F/E为域的 $|F| = p^n$ $F^* = (r)$

$\boxed{F^* = F\backslash\{0\}}$ $\boxed{p^n-1}$阶循环 $= \{1, r, r^2, \dots, r^{p^n-2}\}$

$= E(r)$

(1) 记 $E = \{me: m \in \mathbb{Z}\}$ 为 F 的最小子域 其中 e 为 F 的乘法单位元。证明 F/E 为域的单扩张，即有 $\gamma \in F$ 使得 $F = E(\gamma)$.

易知 $m=p$

由于 $F^* = F/\{0\}$ 为 p^n-1阶循环群 即有生成元 γ. $\forall \alpha \in F$. $\alpha = \gamma^k$. $k = 0, 1, \dots, p^n-2$

故 $\forall \alpha \in F$

$\alpha = a_0 + a_1\gamma^1 + \dots + a_{p^n-2}\gamma^{p^n-2}$ 其中 $a_1 \dots a_n \in E$ $e \in E$. $0 \in E$.

从而 F/E 为域的单扩张 即 $\exists \gamma \in F$ s.t. $F = E(\gamma)$ $\alpha = a_0 + a_1\gamma^1 + \dots + a_{p^n-2}\gamma^{p^n-2}$.

P113. 3.6.3.(2) $F = \{0, r, r^2, \dots, r^{p^n-2}\} = E(r)$.

P116. 3.7.1. 九、（10分）以下两小题任选一题

(i) 设 R 为主理想整环，证明 R 中非零非单位元 a 必有不可约因子。[提示：利用 R 为 Noether 环]

P112. 3.6.3. (ii) 用反证法证明多项式环 $\mathbb{Z}[x]$ 中理想 $I = (2, x)$（由 2 与 x 生成）不是主理想。

记 R 为 PID

则 R 的每个理想均为主理想，且 R 中的不可约元 $\Leftrightarrow$ 素元

素元也为不可约元

① 若 a 本身为不可约元 则 a 的不可约因子为 a

② 若 a 不为不可约元 则 a 也不是素元

从而 $\exists a_1$ s.t. $a_1 | a$

同样对 a_1 讨论 ①② 可得 $\exists k$ s.t. a_k 为素元

从而 $a_k | a$ a_k 即为 a 的不可约因子

R为PID 故：不可约元 $\Leftrightarrow$ 素元.

取 a 非0非单位

1) a 不可约. √

2) a 不是不可约元. a 也不是素元.

$\exists a_1$, $a_1 | a$ 且 $a \nmid a_1$

$\langle a_1 \rangle$. ~~$a \in \langle a_1 \rangle$~~ 且 $\langle a \rangle \subsetneq \langle a_1 \rangle$

显然 $\langle a_0 \rangle \subsetneq \langle a_1 \rangle \subsetneq \cdots$ 无限升的理想升链.

与 R 为 Noether 环矛盾

$\mathbb{Z}[x]$ 为交换幺环.

故 $\langle 2, x \rangle = \{2f_1(x) + x f_2(x) \mid f_1(x), f_2(x) \in \mathbb{Z}[x]\}$

$= \{2a_0 + a_1x + \dots + a_nx^n : a_i \in \mathbb{Z}, n \geq 0\}$

若 $\langle 2, x \rangle = (g(x))$ $\exists p(x) \in \mathbb{Z}[x]$ s.t. $p(x)g(x) = 2$

$g(x) | 2$ $\Rightarrow g(x) = b \neq 0$

$b | x$ $\Rightarrow b = \pm 1$.

矛盾

$2 = g(x)s(x)$

$x = g(x)t(x)$

$g(x) = c$ 为非零整数.

故 $x = c\,t(x)$ $c = \pm 1$

$g(x) = \pm 1 \notin (2, x)$ 矛盾!