有限体の拡大体の存在について

BV21064 山下泰平

令和 5 年 5 月 21 日

目次

1　研究背景

有限体 $\mathbb{F}_p$ という有限個の元からなる体は有限という特性上，純粋数学だけでなく応用数学でも重要な研究対象である．そのため，任意の $n \in \mathbb{Z}_{\geq 0}$ に対して，$\mathbb{F}_p$ の n 次拡大体が存在するという定理の理解は今後，有限体の研究を行う上で重要だと考え，研究対象とした．

2　単拡大

2.1　部分体，拡大体

定義 2.1. 体 E の部分集合 F が少なくとも二つの元を含み，

(1) $x,\ y \in F \Rightarrow x - y \in F,\ xy \in F$
(2) $a \in F,\ a \neq 0 \Rightarrow a^{-1} \in F$

を満たすとき，F を E の部分体 (subfield) という．

体 F が体 E の部分体であるとき，E を F の拡大体 (extension field) といい，拡大 E/F で表す．また，体の拡大 E/F において，$F \subseteq E' \subseteq E$ である E の部分体 E' を拡大 E/F の中間体 (intermediate field) という．

定義 2.2. F を体 E の部分体，T を E の部分集合，$\{F_\alpha\}$ を T を含む E/F の中間体の族とする．$E \in \{F_\alpha\}$ であるから，$\{F_\alpha\}$ は空でない．また，$T \subseteq \bigcap_\alpha F_\alpha \subseteq F_\alpha$ であるから，$\bigcap_\alpha F_\alpha$ は F と T とを含む最小の E の部分体である．この $\bigcap_\alpha F_\alpha$ を $F(T)$ で表し，F 上 T で生成される体または F に T を添加して得られる体という．T が有限集合 $\{t_1, \ldots, t_n\}$ のとき，$F(T) = F(t_1, \ldots, t_n)$ を F 上有限生成である体という．とくに，$F(t)$ を単拡大体 (simple extension field) といい，$F(t)/F$ を単拡大 (simple extension) という．また，t を体 $F(t)$ の F 上の原始元 (primitive element) という．

定理 2.3. F を体 E の部分体，T, T_1, T_2 を E の部分集合とする．このとき，(1)-(3) が成り立つ．

(1) $F(T_1 \cup T_2) = F(T_1)(T_2)$.
(2) T の有限部分集合を S とするとき，$F(T) = \bigcup_S F(S)$（和集合）である．
(3) $T = \{t_1, \ldots, t_n\}$ が有限集合のとき

$$F(T) = \left\{ \frac{f(t_1, \ldots, t_n)}{g(t_1, \ldots, t_n)} \middle| f, g \in F[X_1, \ldots, X_n], g(t_1, \ldots, t_n) \neq 0 \right\}$$

である．

証明. (1)F, $T_1 \subseteq F(T_1)$ であり，$F(T_1)$, $T_2 \subseteq F(T_1)(T_2)$ であるから，F, T_1, $T_2 \subseteq F(T_1)(T_2)$ で F, $T_1 \cup T_2 \subseteq F(T_1)(T_2)$ である．一方，$F(T_1 \cup T_2)$ は F, $T_1 \cup T_2$ を含む最小の E の部分体であるから，$F(T_1 \cup T_2) \subseteq F(T_1)(T_2)$ となる．逆に，F, T_1, $T_2 \subseteq F(T_1 \subseteq T_2)$ であるから，$F(T_1)$, $T_2 \subseteq F(T_1 \cup T_2)$ である．よって，$F(T_1)(T_2) \subseteq F(T_1 \cup T_2)$ となる．したがって $F(T_1 \cup T_2) = F(T_1)(T_2)$.

(2) 任意の S について $F(S) \subseteq F(T)$ である．実際，$S \subseteq T$ であり，F, $S \subseteq F(T)$ だからである．よって，$\bigcup_S F(S) \subseteq F(T)$ である．逆に，$L = \bigcup_S F(S)$ とし，$\alpha, \beta \in L$ とすると，$\alpha \pm \beta \in L$ および $\alpha\beta^{-1} \in L$ $(\beta \neq 0)$ であり，L は E の部分体である．実際，$\alpha \in F(S_1)$, $\beta \in F(S_2)$ なる T の有限部分集合 S_1, S_2 が存在する．$S = S_1 \cup S_2 \subseteq T$ とおけば，$\alpha, \beta \in F(S)$ であり，$F(S)$ は体であるから，$\alpha \pm \beta \in F(S) \subseteq L$, $\alpha\beta^{-1} \in F(S) \subseteq L$ である．よって，L は E の部分体で F と T を含むから $F(T) \subseteq L$ となる．したがって，$F(T) = L$ である．

(3)F は体 $F(T)$ の部分体であり，$t_1, \ldots, t_n \in F(T)$ であるから，$F(T)$ の元の加減乗除を用いてつくられた元 $f(t_1, \ldots, t_n)/g(t_1, \ldots, t_n)$, $f, g \in F[X_1, \ldots, X_n]$ はすべて $F(T)$ に属する．一方，$M = \{f(t_1, \ldots, t_n)/g(t_1, \ldots, t_n) \mid f, g \in F[X_1, \ldots, X_n], g(t_1, \ldots, t_n) \neq 0\}$ は F と T を含む E の部分体であるから，$F(T) \subseteq M$ である．したがって，$F(T) = M$ である．　□

定義 2.4. F を体 E の部分体とする．F の元の作用 $\phi\colon F \times E \ni (r, x) \mapsto rx$ を体の乗法で定義すると E を体 F 上のベク

トル空間とみなせる．このとき，E の F 上のベクトル空間としての次元を体 E の F 上の次数 (degree) といい，$[E:F]$ で表す．体 E の部分体 F 上のベクトル空間としての基底を体 E の F 上の基底 (base) という．

2.2 素体

定義 2.5. 真の部分体をもたない体を素体 (prime field) という．

定理 2.6. 体 F が素体 $\Leftrightarrow F \simeq \mathbb{Q}$ または $F \simeq \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$　　(p は素数)

証明. ($\Leftarrow$) L を $\mathbb{Q}$ の任意の部分体とすると，$1 \in L$ より $\mathbb{Z} \subseteq L$ である．よって，$m/n \in L$　$(m, n \in \mathbb{Z}, n \neq 0)$ となり，$\mathbb{Q} \subseteq L$ である．したがって，$L = \mathbb{Q}$ である．また，L を $\mathbb{F}_p$ の任意の部分体とすると，$\mathbb{F}_p$ の単位元 $1_{\mathbb{F}_p} = e$ は $e \in L$ であるから，$e, 2e, \ldots, (p-1)e \in L$ である．ゆえに，$\mathbb{F}_p \subseteq L$ で $L = \mathbb{F}_p$ である．以上より，$\mathbb{Q}$ と $\mathbb{F}_p$ は素体であり，これらと同型な体 F も素体である．

($\Rightarrow$) F を素体とし，$e = 1_F$ とする．環準同型 $\phi: \mathbb{Z} \ni n \mapsto ne \in F$，$\mathfrak{a} = \ker\phi$ とすれば $\mathbb{Z}/\mathfrak{a} \simeq \phi(\mathbb{Z}) \subseteq F$ である．$\phi(\mathbb{Z})$ は整域であるから，$\mathbb{Z}/\mathfrak{a}$ は整域となり $\mathfrak{a}$ は $\mathbb{Z}$ の素イデアルとなる．よって，$\mathfrak{a} = (0)$ または $\mathfrak{a} = (p)$ である．

$\mathfrak{a} = (0)$ であるとき，環準同型 $\phi: \mathbb{Z} \to F$ は単射であり，局所化の普遍性から単準同型 ϕ は $\mathbb{Z}$ の商体 $\mathbb{Q}$ から F の中への単準同型 $\phi: \mathbb{Q} \to F$ に一意に拡張される．$\phi(\mathbb{Q})$ は明らかに F の部分体であり，F は素体であるから $\phi(\mathbb{Q}) = F$ である．よって，$\mathbb{Q} \simeq F$ となる．

また，$\mathfrak{a} = (p)$ であるとき，$\mathbb{Z}/\mathfrak{a}$ は体であり，$\mathbb{Z}/\mathfrak{a} \simeq \phi(\mathbb{Z})$ より，$\phi(\mathbb{Z})$ は F の部分体である．F は素体であるから，$\phi(\mathbb{Z}) = F$ である．ゆえに，$\mathbb{F}_p \simeq F$ となる．　□

定義 2.7. F を任意の体とする．F_0 を F のすべての部分体の共通集合とすると，F_0 は F の最小の部分体であるから，真の部分体を含まない．したがって F_0 は素体である．このとき，F_0 を体 F の素体といい，定理 2.6 より，$F_0 \simeq \mathbb{Q}$ または $F_0 \simeq \mathbb{F}_p$ である．$F_0 \simeq \mathbb{Q}$ のとき F の標数 (characteristic) を 0，$F_0 \simeq \mathbb{F}_p$ のとき F の標数を p と定義し，体 F の標数を $\mathrm{ch}(F)$ で表す．

補題 2.8. F を任意の体とすると，$x \in F$，$n \in \mathbb{Z}$ について，

$$nx = 0 \Leftrightarrow x = 0 \text{ または } n \equiv 0 \pmod{\mathrm{ch}(F)}.$$

ただし，e を F の単位元として，$ne = \underbrace{e + \cdots + e}_{n\text{個}}$ を $\mathbb{Z}$ から F への自然な準同型として定める．

証明. e を F の単位元とするとき，$nx = (ne)x$ であるから，e が $\mathbb{F}_p$ もしくは $\mathbb{Q}$ と同型な F の素体の元であることに注意すれば，

$$nx = 0 \Leftrightarrow (ne)x = 0 \Leftrightarrow ne = 0 \text{ または } x = 0 \Leftrightarrow n \equiv 0 \pmod{\mathrm{ch}(F)} \text{ または } x = 0.$$

よって，補題が示された．　□

定理 2.9. $\mathrm{ch}(F) = p > 0$ とするとき，$x, y \in F$，$n \in \mathbb{Z}\,(n \geq 0)$ について

(1) $(x \pm y)^{p^n} = x^{p^n} \pm y^{p^n}$，$(xy)^{p^n} = x^{p^n} y^{p^n}$
(2) $\phi: F \ni x \mapsto x^{p^n} \in F$ は単準同型である．

証明. (1)$(x+y)^p = x^p + \binom{p}{1}x^{p-1}y + \cdots + \binom{p}{i}x^{p-i}y^i + \cdots + y^p$ である．$1 \geq i \geq p-1$ について $p \mid \binom{p}{i}$ であるから，補題 2.8 より，$(x+y)^p = x^p + y^p$ である．これを用いて n に関する帰納法を使えば，$(x \pm y)^{p^n} = x^{p^n} \pm y^{p^n}$ が示される．また，$(xy)^{p^n} = x^{p^n} y^{p^n}$ は n に関する帰納法ですぐに示される．

(2)(1) より ϕ は準同型である．また，$\phi(x) = x^{p^n} = 0$ ならば F が整域であることから，$x = 0$．ゆえに，ϕ は単準同型である．　□

2.3 単拡大

補題 2.10. R を単位元をもつ可換環，$\mathfrak{m}$ を R の極大イデアル，F を R の部分体とする．このとき，自然な準同型 $\phi: R \to R/\mathfrak{m} = K$ の F への制限 $\psi = \phi|_F$ により，$F \simeq \phi(F) \subseteq K$ である．つまり，体 K を F の拡大体とみなせる．

証明. $\mathfrak{m}$ は R の極大イデアルだから，$R/\mathfrak{m} = K$ は体である．よって，ϕ の F への制限 ψ は F が体であるから単射となり，F から K への同型写像になる．したがって，$F \simeq \phi(F) \subseteq K$ である． □

定理 2.11. F を体，$f(X) \in F[X]$ を F 上の n 次既約単多項式とする．このとき，F の拡大体 K と $\theta \in K$ で，$f(\theta) = 0$ であり，単拡大体 $K = F(\theta)$ であるものが存在する．$K = F(\theta)$ は F の n 次拡大体で，$1, \theta, \ldots, \theta^{n-1}$ は $K = F(\theta)$ の F に関する基底である．

証明. $f(X)$ により生成される $F[X]$ のイデアル $(f(X))$ は $f(X)$ が $F[X]$ の既約元であり，$F[X]$ が単項イデアル整域であることから $F[X]$ の極大イデアルとなる．よって，補題 2.10 より $K = F[X]/(f(X))$ は体 F の拡大体である．ここで，$\theta = \phi(X) \in K$ とおく．$g(X) = \sum_{i=0}^{m} b_i X_i \in F[X]$ として，$\phi(g(X)) = g(\theta) = \sum_{i=0}^{m} b_i \theta_i$ であるから，$K = \phi(F[X]) = \{g(\theta) \mid g(X) \in F[X]\} = F[\theta]$ である．K は体であるから，$K = F[\theta] = F(\theta)$ となって K は F の単拡大である．

次に，θ が K の F に関する基底であることを示す．$g(X) \in F[X]$ に対して，$g(\theta) = 0 \Leftrightarrow \phi(g(X)) = 0 \Leftrightarrow g(X) \in \mathfrak{m} = (f(X)) \Leftrightarrow f(X) | g(X)$ である．任意の $y \in K$ に対して，$h(X) \in F[X]$ が存在して，$y = h(\theta)$ と表される．$h(X) = q(X)f(X) + r(X)$，$r(X) = 0$ または $\deg r < \deg f = n$ とすれば，$y = h(\theta) = q(\theta)f(\theta) + r(\theta) = r(\theta)$ $(q(X), r(X) \in F[X])$ である．それゆえ，$r(X) = b_0 + b_1 X + \cdots + b_{n-1} X^{n-1}$ $(b_i \in F)$ とすれば，$y = b_0 + b_1\theta + \cdots + b_{n-1}\theta^{n-1}$ となるから，K の元はすべて F の元を係数として $1, \theta, \ldots, \theta^{n-1}$ の 1 次結合として表される．また，$1, \theta, \ldots, \theta^{n-1}$ は F に関して 1 次独立である．実際，$c_0 + c_1\theta + \cdots + c_{n-1}\theta^{n-1} = 0$ $(c_i \in F)$ ならば，$g(X) = c_0 + c_1 X + \cdots + c_n X^{n-1} \in F[X]$ とおくと，$g(\theta) = 0$ となる．よって，$g(\theta) = 0 \Leftrightarrow f(X) \mid g(X)$ である．一方，$\deg g \leq n - 1 < \deg f$．ゆえに，$g(X) = 0 \Rightarrow c_i = 0$ $(0 \leq i \leq n-1)$ である．よって，$1, \theta, \ldots, \theta^{n-1}$ は $K = F(\theta)$ の F に関する基底である．それゆえ，$[K : F] = n = \deg F$ である． □

定義 2.12. R を単位元をもつ可換環，F を R の部分体とする．$\alpha \in R$ で 0 でない $f(X) \in F[X]$ が $f(\alpha) = 0$ であるとき，α は F に関して代数的であるといい，$\alpha \in R$ が代数的でないとき，α は F に関して超越的であるという．

定理 2.13. 体 $E = F(\alpha)$ を体 F の単拡大体とする．このとき，以下が成り立つ．

(1) 元 α が F に関して超越的ならば，E から $F(X)$ の上への F 同型 ω で $\omega(\alpha) = X$ となるものが存在する．
(2) α が F に関して代数的ならば既約単多項式 $p(X) \in F(X)$ で $p(\alpha) = 0$ となるものが α に関して一意的に定まる．$\mathfrak{p} = (p(X))$ を $F[X]$ の極大イデアルとすれば，E から体 $F[X]/\mathfrak{p}$ の上への F 同型 ω で $\omega(\alpha) = X \pmod{\mathfrak{p}}$ となるものが存在する．さらに，体 $F(\alpha)$ は整域 $F[\alpha]$ と一致し，$\deg p(X) = [E : F] = n$ であり，$1, \alpha, \ldots, \alpha^{n-1}$ は E/F の基底である．

証明. 写像 $\phi: F[X] \ni f(X) \mapsto f(\alpha) \in E$ は環として F 準同型である．$\mathrm{Im}\,\phi = F[\alpha] = \{f(\alpha) \mid f(X) \in F[X]\}$ は体 E の部分整域であることより，$\mathfrak{p} = \ker\phi = \{f(X) \in F[X] \mid f(\alpha) = 0\}$ であることに注意すれば，$\mathfrak{p}$ は単項イデアル整域 $F[X]$ の素イデアルとなる．したがって，$\mathfrak{p}$ は (0) または $(p(X))$ である．ただし，$p(X)$ は $F[X]$ における既約多項式である．よって，$\mathfrak{p} = \ker\phi$ より，

$$\mathfrak{p} = (0) \Leftrightarrow 0 \text{ でない任意の } f(X) \in F[X] \text{ に対して } f(\alpha) \neq 0 \Leftrightarrow \alpha \text{は } F \text{ に関して超越的}$$

$$\mathfrak{p} = (p(X)) \Leftrightarrow 0 \text{ でない } f(X) \in F[X] \text{ が存在して } f(\alpha) = 0 \Leftrightarrow \alpha \text{は } F \text{ に関して代数的}$$

であることがわかった．次に (1)(2) を示す．

(1)α が超越的であるとき $\mathfrak{p} = (0)$ であることと同値であるから，ϕ が単射であることも同値である．したがって，ϕ は整域 $F[X]$ から整域 $F[\alpha]$ の上への F 同型である．それゆえ，局所化の普遍性により ϕ は $F[X]$ の商体 $F(X)$ から

$F[\alpha]$ の商体 $F(\alpha)$ への F 同型

$$\phi\colon F(X) \ni \frac{f(X)}{g(X)} \mapsto \frac{f(\alpha)}{g(\alpha)} \in F(\alpha)$$

に一意的に拡張される．$\omega = \phi^{-1}\colon F(\alpha) \to F(X)$ とすれば，ω は E から $F(X)$ の上への F 同型で $\omega(\alpha) = X$ である．

(2)α が F に関して代数的であるとき $\mathfrak{p} = \ker\phi = (p(X))$ であることと同値である．このとき，F が体であることから，既約多項式 $p(X)$ は既約単多項式にできる．まず，$p(\alpha) = 0$ となる既約単多項式 $p(X)$ が α に対して一意的であることを示す．$p_1(X)$ を $p_1(\alpha) = 0$ である既約単多項式とすれば，$p_1(X) \in \mathfrak{p}$ より $p_1(X) = p(X)q(X)$ となる $q(X) \in F[X]$ が存在する．$p_1(X)$ は既約であるから，$q(X) = c \in F^\times$ であり，$p_1(X)$ と $p(X)$ は単多項式であるから，$c = 1$ で $p_1(X) = p(X)$ となる．次に，$F(\alpha) = F[\alpha]$ を示す．自然な準同型 $\psi\colon F[X] \to F[X]/\mathfrak{p}$ とするとき，下のような可換図式になる．

$$\begin{array}{ccc} F[X] & \xrightarrow{\phi} & \phi(F[X]) \\ \downarrow{\scriptstyle \psi} & \nearrow{\scriptstyle \simeq} & \\ F[X]/\mathfrak{p} & & \end{array}$$

ここで，$\phi(F[X]) = F[\alpha] \subseteq F(\alpha)$ であり，$\mathfrak{p}$ は $F[X]$ の極大イデアルだから，$F[X]/\mathfrak{p}$ は体である．ゆえに，可換図式より $F[\alpha]$ は $F(\alpha)$ の部分体であるが，$F(\alpha)$ の定義より，$F(\alpha)$ は F と α を含む最小の体であるから，$F(\alpha) = F[\alpha]$ である．また，F 同型 $F[X]/\mathfrak{p} \to F(\alpha)$ の逆写像も F 同型であり，それを ω とすれば，$\omega(\alpha) = X \pmod{\mathfrak{p}}$ である．

最後に，$1, \alpha, \ldots . \alpha^{n-1}$ が基底であることを示す．上記の議論から，任意の $\gamma \in E$ はある $f(X) \in F[X]$ により $\gamma = f(\alpha)$ と表される．$f(X) = p(X)q(X)+r(X)$, $q(X), r(X) \in F[X]$, $\deg r < \deg p$ とすれば, $F(\alpha) \simeq F[X]/\mathfrak{p}$ より, $\gamma = f(\alpha) = r(\alpha)$ である．したがって，$E = F(\alpha)$ の任意の元は，$\gamma = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}$，$c_i \in F\,(0 \le i \le n = \deg p)$ の形に表される．さらに，$\gamma = \sum_{i=0}^{n-1} c_i\alpha^i = \sum_{i=0}^{n-1} c_i'\alpha^i \quad (c_I, c_i' \in F)$ とすれば，$g(X) = \sum_{i=0}^{n-1} X^i \in F[X]$ に対して $g(\alpha)$ に対して $g(\alpha) = 0$ である．$g(X) \in (p(X))$ より $p(X) \mid g(X)$ であるが，$\deg g \le n-1 \le \deg p$ であるから $g(X) = 0$ である．すなわち，$c_i - c_i' = 0\,(0 \le i \le n-1)$ である．したがって，$\gamma \in E$ の一意性が示されたので， $1, \alpha, \ldots, \alpha^{n-1}$ は $E = F(\alpha)$ の F に関する基底で $[E\colon F] = n$ である． □

系 2.14. 体 F の単拡大体 $E = F(\alpha)$ に対して (1)(2) は同値である．

(1) E は F の有限次拡大
(2) 元 α は F に関して代数的

証明. (2) ⇒ (1) は定理 2.13(2) より明らかに成り立つ．

(1) ⇒ (2) は対偶をとれば，定理 2.13(1) より，F 同型 $\omega\colon F(\alpha) \to F(X)$ が存在する．したがって，$F(X)$ は F の無限次拡大で $F(\alpha)$ は F の無限次拡大である． □

定義 2.15. 体 F の拡大体の元 α が F に関して代数的であるとき，α について一意に定まる $p(\alpha) = 0$ となる $F[X]$ の既約単多項式 $p(X)$ を F に関する最小多項式 (minimal polynomial) という．

定理 2.16. 体 F の拡大体の元 α は F に関して代数的とする．このとき，$f(X) \in F[X]$ について次の 3 条件は同値である．

(1) $f(X)$ は α の F に関する最小多項式.
(2) $f(X)$ は単多項式であり，$g(X) \in F[X]$ に対して

$$g(\alpha) = 0 \Leftrightarrow f(X) \mid g(X).$$

(3) $f(X)$ は単多項式であり $f(\alpha) = 0$ かつ $g(X) \in F[X]$，$g(X) \neq 0$，に対して $g(\alpha) = 0$ ならば $\deg f \le \deg g$.

証明. (1) ⇒ (2)F 準同型 $F[X] \ni g(X) \mapsto g(\alpha) \in F[\alpha]$ の核は定理 2.13 の証明から $(f(X))$ である．ゆえに，$g(\alpha) = 0 \Leftrightarrow g(X) \in (f(X)) \Leftrightarrow f(X) \mid g(X)$.

(2) ⇒ (3) $g(\alpha) = 0 \Leftrightarrow f(X) \mid g(X) \Rightarrow \deg f \le \deg g$.

(3) $\Rightarrow$ (1)$f(X)$ が $F(X)$ において可約であると仮定すると，$f(X) = f_1(X)f_2(X)$，$0 < \deg f_1, \deg f_2 < \deg f$ となる $f_1(X), f_2(X) \in F[X]$ が存在する．$f(\alpha) = 0$ であるから $f_1(\alpha) = 0$ または $f_2(\alpha) = 0$ となる．よって，(3) より $\deg f \leq \deg f_1$ または $\deg f \leq \deg f_2$ となり矛盾．したがって，$f(X)$ は $f(\alpha) = 0$ なる $F[X]$ の既約単多項式であるから，α の F に関する最小多項式である． □

3　今後の課題

本研究では，時間の都合上有限体の拡大体の存在を示すところまで至ることができなかった．有限体の拡大体の存在の証明の概要は掴めているので，次回の芝浦祭に向けて有限体の拡大体の存在に加え，Wedderburn の定理などの有限体の諸定理についてもまとめたい．

参考文献

[1] 藤崎 源次郎，体と Galois 理論 I，岩波書店，1997.
[2] 雪江 明彦，環と体とガロア理論，日本評論社，2010.