Ding と Yuan による平面関数から得られた semifields の nucleus について

南 香織*, 中川 暢夫**

On the Nucleus of the Semifields Obtained from Ding and Yuan Planar Functions

Kaori MINAMI* and Nobuo NAKAGAWA**

Finite affine planes coming from Ding and Yuan planar functions $g(x) = x^{10} - \alpha x^6 - \alpha^2 x^2$ ($\alpha \in \mathbf{F}_{3^n}^{\times}$) become semifields. The geometric properties are obtained from the structure of automorphism groups of the semifields. It is proved in this paper that each nucleus of the semifields is the prime field in the case $\alpha = 1$.

Key words: Planar function, Finite field, Finite semifield, Nucleus, Affine plane

1 序

有限射影平面や有限アフィン平面については, 以前から多くの有限幾何及び組合せ論研究者によって研究されている. これらの有限平面と代数構造には深い関係があり, 以下のような対応をもつ.

有限体 $\longleftrightarrow$ Desargue 平面,
semifield $\longleftrightarrow$ semifield 平面,
leftquasifield $\longleftrightarrow$ translation 平面,
rightquasifield $\longleftrightarrow$ 双対 translation 平面,
Cartesian 群 $\longleftrightarrow$ 点 P と直線 ℓ に対して
(P,ℓ)-transitive 平面 (P は ℓ 上にある).

ある種のアフィン平面は平面関数と呼ばれる有限群間の写像から代数構造を経由して構成される. こうして構成されたアフィン平面の自己同型群の構造を決定することは, その平面を知る上で非常に重要である. またこのことは, 未解決問題として残されている点集合上正則に作用する自己同型群をもつ平面の分類にもつながる.

本論文では, Ding と Yuan による平面関数から構成される semifield 平面の全自己同型群を決定する第一歩として, この平面と対応する代数構造 semifield の部分構造 (nucleus) を考える. この乗法群はホモロジー群と同型であることが知られている. ホモロジー群は, 平面の幾何学的性質と密接に関わっている.

2 準備

まず, 平面関数を定義する.

定義 1. G, H 有限群, $|G| = |H| = n$ とし, f を G から H への写像とする. G の元 u に対して, f_u を

$$\begin{aligned} f_u : G &\longrightarrow H \\ x &\longmapsto f_u(x) := f(ux)f(x)^{-1} \end{aligned}$$

によって定義する. 任意の $u (u \neq 1)$ に対して f_u が全単射であるとき, f を平面関数と定義する.

平面関数の例として次のようなものがある.

例 1.

$$\begin{aligned} f : (\mathbf{F}_q, +) &\longrightarrow (\mathbf{F}_q, +) \ (q : \text{奇素数べき}) \\ x &\longmapsto x^2. \end{aligned}$$

例 2. (Coulter-Matthews, [1])

$$\begin{aligned} f : (\mathbf{F}_{3^e}, +) &\longrightarrow (\mathbf{F}_{3^e}, +) \\ x &\longmapsto x^{\frac{3^a+1}{2}} \ (\gcd(a, 2e) = 1). \end{aligned}$$

f が G から H への平面関数ならば, この f から群 $G \times H$ が点集合に正則に作用するようなアフィン平面 $I(G, H; f)$ がつくられる. ここで, アフィン平面 $I(G, H; f)$ の点集合は $G \times H$, 直線集合は,

$$\begin{aligned} L(a, \alpha) &= \{(xa, f(x)\alpha) | x \in G\} \ \ (a \in G, \alpha \in H) \\ L(c) &= \{(c, y) | y \in H\} \ \ (c \in G) \end{aligned}$$

である.

本論文で扱う Ding と Yuan による平面関数とは, 2005 年の上海における国際会議において与えられたもので, 次のものを言う ([3] 参照).

$\mathbf{F}_{3^n}{}^{\times}$ (n : 奇数) の固定した任意の元 α に対し,

$$\begin{aligned} g : (\mathbf{F}_{3^n}, +) &\longrightarrow (\mathbf{F}_{3^n}, +) \\ x &\longmapsto g(x) := x^{10} - \alpha x^6 - \alpha^2 x^2 \end{aligned}$$

とすると g は平面関数となる.

平成２０年６月２１日受理
＊ 大学院総合理工学研究科理学専攻
＊＊ 理学科

Ding と Yuan による平面関数から, semifield が構成できる. まず, semifield の定義を述べる.

定義 2. 二つの演算 $(+, \circ)$ をもつ集合 E が, 次の条件を満たすとき, E は semifield である.
(1) 加法に関して群をなす.
(2) 積 $(\circ)$ に関して単位元をもつ.
(3) $a \circ (b+c) = a \circ b + a \circ c$,
$(a+b) \circ c = a \circ c + b \circ c \quad (\forall a, b, c \in E)$.
(4) $a \circ b = 0 \Longrightarrow a = 0$ or $b = 0$.

平面関数から代数構造を構成するために, 関数 $g(x)$ を正規化した関数を考える. $g(x)$ の正規化関数とは $g(x)$ に対して $f(x) := g(x-a) + b$ で, $f(0) = 0, f(1) = 0$ を満たす $f(x)$ である. 明らかに, $f(x)$ は平面関数である.

以下, $g(x)$ は Ding と Yuan の平面関数とする.

$(\mathbf{F}_{3^n}, +)$ における $g(x)$ の正規化関数 $f(x)$ に対して写像 μ は,

$$\begin{aligned} \mu : (\mathbf{F}_{3^n}, +) &\longrightarrow (\mathbf{F}_{3^n}, +) \\ x &\longmapsto x^\mu := -f(x) + f(x+1) \\ &\qquad = x^9 + \alpha x^3 + (1+\alpha^2)x \end{aligned}$$

であり, μ は平面関数の定義から全単射な線型写像となる. また, $\varphi := \mu^{-1}$ とする. Dembowski と Ostrom に倣い, このような φ を用いて, 次のような積 $(\circ)$([2] 参照) を定義する. 任意の $u, v \in \mathbf{F}_{3^n}$ に対して,

$$u \circ v = -f(u^\varphi) + f(u^\varphi + v^\varphi) - f(v^\varphi). \tag{1}$$

有限体の加法群とこの積 $(\circ)$ により $E(g) := (\mathbf{F}_{3^n}, +, \circ)$ は可換 semifield となる ([4] 参照).
次に, この可換 semifield の部分構造である nucleus を考える.

定義 3. 有限 semifield E に対して, right nucleus, middle nucleus, left nucleus はそれぞれ次のように定義する.
$N_r(E) := \{a \in E | (x \circ y) \circ a = x \circ (y \circ a), \forall x, \forall y \in E\}$,
$N_m(E) := \{a \in E | (x \circ a) \circ y = x \circ (a \circ y), \forall x, \forall y \in E\}$,
$N_\ell(E) := \{a \in E | (a \circ x) \circ y = a \circ (x \circ y), \forall x, \forall y \in E\}$.

補題 1. 有限 semifield E における nucleus は体である.

証明 有限 semifield であるので, 逆元の存在はすぐに分かる. さらに, nucleus の定義から, 積の関する結合律が成り立つので斜体となる. Wedderburn の定理より, 有限斜体は有限体である. □

定義 4. P 点集合, L 直線集合, $\mathbf{P} = (P, L)$ を有限アフィン平面とする. $p \in P, \ell \in L$ において, σ が (p, ℓ)-ホモロジーであるとは, 次を満たすことを言う.
(1) $\sigma \in \mathrm{Aut}(\mathbf{P})$.
(2) (p) の各直線, (ℓ) の各点を固定する.
ここで, (p) は点 p を通る直線全体, (ℓ) は直線 ℓ 上の点全体を表す.

3 結果

今回, Ding と Yuan による平面関数の中で特別な場合において次のような結果を得た. 以下, $E(g) = E$ とする.

定理 1. Ding と Yuan による平面関数 g に対して, $\alpha = 1$ とすると, $n \geq 5$ (奇数) ならば, $N_r(E), N_m(E), N_\ell(E) = \mathbf{F}_3$ である. $n = 3$ ならば, $N_r(E), N_m(E), N_\ell(E) = E \cong \mathbf{F}_{3^3}$ である.

証明 $n \geq 5$ の場合で $N_r(E) = \mathbf{F}_3$ を示す. $N_r(E)$ は, 補題 1 から体となるので $N_r(E) \supset \mathbf{F}_3$ は明らかである. 従って, $N_r(E) \subset \mathbf{F}_3$ を示す. すなわち, 任意の $u, v \in E$ に対して,

$$(u \circ v) \circ w = u \circ (v \circ w)$$

を満たすとき, $w \in \mathbf{F}_3$ となることを示す. ここで, $x = u^\varphi, y = v^\varphi, z = w^\varphi$ とすると, 積 $u \circ v$ は式 (1) により,

$$u \circ v = -f(x) + f(x+y) - f(y) =: \ell(x, y)$$

と表せる. つまり, 上の結合律は次のように置き換えることができる.

$$\begin{aligned} &(u \circ v) \circ w = u \circ (v \circ w), \\ &\Leftrightarrow \ell(\ell(x, y)^\varphi, z) = \ell(x, \ell(y, z)^\varphi). \end{aligned} \tag{2}$$

ここで, $x^\mu = x^9 + x^3 - x$ とかけ, $\mathbf{F}_3$ 上線型写像なので, $x^\varphi = \sum_{0 \leq k \leq n-1} \beta_k x^{3^k}$ と表すことができる. 従って, $w \in N_r(E)$ であるとき, 以下の式が成立しなければならない.

$$\begin{aligned} &\ell(\ell(x, y)^\varphi, z) \\ &= \{\beta_{n-1}(x^9y + xy^9 + x^3y^3 + xy)^{3^{n-1}} + \beta_{n-2}(x^9y + xy^9 + \\ &x^3y^3 + xy)^{3^{n-2}} + \cdots \\ &+\beta_1(x^9y + xy^9 + x^3y^3 + xy)^3 + \beta_0(x^9y + xy^9 + x^3y^3 + \\ &xy)\}^9 z \\ \\ &+\{\beta_{n-1}(x^9y + xy^9 + x^3y^3 + xy)^{3^{n-1}} + \beta_{n-2}(x^9y + xy^9 + \\ &x^3y^3 + xy)^{3^{n-2}} + \cdots \\ &+\beta_1(x^9y + xy^9 + x^3y^3 + xy)^3 + \beta_0(x^9y + xy^9 + x^3y^3 + \\ &xy)\}z^9 \\ \\ &+\{\beta_{n-1}(x^9y + xy^9 + x^3y^3 + xy)^{3^{n-1}} + \beta_{n-2}(x^9y + xy^9 + \\ &x^3y^3 + xy)^{3^{n-2}} + \cdots \\ &+\beta_1(x^9y + xy^9 + x^3y^3 + xy)^3 + \beta_0(x^9y + xy^9 + x^3y^3 + \\ &xy)\}^3 z^3 \\ \\ &+\{\beta_{n-1}(x^9y + xy^9 + x^3y^3 + xy)^{3^{n-1}} + \beta_{n-2}(x^9y + xy^9 + \\ &x^3y^3 + xy)^{3^{n-2}} + \cdots \\ &+\beta_1(x^9y + xy^9 + x^3y^3 + xy)^3 + \beta_0(x^9y + xy^9 + x^3y^3 + xy)\}z \\ \\ &\ell(x, \ell(y, z)^\varphi) \\ &= x^9\{\beta_{n-1}(y^9z + yz^9 + y^3z^3 + yz)^{3^{n-1}} + \beta_{n-2}(y^9z + \\ &yz^9 + y^3z^3 + yz)^{3^{n-2}} + \cdots \\ &+\beta_1(y^9z + yz^9 + y^3z^3 + yz)^3 + \beta_0(y^9z + yz^9 + y^3z^3 + yz)\} \\ \\ &+x\{\beta_{n-1}(y^9z + yz^9 + y^3z^3 + yz)^{3^{n-1}} + \beta_{n-2}(y^9z + yz^9 + \\ &y^3z^3 + yz)^{3^{n-2}} + \cdots \\ &+\beta_1(y^9z + yz^9 + y^3z^3 + yz)^3 + \beta_0(y^9z + yz^9 + y^3z^3 + yz)\}^9 \\ \\ &+x^3\{\beta_{n-1}(y^9z + yz^9 + y^3z^3 + yz)^{3^{n-1}} + \beta_{n-2}(y^9z + yz^9 + \\ &y^3z^3 + yz)^{3^{n-2}} + \cdots \\ &+\beta_1(y^9z + yz^9 + y^3z^3 + yz)^3 + \beta_0(y^9z + yz^9 + y^3z^3 + yz)\}^3 \\ \\ &+x\{\beta_{n-1}(y^9z + yz^9 + y^3z^3 + yz)^{3^{n-1}} + \beta_{n-2}(y^9z + yz^9 + \end{aligned}$$

$y^3z^3+yz)^{3^{n-2}}+\cdots$
$+\beta_1(y^9z+yz^9+y^3z^3+yz)^3+\beta_0(y^9z+yz^9+y^3z^3+yz)\}$

上の両辺の，ある項を比較することにより $w\in\mathbf{F}_3$ を導く．

そのためにまず，β_i の値を決定する．$(x^\mu)^\varphi=x$ から次のような行列を得る．

$$\begin{pmatrix} -1 & & & & & 1 & 1 \\ 1 & -1 & & & & & 1 \\ 1 & 1 & -1 & & & & \\ & 1 & 1 & & & & \\ & & \ddots & \ddots & \ddots & & \\ & & & & 1 & -1 & \\ & & & & 1 & 1 & -1 \end{pmatrix} \begin{pmatrix} \beta_0 \\ \beta_1 \\ \beta_2 \\ \vdots \\ \beta_{m-2} \\ \beta_{m-1} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}.$$

これを，連立方程式で表すと次のようになる．

$$\begin{cases} -\beta_0+\beta_{m-2}+\beta_{m-1}=1 \\ \beta_0-\beta_1+\beta_{m-1}=0 \\ \beta_0+\beta_1-\beta_2=0 \\ \beta_1+\beta_2-\beta_3=0 \\ \cdots \\ \beta_{m-3}+\beta_{m-2}-\beta_{m-1}=0 \end{cases}$$

以上の式から β_i は次のように定まる．

	β_0	β_1	β_2	β_3	β_4	β_5	β_6	β_7
$n\equiv 1(8)$	1	-1	0	-1	-1	1	0	1
$n\equiv 3(8)$	0	-1	-1	1	0	1	1	-1
$n\equiv 5(8)$	-1	0	-1	-1	1	0	1	1
$n\equiv 7(8)$	1	0	1	1	-1	0	-1	-1

従って，(2) の両辺において，ある項を比較すればよい．
x^3y の項を両辺比較すると，
(左辺) $=0$,
(右辺) $=\beta_{n-1}{}^3z^9+\beta_{n-1}{}^3z+\beta_{n-2}{}^3z+\beta_{n-3}{}^3z^{3^{n-2}}$.
$n\equiv 1,3$ とすると，$z=0,z^8=1$ となる．
次に x^3y^9 の項を両辺比較すると，
(左辺) $=0$,
(右辺) $=\beta_{n-1}z+\beta_1z^{81}+\beta_0z^9+\beta_1z^9$.
$n\equiv 5,7$ とすると，$z=0,z^8=1$ となる．

$z^8=1$ より $z\in\mathbf{F}_{3^2}$ となる．ところが，n は奇数であるので，$z=\pm1$ でなければならない．$z=w^\varphi$ であるので，$w=z^\mu$．これを計算すると，$w=0,\pm1$.

以上より，$N_r(E)\subset\mathbf{F}_3$ である．同様に $N_m(E),N_\ell(E)=\mathbf{F}_3$ を得る．

$n=3$ の場合，$\alpha=1$ は平方数なので，[4] により $N_r(E),N_m(E),N_\ell(E)=E\cong\mathbf{F}_{3^3}$ が成り立つ．□

定理 2. Ding と Yuan による平面関数 g に対して，$n=p$, ($p\geq 5$: 素数) としたとき $N_r(E),N_m(E),N_\ell(E)$ は $\mathbf{F}_3$ と同型である．

証明. semifield E で $\mathbf{F}_3$ と同型な E_0 が存在することはすぐにわかる．今，$\mathbf{F}_{3^n}=\mathbf{F}_{3^p}$ でかつ $E=(\mathbf{F}_{3^n},+,\circ)$ であるから，E は E_0 上 p 次拡大であり，$E_0\subset N_r(E)\subset E$ である．一方 p は素数なので，$N_r(E)=E_0$ または $N_r(E)=E$ であるが $p\geq 5$ より，$N_r(E)\neq E$ である ([4] 参照)．ゆえに，$N_r(E)=E_0\cong\mathbf{F}_3$．同様に $N_m(E),N_\ell(E)=E_0\cong\mathbf{F}_3$ を得る．□

参考文献

1) R. S. Coulter and R. W. Matthews, "Planar Functions and Planes of Lenz-Barlotti Class II", *Designs, Codes and Cryptography*, 10(1997) pp.167-184.

2) P. Dembowski and T. G. Ostrom, "Planes of Order n with Collineation Groups of Order n^2", *Math. Z.* ,Vol. 103(1968) pp. 239-258.

3) C. Ding and J. Yuan, "A family of skew Hadamard difference sets", *Journal of Combinatorial Theory*, Series A, Vol. 113(2006), no. 7, pp. 1526-1535.

4) K. Minami and N. Nakagawa, "On planar functions of elementary abelian p-group type", to appear in Vol. 37(2008) pp. 531-544 of *Hokkaido Mathematical Journal*.