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

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．

定義 2.3. 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，$[E\colon F]$ 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 2.4. 真の部分体をもたない体を素体 (prime field) という．

定理 2.5. 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)

定義 2.6. 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 2.5 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 2.7. 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．

2.3　単拡大

定義 2.8. 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 2.9. 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，$\deg p(X) = [E\colon F] = n$ であり，$1, \alpha, \ldots, \alpha^{n-1}$ は E/F の基底である．

系 2.10. 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) $\Rightarrow$ (1) は定理 2.9(2) より明らかに成り立つ．

(1) $\Rightarrow$ (2) は対偶をとれば，定理 2.9(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．　□

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.