1. $\alpha \in E, \alpha \notin F \Rightarrow E \supseteq F(\alpha) \supseteq F$

$\Rightarrow [E:F] = [E:F(\alpha)][F(\alpha):F] = p$

$\Rightarrow [F(\alpha):F] = p$ 或 1

当 $[F(\alpha):F]$ 时, $F(\alpha) = F \Rightarrow \alpha \in F$, 矛盾

$\Rightarrow [F(\alpha):F] = p$, $[E:F(\alpha)] = 1$

$\Rightarrow E = F(\alpha)$

3. $u^2 \in F(u) \Rightarrow F \subseteq F(u^2) \subseteq F(u)$

$\Rightarrow [F(u):F] = [F(u):F(u^2)][F(u^2):F]$

若 $[F(u^2):F]$ 为偶数, 则 $[F(u):F]$ 为偶数, 矛盾

$\Rightarrow [F(u^2):F]$ 为奇数

又因为 $F(u) = F(u^2, u) = F(u^2)(u)$

即 $F(u)$ 为 $F(u^2)$ 上的单扩域

$x^2 - u^2 \in F(u^2)[x] \Rightarrow u$ 在 $F(u^2)$ 上的极小多项式 $q(x) \mid x^2 - u^2$

又 $[F(u):F(u^2)]$ 为奇数 $\Rightarrow [F(u):F(u^2)] = 1$

$\Rightarrow F(u) = F(u^2)$

4. α 是 E 上的代数元, 设 α 满足 $f(x) = \sum_{i=0}^{n} a_i x^i$

$F(a_0, a_1, \cdots, a_n)$ 是 F 上的有限扩域

α 是 $F(a_0, a_1, \cdots, a_n)$ 上的代数元

$\Rightarrow F(a_0, a_1, \cdots, a_n, \alpha)$ 是 $F(a_0, a_1, \cdots, a_n)$ 的代数扩域

$\Rightarrow \alpha$ 是 F 上的代数元

11. $\mathbb{Z}_2/\langle x^2+x+1\rangle = \{0, 1, x, x+1\}$

+	0	1	x	x+1
0	0	1	x	x+1
1	1	0	x+1	x
x	x	x+1	0	1
x+1	x+1	x	1	0

*	0	1	x	x+1
0	0	0	0	0
1	0	1	x	x+1
x	0	x	x+1	1
x+1	0	x+1	1	x

是域

13. $F_9 = \{0, 1, 2, \alpha, 1+\alpha, 2+\alpha, 2\alpha, 1+2\alpha, 2+2\alpha\}$

其中 α 满足 $f(\alpha) = \alpha^2+1 = 0$

本原元为 $\xi = 1+\alpha$, ξ^3, ξ^5, ξ^7

$F_{17} = \mathbb{Z}_{17} = \{0, 1, 2, \cdots, 16\}$

本原元为 3, 10, 5, 11, 14, 7, 12, 6

15. $F_{25} = \{a\alpha+b \mid a, b \in F_5\}$

$= \{0, 1, 2, 3, 4,$

$\alpha, \alpha+1, \alpha+2, \alpha+3, \alpha+4,$

$2\alpha, 2\alpha+1, 2\alpha+2, 2\alpha+3, 2\alpha+4,$

$3\alpha, 3\alpha+1, 3\alpha+2, 3\alpha+3, 3\alpha+4,$

$4\alpha, 4\alpha+1, 4\alpha+2, 4\alpha+3, 4\alpha+4\}$

21. $f(x) = x^3+x+1$

$$A = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

$F_8 = \{ 0, I, A, A+I, A^2, A^2+I, A^2+A, A+I \}$

其中 $0 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$, $I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

22. 假设 F 为无限域

因为 F^* 是循环群 $\Rightarrow$ $\exists\, a \in F^*$ s.t. $F^* = F \setminus \{0\} = \langle a \rangle$

$\langle a \rangle = \{ \cdots, a^{-2}, a^{-1}, 1, a^1, a^2, \cdots \}$

若 $\mathrm{char} F \neq 2$, 则 $-1 \neq 1$

而 $(-1)^2 = 1$, 不是无限阶元, 矛盾

若 $\mathrm{char} F = 2$, 则 $\exists\, n$ s.t. $1 + a = a^n$

$\Rightarrow$ a 是 $F_2 = \{0, 1\}$ 上的代数元

$\Rightarrow$ $F = F_2(a)$ 为有限扩张

$\Rightarrow$ F 是有限域, 矛盾

所以 F 为有限域