> **命题 3.12（可逆多项式的不可约性）**
> 设 $f(x) \in \mathbb{F}_q[x]$ 是**不可约多项式**，并且满足 $f(0) \neq 0$，则它的**互反多项式（reciprocal polynomial）**

$$f^*(x) := x^{\deg f} f\left(\frac{1}{x}\right)$$

在 $\mathbb{F}_q[x]$ 中也是不可约的。

✅ 预备知识

✅ 互反多项式（Reciprocal Polynomial）

若 $f(x) = a_0 + a_1 x + \cdots + a_d x^d$，则它的互反多项式是：

$$f^*(x) = x^d f\left(\frac{1}{x}\right) = a_d + a_{d-1} x + \cdots + a_0 x^d$$

即把系数翻转，首项变末项，末项变首项。

这个定义前提是：$f(0) \neq 0$，这样才不会在 $x = 0$ 处有极点。

🧠 要证明的目标：

我们要证明：

> 若 $f \in \mathbb{F}_q[x]$ 是不可约，且 $f(0) \neq 0$，则 $f^*(x)$ 也是不可约的。

✅ 证明

我们采用**反证法**。假设 f^* 是**可约的**，我们将推导出 f 也必须是可约的，矛盾。

第一步：f^* 可约的假设

假设

$$f^*(x) = g(x)h(x)$$

其中 $g, h \in \mathbb{F}_q[x]$ 且 $\deg g, \deg h < \deg f$，即 f^* 是非平凡可约的。

第二步：构造互反再互反还原原多项式

我们注意到一个重要性质：

> 对任意 $f(x)$ 满足 $f(0) \neq 0$，有：
>
> $$(f^*)^*(x) = f(x)$$

即互反两次等于原多项式。

因为：

$$(f^*)^*(x) = x^d f^*\left(\frac{1}{x}\right) = x^d \cdot x^{-d} f(x) = f(x)$$

第三步：将因式分解带入互反

我们有：

$$f^* = g \cdot h \Rightarrow f = (f^*)^* = (gh)^* = g^* \cdot h^*$$

由于 g, h 次数都小于 $\deg f$，所以 g^*, h^* 的次数也小于 $\deg f$，因为互反不改变次数。

所以：

- $f = g^* h^*$ 是一个**非平凡因式分解**，与 f 是不可约的假设矛盾。

✅ 结论

所以我们只能推出：

- 若 $f(x)$ 在 $\mathbb{F}_q[x]$ 上不可约，且 $f(0) \neq 0$,
- 则它的互反多项式 $f^*(x)$ 也在 $\mathbb{F}_q[x]$ 中不可约。

$$\boxed{\text{If } f \in \mathbb{F}_q[x] \text{ is irreducible and } f(0) \neq 0, \text{ then } f^*(x) \text{ is irreducible over } \mathbb{F}_q.}$$

🔎 补充说明

- $f(0) \neq 0$ 是必要条件；否则 $f^*(x)$ 包含 x 的因子（最低次项为 0），会导致不可逆或有零因子。
- 该结论在有限域上应用广泛，比如构造本原多项式时经常会同时考虑其互反性。

> **命题 3.13（自互反多项式的因子结构）**
> 设 $f \in \mathbb{F}_q[x]$ 是非零自互反多项式（即 $f = f^*$），并满足：

$$f = gh, \quad \text{其中 } g, h \in \mathbb{F}_q[x] \text{ 都是不可约的}$$

则有两种可能：

- (i) $h^* = ag$，其中 $a \in \mathbb{F}_q^*$，即 g 与 h^* 成比例；
- (ii) $g^* = bg$，$h^* = bh$，其中 $b = \pm 1$，即 g, h 都是自互反多项式（up to sign）。

🧠 关键概念

1. **互反多项式**：
   给定 $f(x) \in \mathbb{F}_q[x]$，其互反多项式为：

$$f^*(x) := x^{\deg f} f\left(\frac{1}{x}\right)$$

   它是将多项式的系数“反转”。
2. **自互反多项式**：
   若 $f = f^*$，则称 f 是自互反的（self-reciprocal）。

✅ 证明思路概览

已知 $f = gh$，且 $f = f^*$，我们利用互反的分布性：

$$f^* = (gh)^* = h^* g^*$$

而又因 $f = f^*$，所以：

$$gh = h^* g^*$$

我们想研究这个式子在不可约因子意义下说明了什么。

🧩 分析因式结构

我们有两个表达式相等：

$$gh = h^* g^*$$

两边都是 $\mathbb{F}_q[x]$ 中的**因式分解**，由于 g, h 都是不可约的，我们来分析右边是怎么构成左边的。

🧷 情况一：g 与 h^* 成比例

假设存在 $a \in \mathbb{F}_q^*$，使得 $h^* = ag$。

那么：

- $g^* = a^{-1} h,$
- 所以右边变为：

  $$h^* g^* = (ag)(a^{-1}h) = gh$$

  与左边相等。
  ✅ 这种情况下成立，对应 **情况 (i)**。

📎 情况二：$g^* = \lambda g$，$h^* = \lambda h$，且 $\lambda^2 = 1$

假设 $g^* = \lambda g$，$h^* = \lambda h$，其中 $\lambda \in \mathbb{F}_q^*$。

代入右边：

$$f^* = h^* g^* = (\lambda h)(\lambda g) = \lambda^2 hg = \lambda^2 f$$

但又已知 $f = f^*$，所以：

$$f = \lambda^2 f \Rightarrow \lambda^2 = 1 \Rightarrow \lambda = \pm 1$$

这对应于 g, h 都是自互反（或负自互反）：

- $g^* = \pm g$，$h^* = \pm h$

✅ 这对应于 **情况 (ii)**。

🔚 结论总结

我们已经覆盖了所有可能，使得 $gh = h^* g^*$ 与 $f = f^*$ 同时成立的情况，唯一的可能就是以下二者之一：

$$\boxed{\begin{array}{l} \text{若 } f = gh \text{ 且 } f = f^*\text{，则：} \\ \text{(i) } h^* = ag\text{，对某个 } a \in \mathbb{F}_q^*; \\ \text{或 (ii) } g^* = bg, h^* = bh \text{ 且 } b = \pm 1. \end{array}}$$