问题 3.83 的详细解答

问题： 设 b 是素域 $\mathbb{F}_p$ 中的非零元素。证明三项式 $x^p - x - b$ 在 $\mathbb{F}_{p^n}[x]$ 中不可约当且仅当 n 不被 p 整除。

证明：

设 $f(x) = x^p - x - b$，其中 $b \in \mathbb{F}_p^*$。

1. **根的性质与分裂域：**
   - 设 α 是 $f(x) = 0$ 的一个根，即 $\alpha^p - \alpha - b = 0$ 或 $\alpha^p = \alpha + b$。
   - 应用 Frobenius 自同构 $\sigma : x \mapsto x^p$ 重复作用：

     $$\alpha^{p^2} = (\alpha^p)^p = (\alpha + b)^p = \alpha^p + b^p = (\alpha + b) + b = \alpha + 2b,$$

     因为 $b \in \mathbb{F}_p$，有 $b^p = b$。一般地：

     $$\alpha^{p^k} = \alpha + kb, \quad k = 0, 1, 2, \ldots$$

   - 因此，$f(x)$ 的所有根为：

     $$\alpha,\ \alpha + b,\ \alpha + 2b,\ \ldots,\ \alpha + (p-1)b.$$

     共有 p 个不同的根（因为 $b \neq 0$）。
   - 所以 $f(x)$ 的分裂域是 $\mathbb{F}_p(\alpha)$，且 α 在 $\mathbb{F}_p$ 上的最小多项式次数为 $\deg(m_{\alpha,\mathbb{F}_p}) = [\mathbb{F}_p(\alpha) : \mathbb{F}_p] = p$（因为根集有 p 个元素，且无真子域包含 α）。
2. **在 $\mathbb{F}_{p^n}$ 上的最小多项式：**
   - 考虑基域 $\mathbb{F}_{p^n}$。α 在 $\mathbb{F}_{p^n}$ 上的最小多项式 $m_{\alpha,\mathbb{F}_{p^n}}(x)$ 是 $f(x)$ 的不可约因子，其次数为：

     $$\deg(m_{\alpha,\mathbb{F}_{p^n}}) = [\mathbb{F}_{p^n}(\alpha) : \mathbb{F}_{p^n}].$$

   - 扩张次数计算：

     $$[\mathbb{F}_{p^n}(\alpha) : \mathbb{F}_{p^n}] = \frac{[\mathbb{F}_{p^n}(\alpha) : \mathbb{F}_p]}{[\mathbb{F}_{p^n} : \mathbb{F}_p]} = \frac{[\mathbb{F}_p(\alpha, \mathbb{F}_{p^n}) : \mathbb{F}_p]}{n}.$$

     由于 $\mathbb{F}_p(\alpha) \subseteq \mathbb{F}_{p^n}(\alpha)$ 且 $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^n}(\alpha)$，复合域 $\mathbb{F}_p(\alpha, \mathbb{F}_{p^n}) = \mathbb{F}_p(\alpha) \cdot \mathbb{F}_{p^n}$ 是 $\mathbb{F}_p(\alpha)$ 和 $\mathbb{F}_{p^n}$ 的复合。
   - 域扩张维度公式：

$$[\mathbb{F}_p(\alpha)\cdot\mathbb{F}_{p^n}:\mathbb{F}_p]=\frac{[\mathbb{F}_p(\alpha):\mathbb{F}_p]\cdot[\mathbb{F}_{p^n}:\mathbb{F}_p]}{[\mathbb{F}_p(\alpha)\cap\mathbb{F}_{p^n}:\mathbb{F}_p]}=\frac{p\cdot n}{d},$$

其中 $d=[\mathbb{F}_p(\alpha)\cap\mathbb{F}_{p^n}:\mathbb{F}_p]$。

- 由于 $\mathbb{F}_p(\alpha)\cong\mathbb{F}_{p^p}$ 和 $\mathbb{F}_{p^n}\cong\mathbb{F}_{p^n}$，它们的交集 $\mathbb{F}_p(\alpha)\cap\mathbb{F}_{p^n}=\mathbb{F}_{p^d}$ 满足 $d=\gcd(p,n)$。
  > 有限域 $\mathbb{F}_{p^a}\cap\mathbb{F}_{p^b}=\mathbb{F}_{p^{\gcd(a,b)}}$。
- 因此：

$$[\mathbb{F}_{p^n}(\alpha):\mathbb{F}_{p^n}]=\frac{p\cdot n/\gcd(p,n)}{n}=\frac{p}{\gcd(p,n)}.$$

3. **不可约的充要条件：**
   - $f(x)$ 在 $\mathbb{F}_{p^n}[x]$ 中不可约当且仅当它是 α 在 $\mathbb{F}_{p^n}$ 上的最小多项式，即当：

$$\deg(m_{\alpha,\mathbb{F}_{p^n}})=p.$$

   由上式，这等价于：

$$\frac{p}{\gcd(p,n)}=p\iff\gcd(p,n)=1\iff p\nmid n.$$

   - 若 $p\mid n$，则 $\gcd(p,n)=p$，此时：

$$\deg(m_{\alpha,\mathbb{F}_{p^n}})=\frac{p}{p}=1,$$

   故 $f(x)$ 在 $\mathbb{F}_{p^n}$ 中有根（可约）。

结论： x^p-x-b 在 $\mathbb{F}_{p^n}[x]$ 中不可约当且仅当 $p\nmid n$。

证明完成

问题 3.84 的详细解答

问题： 证明形式为 $x^q-ax-b\in\mathbb{F}_q[x]$（其中 $a\neq1$）的任意多项式在 $\mathbb{F}_q$ 中有根。

证明：

设 $g(x)=x^q-ax-b\in\mathbb{F}_q[x]$，其中 $a,b\in\mathbb{F}_q$ 且 $a\neq1$。

1. **利用 Frobenius 自同构：**

- 在有限域 $\mathbb{F}_q$ 中，Frobenius 自同构 $\sigma : x \mapsto x^q$ 满足 $\sigma(c) = c$ 对所有 $c \in \mathbb{F}_q$ 成立（即 $c^q = c$）。
- 因此，对任意 $c \in \mathbb{F}_q$，有：

$$g(c) = c^q - ac - b.$$

代入 $c^q = c$ 得：

$$g(c) = c - ac - b = (1 - a)c - b.$$

2. **解代数方程：**
   - 设 $g(c) = 0$，即：

$$(1 - a)c - b = 0 \iff (1 - a)c = b.$$

   - 由于 $a \neq 1$，有 $1 - a \neq 0$。在域 $\mathbb{F}_q$ 中，$1 - a$ 有乘法逆元 $(1 - a)^{-1}$。
   - 解出 c：

$$c = b \cdot (1 - a)^{-1}.$$

   由于 $b \in \mathbb{F}_q$ 且 $(1 - a)^{-1} \in \mathbb{F}_q$，故 $c \in \mathbb{F}_q$.
3. **验证根的存在性：**
   - 对 $c = b(1 - a)^{-1}$，直接计算：

$$g(c) = c^q - ac - b = c - ac - b = (1 - a)c - b = (1 - a) \cdot \left(\frac{b}{1 - a} \right) - b = b - b = 0.$$

   - 因此 c 是 $g(x) = 0$ 的一个根。

结论： 任意多项式 $x^q - ax - b$ $(a \neq 1)$ 在 $\mathbb{F}_q$ 中有根 $c = b(1 - a)^{-1}$.

证明完成