①

关于素域

书上 P138 定理4 写得比较简略

以下是详细的说明.

1. 特征零情形

设 $(F, +, 0, \cdot, 1)$ 是特征零的域,

$U = \{ m(n\cdot 1)^{-1} \mid m \in \mathbb{Z}, n \in \mathbb{Z}\setminus\{0\} \}$

断言: U 是 F 的素域

断言的证明:

因为 $\mathrm{char}(F) = 0$, 所以 $n\cdot 1 \neq 0$

于是 U 是良定义的.

设 $u_1, u_2 \in U$. 则 $\exists\, m_1, m_2 \in \mathbb{Z}$, $n_1, n_2 \in \mathbb{Z}\setminus\{0\}$

使得 $u_1 = m_1 (n_1\cdot 1)^{-1}$, $u_2 = m_2 (n_2\cdot 1)^{-1}$

$$u_1 - u_2 = m_1 (n_1\cdot 1)^{-1} - m_2 (n_2\cdot 1)^{-1}$$

$$= \left[m_1 (n_1\cdot 1)^{-1} - m_2 (n_2\cdot 1)^{-1} \right] \left((n_1 n_2)\cdot 1\right)\left[(n_1 n_2)\cdot 1\right]^{-1}$$

(去分母)

$$= \left[m_1 (n_1\cdot 1)^{-1} (n_1 n_2 \cdot 1) - m_2 (n_2\cdot 1)^{-1} (n_1 n_2 \cdot 1) \right] (n_1 n_2 \cdot 1)^{-1}$$

$$= \left((m_1 n_2)\cdot 1 - (m_2 n_1)\cdot 1 \right) (n_1 n_2 \cdot 1)^{-1} \quad (\text{于}\ F\ \text{分配律})$$

$$= (m_1 n_2 - m_2 n_1)(n_1 n_2 \cdot 1)^{-1} \in U$$

于是 $(U, +, 0)$ 是 $(F, +, 0)$ 的子群.

$$u_1 u_2 = \left[m_1 (n_1\cdot 1)^{-1} \right] \left[m_2 (n_2\cdot 1)^{-1} \right]$$

$$= (m_1 m_2) \left[(n_1\cdot 1)^{-1} (n_2\cdot 1)^{-1} \right] \quad (\text{于}\ F\ \text{分配律})$$

$$= (m_1 m_2) (n_1 n_2 \cdot 1)^{-1} \quad (\text{于}\ F\ \text{分配律, 乘法逆元})$$

于是 $u_1 u_2 \in U$

$1 = 1\cdot 1^{-1} \in U$

于是 $(U, \cdot, 1)$ 是含幺半群.

设 $u_1 \neq 0$, 则 $m_1 \neq 0$. 令 $v_1 = n_1 \cdot (m_1\cdot 1)^{-1}$

$$u_1 v_1 = \left(m_1 \cdot (n_1\cdot 1)^{-1} \right) \left(m_1 (m_1\cdot 1)^{-1} \right)$$

$$= \left[(m_1\cdot 1)(n_1\cdot 1)^{-1} \right] \left[(n_1\cdot 1)(m_1\cdot 1)^{-1} \right]$$

$= (m_1 \cdot 1)(m_1 \cdot 1)^{-1} \quad (n_1 \cdot 1)^{-1}(n_1 \cdot 1) = 1$

于是 v_1 是 u_1 的乘法逆. 且 $v_1 \in U$.

又因为 $U \subset F$, 所以 F 的所有运算

规律在 U 上都满足. U 是 F 的子域

设 K 是 F 的任一子域. 则 $1 \in K$

$\forall\, n \in \mathbb{Z} \setminus \{0\} \qquad n \cdot 1 \in K$

$\Rightarrow \quad (n \cdot 1)^{-1} \in K \Rightarrow \forall\, m \in \mathbb{Z},\ m(n \cdot 1)^{-1} \in K$

$\Rightarrow U \subset K$

于是 U 是 F 的"最小子域"

即素域

2. 特征 $p > 0$ 情形

设 $(F, +, 0, \cdot, 1)$ 的特征为 p.

设 $U = \{ m \cdot 1 \mid m \in \{0, 1, \cdots p-1\} \}$

断言: U 是 F 的素域

断言的证明

设 $u_1, u_2 \in U$. 则 $\exists\, m_1, m_2 \in \{0, 1, \cdots p-1\}$

使得 $u_1 = m_1 \cdot 1 \qquad u_2 = m_2 \cdot 1$

$u_1 - u_2 = (m_1 - m_2) \cdot 1$

由带余除法: $(m_1 - m_2) = qp + r. \quad r \in \{0, 1, \cdots p-1\}$

$u_1 - u_2 = qp \cdot 1 + r \cdot 1 = r \cdot 1 \in U$

于是 $(U, +, 0)$ 是 $(F, +, 0)$ 的子群

$u_1 \cdot u_2 \subseteq m_1 m_2 \cdot 1$

由带余除法 $m_1 \cdot m_2 = qp + r, \ r \in \{0, 1 \cdots p-1\}$

$u_1 m_2 = qp \cdot 1 + r \cdot 1 = r \cdot 1 \in U$

$1 \in U$

$\Rightarrow (U, \cdot, 1)$ 是含幺子群

设 $m_1 \neq 0$. 则 $\gcd(m_1, p) = 1$. $\exists\, \alpha, \beta \in \mathbb{Z}$

$\alpha m_1 + \beta p = 1 \quad \Rightarrow \quad 1 = \alpha m_1 \cdot 1 + \beta p \cdot 1$

$\Rightarrow \quad 1 = (\alpha \cdot 1)(m_1 \cdot 1). \Rightarrow (\alpha \cdot 1) = (m_1 \cdot 1)^{-1}$

③

再由带余除法可知：

α 可取为 $\{0, 1, 2, \cdots p-1\}$ 中的

某数

于是 $(m \cdot 1)^{-1} \in U$.

即 U 是 F 的子域

设 K 是 F 的任一子域

于 $1 \in K$. 由此可知

$\forall n \in \mathbb{Z} \quad n \cdot 1 \in K$

$\Rightarrow U \subset K$ 图