

学 位 論 文 題 名

On the planar functions of degree p^n (次数 p^n の平面関数について)

学位論文内容の要旨

射影幾何の次元が3以上ならば、その結合構造は或る斜体上のベクトル空間とその全ての部分空間が作る結合構造に同型であることが、1916年にベブレンとヤングにより示された。次元が3以上ならば、デサルグの定理(単体対応が付いた二つの三角形において、それぞれ対応する頂点を結ぶ直線が共点ならば、それぞれの対応する二つの辺は交わり、それらの三つの交点は共線である)が成り立ち、そのことが斜体を構成しうる根拠となっている。

さてこれから考える結合構造は全て有限とする。2次元射影幾何は射影平面と呼ばれる。デサルグの定理が成立しない射影平面はこれまでに数多く構成されている。射影平面 P は或る自然数 n ($n \geq 2$) に対し、対称 $(n^2+n+1, n+1, 1)$ - デザインとなる。このとき P の位数は n であると言う。射影平面 P と P の一つの直線 ℓ に対し、 P の結合構造から直線 ℓ と ℓ 上の全ての点を取り去ることにより得られる結合構造を $P \setminus \ell$ と書いて、(P から得られる ℓ に関する) アフィン平面と呼ぶ。点集合上の作用において可移度の高い、十分大きな自己同型群をもつ射影平面やアフィン平面は、ある意味でデサルグ平面に近い構造を持つと予想される。実際点集合上二重可移に働く自己同型群を有する射影平面はデサルグ平面となり、点集合上原始的に働く自己同型群を有するアフィン平面は移行平面 (translation planes) となることが知られている。(移行平面の構造については、後述する。)

以下アフィン平面と射影平面との関係、移行平面、正則アフィン平面と平面関数との関係を述べた後、次数 p^n の平面関数に関して私が得た三つの定理を与え、それらの証明の概略を示して行くことにする。

アフィン平面とは次の三つの公理を満たす、点集合と直線集合からなる結合構造である。

- (1) 任意の異なる二点は唯一つの直線上にある。
- (2) 与えられた任意の直線 ℓ と ℓ 上にない任意の点 P に対し、 P を通り ℓ と共有点を持たない直線 m が唯一つ存在する。
- (3) 共線でない三点が存在する。

二つの直線 ℓ 、 m に対し、 $\ell = m$ 又は ℓ と m が共有点を持たないとき ℓ と m は平行であるという。このとき“平行性”は同値関係となる。 A より射影平面 $P(A)$ が構成される。即ち $P(A)$ の点集合として A の点集合に A の全ての平行類を加えて考え、 $P(A)$ の直線集合として A の直線集合に新しい直線 $\ell(\infty)$ を加えて考える。 $P(A)$ の結合関係は次のように定義される。

- (a) A の点 P が A の直線 ℓ 上にある時に限り、 $P(A)$ において点 P が直線 ℓ 上にある。
- (b) A の直線 ℓ が平行類 P^* に属する時に限り、 $P(A)$ の点 P^* は直線 ℓ 上にある。
- (c) A の直線の各平行類 P^* に対し、 $P(A)$ の点 P^* は直線 $\ell(\infty)$ 上にある。 A のどの点も直線 $\ell(\infty)$ 上にない。

$P(A)$ は A の射影閉包と呼ばれ、時々 A と $P(A)$ は同一視される。 $P(A)$ の位数を A の位数ともいう。

点集合の上に正則に作用するような自己同型群を有するアフィン平面を正則平面と呼ぶ。正則平面の中で特に見易い構造をもつものとして、次に定義する移行平面がある。アフィン平面Aの自己同型 τ が各平行類を固定して、ある平行類 P^* に対し P^* に属する各直線を固定するとき、 τ を(P^* を中心とする)Aの平行移動(translation)と呼び、 P^* を中心とするAの平行移動全体がなす群を $T_A(P^*)$ で表す。またAの平行移動全体がなす群 $T(A)$ をAの移行群(translation group)とよぶ。 $T(A)$ がAの点集合の上に正則に作用するとき、Aを移行平面とよぶ。このときAの移行群 $T(A)$ は、或る素数 p に対し基本可換 p -群となり、任意の異なる二つの平行類 P^*, Q^* に対し、 $T(A) = T_A(P^*) \oplus T_A(Q^*)$ となる。

$T(A)$ の自己準同型写像で各 $T_A(P^*)$ を不変にするもの全ての集合を F と置く。自然に定義される演算で F は標数 p の有限体をなし、 $T(A)$ や各 $T_A(P^*)$ は F 上のベクトル空間となる。Aの点集合と $T(A)$ をうまく同一視するとき、Aの直線は $T(A)$ の、各部分群 $T_A(P^*)$ による剰余類となる。このように移行平面は、 $2d$ 次元ベクトル空間とその d 次元部分空間の言葉で、記述することができる。($d=1$ のとき、Aはデザルグ平面となる。) 特に移行平面の位数は素数中となる。

G と H を位数 m の群とし、 f を G から H への写像 f とする。 $u \in G$ に対し、 G から H への写像 f_u を次のように定義する。

$$f_u: x \longrightarrow f(ux)f(x)^{-1}$$

単位元でない任意の G の元 u に対し f_u が単射になるとき、 f は次数 m の平面関数とよばれる。 G から H への平面関数 f から、次のようにして位数 m のアフィン平面 $S(G, H, f)$ が生じる。

点集合 : G と H の直積 $G \times H$ の元全体

直線集合 : $L(a, a) = \{(x, f(xa^{-1})a) \mid x \in G\}$, $a \in G$, $a \in H$,

$L(c) = \{(c, a) \mid a \in H\}$, $c \in G$

結合関係 : 通常の包含関係

このとき、群 $G \times H$ は自然な作用で、 $S(G, H, f)$ の自己同型群になり、 $S(G, H, f)$ の点集合上に正則に作用する。更に次の二条件が満たされる。

H の各元は、平行類 $P^* = \{L(c) \mid c \in G\}$ を中心とする平行移動である。

G は $\mathcal{L}(\infty) \setminus \{P^*\}$ 上に可移にはたらく。

逆に位数 m の群 G, H において、群 $G \times H$ がAの自己同型群として、Aの点集合上に正則に作用して、上の二条件を満たすならば、 G から H への平面関数 f が存在し、アフィン平面 $S(G, H, f)$ はAと同型となる。即ち上で述べたような正則平面の研究は、平面関数の研究に帰着される。

平面関数に関して次の諸定理が得られた。

主定理: p を奇素数とし、 n を2以上の整数とする。また e を n が奇数ならば $e \geq (n+3)/2$ 、 n が偶数ならば $e \geq (n+2)/2$ となる整数とする。更に G と H を位数 p^n の群とし、 H が位数 p^n の巡回部分群を直積因子として含むものとする。このとき G から H への平面関数は存在しない。

定理A: p を奇素数とし、 n を2以上の整数とする。更に G を位数 p^n の巡回群とし、 H を G と同位数の群とする。このとき G から H への平面関数は存在しない。

定理B: p を奇素数とし、 G をガロア体 $GF(p^2)$ の加法群、 α を $GF(p)$ の乗法群の生成元、 θ を $\theta^2 = \alpha$ なる $GF(p^2)$ の元とする。 $GF(p^2)$ から $GF(p^2)$ への写像 f を、 $f(x) = (a+b\theta)x^2 + (c+d\theta)x^{p+1} + (u+v\theta)x^{2p}$ とおく。このとき f が G から G への平面関数になるための必要十分条件は下記の値が $GF(p)^*$ の平方数になることである。

$$\alpha(c\xi_1 - d\eta_1)^2 + (\alpha\xi_2(\xi_1 - d) - \eta_2(\eta_1 - c))(\alpha\xi_2(\xi_1 + d) - \eta_2(\eta_1 + c))$$

$$(\text{且 } \eta_1 = a+u, \eta_2 = a-u, \xi_1 = b+v, \xi_2 = b-v \text{ とする。})$$

このとき、 f から得られるアフィン平面 $S(G, H, f)$ は、移行平面となる。

主定理の証明の概略：主定理の条件を満たす平面関数 f が在ったとして矛盾を導く。 G の任意の一次指標 χ 、 H の単位指標でない任意の一次指標 ρ に対し、 $z(\chi, \rho) = \sum_{x \in G} \chi(x) \rho(f(x))$ と置くと、次の関係式が成り立つ。

$$z(\chi, \rho) \overline{z(\chi, \rho)} = p^n \quad (1)$$

n を奇数とせよ。 λ を $GF(p)^*$ の位数 2 の指標、 $\lambda(0)=0$ とし、 ω を 1 の原始 p 乗根とする。

$\tau = \sum_{x \in GF(p)} \lambda(x) \omega^x$ とおくと、 $\tau \overline{\tau} = p$ が成り立つ。

H_0 を H の位数 p^n の巡回部分群とし、 $H = H_0 \times K$ とする。 $\chi = 1_0$ 、 $\rho = \phi_i \times 1_K$ (ϕ_i は H_0 の位数 p^i の指標 ($1 \leq i \leq n$)) とするとき、(1) 式とクンマーの定理より、 $z(\chi, \rho) = \varepsilon p^{(n-1)/2} \tau$ ($\varepsilon \in \mathbb{Z}[\zeta_i]$ の単数、 ζ_i は 1 の原始 p^i 乗根) が成り立つ。 $z(\chi, \rho)$ と $p^{(n-1)/2} \tau$ をそれぞれ $\{\zeta_i^{j'} \mid 0 \leq j' \leq p^i - 1\}$ の一次結合で表し、 Q 上一次独立な項にまとめて両辺の係数を比較することにより、数 p^n が p^i 個の数 $M_j(i)$ ($0 \leq j \leq p^i - 1$) の和と書けて、これらの p 個ずつが各 $M_j(i-1)$ ($0 \leq j \leq p^{i-1} - 1$) の細分と成っている。また一つの $M_j(i-1)$ を除いて、他の $M_j(i-1)$ は均等に p 個の $M_j(i)$ の和に細分される。特に $i=1$ のとき、 $M_j(1) = p^{n-1} + \varepsilon' p^{(n-1)/2} \lambda(j)$ ($\varepsilon' = \pm 1$) が成り立つ。 p^n のこの一番目の配分の偏りが最後まで尾をひいて、 $M_j(e-1) \not\equiv 0 \pmod{p}$ ($\exists j$) となるが、一方では前述のごとく、 $M_j(e-1) = p M_j(e)$ となり矛盾が導かれる。 n が偶数の場合も概ね同じような証明をたどればよい。

定理 A の証明の概略： G から H への平面関数 f が在ったとして矛盾を導く。

Case ①： $n \geq 3$ の場合、(1) 式の χ として G の位数 p^n の指標、 ρ として H の位数 p の一次指標をとり、(1) 式を使い主定理の証明と同じ手順で $z(\chi, \rho)$ を評価することにより、矛盾を導くことができる。

Case ②： $n=2$ の場合、 H が巡回群のときは主定理により済んでいる。故に H は (p, p) 型の群としてよい。 G の元 x に対し、 $f(x) = (\alpha(x), \beta(x))$ と置き、 H の元 (r, q) に対応する H の指標を (r, q) で表す。即ち $(r, q)(x, y) = \omega^{rx+qy}$ と定義する。(Case ①) で行なったような計算をつきつめると、次に示す結果を得る。

$$(r, q) = \rho \text{ に対し、} GF(p) \text{ 上の置換 } s(\rho)' \text{ と } i \text{ にのみ依存する定数 } c(\rho)(i) \text{ が存在して、} \\ r\alpha(pt+s(\rho)'(i)) + q\beta(pt+s(\rho)'(i)) = -i^{-1}t + c(\rho)(i) \quad (\text{if } i \neq 0), \quad c(\rho)(0) \quad (\text{if } i=0) \quad (2)$$

$s((1, 0))' = s'$, $s((0, 1))' = u'$, $c((1, 0)) = c$, $c((0, 1)) = d$ と置く。まず $s'(0) \neq u'(0)$ とせよ。この時、 $s'(0) = u'(k)$ ($\exists k \neq 0$) 且つ $s'(i) = u'(j)$ ($\exists i \neq 0, \exists j \neq 0$)。前の値を m 、後の値 g とすると $m \neq g$ である。 $r = i(k^{-1} - j^{-1})$, $q = 1$ とすると $r\alpha(pt+m) + \beta(pt+m) = r\alpha(pt+s'(0)) + \beta(pt+u'(k)) = -k^{-1}t + rc(0) + d(k)$ と成り式(2)より $m = s(\rho)'(k)$ 。(但し $\rho = (r, 1)$) 他方同じ r, q に対し、 $r\alpha(pt+g) + \beta(pt+g) = r\alpha(pt+s'(i)) + \beta(pt+u'(j)) = -k^{-1}t + rc(i) + d(j)$ と成り式(2)より $g = s(\rho)'(j)$ 。故に $m = g$ がでて矛盾が生じる。 $s'(0) = u'(0)$ のときもほぼ同様の議論を繰り返し、矛盾が導かれる。

定理 B の証明の概略： G と H が可換群の場合、 G から H への写像 f が平面関数となるための必要十分条件は G の任意の指標 χ と H の任意の指標 ρ ($\rho \neq 1_H$) に対し、式(1)が成り立つことである。今 G の位数が p^2 より $z(\chi, \rho) = \pm p \omega^t$ ($t \in \mathbb{Z}$ と ρ により決定) が成り立つこととなる。さて $f(x, y) = (\alpha(x, y), \beta(x, y))$ と置くと、 $\chi = (u, v)$, $\rho = (r, s)$ のとき、 $z(\chi, \rho) = \sum_{(x, y) \in G} \omega^{ux+vy+r\alpha(x, y)+s\beta(x, y)}$ だから、

$|z(\chi, \rho)| = \pm p \omega^t \Leftrightarrow |\{(x, y) \mid ux+vy+r\alpha(x, y)+s\beta(x, y) = i\}| = \varepsilon p - 1$ ($\varepsilon = 2$ if $i=t$, $\varepsilon = 1$ if $i \neq t$) 且つ $\varepsilon' p + 1$ ($\varepsilon' = 0$ if $i=t$, $\varepsilon' = 1$ if $i \neq t$)。 $\alpha(x, y), \beta(x, y)$ が二次形式のときは、上の条件の右方が成立するためには $r\alpha(x, y) + s\beta(x, y)$ が正則になることが必要十分であると、計算により分かる。定理 B の f において、 $\alpha(x, y), \beta(x, y)$ は二次形式であるから、 $r\alpha(x, y) + s\beta(x, y)$ が $(r, s) \neq (0, 0)$ なる任意の r, s に対して正則になる条件を計算すればよい。

学位論文審査の要旨

主 査 教 授 都 筑 俊 郎

副 査 教 授 諏 訪 立 雄

副 査 教 授 吉 田 知 行 (熊本大・理)

副 査 助教授 日 比 孝 之

学 位 論 文 題 名

On the planar functions of degree p^n

(次数 p^n の平面関数について)

中川暢夫氏提出の学位論文は、有限射影平面に関するものである。特に、可移な自己同型群の構造がかなり強い制限を受ける事を示した事は大きな成果である。自己同型群を持つ有限幾何は、古くからある研究対象であるが、近年では他の組み合わせ論の分野や情報理論への応用が目立つ。中川氏の得た結果とその証明の方法は、この方面の研究にとって大きな意義がある。

射影平面とは、点と直線、それらの間の結合関係からなる幾何で、次の公理を満たすものである: (1) 相異なる2点を含む直線がただ1本存在する。(2) 相異なる3点 p_0, p_1, p_2 と $q_1 \in \overline{p_0, p_1}$, $q_2 \in \overline{p_0, p_2}$, $q_1 \neq q_2$ に対し、 $\overline{p_1, p_2}$ と $\overline{q_1, q_2}$ は交わる。(3) 各直線は3個以上の点を含む。

いろいろな幾何学と同様に、射影幾何学にも部分空間、次元、自己同型群といった概念が定義される。問題は有限次元の射影幾何学の分類である。

射影平面の古典的な例は、斜体上の n -次元ベクトル空間において、1次元部分空間を点とし、2次元部分空間を直線としてできる $(n-1)$ -次元射影空間である。この射影幾何ではいわゆる Desargue の定理が成り立っている。逆に Desargue の定理が成り立つ有限次元の射影幾何には座標が入り、そのような幾何は古典的なものとなる。さらに3次元以上の射影幾何学では Desargue の定理が成り立ち、したがって3次元以上の有限次元射影幾何学は古典的なものとなる (O.Veblen-J.W.Young 今世紀はじめ頃)。

これに対し、2次元の射影幾何学、つまり射影平面では一般に Desargue の定理は成り立たない。実際そのような非 Desargue 平面はたくさん見つかっており、中川氏自身も新しい有限射影平面を見つけている。

射影平面は、点と直線からなり、次の公理を満たすものとしても定義できる: (1) 相異なる2点を含む直線がただ1本存在する。(2) 相異なる2直線は1点で交わる。(3) 退化しない4角形が存在する。

以下幾何はすべて有限幾何とする。ひとつの射影平面では、各直線は $n+1$ 個の点を含み、点は全部で n^2+n+1 個存在する。この n を射影平面の位数という。古典的な例では、位数は斜体に入る元の個数である。有限射影平面に関する基本的予想として、位数は素数のべきであろう、というものがある。また射影平面が 2 重可移な自己同型群を持てば、それは Desargue 平面である (Wagner)。そこで大きな自己同型群を持つ射影平面の分類が有限幾何学の大きな問題になっている。

ある射影平面から 1 つの直線を除いてできる平面を affine 平面という。これは次の公理でも定義される: (1) 相異なる 2 点を通る直線はただ 1 本存在する; (2) 任意の点 p と直線 l に対し、 p を通り l に平行な直線がただひとつ存在する; (3) 退化しない 3 角形が存在する。有限射影平面を考えても affine 平面を考えても同じ事である。affine 平面のひとつの直線に入る点の個数 (直線によらず一定) を位数と呼ぶ。

ある affine 平面 A の平行移動全体のなす群を移行群と呼び $T(A)$ で表す。 $T(A)$ が A の点集合上に正則に作用するとき、 A を移行平面 (translation plain) という。移行平面では、位数はある素数 p のべきであって、 $T(A)$ は基本可換 p -群である。移行平面は Desargue 平面に似ているため、非 Desargue 有限平面の内では最も良く研究されている。

中川氏は有限 affine 平面の自己同型群が有限群の直積を含むかどうかを研究した。位数 m のふたつの群 G と H をとる。写像 $f: G \rightarrow H$ が次数 m の平面関数であるとは、任意の $u \in G$ に対して決まる写像

$$f_u: G \rightarrow H; x \mapsto f(ux)f(x)^{-1}$$

がすべて単射である事をいう。平面関数 f から次数 m の affine 平面 $S(G, H, f)$ が構成される。この平面には $G \times H$ が平行移動の群として正則に作用しており、結局そのような平面は移行平面となる。

さて次が本論文における主定理である。

主定理: p を奇素数、 $n \geq 2$, $e \geq [(n+3)/2]$ とする。 G と H を位数 p^n の群とする。 G から H への平面関数が存在すれば、 H は位数 p^e の巡回群を直積因子として持たない。

基本予想により、 G と H は p -群になることが予想されるので、この定理は平面関数の存在についての強い必要条件を与える。定理の証明も興味深いもので、群指標の理論と整数論におけるガウス和やクンマーの定理などが用いられている。

中川氏はさらにふたつの定理 (定理 A, B) を示している。特に定理 B では、 G がガロア体 $GF(p^2)$ ($p \neq 2$) の加法群のとき、ある種の多項式写像 $f: G \rightarrow G$ が平面関数になるための整数論的必要十分条件を与えている。これからできる affine 平面は新しい移行平面のクラスを与えている。

中川氏の結果は、大きな拡張の可能性を持っており、今後の研究の進展が待たれる。

以上見たように、本論文は学位論文として十分な内容を備えていると判断される。