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

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

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

   (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 $(a_0,a_1,a_2,\dots,a_{n-1})$ 循环右移 d 位后与原先的排列相同。也就是说:

$$\begin{aligned}
a_0 = \quad & a_d = & a_{2d} = & \quad \dots = & a_{(\frac{n}{d}-1)d} \\
a_1 = \quad & a_{d+1} = & a_{2d+1} = & \quad \dots = & a_{(\frac{n}{d}-1)d+1} \\
\dots & & & & \\
a_{d-1} = \quad & a_{2d-1} = & a_{3d-1} = & \quad \dots = & a_{n-1}
\end{aligned}$$

回到题目的问题，系数 $a_0,a_1,a_2,\dots,a_{n-1}$ 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：

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

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

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

■