1　素体と標数

定義 1.1.　自分自身を除いて部分体をもたないような体を**素体**という．つまり，体 F の部分体が必ず F と一致するとき，F を素体という．

定理 1.2.　素体は有理数体 $\mathbb{Q}$ か，または素数 p を法とする剰余環 $\mathbb{Z}/p\mathbb{Z}$ に同型である．

F を体とします．F のすべての部分体の共通部分 F_0 は F の最小の部分体です．したがって F_0 は素体です．

定義 1.3.　F_0 を F の**素体**という．

定義 1.4.　体 F の素体を F_0 とする．F の**標数**を次のように定める：

(i)　$F_0 \simeq \mathbb{Q}$ のとき，F の標数は 0 であるとする．

(ii)　ある素数 p が存在して $F_0 \simeq \mathbb{Z}/p\mathbb{Z}$ となるとき，F の標数は p であるとする．

体 F の標数を $\mathrm{char}(F)$ で表す．

任意の素数 p に対して，$\mathbb{Q}$ と $\mathbb{Z}/p\mathbb{Z}$ とは体として同型ではありません．また，異なる二つの素数 p, q に対して，$\mathbb{Z}/p\mathbb{Z}$ と $\mathbb{Z}/q\mathbb{Z}$ とは体として同型ではありません．ですから，体 F が二つの異なる標数を同時に持つことはありません．

定理 1.5.　F を体とする．$x \in F$ と $n \in \mathbb{Z}$ に対して，

$$nx = 0 \Longleftrightarrow n \equiv 0 \,(\mathrm{mod}\ \mathrm{char}(F)\,)$$

が成り立つ．ただし $\mathrm{char}(F) = 0$ のとき右辺は $n = 0$ を意味する．

例 1.6.　$\mathrm{char}(\mathbb{Q}) = \mathrm{char}(\mathbb{R}) = \mathrm{char}(\mathbb{C}) = 0$.

例 1.7.　p を素数とするとき，$\mathrm{char}(\mathbb{Z}/p\mathbb{Z}) = p$.

例 1.8.　体 F の上の有理関数体 $K = F(X_1, \ldots, X_n)$ について，$\mathrm{char}(K) = \mathrm{char}(F)$ が成り立つ．

特に $\mathrm{char}(F) = p > 0$ のとき，体 F の上の有理関数体は標数が 0 でないような体で，元の個数が無限であるものの例になっています．ちなみに，有限個の元からなる標数 0 の体は存在しません．そして，標数 0 の体のなかで（同型を除いて，包含関係について）最小のものは有理数体 $\mathbb{Q}$ です．

定理 1.9.　F を標数 $p > 0$ の体とする．このとき任意の $a, b \in F$ と任意の整数 $n \geq 0$ に対して，

$$(x+y)^{p^n} = x^{p^n} + y^{p^n}, \quad -x^{p^n} = (-x)^{p^n}, \quad (xy)^{p^n} = x^{p^n} y^{p^n}$$

が成り立つ．

定理 1.10.　F を標数 $p > 0$ の体とし，$n \geq 1$ を整数とする．このとき，写像

$$F \longrightarrow F, \quad x \longmapsto x^{p^n}$$

は F から F の中への同型写像である．つまり単射準同型である．

系 1.10.1.　F を標数 $p > 0$ の体，Ω を F の代数的閉包とする．このとき，任意の $a \in F$ と任意の整数 $n \geq 0$ に対して，$x^{p^n} = a$ となる $x \in \Omega$ がただ一つ存在する．

定義 1.11. F を標数 $p>0$ の体，Ω を F の代数的閉包とする．$a\in F$ と整数 $n\geq 0$ に対して，$x^{p^n}=a$ となる $x\in\Omega$ を a^{1/p^n} と書く．

定理 1.12. F を標数 $p>0$ の体とする．このとき，任意の $x,\ y\in F$ と任意の整数 $n\geq 0$ に対して，

$$(x+y)^{1/p^n}=x^{1/p^n}+y^{1/p^n},\quad -x^{1/p^n}=(-x)^{1/p^n},\qquad (xy)^{1/p^n}=x^{1/p^n}y^{1/p^n}$$

が成り立つ．

定義 1.13. 有限個の元からなる体を**有限体**という．元の個数が q であるような有限体を $\boldsymbol{F}_q$ で表す．

例 1.14. p を素数とするとき，$\boldsymbol{F}_p=\mathbb{Z}/p\mathbb{Z}$.

注意 1.15. $q>1$ が素数ではない整数のとき，剰余環 $\mathbb{Z}/q\mathbb{Z}$ は体にならない（整域にすらならない）ので，$\boldsymbol{F}_q\neq\mathbb{Z}/q\mathbb{Z}$.

定理 1.16. $\mathrm{char}(\boldsymbol{F}_q)>0$．すなわち，$p=\mathrm{char}(\boldsymbol{F}_q)$ とすれば，p は素数であり，$\boldsymbol{F}_q$ の素体は $\boldsymbol{F}_p=\mathbb{Z}/p\mathbb{Z}$ である．

2　1の根

定義 2.1. F を体とし，$\zeta\in F$ とする．ζ が**1の根**であるとは，ある $n\in\mathbb{N}$ が存在して $\zeta^n=1$ が成り立つことをいう．また，$n\in\mathbb{N}$ を固定したとき，$\zeta^n=1$ となるような ζ を**1の n 乗根**という．

定義 2.2. F を体とし，$\zeta\in F$，$n\in\mathbb{N}$ とする．ζ が1の**原始 n 乗根**であるとは，ζ が1の n 乗根であって，$m\in\mathbb{N}$ について

$$1\leq m<n\Longrightarrow\zeta^m\neq 1$$

が成り立つことをいう．

W_F を F に含まれる1の根全体の集合とすれば，W_F は乗法群 $F^\times=F\backslash\{0\}$ の部分群になります．また，$W_{F,n}$ を F に含まれる1の n 乗根全体とすれば，$W_{F,n}$ は W_F の有限部分群になります．

補題 2.3. 体 F の乗法群 $F^\times$ の有限部分群は巡回群である．

系 2.3.1. 任意の体 F に対して，$W_{F,n}$ は有限巡回群になる．

系 2.3.2. q 個の元からなる有限体 $F=\boldsymbol{F}_q$ の乗法群 $F^\times=F\backslash\{0\}$ は，乗法について位数 $q-1$ の巡回群になる．

系 2.3.3. 任意の有限体 F に対して，$F^\times=W_F$ が成り立つ．

証明. 有限体 F の乗法群 $F^\times$ は有限群であるから，任意の $x\in F^\times$ に対して，ある $n\in\mathbb{N}$ が存在して $x^n=1$ が成り立つ．ゆえに $F^\times\subseteq W_F$ である．逆の包含関係は明らかである．したがって $F^\times=W_F$ である． □

定理 2.4. $W_{F,n}$ の位数は n の約数である．

定理 2.5. $W_{F,n}$ の位数がちょうど n であるための必要十分条件は，F が 1 の原始 n 乗根を含むことである．

定理 2.6. F が 1 の原始 n 乗根を含むならば，F に含まれる 1 の原始 n 乗根の個数は $\varphi(n)$ である．ここで φ は Euler の関数である．

定理 2.7. F が 1 の原始 n_i 乗根 $(1 \leq i \leq s)$ を含むとき，n を $n_1, \ldots, n_s$ の最小公倍数とすれば，F は 1 の原始 n 乗根を含む．

例 2.8. 複素数体 $\mathbb{C}$ に属する 1 の n 乗根全体からなる巡回群を W_n とする．W_n の元はすべて多項式 $X^n - 1$ の根なので，W_n の元の個数は n である．一方，

$$W_n = \bigcup_{1 \leq d | n} \{\zeta \in \mathbb{C} \mid \zeta \text{ は 1 の原始 } d \text{ 乗根 }\} \quad (\text{直和})$$

であり，各 $d \geq 1$ に対して $\mathbb{C}$ に含まれる 1 の原始 d 乗根の個数は $\varphi(d)$ であるから，

$$\sum_{1 \leq d | n} \varphi(d) = n$$

が成り立つ．

定理 2.9. F が標数 $p > 0$ の体であるとき，F が 1 の原始 n 乗根を含むならば $p \nmid n$ である．

定理 2.10. Ω を標数 $p > 0$ の代数的閉体とすれば，p で割れない任意の自然数 n に対して，Ω は $\varphi(n)$ 個の 1 の原始 n 乗根を含む．

系 2.10.1. 標数 $p > 0$ の代数的閉体 Ω の元の個数は有限ではない．

証明. p と互いに素な素数を q とすれば，任意の $n \in \mathbb{Z}$, $n \geq 1$ に対して，Ω は少なくとも一つの 1 の原始 q^n 乗根を含む． □

Ω を標数 $p > 0$ の代数的閉体とし，n を p で割れない自然数とします．Ω に属する 1 の原始 n 乗根 ζ を一つ固定し，

$$\Phi_n(X) = \prod_{\substack{1 \leq a < n \\ (a,\, n) = 1}} (X - \zeta^a) \in \Omega[X]$$

とおきます．$\Phi_n(X)$ の定義は，ζ の選び方には依存しません．

定義 2.11. $\Phi_n(X)$ を**円分多項式**あるいは**円周等分多項式**と呼ぶ．

定理 2.12. $\Omega[X]$ において，

$$X^n - 1 = \prod_{1 \leq d | n} \Phi_d(X)$$

が成り立つ．

定理 2.13. $p \nmid n$ とする．このとき $\Phi_n(X)$ は $\boldsymbol{F}_p[X]$ における $\varphi(n)$ 次の単多項式である．

例 2.14. 標数 2 のとき

$$\begin{aligned} \Phi_7(X) &= X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 \\ &= (X^3 + X^2 + 1)(X^3 + X + 1) \end{aligned}$$

が成り立つ．

定理 2.15.

$$\Phi_n(X) = \prod_{1 \leq d \mid n} (X^d - 1)^{\mu(n/d)}.$$

ただし μ は Möbius の関数である．

3　有限体の拡大

定理 3.1.　$p = \mathrm{char}(\boldsymbol{F}_q)$ とする．このとき，体の拡大 $\boldsymbol{F}_q/\boldsymbol{F}_p$ は有限次拡大である．

証明.　$\boldsymbol{F}_q$ を $\boldsymbol{F}_p$ 上の線型空間とみたとき，$\boldsymbol{F}_q$ は有限体なので，有限個の $\boldsymbol{F}_p$ 上の基底をもつ．したがって $\boldsymbol{F}_q$ の $\boldsymbol{F}_p$ 上の次元は有限である．□

定理 3.2.　$p = \mathrm{char}(\boldsymbol{F}_q)$，$f = [\boldsymbol{F}_q : \boldsymbol{F}_p]$ とする．このとき，$q = p^f$ が成り立つ．

証明.　$\boldsymbol{F}_q$ は $\boldsymbol{F}_p$ 上の f 次元線型空間であるから，$\boldsymbol{F}_q$ は $\boldsymbol{F}_p^f$ に線型空間として同型である．したがって $q = p^f$ である．□

定理 3.3.　$\boldsymbol{F}_q[X]$ において，

$$X^q - X = \prod_{\alpha \in \boldsymbol{F}_q} (X - \alpha), \quad X^{q-1} - 1 = \prod_{\alpha \in \boldsymbol{F}_q^\times} (X - \alpha)$$

が成り立つ．ここで $\boldsymbol{F}_q^\times$ は $\boldsymbol{F}_q$ の乗法群である．

系 3.3.1.　有限体 $\boldsymbol{F}_q$ の代数的閉包 Ω を一つ固定し，$f \geq 1$ を整数とする．このとき，$x \in \Omega$ について

$$x \in \boldsymbol{F}_{q^f} \iff x^{q^f} = x$$

が成り立つ．

系 3.3.2.　有限体 $\boldsymbol{F}_q$ の代数的閉包 Ω を一つ固定する．このとき

$$\boldsymbol{F}_q = \{x \in \Omega \mid x^q = x\}$$

が成り立つ．

系 3.3.3.　$p = \mathrm{char}(\boldsymbol{F}_q)$ とする．$\boldsymbol{F}_q$ は多項式 $X^q - X$ および $X^{q-1} - 1$ の $\boldsymbol{F}_p$ 上の最小分解体である．

定理 3.4.　二つの有限体 $\boldsymbol{F}_q$, $\boldsymbol{F}_{q'}$ について

$$\boldsymbol{F}_q \simeq \boldsymbol{F}_{q'} \iff q = q'$$

が成り立つ．

定理 3.5.　標数 p の体に含まれる二つの有限体 $F_q\,(q = p^f)$, $F_{q'}\,(q' = p^{f'})$ に対して，

$$\boldsymbol{F}_q \subseteq \boldsymbol{F}_{q'} \iff f \mid f'$$

が成り立つ．

定理 3.6. 任意の素数 p の冪 $q = p^f$ に対して，q 個の元からなる標数 p の有限体が同型を除いて一意的に存在する．

定理 3.7. 任意の有限体 $\boldsymbol{F}_q$ と任意の整数 $f \geq 1$ に対して，$\boldsymbol{F}_q$ の f 次拡大体が同型を除いて一意的に存在する．

定理 3.8. 有限体 $\boldsymbol{F}_q$ の代数的閉包を Ω とし，$f \geq 1$ を整数とする．このとき

$$\Omega = \bigcup_{f \geq 1} \boldsymbol{F}_{q^f}$$

が成り立つ．

注意 3.9. 素数 p と自然数 $n \geq 2$ をそれぞれ固定する．$i \geq 1$ に対して元の個数が p^{n^i} となる体 F_i を考えると，$F_1 \subseteq F_2 \subseteq \cdots$ となり，$F = \bigcup_{i=1}^{\infty} F_i$ とすると $F/\boldsymbol{F}_p$ は無限次代数拡大になる．しかし，n と素な自然数 $m \geq 2$ をとり，$\boldsymbol{F}_p$ 上の最小多項式の次数が m であるような元 α を考えれば，任意の $i \geq 1$ に対して $\alpha \notin F_i$ なので，$\alpha \notin F$ である．したがって F は代数的閉体ではない（[2] II §2.12 問題 3）．

定理 3.10. 有限体 $\boldsymbol{F}_{q^f}$ の乗法群 $\boldsymbol{F}_{q^f}^{\times}$ の生成元を θ とする．このとき $\boldsymbol{F}_{q^f} = \boldsymbol{F}_q(\theta)$ が成り立つ．

K/F を有限体の拡大とします．有限体 K の乗法群 $K^{\times}$ は巡回群なので，ある $\theta \in K^{\times}$ が存在して，$K^{\times}$ は θ によって生成されます．このとき，$K = F(\theta)$ が成り立つことは容易にわかります．したがって，次のことが示されました：

定理 3.11. 有限体の有限次拡大体は単純拡大体である．

注意 3.12. $\boldsymbol{F}_{q^f} = \boldsymbol{F}_q(\theta)$ となる θ は必ずしも $\boldsymbol{F}_{q^f}^{\times}$ の生成元になるとは限らない．例えば，$f(X) = X^4 + X^3 + X^2 + X + 1$ は $\boldsymbol{F}_2[X]$ において既約であり，θ を $f(X)$ の根とすれば，$\boldsymbol{F}_2(\theta) = \boldsymbol{F}_{16}$ である．一方，$\theta^5 - 1 = (\theta - 1)f(\theta) = 0$ であるから，θ は $\boldsymbol{F}_{16}^{\times}$ の生成元ではない．

注意 3.13. F を標数 $p > 0$ の体とし，t, u を F 上代数的独立な元として，$K = F(t, u)$ を考える．$t = \alpha^p$, $u = \beta^p$ となる α, β をとり，$L = K(\alpha, \beta)$ とする．このとき $[L : K] = p^2$ である．しかしながら，L は K の単純拡大体とはならない（[2] II §2.5 問題 1）．

一般に，標数 $p > 0$ の体について，次のことが成り立ちます（[1] 第 2 章問題 68）．

定理 3.14. K/F を標数 $p > 0$ の体 F の有限次拡大とする．次の二つの条件は同値である．

(i) K/F は単純拡大である．

(ii) K の各元の F に関する最小多項式の非分離次数の最大値と K/F の非分離次数 $[K : F]_i$ とが一致する．

定理 3.15. 有限個の元からなる整域は体である．

証明. R を有限個の元からなる整域とする．任意の $a \in R$, $a \neq 0$ に対して，写像

$$R \longrightarrow R, \quad x \longmapsto ax$$

は単射であり，R の元の個数が有限であることから同時に全射であることもいえる．したがって各々の a に対して $ax = 1$ となる $x \in R$ が存在する．すなわち R の 0 以外の元はすべて単元である． □

定理 3.16 (Wedderburn). 有限個の元からなる斜体（非可換体）は体である．

定理 3.17. $\boldsymbol{F}_q[X]$ における $n \geq 1$ 次の既約多項式の個数 $N(q, n)$ は

$$N(q, n) = \frac{1}{n} \sum_{1 \leq d | n} \mu\left(\frac{n}{d}\right) q^d$$

である．ここで μ は Möbius の関数である．

定理 3.18. F を有限体とする．このとき，多項式環 $F[X]$ に属する既約多項式 $f(X)$ はすべて分離的である．すなわち，F の代数的閉包 Ω を一つ固定したとき，Ω における $f(X)$ の根はすべて互いに異なる．

注意 3.19. F を標数が 0 の体とすれば，$F[X]$ に属する既約多項式は常に分離的である．

証明. もし仮に $f(X) = a_0 X^n + \cdots + a_n$ が定数ではない既約多項式であって，かつ分離的でないとすれば，$f'(X) = n a_0 X^{n-1} + \cdots + a_{n-1} = 0$ である．F の標数は 0 だから $a_0 = \cdots = a_{n-1} = 0$, よって $f(X)$ は定数となる．これは矛盾である． □

注意 3.20. p を素数とし，$F = \boldsymbol{F}_p$ を標数 p の素体とする．t を F 上超越的な元とし，$K = F(t)$ とおく．さらに，$t \notin K^p$ と仮定する．このとき $X^p - t$ は $K[X]$ に属する既約多項式である．一方，$t = \alpha^p$ となる $\alpha \notin K$ が K の代数的閉包の中に存在して，$X^p - t = (X - \alpha)^p$ となる．したがって $X^p - t$ は分離的ではない．

4 有限体の Galois 理論

定理 4.1. $\boldsymbol{F}_q$ を q 個の元からなる有限体とし，K を $\boldsymbol{F}_q$ の代数拡大体とする．このとき，写像

$$K \longrightarrow K, \quad x \longmapsto x^q$$

は K の $\boldsymbol{F}_q$ 自己同型である．

定理 4.2. q 個の元からなる有限体 $\boldsymbol{F}_q$ の f 次の拡大体 $\boldsymbol{F}_{q^f}$ は $\boldsymbol{F}_q$ の巡回拡大体である．その Galois 群は

$$\sigma_F : \boldsymbol{F}_{q^f} \longrightarrow \boldsymbol{F}_{q^f}, \quad x \longmapsto x^q$$

を生成元とする位数 f の巡回群である．

定義 4.3. σ_F を **Frobenius 自己同型写像**という．

例 4.4. 拡大 $\boldsymbol{F}_{81}/\boldsymbol{F}_3$ について考える．$81 = 3^4$ なので，この拡大は 4 次の巡回拡大である．Frobenius 自己同型写像 σ_F は $\sigma(x) = x^3$ $(x \in \boldsymbol{F}_{81})$ によって定義される．$\boldsymbol{F}_{81}$ の $\boldsymbol{F}_3$ 自己同型写像は

$$\begin{aligned}
\mathrm{id} &: \boldsymbol{F}_{81} \longrightarrow \boldsymbol{F}_{81}, \quad x \longmapsto x, \\
\sigma_F &: \boldsymbol{F}_{81} \longrightarrow \boldsymbol{F}_{81}, \quad x \longmapsto x^3, \\
\sigma_F^2 &: \boldsymbol{F}_{81} \longrightarrow \boldsymbol{F}_{81}, \quad x \longmapsto x^9, \\
\sigma_F^3 &: \boldsymbol{F}_{81} \longrightarrow \boldsymbol{F}_{81}, \quad x \longmapsto x^{27}
\end{aligned}$$

がすべてであり，$\boldsymbol{F}_{81}/\boldsymbol{F}_3$ の Galois 群は $G = \{\mathrm{id}, \sigma_F, \sigma_F^2, \sigma_F^3\}$ である．このとき，$\boldsymbol{F}_{81}/\boldsymbol{F}_3$ の中間体と G の部分群とは図 1 のように対応する．

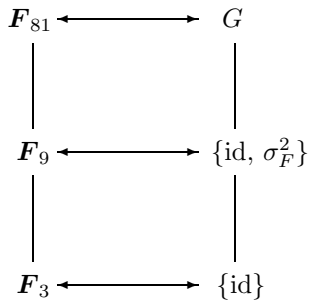

図 1: $\boldsymbol{F}_{81}/\boldsymbol{F}_3$ の中間体と G の部分群との対応

例 4.5. $\boldsymbol{F}_q$ を q 個の元からなる有限体とし，$p = \mathrm{char}\,(\boldsymbol{F}_q)$ とする．ζ を標数 p の素体 $\boldsymbol{F}_q$ の代数的閉包に属する 1 の原始 $q-1$ 乗根とする．このとき $\boldsymbol{F}_q = \boldsymbol{F}_p(\zeta)$ と書ける．$\boldsymbol{F}_q^\times$ は ζ で生成される巡回群である．$\boldsymbol{F}_q/\boldsymbol{F}_p$ の Galois 群は，位数 $f = [\boldsymbol{F}_q : \boldsymbol{F}_p]$ の巡回群である．

例 4.6. $\boldsymbol{F}_q$ を q 個の元からなる有限体とし，$m \geq 2$ を $(m,\, q) = 1$ であるような自然数，ζ_m を 1 の原始 m 乗根，$K = \boldsymbol{F}_q(\zeta_m)$ とする．このとき $W_K = K^\times$ である．$f = [K : \boldsymbol{F}_q]$ とすれば，f は $q \equiv 1 \,(\mathrm{mod}\, m\,)$ となる最小正指数，すなわち，$(\mathbb{Z}/m\mathbb{Z})^\times$ における $q \bmod m$ の位数である．Galois 群 $G(K/\boldsymbol{F}_q)$ は $q \bmod m$ の生成する $(\mathbb{Z}/m\mathbb{Z})^\times$ の巡回部分群に同型である．

p を素数，$f \geq 1$ を整数とし，$q = p^f$ とします．$F = \boldsymbol{F}_q$ を q 個の元からなる有限体とし，Ω を F の代数的閉包とします．素数 l を一つとり，$F_n = \boldsymbol{F}_{q^{l^n}}$ $(n \geq 0)$ とおき，$K = \bigcup_{n\geq 0} F_n$ とおきます．このとき，K/F は Galois 拡大になります．

K から K 自身への写像 σ を $\sigma(x) = x^q$ によって定義すれば，σ は K の F 自己同型写像になります．

定義 4.7. G を群とし，$\mathcal{N}$ を G の指数有限な正規部分群の全体とする．このとき，

$$\mathcal{B} = \{gN \mid g \in G,\, N \in \mathcal{N}\}$$

により生成される G の位相を G の **Krull 位相**という．

一般に，Krull 位相を導入した群は位相群になります．

K/F の Galois 群を $Gal(K/F)$ とすれば，$\{\sigma^n \mid n \in \mathbb{Z}\}$ は $Gal(K/F)$ の部分群であり，$Gal(K/F)$ において稠密です．

$\mathbb{Z}_l$ を l 進整数の全体からなる加法群とします．$\alpha \in \mathbb{Z}_l$ に対して，l 進位相に関する極限を考え，$\alpha = \lim_{m\to\infty} a_m\, (a_m \in \mathbb{Z})$ とおき，$Gal(K/F)$ の Krull 位相に関する極限をとって $\sigma^\alpha = \lim_{m\to\infty} \sigma^{a_m} \in Gal(K/F)$ とおきます．σ^α は $(a_m)_{m\geq 0}$ の取り方によらずに定まります．

定理 4.8. 記号を上述の通りとする．

K/F は無限次 Abel 拡大である．K/F の Galois 群 $Gal(K/F)$ は

$$\mathbb{Z}_l \longrightarrow Gal(K/F), \quad \alpha \longmapsto \sigma^\alpha$$

なる写像によって $\mathbb{Z}_l$ に位相群として同型である．

K/F の有限次の中間体は $F_n\, (n \geq 0)$ のみである．F_n/F は l^n 次巡回拡大である．σ の F_n への制限は F_n/F の Galois 群の生成元である．

今度は $F_n = \boldsymbol{F}_{q^{n+1}}$ $(n \geq 0)$ とおきます．すると，$\Omega = \bigcup_{n\geq 0} F_n$ が成り立ちます．Ω/F は Galois 拡大です．

Ω から Ω 自身への写像 σ を $\sigma(x) = x^q$ によって定義すれば，σ は Ω の F 自己同型写像になります．Ω/F の Galois 群を $Gal(\Omega/F)$ とすれば，$\{\sigma^n \mid n \in \mathbb{Z}\}$ は $Gal(\Omega/F)$ の部分群であり，$Gal(\Omega/F)$ において稠密です．

$Z = \prod_l \mathbb{Z}_l$ (l は素数全体を動く) とおきます．単射準同型 $\mathbb{Z} \longrightarrow Z$, $n \longmapsto (\cdots, n, \cdots)$ によって $\mathbb{Z}$ を Z の部分群とみなすことができます．$\mathbb{Z}$ は Z において稠密です．すなわち，任意の $\alpha \in Z$ に対して，ある $\mathbb{Z}$ の元の列 $(a_m)_{m\geq 0}$ が存在して，各 $\mathbb{Z}_l$ の l 進位相の直積位相についての極限をとって $\alpha = \lim_{m\to\infty} a_m$ となります．そこで，$\alpha \in Z$ に対して，$Gal(\Omega/F)$ の Krull 位相に関する極限をとって $\sigma^\alpha = \lim_{m\to\infty} \sigma^{a_m} \in Gal(\Omega/F)$ とおきます．σ^α は $(a_m)_{m\geq 0}$ の取り方によらずに定まります．

定理 4.9. 記号を上述の通りとする．

Ω/F は無限次 Abel 拡大である．Ω/F の Galois 群 $Gal(\Omega/F)$ は

$$Z \longrightarrow Gal(\Omega/F), \quad \alpha \longmapsto \sigma^\alpha$$

なる写像によって Z に位相群として同型である．

Ω/F の有限次の中間体は F_n $(n \geq 0)$ のみである．F_n/F は $n+1$ 次巡回拡大である．σ の F_n への制限は F_n/F の Galois 群の生成元である．

定理 4.10. p を素数とし，Ω を標数 p の素体 $\boldsymbol{F}_p$ の代数的閉包とする．このとき，Ω は $\boldsymbol{F}_p$ に p と異なるすべての素数 l についての 1 の原始 l 乗根 $\zeta_l \in \Omega$ を添加した体と一致する．

定理 4.11. F を標数 $p > 0$ の体とし，K を $f(X) \in F[X]$ の F に関する最小分解体として，$p \nmid [K : F]$ とする．このとき，次の二つの条件は同値である．

(i) 方程式 $f(X) = 0$ は F に関して根号により解ける．

(ii) K/F は有限次可解拡大である．

定理 4.12. $F = \boldsymbol{F}_q$ を q 個の元からなる有限体，K/F を有限体の拡大とし，$N_{K/F} : K^\times \longrightarrow F^\times$ を K/F のノルムとする．このとき，$\mathrm{Ker}\, N_{K/F} = (K^\times)^{q-1}$ が成り立つ．

定理 4.13. 有限体の有限次拡大 K/F のノルム $N_{K/F} : K^\times \longrightarrow F^\times$ は乗法群としての全射準同型写像である．

定理 4.14. $F = \boldsymbol{F}_q$ を q 個の元からなる有限体，K/F を有限体の拡大とし，$G = Gal(K/F)$ を K/F の Galois 群，$\sigma_F \in G$ を Frobenius 自己同型写像とする．このとき，乗法群の完全系列

$$0 \longrightarrow F^\times \longrightarrow K^\times \xrightarrow{\xi} K^\times \xrightarrow{N_{L/K}} F^\times \longrightarrow 0$$

が存在する．ここで ξ は

$$\xi(x) = \sigma_F(x)/x = x^{q-1} \quad (x \in K^\times)$$

によって定義される写像である．

定理 4.15. $F = \boldsymbol{F}_q$ を q 個の元からなる有限体，K/F を有限体の拡大とし，$T_{K/F} : K^\times \longrightarrow F^\times$ を K/F のトレースとする．このとき，$\mathrm{Ker}\, T_{K/F} = \{x^q - x \mid x \in K^\times\}$ が成り立つ．

定理 4.16. 有限体の有限次拡大 K/F のトレース $T_{K/F} : K \longrightarrow F$ は加法群としての全射準同型写像である．

定理 4.17. $F = \boldsymbol{F}_q$ を q 個の元からなる有限体，K/F を有限体の拡大とし，$G = Gal(K/F)$ を K/F の Galois 群，$\sigma_F \in G$ を Frobenius 自己同型写像とする．このとき，加法群の完全系列

$$0 \longrightarrow F \longrightarrow K \xrightarrow{\eta} K \xrightarrow{T_{L/K}} F \longrightarrow 0$$

が存在する．ここで η は

$$\eta(x) = \sigma_F(x) - x = x^q - x \quad (x \in K)$$

によって定義される写像である．

定義 4.18. K/F を有限次 Galois 拡大とし，$G = Gal(K/F)$ を K/F の Galois 群とする．集合 $\{\alpha^\sigma \mid \sigma \in G\}$ が K/F の基底となるとき，この基底を K/F の**正規底**と呼ぶ.

定理 4.19 (正規底定理). 任意の有限次 Galois 拡大 K/F に対して正規底が存在する．

有限体に関しては，もっと強い結果があります.

定理 4.20 (Lenstra, Schoof [3]). 任意の素数の冪 q と任意の整数 $f \geq 1$ に対して，$\boldsymbol{F}_{q^f}/\boldsymbol{F}_q$ の正規底 $\{\alpha, \alpha^q, \ldots, \alpha^{q^{f-1}}\}$ で，α が乗法群 $\boldsymbol{F}_{q^f}^\times$ の生成元であるものが存在する．

5 有限体上の方程式の解の個数

$F = \boldsymbol{F}_q\,(q = p^f)$ を q 個の元からなる標数 p の有限体とします.

$$f_i(X_1, \ldots, X_n) \in F[X_1, \ldots, X_n] \quad (i = 1, \ldots, s)$$

とし，それらの共通零点の集合を V とします：

$$V = \{(x_1, \ldots, x_n) \in F^n \mid f_i(x_1, \ldots, x_n) = 0\ (i = 1, \ldots, s)\}.$$

V の元の個数 $\#V$ は有限です．また，

$$\delta = \sum_{i=1}^{s} \deg f_i$$

とおきます.

定理 5.1 (Chevalley-Warning). $\delta < n$ ならば，$\#V \equiv 0 \pmod{p}$ が成り立つ.

系 5.1.1. $\delta < n$ であり，さらに，すべての $f_i\,(i = 1, \ldots, s)$ の定数項が 0 ならば，連立方程式

$$f_i(X_1, \ldots, X_n) = 0 \quad (i = 1, \ldots, s)$$

は F^n において自明でない解を持つ.

系 5.1.2. $\delta < n$ であり，さらに，すべての $f_i\,(i = 1, \ldots, s)$ が定数でない同次多項式ならば，連立方程式

$$f_i(X_1, \ldots, X_n) = 0 \quad (i = 1, \ldots, s)$$

は F^n において自明でない解を持つ.

系 5.1.3. 同次多項式 $f(X_1, \ldots, X_n) \in F[X_1, \ldots, X_n]$ について，$0 < \deg f < n$ ならば，方程式 $f(X_1, \ldots, X_n) = 0$ は F^n において自明でない解を持つ．

系 5.1.4. F の元を係数とする，3 変数以上の二次形式は F において自明でない解を持つ．

定理 5.2. $F = \boldsymbol{F}_q$ を q 個の元からなる有限体とする．方程式

$$a_1X_1 + \cdots + a_nX_n = b,$$
$$a_1, \ldots, a_n, b \in F, \quad a_1 \cdots a_n \neq 0$$

の解の個数は q^{n-1} である．

証明. 任意の $x_1, \ldots, x_{n-1} \in F$ に対して，$x_n = (b - a_1x_1 - \cdots - a_{n-1}x_{n-1})/a_n$ とおくと，$x_n \in F$ であり，$(x_1, \ldots, x_n)$ は上の方程式の解である． □

以下，$F = \boldsymbol{F}_q$ を，標数が 2 ではないような，q 個の元からなる有限体とします．方程式

$$a_1X_1^2 + \cdots + a_nX_n^2 = b,$$
$$a_1, \ldots, a_n, b \in F, \quad a_1 \cdots a_n \neq 0$$

の F における解の個数を N とします：

$$N = \#\{(x_1, \ldots, x_n) \in F^n \mid a_1x_1^2 + \cdots + a_nx_n^2 = b\}.$$

定理 5.3. N は次のように表される．

(I) $b = 0$ のとき：

(i) $n = 2m + 1$ のとき，$N = q^{2m}$.

(ii) $n = 2m$ のとき：

(a) $(-1)^m a_1 \cdots a_{2m} \in F^{\times 2}$ のとき，$N = q^{2m-1} + q^m - q^{m-1}$.

(b) $(-1)^m a_1 \cdots a_{2m} \notin F^{\times 2}$ のとき，$N = q^{2m-1} - q^m + q^{m-1}$.

(II) $b \neq 0$ のとき：

(i) $n = 2m + 1$ のとき：

(a) $(-1)^m a_1 \cdots a_{2m+1} \in F^{\times 2}$ のとき，$N = q^{2m} + q^m$.

(b) $(-1)^m a_1 \cdots a_{2m+1} \notin F^{\times 2}$ のとき，$N = q^{2m} - q^m$.

(ii) $n = 2m$ のとき：

(a) $(-1)^m a_1 \cdots a_{2m} \in F^{\times 2}$ のとき，$N = q^{2m-1} - q^{m-1}$.

(b) $(-1)^m a_1 \cdots a_{2m} \notin F^{\times 2}$ のとき，$N = q^{2m-1} + q^{m-1}$.

注意 5.4. F が標数 2 の体であるとき，すなわち $F = \boldsymbol{F}_q$, $q = 2^f$ のとき，$x_1, \ldots, x_n \in F$ に対して，

$$\begin{aligned} a_1x_1^2 + \cdots + a_nx_n^2 = b &\iff (a_1x_1^2 + \cdots + a_nx_n^2)^{2^{f-1}} = b^{2^{f-1}} \\ &\iff a_1^{2^{f-1}}x_1^{2^f} + \cdots + a_n^{2^{f-1}}x_n^{2^f} = b^{2^{f-1}} \\ &\iff a_1^{2^{f-1}}x_1 + \cdots a_n^{2^{f-1}}x_n = b^{2^{f-1}} \end{aligned}$$

が成り立つ．したがって，$a_1x_1^2 + \cdots + a_nx_n^2 = b$ の形の方程式を解くことは，$a_1'x_1 + \cdots + a_n'x_n = b'$ の形の方程式を解くことに帰着する．

参考文献

[1] 藤崎源二郎：体とガロア理論，岩波書店 (1991)

[2] 永田雅宜：可換体論（新版），裳華房 (1985)

[3] H. W. Lenstra, Jr. and R. J. Schoof, Primitive normal basis for finite fields, Math. Comp., **48**(1987), 217-231.