有限体の基礎

カプースタ　(Twitter：@s3tudyroom)

はじめに

本 PDF では有限体 (ここで体とは可換な可除環のことをさす) に関する基本的な性質をまとめる. (本 PDF の内容は参考文献 [1] の第 2 章の一部をまとめたものである.) これから議論していく上で一般の体や環に関する事実は前提知識とする. 特に重要なものは以下に記しておく.

任意の素数 p について剰余環 $\mathbb{Z}/p\mathbb{Z}$ が体となることは有名な事実である (ここでは証明はしない). また, $\mathbb{Z}/p\mathbb{Z}$ は p 元体であり, $\{0,1,\ldots,p-1\}$ が完全代表系となることも知られている. $\mathbb{F}_p=\{0,1,\ldots,p-1\}$ とおき, 自然な全単射 $\mathbb{Z}/p\mathbb{Z}\to\mathbb{F}_p$ が準同型になるように $\mathbb{F}_p$ 上の加法と乗法を定める. (つまり, $\mathbb{F}_p$ 上の演算は一度 $\mathbb{Z}/p\mathbb{Z}$ に自然に写して $\mathbb{Z}/p\mathbb{Z}$ 内で演算し, その結果を再び $\mathbb{F}_p$ に戻すことで計算する.) 結果, $\mathbb{F}_p$ 上の演算は p を法として計算することと一致する.

標数 p の体 F に対して, 写像 $\mathrm{Frob}_{p^s}:F\to F$ $(s\in\mathbb{N})$ を

$$\mathrm{Frob}_{p^s}(a)=a^{p^s}\qquad(a\in F)$$

と定める. これは体の準同型であり, Frobenius 準同型と呼ばれる. 特に, Frobenius 準同型が和を保存することから任意の $a,b\in F$ と p の冪数 q に対して

$$(a+b)^q=a^q+b^q$$

が成り立つことに注意せよ.

体 F と正整数 n に対して, F の標数 p が n を割り切らないとき F 上の 1 の原始 n 乗根 (F の拡大体の元で乗法に関する位数が n となるもの) がとれる. その 1 つを ζ としたとき多項式

$$\Phi_n(x)=\prod_{\substack{s=1\\ \gcd(s,n)=1}}^{n}(x-\zeta^s)$$

は 1 の原始 n 乗根 ζ の取り方に依らず等しく, F 上の n-円分多項式と呼ばれる. F 上の n-円分多項式 $\Phi_n(x)$ は F の素体 F_0 上の多項式である. また, n の正の約数 d に対して, $\Phi_n(x)$ は $\dfrac{x^n-1}{x^d-1}$ を割り切る.

1　有限体の特徴付け

補題 1.1

F/K を有限体の拡大, $|K|=q,[F:K]=m$ とする. このとき, $|F|=q^m$ となる.

証明： F は K 上のベクトル空間であり, F は有限なので, F は K 上の有限次元ベクトル空間である. $[F:K]=m$ とすれば, F は m 個の元からなる K 上の基底をもつ. それを $b_1,\dots,b_m$ とする. このとき, F の任意の元は $a_1,\dots,a_m\in K$ を用いて $a_1b_1+\cdots+a_mb_m$ と一意的に表される. 各係数 $a_1,\dots,a_m$ はそれぞれ q 通りの選び方があるので $|F|=q^m$ となる. □

定理 1.2

有限体 F の位数は素数 p と正整数 n を用いて p^n と表される. ここで, 素数 p は F の標数であり, 正整数 n は F の素体上の拡大次数である.

証明： F は有限体なので有限の標数 p をもつ (特に p は素数). F の標数が p なので, F の素体 F_0 は p 元体である. $[F:F_0]=n$ とすれば, 補題 1.1 より $|F|=p^n$ となる. □

補題 1.3

F を q 元体とする. このとき, 任意の $a\in F$ に対して $a^q=a$ が成り立つ.

証明： $a=0$ なら明らかなので $a\neq 0$ とする. $F\setminus\{0\}$ は乗法に関して位数 $q-1$ の群なので, $a^{q-1}=1$ が成り立つ. したがって, $a^q=a$ となる. □

補題 1.4

F を q 元体, K を F の部分体とする. このとき, K 上の多項式 x^q-x は F 上で

$$x^q-x=\prod_{a\in F}(x-a)$$

と分解できる. また, F は x^q-x の K 上最小分解体である.

証明： 次数 q の多項式 x^q-x は F に高々 q 個の根をもつ. 一方, 補題 1.3 より F の元はすべて x^q-x の根である. F は q 元体なので,

$$x^q-x=\prod_{a\in F}(x-a)$$

と分解できる. また, F より真に小さい体では x^q-x は分解しきれない. □

系 1.5

E/F を有限体の拡大, $|F|=q$ とする. このとき, 任意の $\alpha\in E$ に対して次が成り立つ.

$$\alpha^q=\alpha \quad\Longleftrightarrow\quad \alpha\in F$$

証明： $\alpha^q=\alpha$ が成り立っているとすれば, α は多項式 x^q-x の根となる. 補題 1.4 より $\alpha\in F$ となる. この逆は補題 1.3 そのものである. □

定理 1.6

任意の素数 p と正整数 n に対して, p^n 元体が存在する. また, それらは同型を除いて一意である.

証明： $q=p^n$ とおく. F を x^q-x の $\mathbb{F}_p$ 上最小分解体とする. x^q-x の導多項式 $qx^{q-1}-1$ は $\mathbb{F}_p$ 上で -1 なので, x^q-x は重根をもたない. つまり, x^q-x は F に相異なる q 個の根をもつ.

ここで, $S = \{a \in F \mid a^q - a = 0\}$ とおく. $0, 1 \in S$ は明らかである. 任意に $a, b \in S$ をとる. このとき,

$$(a-b)^q = a^q - b^q = a - b$$

となるので, $a - b \in S$ である. また, $b \neq 0$ なら

$$(ab^{-1})^q = a^q b^{-q} = ab^{-1}$$

となるので, $ab^{-1} \in S$ となる. したがって, S は F の部分体である. S は $x^q - x$ の根をすべて含むので, $x^q - x$ は S 上で分解できる. F の最小性から $F = S$ であり, $|F| = |S| = q$ となる.

E を p^n 元体とする. このとき, 定理 1.2 より E の標数は p であり, $\mathbb{F}_p$ からの埋め込み ι が存在する. 補題 1.4 より E は $x^q - x$ の素体 $\iota(\mathbb{F}_p)$ 上最小分解体である. したがって, $x^q - x$ の $\mathbb{F}_p$ 上最小分解体 F は E と同型である. □

定理 1.7

p^n 元体の部分体の位数は n の正の約数 m を用いて p^m と表される. 逆に, n の正の約数 m に対して, 位数 p^m の部分体がただ 1 つ存在する.

証明： F を p^n 元体, K を F の部分体とする. K の標数は F と同じ p であり, 定理 1.2 より $|K| = p^m$ となる. $[F : K] = s$ とすれば, $p^n = (p^m)^s = p^{ms}$ となり, $n = ms$ である.

m を n の正の約数とする. $p^m - 1$ は $p^n - 1$ を割り切るので, $F_0[x]$ において $x^{p^m-1} - 1$ は $x^{p^n-1} - 1$ を割り切る. ($F_0 (\simeq \mathbb{F}_p)$ は F の素体である.) つまり, $x^{p^m-1} - 1$ の根はすべて $x^{p^n-1} - 1$ の根である. よって, F は $x^{p^m-1} - 1$ の F_0 上最小分解体を含んでいる. それが位数 p^m の部分体である.

また, $K, L \subset F$ を位数 p^m の部分体とすれば, K, L は $x^{p^m-1} - 1$ の F における根 (p^m 個) をもっている. $|K| = |L| = p^m$ なので $K = L$ でなければいけない. □

この定理によって, 有限体はその位数によって (同型を除いて) ただ 1 つに定まる. なので, 以降 q 元体を記号 $\mathbb{F}_q$ で表すことにする. また, 有限体 F に対して有限次拡大体を (同型を除いて) ただ 1 つとることができ, そのつど記号 $\mathbb{F}_q$ はこういった拡大体を表すものとする. (例えば, q 元体 F の議論中に記号 $\mathbb{F}_{q^n}$ を用いたとき, これは F の n 次拡大体のうちのひとつを表すことになる. ただし, 素数 p についての $\mathbb{F}_p$ は冒頭にある通り特定の体を表すので注意せよ.) さらに, $\mathbb{F}_q$ と書くとき q は素数の冪数でないとならないことに注意するべきである.

定理 1.8

有限体 F の乗法群 $F^\times$ は巡回群である.

証明： $|F| = 2$ のときは明らかなので, $|F| = q \geq 3$ とし, $q - 1 = p_1^{r_1} \cdots p_m^{r_m}$ を素冪分解とする. 各 $i = 1, \ldots, m$ に対して, 多項式 $x^{\frac{q-1}{p_i}} - 1$ は F において高々 $\dfrac{q-1}{p_i}$ 個の根をもつ. $\dfrac{q-1}{p_i} < q - 1$ なので, $x^{\frac{q-1}{p_i}} - 1$ の根にならない元 $a_i \in F^\times$ がとれる. ここで, $b_i = a_i^{(q-1)p_i^{-r_i}}$ $(i = 1, \ldots, m)$ おく. $b_i^{p_i^{r_i}} = a_i^{q-1} = 1$ より b_i の位数は $p_i^{r_i}$ の約数である. 一方, $b_i^{p_i^{r_i-1}} = a_i^{\frac{q-1}{p_i}} \neq 1$ なので b_i の位数は $p_i^{r_i}$ である.

$b = b_1 \cdots b_m$ とおき, b の位数が $q - 1$ であることを背理法で示す. b の位数 s は $q - 1$ 未満であるとする. このとき, s は $q - 1$ を割り切り

$$s \;\Big|\; \frac{q-1}{p_i}$$

となる $i \in \{1, \ldots, m\}$ がとれる. したがって,

$$b_1^{\frac{q-1}{p_i}} \cdots b_m^{\frac{q-1}{p_i}} = b^{\frac{q-1}{p_i}} = 1$$

が成り立つ. 各 $j = 1, \ldots, m, j \neq i$ に対して $p_j^{r_j}$ は $\dfrac{q-1}{p_i}$ を割り切るので, $b_j^{\frac{q-1}{p_i}} = 1$ $(j = 1, \ldots, m, j \neq i)$ である. よって, $b_i^{\frac{q-1}{p_i}} = 1$ となるが, これは b_i の位数が $p_i^{r_i}$ であることに矛盾する. □

【定義 1.9】
有限体 F の乗法群の生成元を F の**原始元** (primitive element) という.

定理 1.10
有限体の拡大 E/F は単純代数的拡大である. また, ζ を E の原始元とすれば $E = F(\zeta)$ となる.

証明： ζ を E の原始元とする. $F(\zeta) \subset E$ は明らかである. 一方, ζ は $E^\times$ を生成し, $0 \in F(\zeta)$ なので $E \subset F(\zeta)$ となる. □

系 1.11
有限体 F と正整数 n に対して, F 上の n 次既約多項式が存在する.

証明： E を F の n 次拡大体とする. 定理 1.9 より $E = F(\zeta)$ となる $\zeta \in F$ がとれる. ζ の F 上最小多項式は n 次既約多項式である. □

2 既約多項式の根

補題 2.1
f を q 元体 F 上の m 次既約多項式とする. このとき, 次が成り立つ.

$$f(x) \mid x^{q^n} - x \quad \Longleftrightarrow \quad m \mid n$$

証明： $f(x) \mid x^{q^n} - x$ を仮定する. E を f の F 上最小分解体とし, $\alpha \in E$ を f の根とする. $\alpha^{q^n} = \alpha$ なので α は q^n 元体 $\mathbb{F}_{q^n}$ の元となる. したがって, $F(\alpha)$ は $\mathbb{F}_{q^n}$ の部分体である. $[F(\alpha) : F] = m, [\mathbb{F}_{q^n} : F] = n$ なので $m \mid n$ である.

$m \mid n$ を仮定する. $\mathbb{F}_{q^m}$ は $\mathbb{F}_{q^n}$ の部分体である. α を f の F 上最小分解体における f の根とする. このとき, $[F(\alpha) : F] = m$ より $F(\alpha) = \mathbb{F}_{q^m}$ となる. したがって, $\alpha \in \mathbb{F}_{q^n}$ となり, $\alpha^{q^n} = \alpha$ が成り立つので, α は $x^{q^n} - x$ の根である. よって, $f(x) \mid x^{q^n} - x$ となる. □

定理 2.2
q 元体 F 上の m 次既約多項式 f は $\mathbb{F}_{q^m}$ に根をもつ. その 1 つを α とすれば, f の根は $\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}$ の m 個である.

証明： α を f の F 上最小分解体における f の根とする. このとき, $[F(\alpha) : F] = m$ なので $F(\alpha) = \mathbb{F}_{q^m}$ で

ある.

f の根 $\beta \in \mathbb{F}_{q^m}$ に対して, β^q が再び f の根になることを示す.

$$f(x) = a_m x^m + \cdots + a_1 x + a_0$$

となる $a_0, \ldots, a_m \in F$ がある. このとき,

$$\begin{aligned} f(\beta^q) &= a_m \beta^{qm} + \cdots + a_1 \beta^q + a_0 \\ &= a_m^q \beta^{qm} + \cdots + a_1^q \beta^q + a_0^q \\ &= (a_m \beta^m + \cdots + a_1 \beta + a_0)^q \\ &= f(\beta)^q \qquad = 0 \end{aligned}$$

となるので, β^q は f の根である.

したがって, $\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}$ はすべて f の根である. $\alpha^{q^j} = \alpha^{q^k}, j \neq k$ となる $j, k \in \{0, \ldots, m-1\}$ があるとして矛盾を導く. $j < k$ としても一般性を失わない. このとき,

$$\alpha^{q^{m-k+j}} = \alpha^{q^m q^{-k} q^j} = \alpha^{q^m} = \alpha$$

となるので, α は $x^{q^{m-k+j}} - x$ の根である. 補題 2.1 より m が $m-k+j$ を割り切ることになるが, $0 < m-k+j < m$ なのでこれは不可能である. □

系 2.3

q 元体 F 上の m 次既約多項式 f の F 上最小分解体は $\mathbb{F}_{q^m}$ で得られる.

証明： 定理 2.2 より f は $\mathbb{F}_{q^m}$ 上で分解される. さらに, $\alpha \in \mathbb{F}_{q^m}$ を f の根とすれば, $F(\alpha, \ldots, \alpha^{q^{m-1}}) = F(\alpha) = \mathbb{F}_{q^m}$ とできる. $F(\alpha, \ldots, \alpha^{q^{m-1}})$ は f の F 上最小分解体である. □

系 2.4

f, g を有限体 F 上の既約多項式, $\deg f = \deg g$ とする. このとき, f の F 上最小分解体と g の F 上最小分解体は同型である.

証明： $\deg f = \deg g = n$ とすれば, f, g の F 上最小分解体はどちらも $\mathbb{F}_{q^n}$ で得られる. □

系 2.5

F を q 元体, E を F の m 次拡大体, $\alpha \in E$ とする. α の F 上の共役全体は $\{\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}\}$ で得られる. また, α の F 上最小多項式の次数が d のとき, α の F 上の共役は $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}$ の d 個である.

証明： α の F 上最小多項式 f は F 上の d 次既約多項式である. 定理 2.2 より $\alpha \in \mathbb{F}_{q^d} (\subset E)$ とでき, α の共役 (f の根) は $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}$ の d 個である. また, $\alpha \in \mathbb{F}_{q^d}$ なので $\alpha^{q^d} = \alpha$ とでき,

$$\{\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}\} = \{\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}\}$$

が成り立つ. □

特に, d は m の約数であり, $\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}$ の並びには $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}$ という最小の並びが $\dfrac{m}{d}$ 回繰り返されている.

定理 2.6

有限体の元の任意の共役はすべて同じ位数をもつ.

証明： F を q 元体, $\alpha \in F$ の位数を n とする (n は $q-1$ の約数である). K を F の部分体, $|K| = r, q = r^m$ とする. 任意に $k \in \{0, 1, \ldots, m-1\}$ をとる. q^k と $q-1$ は互いに素なので, r^k と n も互いに素. したがって, $\langle \alpha^{r^k} \rangle$ は位数 $\dfrac{n}{\gcd(r^k, n)} = n$ の巡回群となる. つまり, α^{r^k} の位数は n である. □

系 2.7

有限体において, 原始元の共役は原始元である.

$F/K/L$ を体の拡大において, $\alpha \in F$ の K 上の共役は L 上の共役でもある. したがって, F の元の任意の部分体上の共役はすべて素体 F_0 上の共役となる. 実際, 有限体の拡大 $\mathbb{F}_{p^{nm}}/\mathbb{F}_{p^n}/\mathbb{F}_p$ において, $\alpha \in \mathbb{F}_{p^{nm}}$ の $\mathbb{F}_{p^n}$ 上の共役は

$$\alpha, \alpha^{p^n}, \ldots, \alpha^{p^{n(m-1)}}$$

の $m-1$ 個であり, これらは $\mathbb{F}_p$ 上の共役

$$\alpha, \alpha^{p}, \ldots, \alpha^{p^{nm-1}}$$

のなかに含まれている.

定理 2.8

F を q 元体, E を F の m 次拡大体とする. 各 $i = 0, 1, \ldots, m-1$ に対して, 写像 $\sigma_i : E \to E$ を

$$\sigma_i(\alpha) = \alpha^{q^i} \qquad (\alpha \in E)$$

で定めると, これらは相異なる E の F 上自己同型となる. また, E/F の自己同型群は $\{\sigma_0, \sigma_1, \ldots, \sigma_{m-1}\}$ となる.

証明： $\sigma_0, \sigma_1, \ldots, \sigma_{m-1}$ が E の自己準同型であることは容易である. また, $|F| = q$ なので各 σ_i ($i = 0, 1, \ldots, m-1$) は F を不変とする. つまり, 各 σ_i は E の F 上自己準同型である. E が体より各 σ_i は単射であり, E が有限なの各 σ_i は全射となる. したがって, $\sigma_0, \sigma_1, \ldots, \sigma_{m-1}$ は E の F 上自己同型である.

また, $1 = q^0 < q^1 < \cdots < q^{m-1} < q^m - 1 = |E^\times|$ なので, E の原始元は $\sigma_0, \sigma_1, \ldots, \sigma_{m-1}$ によって異なる元に写される. よって, $\sigma_0, \sigma_1, \ldots, \sigma_{m-1}$ は相異なる写像である.

$|\mathrm{Aut}(E/F)| \leq [E : F] = m$ であり, $|\{\sigma_0, \sigma_1, \ldots, \sigma_{m-1}\}| = m$ より $\mathrm{Aut}(E/F) = \{\sigma_0, \sigma_1, \ldots, \sigma_{m-1}\}$ となる. □

3　トレース・ノルム

【定義 3.1】

F を q 元体, E を F の m 次拡大体とする. 各 $\alpha \in E$ に対して

$$\mathrm{Tr}_{E/F}(\alpha) = \sum_{\sigma \in \mathrm{Aut}(E/F)} \sigma(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}}$$

となるように写像 $\mathrm{Tr}_{E/F} : E \to E$ を定める. この写像を E の F 上の**トレース** (trace), また, $\mathrm{Tr}_{E/F}(\alpha)$ を α の F 上のトレースという. 特に, 素体上のトレースは**絶対トレース** (absolute trace) といい, 単に Tr_E で表す.

補題 3.2

有限体の拡大 E/F に対して, E の F 上のトレースは F への写像である.

証明： $|F| = q, |E| = q^m$ とする. 任意に $\alpha \in E$ をとり, α の位数を d とする. f を α の F 上最小多項式とし, $g(x) = f(x)^{\frac{m}{d}} \in F[x]$ とおく. このとき, g は m 次多項式であり, 系 2.5 の証明から

$$\begin{aligned} g(x) &= \underbrace{\{(x-\alpha)\cdots(x-\alpha^{q^{d-1}})\}\cdots\{(x-\alpha)\cdots(x-\alpha^{q^{d-1}})\}}_{\frac{m}{d}\text{回繰り返す}} \\ &= (x-\alpha)\cdots(x-\alpha^{q^{m-1}}) \end{aligned}$$

とできる. ここで, g の $m-1$ 次の係数は $\mathrm{Tr}_{E/F}(\alpha)$ であり, $g \in F[x]$ より $\mathrm{Tr}_{E/F}(\alpha) \in F$ となる. □

定理 3.3

F を q 元体, E を F の m 次拡大体とする. このとき, E の F 上のトレースは E から F への全射 F 線形写像である. また, 次が成り立つ.

$$^\forall a \in F, \mathrm{Tr}_{E/F}(a) = \underbrace{a + \cdots + a}_{m\text{ 個}}$$

$$^\forall \alpha \in E, \mathrm{Tr}_{E/F}(\alpha^q) = \mathrm{Tr}_{E/F}(\alpha)$$

証明： 任意に $\alpha, \beta \in E, a \in F$ をとる.

$$\begin{aligned} \mathrm{Tr}_{E/F}(\alpha+\beta) &= (\alpha+\beta) + (\alpha+\beta)^q + \cdots + (\alpha+\beta)^{q^{m-1}} \\ &= \alpha + \beta + \alpha^q + \beta^q + \cdots + \alpha^{q^{m-1}} + \beta^{q^{m-1}} \\ &= \mathrm{Tr}_{E/F}(\alpha) + \mathrm{Tr}_{E/F}(\beta) \end{aligned}$$

$$\begin{aligned} \mathrm{Tr}_{E/F}(a\alpha) &= a\alpha + a^q\alpha^q + \cdots + a^{q^{m-1}}\alpha^{q^{m-1}} \\ &= a\alpha + a\alpha^q + \cdots + a\alpha^{q^{m-1}} \\ &= a\mathrm{Tr}_{E/F}(\alpha) \end{aligned}$$

となるので, $\mathrm{Tr}_{E/F}$ は F 線形写像である.

F 上の多項式 $f(x) = x^{q^{m-1}} + \cdots + x^q + x$ は高々 q^{m-1} 個の根を E にもつが, $|E| = q^m$ なので f の根とならない $\alpha \in E$ がとれる. ここで, $a = \mathrm{Tr}_{E/F}(\alpha) = f(\alpha) \neq 0$ とおく. 任意の $b \in F$ に対して,

$$\mathrm{Tr}_{E/F}(ba^{-1}\alpha) = ba^{-1}\mathrm{Tr}_{E/F}(\alpha) = ba^{-1}a = b$$

となるので, $\mathrm{Tr}_{E/F} : E \to F$ は全射である.

また, 任意の $a \in F, \alpha \in E$ に対して

$$\begin{aligned}\mathrm{Tr}_{E/F}(a) &= a + a^q + \cdots + a^{q^{m-1}} \\ &= \underbrace{a + a + \cdots + a}_{m \text{ 個}}\end{aligned}$$

$$\begin{aligned}\mathrm{Tr}_{E/F}(\alpha^q) &= \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{m-1}} + \alpha^{q^m} \\ &= \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{m-1}} + \alpha \\ &= \mathrm{Tr}_{E/F}(\alpha)\end{aligned}$$

とできる. □

定理 3.4

E/F を有限体の拡大とする. 各 $\beta \in E$ に対して, 写像 $L_\beta : E \to F$ を

$$L_\beta(\alpha) = \mathrm{Tr}_{E/F}(\beta\alpha) \qquad (\alpha \in F)$$

で定めると, 各 L_β は F 線形写像となる. また, 各 $\beta \in E$ に $L_\beta \in \mathrm{Hom}_F(E, F)$ を対応させる写像 $E \to \mathrm{Hom}_F(E.F)$ は全単射である.

証明： 各 L_β $(\beta \in E)$ が F 線形写像となることは容易である. $\beta, \gamma \in E$ を任意にとり, $\beta \neq \gamma$ とする. 定理 3.3 より $\mathrm{Tr}_{E/F}(\delta) \neq 0$ となる $\delta \in E$ がとれる. $\alpha = (\beta - \gamma)^{-1}\delta$ とすれば

$$\begin{aligned}L_\beta(\alpha) - L_\gamma(\alpha) &= \mathrm{Tr}_{E/F}(\beta\alpha) - \mathrm{Tr}_{E/F}(\gamma\alpha) \\ &= \mathrm{Tr}_{E/F}(\beta\alpha - \gamma\alpha) \\ &= \mathrm{Tr}_{E/F}((\beta - \gamma)\alpha) \\ &= \mathrm{Tr}_{E/F}(\delta) \qquad \neq 0\end{aligned}$$

となるので, $L_\beta \neq L_\gamma$ である.

$|F| = q, |E| = q^m$ とすれば, E は F 上の m 次元ベクトル空間なので, E から F への F 線形写像は q^m 個ある. $|E| = q^m = |\mathrm{Hom}_F(E, F)|$ なので, 単射写像

$$\begin{array}{ccc} E & \longrightarrow & \mathrm{Hom}_F(E, F) \\ \cup & & \cup \\ \beta & \longmapsto & L_\beta \end{array}$$

は全射となる. □

定理 3.5

F を q 元体, E を F の拡大体とする. このとき, 任意の $\alpha \in E$ に対して次が成り立つ.

$$\mathrm{Tr}_{E/F}(\alpha) = 0 \quad \Longleftrightarrow \quad {}^{\exists}\beta \in E \text{ s.t. } \alpha = \beta^q - \beta$$

証明： $[E:F] = m$ とおき, 任意に $\alpha \in E$ をとって, $\mathrm{Tr}_{E/F}(\alpha) = 0$ であるとする. 多項式 $x^q - x - \alpha$ が根をもつように E を適当に拡大し, $x^q - x - \alpha$ の根を β とする. このとき, $\beta^q - \beta = \alpha$ であり,

$$\begin{aligned}
0 &= \mathrm{Tr}_{E/F}(\alpha) \\
&= \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}} \\
&= (\beta^q - \beta) + (\beta^q - \beta)^q + \cdots + (\beta^q - \beta)^{q^{m-1}} \\
&= (\beta^q - \beta) + (\beta^{q^2} - \beta^q) + \cdots + (\beta^{q^m} - \beta^{q^{m-1}}) \\
&= \beta^{q^m} - \beta
\end{aligned}$$

とできる. したがって, $\beta^{q^m} = \beta$ が成り立ち, $\beta \in E$ となる. 逆は定理 3.3 より明らかである. □

定理 3.6

有限体の拡大 $E/F/K$ に対して, 次が成り立つ.

$$\mathrm{Tr}_{E/K} = \mathrm{Tr}_{F/K} \circ \mathrm{Tr}_{E/F}$$

証明： $|K| = q, [F:K] = m, [E:F] = n$ とする. このとき, 任意の $\alpha \in E$ に対して

$$\begin{aligned}
\mathrm{Tr}_{F/K}(\mathrm{Tr}_{E/F}(\alpha)) &= \sum_{i=0}^{m-1} \mathrm{Tr}_{E/F}(\alpha)^{q^i} \\
&= \sum_{i=0}^{m-1} \left(\sum_{j=0}^{n-1} \alpha^{q^{jm}} \right)^{q^i} \\
&= \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \alpha^{jm+i} \\
&= \sum_{k=0}^{mn-1} \alpha^k \\
&= \mathrm{Tr}_{E/K}(\alpha)
\end{aligned}$$

となる. □

【定義 3.7】

F を q 元体, E を F の m 次拡大体とする. 各 $\alpha \in E$ に対して

$$\mathrm{N}_{E/F}(\alpha) = \prod_{\sigma \in \mathrm{Aut}(E/F)} \sigma(\alpha) = \alpha \cdot \alpha^q \cdots \alpha^{q^{m-1}} = \alpha^{\frac{q^m-1}{q-1}}$$

となるように写像 $\mathrm{N}_{E/F} : E \to E$ を定める. この写像を E の F 上の**ノルム** (norm), また, $\mathrm{Tr}_{E/F}(\alpha)$ を α の F 上のノルムという.

補題 3.8

有限体の拡大 E/F に対して, E の F 上のノルムは F への写像である.

証明： 補題 3.2 の証明で考えた F 上の多項式 g の定数項が $\mathrm{N}_{E/F}$ による値になっている. □

定理 3.9

F を q 元体, E を F の m 次拡大体とする. このとき, E の F 上のノルムは E から F への積を保つ全射写像である. 特に, 始域を $E^\times$ に制限すれば $\mathbb{F}^\times$ への全射準同型となる. また, 次が成り立つ.

$$^\forall a \in F, \mathrm{N}_{E/F}(a) = a^m$$

$$^\forall \alpha \in E, \mathrm{N}_{E/F}(\alpha^q) = \mathrm{N}_{E/F}(\alpha)$$

証明： $\alpha, \beta \in F$ を任意にとる. このとき,

$$\begin{aligned}\mathrm{N}_{E/F}(\alpha\beta) &= (\alpha\beta)^{\frac{q^m-1}{q-1}} \\ &= \alpha^{\frac{q^m-1}{q-1}}\beta^{\frac{q^m-1}{q-1}} \\ &= \mathrm{N}_{E/F}(\alpha)\mathrm{N}_{E/F}(\alpha)\end{aligned}$$

となるので, $\mathrm{N}_{E/F}$ は積を保存する写像である.

$\alpha \in E^\times$ を任意にとる. このとき, α は零因子でないので $\mathrm{N}_{E/F}(\alpha) \in F^\times$ となる. よって, $\mathrm{N}_{E/F}$ は $E^\times$ から $F^\times$ への準同型とみることができる. (ここでは, $\mathrm{N}_{E/F} : E^\times \to F^\times$ として議論を進める.) また, $\mathrm{Ker}\,\mathrm{N}_{E/F}$ は F 上の多項式 $x^{\frac{q^m-1}{q-1}} - 1$ の E における根全体である. $|\mathrm{Ker}\,\mathrm{N}_{E/F}| = d$ とおけば, $d \leq \dfrac{q^m-1}{q-1}$ であり, 群の第一同型定理より

$$|\mathrm{Im}\,\mathrm{N}_{E/F}| = \frac{q^m-1}{d} \geq q-1$$

が成り立つ. $|F^\times| = q-1$ なので $\mathrm{Im}\,\mathrm{N}_{E/F} = F^\times$ となる. つまり, $\mathrm{N}_{E/F} : E^\times \to F^\times$ は全射である. また, $\mathrm{N}_{E/F}(0) = 0$ なので $\mathrm{N}_{E/F} : E \to F$ としても全射である.

さらに, 任意の $a \in F$ に対して

$$\begin{aligned}\mathrm{N}_{E/F}(a) &= a \cdot a^q \cdots a^{q^{m-1}} \\ &= \underbrace{a \cdot a \cdots a}_{m\text{ 個}} \qquad = a^m\end{aligned}$$

となる. また, 任意の $\alpha \in E$ に対して, $\mathrm{N}_{E/F}(\alpha) \in F$ なので

$$\mathrm{N}_{E/F}(\alpha^q) = \mathrm{N}_{E/F}(\alpha)^q = \mathrm{N}_{E/F}(\alpha)$$

が成り立つ. □

定理 3.10

有限体の拡大 $E/F/K$ に対して, 次が成り立つ.

$$\mathrm{N}_{E/K} = \mathrm{N}_{F/K} \circ \mathrm{N}_{E/F}$$

証明： $|K| = q, [F : K] = m, [E : F] = n$ とする．このとき, 任意の $\alpha \in E$ に対して

$$\begin{aligned}
\mathrm{N}_{F/K}(\mathrm{N}_{E/F}(\alpha)) &= \mathrm{N}_{F/K}\left(\alpha^{\frac{q^{mn}-1}{q^m-1}}\right) \\
&= \left(\alpha^{\frac{q^{mn}-1}{q^m-1}}\right)^{\frac{q^m-1}{q-1}} \\
&= \alpha^{\frac{q^{mn}-1}{q-1}} \\
&= \mathrm{N}_{E/K}(\alpha)
\end{aligned}$$

となる． □

4 おまけ：Wedderburn の定理

今まで, 有限体についての基本的な議論を展開してきた．そこで「これは非可換な体系ではどうなるのだろうか」という疑問が生まれるだろう．この疑問に答えようと (非可換性を排除せずに) 有限な可除環 (斜体とも) における一般的な議論を始めたいところだが, 実は有限な非可換体 (非可換な可除環) は存在しないことが Wedderburn によって証明されている．ここでは「有限な可除環はすべて可換である」という Wedderburn の主張 (Wedderburn の定理) の証明をしたいと思う．そのためにまず有限群の議論から準備する．

補題 4.1

G を群とし, G 上の二項関係 $\sim$ を

$$a \sim b \quad \Longleftrightarrow \quad {}^{\exists}g \in G \text{ s.t. } gag^{-1} = b$$

で定めると, この関係 $\sim$ は G 上の同値関係となる．

証明： 任意に $a, b, c \in G$ をとる．まず, $eae^{-1} = a$ なので $a \sim a$ となる．また, $a \sim b$ とすれば $gag^{-1} = b$ となる $g \in G$ があり, $g^{-1}b(g^{-1})^{-1} = a$ となるので $b \sim a$ である．$a \sim b, b \sim c$ とすれば, $gag^{-1} = b, hbh^{-1} = c$ となる $g, h \in G$ がある．このとき, $(hg)a(hg)^{-1} = c$ となるので $a \sim c$ である． □

【定義 4.2】
補題 4.1 のおける同値関係 $\sim$ を G の共役関係といい, $a \sim b$ となるとき b は a の共役であるなどという．また, 各 $a \in G$ の共役関係による同値類を a の**共役類** (conjugacy class) といい $C(a)$ で表す．

命題 4.3

G を有限群, $\{a_1, \ldots, a_k\}$ を $G/\sim$ の完全代表系とする．このとき, 次が成り立つ．

$$|G| = \sum_{i=1}^{k} |C(a_i)|$$

また, この等式の右辺の和の項には必ず 1 が現れる．

証明： $G/\sim$ は G の分割 (類別とも) であり, $\{a_1, \ldots, a_k\}$ が完全代表系なので等式が成り立つのは明らかである．また, 単位元 $e \in G$ に対しては $C(e) = \{e\}$ となるので $\{a_1, \ldots, a_k\}$ には e が含まれており, 等式の右辺の和には $|C(e)| = 1$ が現れる． □

この等式を G の**類等式** (class equation) という.

【定義 4.4】
群 G に対して

$$Z(G) = \{z \in G \mid {}^{\forall}g \in G, gzg^{-1} = z\}$$

を G の**中心** (center) という.

補題 4.5

G を有限群, $S \subset G$ を $G/\sim$ の完全代表系とする. このとき, $Z(G) \subset S$ となり, $G/\sim$ の完全代表系は非交和

$$Z(G) \sqcup \{a_1, \ldots, a_k\}$$

と表すことができる. また, G の類等式は

$$|G| = |Z(G)| + \sum_{i=1}^{k} |C(a_i)|$$

となり, 特に右辺の $\sum_{i=1}^{k} |C(a_i)|$ の項には 1 は現れない.

証明： 任意の $z \in Z(G)$ に対して明らかに $C(z) = \{z\}$ なので $z \in S$ となる. $\{a_1, \ldots, a_k\} = S \setminus Z(G)$ とすれば, $S = Z(G) \cup \{a_1, \ldots, a_k\}$ は非交和となる.

任意の $z \in Z(G)$ に対して $|C(z)| = |\{z\}| = 1$ なので, G の類等式は

$$\begin{aligned} |G| &= \sum_{z \in Z(G)} |C(z)| + \sum_{i=1}^{k} |C(a_i)| \\ &= \sum_{z \in Z(G)} 1 + \sum_{i=1}^{k} |C(a_i)| \\ &= |Z(G)| + \sum_{i=1}^{k} |C(a_i)| \end{aligned}$$

となる. また, $a \in G$ が $|C(a)| = 1$ を満たすなら明らかに $a \in Z(G)$ となる. 各 $a_1, \ldots, a_k$ は中心の元でないので $\sum_{i=1}^{k} |C(a_i)|$ に 1 は現れない. □

【定義 4.6】
G を群, $S \subset G, S \neq \emptyset$ とする. このとき,

$$N(S) = \{g \in G \mid gSg^{-1} = S\}$$

と定め, これを S の**正規化群** (normalizer) という.

補題 4.7

G を群, $S \subset G, S \neq \emptyset$ とする. このとき, $N(S)$ は G の部分群である.

証明： 明らかに $eSe^{-1} = S$ なので $e \in N(S)$ である. また, $a, b \in N(S)$ に対して

$$(ab)S(ab)^{-1} = abSb^{-1}a^{-1} = aSa^{-1} = S$$
$$a^{-1}S(a^{-1})^{-1} = a^{-1}(aSa^{-1})a = (a^{-1}a)S(a^{-1}a) = S$$

となるので, $ab, a^{-1} \in N(S)$ となる. □

補題 4.8

G を群, $S \subset G, S \neq \emptyset$ とする. このとき, 写像

$$\begin{array}{ccc} G/N(S) & \longrightarrow & \{gSg^{-1} \mid g \in G\} \\ \cup & & \cup \\ gN(S) & \longmapsto & gSg^{-1} \end{array}$$

は全単射である.

証明： まずはこの写像が well-defined であることをみる. $g, g' \in G$ を任意にとり, $gN(S) = g'N(S)$ であるとする. このとき, $g = g'n$ となる $n \in N(S)$ がとれ

$$gSg^{-1} = (g'n)S(g'n)^{-1} = g'nSn^{-1}g'^{-1} = g'Sg'^{-1}$$

となる. よって, この写像は well-defined である.

$a, b \in G$ を任意にとり, $aSa^{-1} = bSb^{-1}$ とする. このとき, $S = (a^{-1}b)S(a^{-1}b)^{-1}$ とできるので, $a^{-1}b \in N(S)$ である. よって, $aN(S) = bN(S)$ となる. したがって, この写像は単射である. 全射性は明らかである. □

命題 4.9

G を有限群とする. このとき, 任意の $a \in G$ に対して次が成り立つ.

$$|C(a)| = \frac{|G|}{|N(\{a\})|}$$

証明：

$$\begin{aligned} \frac{|G|}{|N(\{a\})|} &= |G/N(\{a\})| \\ &= |\{g\{a\}g^{-1} \mid g \in G\}| \\ &= |\{\{gag^{-1}\} \mid g \in G\}| \\ &= |\{gag^{-1} \mid g \in G\}| \\ &= |C(a)| \end{aligned}$$

□

定理 4.10

G を有限群, $Z(G) \sqcup \{a_1, \ldots, a_k\}$ を $G/\sim$ の完全代表系とする. このとき, 次が成り立つ.

$$|G| = |Z(G)| + \sum_{i=1}^{k} \frac{|G|}{|N(\{a_i\})|}$$

証明： G の類等式と命題 4.9 より明らかである. □

命題 4.11

D を有限な可除環とする.

$$Z(D) = \{z \in D \mid {}^{\forall}d \in D, zd = dz\}$$

と定めれば, Z は体となる. また, 乗法群 $D^\times$ の中心は $Z(D)^\times$ で得られる.

証明： $0, 1 \in Z(D)$ は明らかである. $a, b \in Z(D)$ を任意にとる. このとき, 任意の $d \in D$ に対して

$$(a+b)d = ad + bd = da + db = d(a+b)$$

$$(-a)d = -(ad) = -(da) = d(-a)$$

$$(ab)d = adb = d(ab)$$

となるので, $a+b, -a, ab \in Z(D)$ である. よって, $Z(D)$ は D の部分環 (したがって可除環) である. 明らかに $Z(D)$ は可換環であるので, $Z(D)$ は体となる.

$D^\times = D \setminus \{0\}, Z(D)^\times = Z(D) \setminus \{0\}$ であり, $Z(D)^\times \subset D^\times$ となる. 任意の $z \in Z(D), d \in D$ に対して

$$dzd^{-1} = zdd^{-1} = z$$

となるので $Z(D)^\times$ は $D^\times$ の中心である. □

この $Z(D)$ を D の中心という.

命題 4.12

D を有限な可除環とする. 任意の $a \in D$ に対して

$$N_a = \{d \in D \mid ad = da\}$$

とおけば, N_a は $Z(D)$ を含む可除環である. また, 各 $a \in D^\times$ に対する $\{a\}$ の正規化群は $N_a^\times$ で得られる.

証明： $Z(D) \subset N_a$ は定義から明らかである. 任意の $c, d \in N_a$ に対して

$$a(c+d) = ac + ad = ca + da = (c+d)a$$

$$a(-c) = -(ac) = -(ca) = (-c)a$$

$$a(cd) = cad = (cd)a$$

となるので, $c+d, -c, cd \in N_a$ となる. よって, N_a は D の部分環 (すなわち可除環) である.

$N_a^\times = N_a \setminus \{0\} \subset D^\times$ であり, 任意の $n \in N_a^\times$ に対して

$$n\{a\}n^{-1} = \{nan^{-1}\} = \{ann^{-1}\} = \{a\}$$

となる. したがって, $N_a^\times$ は $D^\times$ における $\{a\}$ の正規化群である. □

命題 4.13

D を有限な可除環, $a \in D$ とする. このとき, D, N_a は $Z(D)$ 上の有限次元ベクトル空間であり, それぞれの $Z(D)$ 上の次元を n, r_a とおくと r_a は n の約数となる. また, $|Z(D)| = q$ とすれば $|D| = q^n, |N_a| = q^{r_a}$ となる.

証明： $Z(D) \subset N_a \subset D$ は可除環の拡大なので D, N_a は $Z(D)$ 上の加群となる. また, $Z(D)$ は体なので D, N_a は $Z(D)$ 上のベクトル空間である. さらに, D, N_a は有限なので $Z(D)$ 上の次元も有限となる. $|Z(D)| = q$ とおけば $|D| = q^n, |N_a| = q^{r_a}$ となることも明らかである.

$N_a^\times$ は $D^\times$ の部分群なので, $q^{r_a} - 1$ は $q^n - 1$ を割り切る.

$$n = r_a m + t \qquad (0 \leq t < r)$$

とすれば $(m, t \in \mathbb{Z})$

$$q^n - 1 = q^{r_a m} q^t - 1 = q^t(q^{r_a m} - 1) + q^t - 1$$

となる. $q^{r_a} - 1$ は $q^n - 1$ と $q^{r_a m} - 1$ を割り切るので, $q^t - 1$ も割り切る. $q^t - 1 < q^{r_a} - 1$ なので $t = 0$ でないといけない. つまり, r_a は n の約数である. □

定理 4.14 (Wedderburn の定理)

有限な可除環は体である.

証明： D を有限な可除環, $|Z(D)| = q$, $\dim_{Z(D)} D = n$ とする. $n = 1$ なら $D = Z(D)$ となり D は体である. $n \geq 2$ と仮定して矛盾を導く.

$Z(D)^\times \sqcup \{a_1, \ldots, a_k\}$ を $D^\times / \sim$ の完全代表系, $\dim_{Z(D)} N_{a_i} = r_i$ $(i = 1, \ldots, k)$ とする. このとき, $D^\times$ の類等式は

$$q^n - 1 = q - 1 + \sum_{i=1}^{k} \frac{q^n - 1}{q^{r_i} - 1}$$

となる. ここで $\Phi_n(x)$ を $\mathbb{Q}$ 上の n-円分多項式とすれば, $\Phi_n(x)$ は各 $\dfrac{x^n - 1}{x^{r_i} - 1}$ $(i = 1, \ldots, k)$ を割り切るので, $\Phi_n(q)$ は $\displaystyle\sum_{i=1}^{k} \frac{q^n - 1}{q^{r_i} - 1}$ を割り切る. また, $\Phi_n(x)$ は $x^n - 1$ も割り切るので, 類等式から $\Phi_n(q)$ は $q - 1$ を割り切らなければならない.

一方, $\zeta \in \mathbb{C}$ を 1 の原始 n 乗根とすれば

$$\Phi_n(x) = \prod_{\substack{s=1 \\ \gcd(s,n)=1}}^{n} (x - \zeta^s)$$

とでき, $n, q \geq 2$ なので

$$\begin{aligned} |\Phi_n(q)| &= \prod_{\substack{s=1 \\ \gcd(s,n)=1}}^{n} |q - \zeta^s| \\ &> \prod_{\substack{s=1 \\ \gcd(s,n)=1}}^{n} |q - 1| \\ &\geq q - 1 \end{aligned}$$

となる. したがって, $\Phi_n(q)$ は $q-1$ を割り切ることはない. これは矛盾である. □

参考文献

[1] Rudolf Lidl and Harald Niederreiter, *Finite Fields*, Cambridge University Press, 1996.

[2] 雪江明彦, 代数学 2 環と体とガロア理論, 日本評論社, 2018.