beta)) + \sigma^d(a_2\sigma^2(\beta)) + \cdots + \sigma^d(a_{n-1}\sigma^{n-1}(\beta)) \\
&= \sigma^d(a_0)\sigma^d(\beta) + \sigma^d(a_1)\sigma^d(\sigma(\beta)) + \sigma^d(a_2)\sigma^d(\sigma^2(\beta)) + \cdots + \sigma^d(a_{n-1})\sigma^d(\sigma^{n-1}(\beta)) \\
&= a_0\sigma^d(\beta) + a_1\sigma^{d+1}(\beta) + a_2\sigma^{d+2}(\beta) + \cdots + a_{n-1}\sigma^{d+n-1}(\beta)
\end{aligned}
$$

$\because \sigma^d(\alpha) = \alpha$ 且 σ^n 为恒等映射,对比相应基底的系数可知:排列 $(a_0, a_1, a_2, \ldots, a_{n-1})$ 循环右移 d 位后与原先的排列相同。也就是说:

$$
\begin{array}{rrrrr}
a_0 = & a_d = & a_{2d} = & \ldots = & a_{(\frac{n}{d}-1)d} \\
a_1 = & a_{d+1} = & a_{2d+1} = & \ldots = & a_{(\frac{n}{d}-1)d+1} \\
\cdots & & & & \\
a_{d-1} = & a_{2d-1} = & a_{3d-1} = & \ldots = & a_{n-1}
\end{array}
$$

回到题目的问题，系数 $a_0, a_1, a_2, \ldots, a_{n-1}$ 之间的关系就是每隔 d 项的系数相等，独立的系数只有 $d-1$ 个，将系数相同的基底合并起来可以写成如下的抽象的形式:

$$
\begin{aligned}
\mathbf{I}(\sigma_q^d) &= \{\alpha | \sigma^d(\alpha) = \alpha\} \\
&= \{a_0\gamma + a_1\sigma(\gamma) + a_2\sigma^2(\gamma) + \cdots + a_{d-1}\sigma^{d-1}(\gamma) | \gamma = \beta + \sigma^d(\beta) + \sigma^{2d}(\beta) + \ldots \\
&\quad + \sigma^{(\frac{n}{d}-1)d}(\beta)\}
\end{aligned}
$$

其中 a_0 到 a_{d-1} 是独立的系数个数，γ 为相同系数的基底合并后的简写。

具体来说 取 $n = 8, d = 2, d|n$, 所以 $(a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7)$ 循环右移 2 位后为 $(a_6, a_7, a_0, a_1, a_2, a_3, a_4, a_5)$，与原先相等，即

$$
\begin{aligned}
&(a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7) \\
=&(a_6, a_7, a_0, a_1, a_2, a_3, a_4, a_5)
\end{aligned}
$$

所以 $a_0 = a_2 = a_4 = a_6, a_1 = a_3 = a_5 = a_7$，$\alpha$ 可表示为

$$
\begin{aligned}
\mathbf{I}(\sigma_q^d) &= \{\alpha | \sigma^d(\alpha) = \alpha\} \\
&= \{a_0\gamma + a_1\sigma(\gamma) | \gamma = \beta + \sigma^2(\beta) + \sigma^4(\beta) + \sigma^6(\beta)\}
\end{aligned}
$$

■

4. 设 $\mathbb{F}_7$ 上的椭圆曲线 $E: y^2 = x^3 + x + 6$，求椭圆曲线点群 $E(\mathbb{F}_7)$ 的所有子群及生成元。

> **知识点** 二次剩余，勒让德符号

Solution.
$\because p = 7,\ \therefore \mathbb{F}_7 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$

$$\begin{aligned}
&x = 0,\quad y^2 = x^3 + x + 6 = 6,\quad \textit{no solution}((\frac{6}{7}) = -1)\\
&x = 1,\quad y^2 = x^3 + x + 6 = 1,\quad y = 1, 6\\
&x = 2,\quad y^2 = x^3 + x + 6 = 2,\quad y = 3, 4\\
&x = 3,\quad y^2 = x^3 + x + 6 = 1,\quad y = 1, 6\\
&x = 4,\quad y^2 = x^3 + x + 6 = 4,\quad y = 2, 5\\
&x = 5,\quad y^2 = x^3 + x + 6 = 3,\quad \textit{no solution}((\frac{3}{7}) = -1)\\
&x = 6,\quad y^2 = x^3 + x + 6 = 4,\quad y = 2, 5
\end{aligned}$$

枚举元素：

$$E(\mathbb{F}_7) = O \cup \{(1, 1), (1, 6), (2, 3), (2, 4), (3, 1), (3, 6), (4, 2), (4, 5), (6, 2), (6, 5)\}$$

所以椭圆曲线点群 $E(\mathbb{F}_7)$ 中元素个数为 $\#(E(\mathbb{F}_7)) = 11$
若点 $P(x_k, y_k)$ 是该点群 $E(\mathbb{F}_7)$ 的元素，则 P 的阶必定为椭圆曲线点群 $E(\mathbb{F}_7)$ 中元素个数 11 的因数。由于 11 是素数，所以该群没有除平凡子群外的子群（平凡子群即零元和群自身）。
所以任何一个非无穷远点都是该群的生成元。 ■

3 鸣谢

特别感谢马可凡同学的帮助，不然作者本人也看不懂题，也就整理不出本文档。