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.

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

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

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

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

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

■

2. 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*

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 $\forall \gamma \in \mathbb{F}_{q^n}$：

$$\begin{aligned} p \cdot \gamma &= 0 \\ \Rightarrow q \cdot \gamma &= p^m \cdot \gamma = 0 \end{aligned}$$

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

(b) 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：

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

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：

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

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

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

■