数理解析研究所講究録
第1214巻 2001年 46-61

有限射影平面概観

熊本大学教育学部数学教室　平峰 豊 (HIRAMINE, Yutaka)
Department of Mathematics, Faculty of Education, Kumamoto University

序

有限射影平面は古くからいろいろな数学の分野に関連して研究されてきたが 1973 年に出版された Huges-Piper の教科書 "Projective Planes" [26] の前書きによればその現代的研究が開始されたのは 1950 年頃である．私個人がこの方面のことを知り始めた 1980 年頃は新しい射影平面が [38] にあるような手法で大量に見つかっていた時期である．この稿ではその後 20 年間のこの分野の研究の変遷と未解決となっている問題について私の知るところを記したい．定義等は可能なかぎり述べるが詳細については [7][15][26][27] を参照されたい．

有限射影平面の定義 点集合 $\mathbb{P}$ と $\mathbb{P}$ の部分集合の族 $\mathbb{L}$ が次の条件をみたすとき $\pi=(\mathbb{P},\mathbb{L})$ を射影平面 (*projective plane*) という．($\mathbb{L}$ の元を π の直線と呼ぶ)

(i) 異なる 2 点を含む直線はただ一つである．
(ii) 異なる 2 直線の交わりはただ一点である．
(iii) 4 角形 (=どの 3 点も同一直線上にない 4 点) が存在する．

$\mathbb{P}$ が有限集合のときは $\pi=(\mathbb{P},\mathbb{L})$ が $(n^2+n+1,n+1,1)$-対称デザイン ([36]) となることが容易にわかる．すなわち，$|\mathbb{P}|=|\mathbb{L}|=n^2+n+1$ であり各点を通りちょうど $n+1$ 直線が存在し各直線はちょうど $n+1$ 点み，異なる 2 点を通る直線はただ 1 つである． n を射影平面 π の位数 (*order*) という．

例 1　有限体 $GF(q)$ 上の 3 次元ベクトル空間 $V(3,q)$ の 1 次元部分空間の全体を $\mathbb{P}$ とし，2 次元部分空間の全体を $\mathbb{L}$ とおく．ここでは 2 次元部分空間 はそれが含む 1 次元部分空間全体の集合と同一視する．このとき $|\mathbb{P}|=|\mathbb{L}|=q^2+q+1$ で，$(\mathbb{P},\mathbb{L})$ は位数 q の射影平面となる．$(\mathbb{P},\mathbb{L})$ はデザルグ平面とよばれて，記号 $PG(2,q)$ で表す．

アフィン平面の定義 点集合 $\mathbb{P}_0$ と $\mathbb{P}_0$ の部分集合のある族 $\mathbb{L}_0$ が次の条件をみたすとき $\pi_0=(\mathbb{P}_0,\mathbb{L}_0)$ をアフィン平面 (*affine plane*) という．($\mathbb{L}_0$ の元を π_0 の直線と呼ぶ)

(i) 異なる 2 点を含む直線はただ一つである．
(ii) 直線 ℓ と点 $P\not\in\ell$ に対して P を通り ℓ と交わらない直線がただ一つ存在する．
(iii) 3 角形 (=同一直線上にない 3 点) が存在する．

$\mathbb{P}$ が有限集合のときは $\pi_0=(\mathbb{P}_0,\mathbb{L}_0)$ が 2-$(n^2,n,1)$-デザインとなることが容易にわかる．すなわち，$|\mathbb{P}_0|=n^2$, $|\mathbb{L}_0|=n^2+n$ であり各点をちょうど $n+1$ 直線が通り，各直線はちょうど n 点を含み，異なる 2 点を通る直線はただ 1 つである． n をアフィン平面 π_0 の位数 (*order*) という．

アフィン平面の直線 g,ℓ が $g=\ell$ または $g\cap\ell=\phi$ のとき g と ℓ が平行であるといい記号 $g/\!/\ell$ で表す．"$/\!/$" は同値関係であることが容易に分かる．この同値関係によりアフィン平面の直線集合 $\mathbb{L}$ は $n+1$ 個の平行類 $\mathbf{C}_1,\cdots,\mathbf{C}_{n+1}$ 分割される：$\mathbb{L}_0=\mathbf{C}_1\cup\cdots\cup\mathbf{C}_{n+1}$, $|\mathbf{C}_1|=\cdots=|\mathbf{C}_{n+1}|=n$.

例 2　$\mathbb{P}_0 = \{(x,y) \mid x,y \in K = GF(q)\}$, $\mathbb{L}_0 = \{y = ax+b \mid a,b \in K\} \cup \{x = c \mid c \in K\}$ とおくと $(\mathbb{P}_0, \mathbb{L}_0)$ は位数 q のアフィン平面となる．この場合各々の平行類は傾きが同じ直線の全体からなる．

位数 n の射影平面 $\pi = (\mathbb{P}, \mathbb{L})$ において，その直線 $\ell \in \mathbb{P}$ とその上にある $n+1$ 点をすべて取り除いたと考えると点が $n+1$ 点，直線が一つ減り n^2 点と n^2+n 直線からなる組合せ構造ができる．これが位数 n のアフィン平面となることが容易にわかる．また逆に位数 n のアフィン平面が与えられると上に述べたように直線集合は $n+1$ 個の平行類に分割されるが，これに対応して新たな $n+1$ 点を考えて同一平行類には同一点を追加するという方法で各直線に 1 点ずつ追加し，さらにこの $n+1$ 点からなる集合を新たな直線 $(= \ell_\infty$ ：無限遠直線) として追加することにより位数 n の射影平面が構成できる ([26] 参照)．したがって射影平面を考えることとアフィン平面を考えることの間には実質的な差はない．

例 2 に述べたアフィン平面から得られる射影平面は $PG(2,q)$ と一致することが分かるのでこのアフィン平面もデザルグ平面と呼ばれる．

1. 有限射影平面の位数について

有限射影平面の中心的問題の一つは位数 n に関するものである．古くから次の予想が組合せ論の中の難問として広く知られている．

予想 1：（**有限射影平面の基本予想**）有限射影平面の位数は素数べきである．

Veblen-Young の定理によれば射影空間は 3 次元以上であれば射影空間 $PG(m,q)$ に一致する．([7] 第 1 章参照) しかし $m = 2$ のときには $PG(2,q)$ でない例が実際に膨大に存在する．これらは非デザルグ平面 (*non-desarguesian plane*) とよばれこの存在が予想 1 のような組合せ論の難問の一つを生じさせる原因となっている．では非デザルグ平面にはどのようなものがあるかというと既知のものは次の 4 種類に分類される．

既知の非デザルグ平面　今までに知られている非デザルグ平面は次のタイプに分類される．

(P1) ternary ring によるもの ([26] 第 5 章参照)：有限体の変形またはその繰り返し
(P2) spread によるもの ([38] 参照)：有限体上のベクトル空間の利用
(P3) derivation によるもの ([26] 第 10 章参照)：直線の一部の変形
(P4) 上記の組合せによるもの．

詳細はそれぞれの文献を参照されたい．

有限射影平面の基本予想に関して知られている一般的定理は次である．

The Bruck-Ryser の定理 ([7][26]) 自然数 n が 4 を法として 1 か 2 で 2 つの整数の平方和に表されなければ位数 n の射影平面は存在しない．

この定理から位数 $6, 14, 21, 22$ の射影平面の非存在が直ちにわかる．しかし $10, 12, 15, 18, 20$ などについては $10 = 1+3^2$, $18 = 3^2+3^2$ および $12 \equiv 20 \equiv 0$, $15 \equiv 3 \pmod 4$ より上の定理は適用できない．

存在が確定していない有限射影平面で位数最小のものは長い間 $n = 10$ のときであった．しかし計算機の発達とコード理論の応用によりついにこの場合の非存在が次により証明された．

◇ (C.W.H Lam, L. Thiel and S. Swiercz, 1989 [34]) 位数 10 の射影平面は存在しない．

位数 10 の射影平面の存在非存在が決定されるときは基本予想が解けるときであるということがいわれた時代があったと聞いたことがある．そのようにならなかったのはおそらく計算機の飛躍的な発達が予想外のことであったからだと考える．従って計算機を用いない非存在の証明の試みが現在でも基本予想の解決の一つのステップとして重要かつ必要だと考える．

先にのべたように今までに構成されてきた有限射影平面はすべて有限体や有限体上のベクトル空間を利用したものである．従ってその位数は必然的に素数べきとなる．このことから基本予想の根拠は十分とはいえないのではないかという意見も少数ながらある．1972 年に R.H. Bruck は次の予想をたてた．

• Bruck の予想

適当な素数べき q に対して有限射影空間 $PG(3,q)$ は $q^4+q^3+q^2$ 点と q^3 直線を追加することにより位数 $q(q+1)$ の射影平面に拡張できる．ただし，拡張の際 $PG(3,q)$ の点と直線の結合関係は保たれているとする．

上の場合 $q=3$ のときは位数が 12 となり Bruck-Ryser の定理からは存在が直接には否定できない場合にあたるので興味をもたれたが次により非存在が示された．

◇ (M. Hall, Jr. and R. Roth, 1984 [16]) $q=3$ のときは Bruck の予想は正しくない．

射影平面 (またはアフィン平面) $\pi=(\mathbb{P},\mathbb{L})$ の自己同型とは点集合 $\mathbb{P}$ から $\mathbb{P}$ への全単射でそれが直線の集合 $\mathbb{L}$ の置換を引き起こすものをいう．射影平面 (またはアフィン平面) の自己同型は *collineation* とも呼ばれる．射影平面の collineation σ がある点 $P\in\mathbb{P}$ を通るすべての直線を固定し，かつある直線 g 上のすべての点を固定するとき σ は P を中心 (*center*) とし g を軸 (*axis*) とする (P,g)-*perspectivity* であるという．特に $P\in g$ なら (P,g)-*elation*, $P\notin g$ なら (P,g)-*homology* と呼んで区別する．射影平面 (またはアフィン平面) π の collineation の全体 $Aut(\pi)$ は群となりその部分群を π の *collineation* 群という．現在までに構成されている多くの射影平面は perspectivity を含んでいる．また perspectivity は特殊な collineation であるにもかかわらず collineation 群を考える際に重要であるが，その理由の一つに次がある．

◇ (R. Baer [7][26]) $\sigma\neq 1$ を位数 n の射影平面の collineation で $\sigma^2=1$ とすると次のいずれかが起こる．

(i) σ の固定点の全体を $\mathbb{P}_1$, 固定直線の全体を $\mathbb{L}_1$ とするとき $(\mathbb{P}_1,\mathbb{L}_1)$ は位数 $\sqrt{n}$ の射影平面 (=*Baer subplane*) となる．

(ii) σ は perspectivity である．

この定理より n が平方数でなければ (ii) だけが起こることになる．また有限射影平面では位数 2 の自己同型は極めて多くの固定点を持つという性質に注目すべきである．

射影平面が "ある程度大きい collineation 群をもつ" という条件のもとでは基本予想の正しさには十分な根拠がある．これに関連する結果について述べる．

位数 12 の射影平面

◇ (Janko-T. van Trung 1982 [28]) 位数 12 の射影平面 π が存在するとき次が成り立つ．

(i) $Aut(\pi)\not\geq \mathbb{Z}_2\times\mathbb{Z}_2$ and

(ii) $Aut(\pi)$ は $\{2,3\}$-group で $Aut(\pi)\not\geq Sym(3)$ である．

◇ (K. Horvatic-Baldasar, E. Kramer and I. Matulic-Bedenic1987 [24]) 位数 12 の射影平面 π が存在するとき $|Aut(\pi)|=2^a,\ 3^b$ $(0\leq a\leq 4,\ 0\leq b\leq 2)$ が成り立つ．

位数 15 の射影平面

位数 15 の射影平面については次の結果がある.

◇ (C. Ho [21]) 位数 15 の射影平面 π が存在するとき $|Aut(\pi)|$ は $2^6, 2^3 3^3, 2 \cdot 5, 2^3 \cdot 3 \cdot 7$ または $2^6 \cdot 7$ の約数である.

素数 7 に関係する部分について上の C. Ho の結果には完全でない部分があって [52] で次のように修正された.

◇ (末竹千博 2000 [52]) 位数 15 の射影平面 π が存在するとき $21, 7^2 \nmid |Aut(\pi)|$ が成り立つ.

位数 p (素数) の射影平面

もし有限射影平面に関する基本予想が正しいならば有限射影平面に何らかの意味で有限体上のベクトル空間が関係している可能性が高い. もしそうであるとすれば, 先に述べた既知の非デザルグ平面の構成法が素数位数の場合は意味を持たないことが容易に分かる. このことからみて次の予想は自然である.

予想 2: 素数位数の射影平面はデザルグ平面である.

これに関係する結果を紹介する.

- $n = 11$

◇ (I. Matulic-Bedenic [43][44][45]) 次のいずれかをみたす位数 11 の射影平面はデザルグ平面である:
(i) order 5 の homology をもつ. (計算機の使用)
(ii) 位数 2 の collineation を含む.

◇ (C. Ho and G. E. Moorhouse [23]) 次のいずれかをみたす位数 11 の射影平面はデザルグ平面である:
(i) 4 次交代群を collineation 群に含む.
(ii) order 5 の homology をもつ.
(iii) 固定点集合が 3 角形である位数 5 の collineation をもつ.

◇ (K. Horvatic-Baldasar, K. Kramer and I. Matulic-Bedenic [25]) 位数 21 の非可換群 (Frobenius となる) を collineation としてもつ位数 11 の射影平面はデザルグ平面である.

- $n = 13$

◇ (I. Matulic-Bedemic, 1991 [46]) 位数 2 の collineation を含む位数 13 の射影平面はデザルグ平面である.

分類の完全に終わった位数

この節で述べた位数 10 の場合の解決と次の定理により位数 10 以下の射影平面はすべて分類されたことになる. 未分類の最小位数の n は $n = 11$ である.

◇ (Lam-Kolesova-Thiel, 1991 [35]) 位数 9 の射影平面はちょうど 4 個 (デザルグ平面, Huges 平面, Hall 平面, 双対 Hall 平面) 存在する.

collineation に関して次の予想があることを付け加える.

予想 3: すべての有限射影平面は位数 2 の collineation をもつ.

有限射影平面の結合行列の研究

$\pi=(\mathbb{P},\mathbb{L})$, $(\mathbb{P}=\{P_1,P_2,\cdots\},\ \mathbb{L}=\{\ell_1,\ell_2,\cdots\})$ を射影平面またはアフィン平面とする．$|\mathbb{P}|$ 行 $|\mathbb{L}|$ 列の行列 $A=(a_{ij})$ を $P_i\in\ell_j$ のとき $a_{ij}=1$，$P_i\notin\ell_j$ のとき $a_{ij}=0$ とおいて定めるとき A を $\pi=(\mathbb{P},\mathbb{L})$ の結合行列 (*incidence matrix*) という．

H. J. Ryser は [51] において (v,k,λ)-対称デザインが存在するための必要十分条件を行列を用いて与えた．これを有限射影平面の場合に述べれば次のようになる．

Ryser の定理 ([51]) 位数 n の射影平面が存在するための必要十分条件は成分が整数の n^2+n+1 次正方行列 A で $A\,{}^tA={}^tAA=J+nI$ をみたすものが存在することである．(J は成分がすべて 1 の行列，I は単位行列．)

Ryser の定理により位数 n の有限射影平面の存在は n^2+n+1 次正方行列 A で表された連立不定方程式 $A\,{}^tA={}^tAA=J+nI$ の整数解の存在と同値である．有限射影平面の結合行列に対する直接のアタックとして J.G. Thompson の [53] がある．J.G. Thompson の研究は現在まではまだ Bruck-Ryser の定理のような強力な結果を与えてはいないが今後とるべき一つの方向を示していると思われるのでここで紹介したい．まず位数 n の射影平面 $\pi=(\mathbb{P},\mathbb{L})$ について次のように記号を定める．

$v=n^2+n+1$,
$\mathfrak{I}=$ π の可能な結合行列の全体
$\mathfrak{T}_v=$ n 次の置換行列のうち互換に対応するもの全体
$f_A(x)=\det(xI-A)\quad(A\in M_n(\mathbb{R}))$
$F_A=$ $f_A(x)$ の分解体
$G_A=\mathrm{Gal}(F_A/\mathbb{Q})$
$\sigma=$ 複素共役写像が定める F_A の位数 2 の元

以上の記号のもとで A の固有多項式の分解体のガロア群の元 σ について次が成り立つ．

◇ (J. G. Thompson, 1997 [53]) n が非平方元で $A\in\mathfrak{I}$ かつ $\langle\sigma\rangle$ が G_A の直和因子とする．このとき $\langle\sigma\rangle$ はすべての $T\in\mathfrak{T}_n$ に対して G_{AT} の直和因子である．

$A\in\mathfrak{I}$, $T\in\mathfrak{T}_n$ とすると $AT\in\mathfrak{I}$ であることは明らかである．また A は $A\,{}^tA={}^tAA=J+nI$ をみたし，$J+nI$ の固有方程式は $(x-(n+1)^2)(x-n)^{n^2+n}$ であるから A の固有値は一つが $n+1$ で残りの n^2+n 個はすべて複素平面上で原点を中心とする半径 $\sqrt{n}$ の円周上にある．A と AT の固有値の複素平面上の分布に関して次の結果が与えられている．

◇ (J. G. Thompson, 1997 [53]) n が非平方元で，$A\in\mathfrak{I}$ かつ $T\in\mathfrak{T}_n$ とする．また $F_A(x)=(x-n-1))D(x)E(x)$ and $F_{AT}(x)=(x-n-1))D(x)F(x)$ とおく $((E(x),F(x))=1)$．このとき $E(x)$ および $F(x)$ は square free でその根は複素平面上で原点を中心とする半径 $\sqrt{n}$ の円周上にあり $E(x)$ の円周上でとなりあう根の間にはただ一つの $F(x)$ の根がある．

位数 n の射影平面が位数 n^2+n+1 の巡回 collineation 群をもつとき巡回平面というがこれに関して次の結果がある．

◇ (Brozovic-Ho-Munemasa, 1999 [4]) π が位数 n の巡回平面で n^2+n+1 が素数であるとすると固有値がすべて異なる結合行列が存在する．

2. Quasi-Regular Collineation Groups

定義 群 G の k-部分集合 D が部分集合 U (ただし $1 \in U$) に関する差集合であるとは $G \setminus U$ の任意の元が $r_1 r_2^{-1}$ $(r_1, r_2 \in R,\ r_1 \neq r_2)$ の形にただ一通りに表され，かつ U の元はこの形には表せないことをいう．とくに U が G の位数 u 指数 m の部分群であるとき U を禁止群 (*forbidden subgroup*) といい，D を $(m, u, k, 1)$-差集合という (このとき $k^2 = k + u(m-1)$ であることに注意)．また，$(m, 1, k, 1)$-差集合は簡単に $(m, k, 1)$-差集合または平面差集合 (*planar difference set*) という．

(注 1) この稿では会合数 1 の差集合だけを取り扱っているので差集合ということばを限定して用いている．しかし，差集合自体はもっと一般的なものである．これに関しては [3], [36] を参照されたい．
(注 2) 差集合の定義から G が位数 2 の元をもてばそれはすべて U にが含まれることになる．
(注 3) G の元 g に対して $U = G$ とおけば $D = \{g\}$ は U を禁止群とする $(1, u, 1, 1)$-差集合となる．これは自明なので以下ではこれは除外して考えることにする．
(注 4) D が G の U に関する差集合ならば任意の $g \in G$ に対して Dg も同じ parameters をもつ差集合となるのは明らかである．Dg を D の *translate* という．このことから $1 \in D$ は必要なら仮定できる．

定義 位数 m^2 の群 G の位数 m の部分群 $H_1, \cdots, H_{m+1}$ が spread であるとは $G = H_1 \cup \cdots \cup H_{m+1}$ が成り立つことをいう．位数を比較することにより，このことは $H_i \cap H_j = \{1\}$ $(\forall i \neq \forall j)$ が成り立つことと同値であることがわかる．

定義 集合 Ω 上の置換群 X が *quasiregular* であるとは Ω 上の任意の X-orbit Δ に対して X の Δ への制限 $X|_\Delta$ が正則となることをいう．(つまり，$X|_\Delta$ の位数 $= |X|$．あるいは同じことであるが X の元が Δ のある点を固定すればその元が Δ のすべての点を固定すること) 位数 n の射影平面 $\pi (= (\mathbb{P}, \mathbb{L}))$ の collineation 群 G が *quasiregular* であるとは $G|_{\mathbb{PUL}}$ が quasiregular であることをいう．

Dembowski の分類定理 位数 n の射影平面 $\pi = (\mathbb{P}, \mathbb{L})$ が位数が $\frac{n^2+n+1}{2}$ より大きい quasiregular な collineation 群 G をもてば G に関して次のいずれかが成り立つ．

(a) $|G| = n^2 + n + 1$ で $(n^2 + n + 1, n + 1, 1)$-差集合 (平面差集合) をもつ．
(b) $|G| = n^2$ で $(n, n, n, 1)$-差集合をもつ．
(c) $|G| = n^2$ で spread をもつ
(d) $|G| = n^2 - 1$ で $(n + 1, n - 1, n, 1)$-差集合 (アフィン差集合ともいう) をもつ．
(e) $|G| = m^4 - m$, $m = \sqrt{n}$ で $(m^2 + m + 1, m^2 - m, m^2, 1)$-差集合をもつ．
(f) $G = HN \rhd N$, $|N| = n$, $|H| = n - 1$ で部分集合 $H \cup N$ に関する差集合 (E-H 差集合ともいう) をもつ．
(g) $|G| = (n-1)^2$, $G = H_i H_j \rhd H_i, H_j$ $\forall i, \forall j \in \{1, 2, 3\}, i \neq j$ (H_1, H_2, H_3 は位数 $n-1$ の部分群) で G は部分集合 $H_1 \cup H_2 \cup H_3$ に関する差集合 (E-E 差集合ともいう) をもつ．
(h) $|G| = (m^2 - m + 1)^2$, $m = \sqrt{n}$ であり，G-軌道は $\mathbb{P}_1, \cdots, \mathbb{P}_{2m+1} (\subset \mathbb{P})$, $\mathbb{L}_1, \cdots, \mathbb{L}_{2m+1} (\subset \mathbb{L})$ で，$(\mathbb{P}_1, \mathbb{L}_1), \cdots, (\mathbb{P}_{2m}, \mathbb{L}_{2m})$ はすべて位数 $m-1$ の射影平面でかつ $|\mathbb{P}_{2m+1}| = |\mathbb{L}_{2m+1}| = (m^2 - m + 1)^2$.

この定理に関して重要なことは，逆に (a)〜(h) のいずれかをみたす群が存在すればその群を quasiregular な collineation 群としてもつ位数 n の射影平面が構成できることである．この定理

にある "位数が $\frac{n^2+n+1}{2}$ より大きい" という仮定はこの点で意味がある．以下では (a)〜(h) のそれぞれの場合について知られた結果を述べる．

Case (a) 平面差集合 (*planar difference sets*)

例 3 位数 $n(\in\{2,3,4,9\})$ の差集合

(i) $n=2,\ G=\langle x\rangle\simeq Z_7,\ D=\{1,x,x^3\}$
(ii) $n=3,\ G=\langle x\rangle\simeq Z_{13},\ D=\{1,x,x^3,x^9\}$
(iii) $n=4,\ G=\langle x\rangle\simeq Z_{21},\ D=\{1,x,x^6,x^8,x^{18}\}$
(iv) $n=9,\ G=\langle x\rangle\simeq Z_{91},\ D=\{1,x,x^3,x^9,x^{27},x^{49},x^{56},x^{61},x^{77},x^{81}\}$

まず最初に次の予想があることに注意されたい．

予想 4：平面差集合から構成される射影平面はデザルグ平面に限る

既知の例はアーベル群，非アーベル群ともに存在するがいずれもデザルグ平面に由来するものだけである．また自己同型群の中に 2 個以上の平面差集合の存在を仮定した Ott の結果とその一般化がある ([22] 参照)．平面差集合の研究で群がアーベル群であればこれを可換平面差集合というが，この場合には "乗数" という強力な方法がある．

定義 整数 m が可換平面差集合 D の乗数 (*multiplier*) であるとは $D^{(m)}=Da$ となる元 $a\in G$ が存在することをいう．ただし，$D^{(m)}=\{d^m\mid d\in D\}$.

可換平面差集合の乗数に関しては次が基本的である．

乗数定理 ([42] 第 7 章，[3] 第 6 章参照) D を $(n^2+n+1,n+1,1)$-可換平面差集合とすると n を割る素数は D の乗数である．

また，次が成り立つことも容易に証明できる．

定理 ([42] 第 7 章，[3] 第 6 章参照) D を $(n^2+n+1,n+1,1)$-可換平面差集合とすると D の translate を適当に選べば D のすべての乗数 m に対して $D^{(m)}=D$ が成り立つと仮定できる．

たとえば素数 2 と 3 を考えて $2|n$ かつ $3|n$ とすると乗数定理より 2^a3^b $(a,b\in\mathbf{N}\cup\{0\})$ はすべて乗数となるが上のことより $D^{(2^a3^b)}=D$ である．とくに任意の $d\in D$ について $d^1,d^2,d^3,d^4\in D$ であるが，$3-1=4-2$ より $d^3d^{-1}=d^4(d^2)^{-1}$．よって差集合の定義から $d^3=d^4$ または $d^3d^{-1}=1$．これは矛盾であるから $6\nmid n$ が分かる．このような議論を適用して可能な位数 n は強い制限を受ける．D が定める射影平面を $\pi(\mathbb{P},\mathbb{L})$, $(\mathbb{P}=G,\ \mathbb{L}=\{Dg\mid g\in G\})$ とおくとき定義より乗数は π の collineation を誘導する．この特殊な collineation の存在が可能な n に強い制限を与えていることになる．これについては例えば [42] 第 7 章参照．

乗数を利用した次の結果もある．

◇ (Wilbrink, 1989 [54]) $p\in\{2,3\}$ とし，D を位数 n の 可換平面差集合とする．もしも $p\mid n$ かつ $p^2\nmid n$ ならば $n=p$ である．

この定理に関して $p>3$ のときの結果は知られていない．

Case (b) $(n,n,n,1)$-差集合および平面関数

例 4 $(n,n,n,1)$-差集合

(i) $K=GF(2^e)$ に対して $G=K^+\times K^+$ に積を $(x_1,y_1)(x_2,y_2)=(x_1+x_2,y_1+y_2+x_1x_2)$ により定めると $\mathbb{Z}_4\times\cdots\times\mathbb{Z}_4$ に同型な群となる．このとき $D=K\times\{0\}$, $U=\{0\}\times K$ とおけば D は G の U に関する $(2^e,2^e,2^e,1)$-差集合である．
(ii) $K=GF(p^e)$ (pは奇素数) に対して $G=K^+\times K^+$ に積を $(x_1,y_1)(x_2,y_2)=(x_1+x_2,y_1+y_2)$ により定めると $\mathbb{Z}_p\times\cdots\times\mathbb{Z}_p$ に同型な群となる．このとき $D=\{(x,x^2)\mid x\in K\}$, $U=\{0\}\times K$ とおけば D は G の U に関する $(p^e,p^e,p^e,1)$-差集合である．

$(n,n,n,1)$-差集合についての最大の目標は次を示すことである．

予想 5： 群 G が $(n,n,n,1)$-差集合をもてば n が素数べきである．

この予想の場合，群の位数が n^2 であるから可能な群についての分析が直接的に n に関する情報となる．この点が Case (a) より詳しい結果が得られている理由になっている．まず偶数位数のアーベル群の場合は抽象群としては次の定理により完全に解決している．

◇ (Ganley, 1976 [12]) D が 偶数位数の群 G における $(n,n,n,1)$-可換差集合ならば $G\simeq(Z_4)^m$ である．

(注 5) Ganley の定理では群の構造は決定して n が 2 べきであることを示しているが対応する射影平面がデザルグ平面かどうかまでは示していない．これも解決すべき問題の一つと考える．

定義 H,U を位数 n の群とする．H から U への関数 f が平面関数 (*planar function*) であるとは $f(xt)f(x)^{-1}$ がすべての $t\neq 1$ に対して H から U への 1 : 1 の関数となることをいう．

例 5 (ii) $K=GF(p^e)$ (p は奇素数) に対して $H=U=K(+)$ とみる．関数 $f:H\longrightarrow U$ を $f(x)=x^2$ で定義すると f は planar 関数となる．

f が位数 n の群 H から位数 n の群 U への planar 関数であるとき $G=H\times U$, $D=\{(x,f(x))\mid x\in H\}$ とおけば D は G の U に関する $(n,n,n,1)$-差集合である．逆に，D を群 G の禁止群 U に関する $(n,n,n,1)$-差集合で U が G の直和因子あるとする．$G=H\times U$ とし，$D=\{(x,f(x))\mid x\in H\}$ とおくとき f は H から U への平面関数となることが容易に分かる．

可換平面関数

先に述べた注意により $G\setminus U$ には位数 2 の元が含まれないので直ちに次が成り立つことが分かる．

◇ (M. J. Ganley, 1976 [12]) 位数 n の 2 つの群 H,U について，H から U への平面関数が存在するならば n は奇数である．

次に H および U が位数 n のアーベル群であるときの H から U への平面関数に関する結果をいくつか述べる．

◇ (D. Gluck 1990 [14] , Y. Hiramine 1990 [17], L. Ronyaiand T.Szonyi 1989 [50]) n が素数のとき，H および U を素体 $GF(n)$ の加法群と同一視すれば H から U への平面関数は $GF(n)$ から $GF(n)$ への 2 次多項式で表される．
◇ (P.V. Kumar, 1988 [33]) H から U への planar 関数が存在するならば，n を割る任意の素数 p,q に対して p を法とする q の位数 $Ord_p(q)$ は奇数である．
◇ (C.I. Fung, M.K. Siu and S. L. Ma, 1990 [9]) H,U が巡回群ならば n は square free である．
◇ (Y. Hiramine, 1992 [19]) $n=3p$ で p が素数ならば $p=3$ かつ $H\simeq U\simeq\mathbb{Z}_3$ のときに限り平面関数が存在する．

- ◇ (S. L. Ma, 1996 [41]) $n=pq$ で p,q が素数ならば $p=q$ かつ $H\simeq U\simeq \mathbb{Z}_p$ のときに限り平面関数が存在する.
- ◇ (K.H. Leung, S.L. Ma and V. Tan, preprint [39]) $n=3pq$ で $p,q(\neq 3)$ が異なる素数ならば平面関数は存在しない.

問題: (i) H か U の少なくとも一方が巡回群でないとき未解決の最小の場合は $n=117(=3^2 13)$ である.

(ii) $H\simeq U\simeq \mathbb{Z}_n$ のとき未解決の最小の場合は $n=15655(=5\cdot 31\cdot 101)$ である.

(iii) $n=pqr$ で $p,q,r(\geq 5)$ が互いに異なる素数のときは未解決である.

p-群における $(n,n,n,1)$-差集合

仮に $(n,n,n,1)$-差集合をもつ群が p-群に限るという予想が示されたとして, その場合 群の構造はどのようになるであろうか. G が可換 p-群で $(p^a,p^a,p^a,1)$-差集合をもつという条件のもとで次が知られている. 次の結果は本来もっと一般的な "半正則相対差集合"のものであるがそれを会合数 1 の場合に適用する. 実際に知られている例は $\mathbb{Z}_4\times\cdots\times\mathbb{Z}_4$ と $\mathbf{Z}_p\times\cdots\times\mathbb{Z}_p$ の場合だけであることに注意されたい.

- ◇ (Davis, 1992 [6]) $\exp(G)\leq p^{\frac{a+1}{2}}\exp(U)$
- ◇ (Pott, 1994 [48]) $\exp(G)\leq p^a$
- ◇ (Ma-Pott, 1995 [40]) $\exp(G)\leq p^{\frac{a+1}{2}}$
- ◇ (Ma-Pott, 1995 [40]) $a=2$ のときは $G\simeq \mathbf{Z}_p\times\mathbf{Z}_p\times\mathbb{Z}_p\times\mathbb{Z}_p$ である.

Case (c) spread

この場合では位数 n^2 の群 G がただ一つの直線を固定する. これを無限遠直線 ℓ_∞ と見て得られる位数 n のアフィン平面 π で, 平行類 $\mathbf{C}_1,\cdots,\mathbf{C}_{n+1}$ の各々の不変部分群 $H_i=\{x\in G\mid \ell x=\ell,\ \forall \ell\in\mathbf{C}_i\}(1\leq i\leq n+1)$ は群 G の spread となる. また, spread を持つ有限群は基本可換 p-群となる ([38] 第 1 章参照). 逆に, 群 G が spread $H_1,\cdots,H_{m+1}$ をもつとき, $\mathbb{P}=G$, $\mathbb{L}=\{H_1x\mid x\in G\}\cup\cdots\cup\{H_{m+1}x\mid x\in G\}$ に対して $\pi=(\mathbb{P},\mathbf{L})$ は位数 m のアフィン平面となり *translation plane* と呼ばれる. ここでは G の各元は右からの作用によって π の collineation と同一視され H_i は平行類 $\{H_ix\mid x\in G\}$ の G における不変部分群となる. 以上のことより Case(c) の問題は素体 $GF(p)$ 上の $2m$ 次元ベクトル空間 $(n=p^m)$ の spread を決定する問題と同値である. この方法で膨大なアフィン平面が構成されている. $m=1$ のときはデザルグ平面だけであるが $m=2$ のときは未決定である. Case(c) の射影平面に関する詳細は [29], [38] を参照されたい.

(注 6) 上に述べたように G は G の spread が定めるアフィン平面の点上可移な collineation 群となっている. これはのちに述べる可移平面の代表的な例となっている.

Case (d) : アフィン差集合

この場合には位数 n^2-1 の群 G がただ一つの直線 ℓ と点 $P(\notin\ell)$ を固定する. 直線 ℓ_0 $(\ell_0\neq\ell,\ P\notin\ell_0)$ と点 P_0 $(P_0\neq P,\ P_0\notin\ell)$ を選んで $D=\{x\in G\mid P_0x\in\ell_0\}$ とおけば D は正規部分群 $U=\{x\in G\mid gx=g,\ \forall g\ni P,\ g\in\mathbb{L}\}$ を禁止群とするアフィン差集合となる.

例 6 $F=GF(p^{2e})\supset K=GF(p^e)$ に対して $G=F^*$ (乗法群) $\simeq\mathbb{Z}_{p^{2e}-1}$, $U=K^*$ (乗法群) $\simeq\mathbb{Z}_{p^e-1}$, $D=\{1+k\omega\mid k\in K\}$ とおく. (ω は乗法群 F^* の生成元) このとき D は G の U に関する $(p^e+1,p^e-1,p^e,1)$-差集合 (i.e. 位数 p^e のアフィン差集合) である.

位数 n のアフィン差集合に関して次の予想がある.

予想 6: 位数 n^2-1 の可換群がアフィン差集合を含めば巡回群でかつ n が素数べきである.

巡回群であるという予想はアーベル群の場合は有限体の乗法群を用いて構成される上の例のもの以外知られていないことによると思われる. 実際に可換アフィン差集合をもつ群の 2-Sylow 群は巡回群である ([2]). また, 次の定理はこの予想に一つの根拠を与えている.

◇ (Garciano-Hiramine, 2001 [13]) $\pi(m)$ で整数 m を割る素数全体の集合を表すとする. $\pi(w) \subset \pi(n)$ のとき $\pi = \pi((w-1, n^2-1))$ に対して G の Hall π-群を H とおく. このとき, $\forall p \in \pi((n+1, w+1))$ に対して G の p-rank は $log_p(|H|+2)$ 以下である.

予想 6 が正しければ $n \equiv 8 \pmod{16}$ のときは $n = 8$ が成り立つことになるが, これについては次の結果がある.

◇ (K.T. Arasu and A. Pott, 1992 [2]) $n \equiv 8 \pmod{16}$ とする. G がアーベル群ならば $n-1$ は素数べきである. また, G が巡回群ならば $n-1$ は素数である.

この結果は $n \equiv 8 \pmod{16}$ ならば $n = 8$ が成り立つことを暗示しているが未解決である.

Case (e): $(m^2+m+1, m^2-m, m^2, 1)$**-差集合**

この場合アーベル群では次の $n = 4$ のときに例が知られているのみである.

例 7 $G = \langle x \rangle \simeq \mathbb{Z}_{14}$, $U = \langle x^7 \rangle \simeq \mathbb{Z}_2$, $D = \{1, x, x^4, x^6\}$ とすると D は G の U に関する $(2^2+2+1, 2^2-2, 2^2, 1)$-差集合である.

非可換群の場合は群 $\mathbb{Z}_{13} \times \mathrm{Sym}(3)$ $(n = 9)$ に例がある ([10] 参照). 可換群のときは次の Ganley-Spence の結果が知られている.

◇ (M.J. Ganley and E. Spence, 1975 [10]) If $n > 4$ ならば n は奇数であり, かつ素数べきではない. さらに, n を割る素数 p は $p \equiv 1 \pmod{4}$ である.

Case (f) : **Elation-Homology 型**

この場合に関しては次が知られている.

◇ (A. Pott, 1994 [49]) Elation-Homology 型では次が成り立つ.

(i) n が偶数のときは n は 2 べきで, G の 2-Sylow 群は基本可換 2 群である.
(ii) n が奇数のときは G の 2-Sylow 群は巡回群である.
(iii) n が素数のときは対応する平面はデザルグ平面である.
(iv) n が平方数でなければ n は素数べきである

Case (g) : **Homology-Homology 型**

この場合, 知られているのはデザルグ平面に対応するものだけである. また, これについては W.M. Kantor の研究がある. ([31] 参照)

Case (h) :

この場合は可換性の仮定なしに $n = 4$ に限ることが Ganley-McFarland 1975 [11] により示されて完全に決定された.

3. PTR (planar ternary rings)

位数 n の有限射影平面は n-集合を用いて"座標付け"されることが知られていて ([26] 参照) そこから得られる"代数系" R は *planar ternary ring* (PTR) と呼ばれ 3 項演算 $T(x,y,z)$ をもつ. 逆に PTR から射影平面が構成できる. また, $a+b=T(1,a,b)$, $ab=T(0,a,b)$ により 3 項演算 $T(x,y,z)$ から 2 項演算をもつ代数系 $R(+,\cdot)$ を得るが, 一般にはこれから 3 項演算を復元できない. しかし, $R(+,\cdot)$ が "適度"の条件をみたすときはこれが可能で自然に PTR が構成されて, したがって射影平面を得る. この適度の条件の一つが quasifiled と呼ばれる代数系である.

定義 有限集合 $Q(+,\cdot)$ が *quasifield* であるとは次の 4 条件をみたすことをいう :

(q1) $Q(+)$ は群.
(q2) $Q^*(\cdot)$ は loop(つまり, 単位元 1 をもち, 3 変数 x,y,z に関する方程式 $xy=z$ のうち 2 変数を定めれば残りは unique に定まる).
(q3) 右分配律をみたす.
(q4) $0x=0 \quad \forall x \in Q$.

quasifield において $Q(+,\cdot)$ は基本可換 p-群であることが示される ([38]). 従って Q の元数 $q(=|Q|)$ は素数べきである. quasifield Q に対してアーベル群 $G=Q\times Q$ と $q+1$ 個の部分群 $H_a=\{(x,y)\mid y=ax\}$ $(a\in Q)$ と $H_\infty=\{0\}\times Q$ を考えればこれらは G の spread を与えて, 先に述べた quasiregular collineation groups の Case (c) に対応する.

1960 年代から 1980 年代にかけて非常に多くの射影平面が quasifield を構成するという方法で得られた. 有限体は quasifield の特別な場合であるが, 有限体を変形することにより大量の quasifield が得られたのであった ([7][26][38]). また quasifield と同値な概念として有限体上の偶数次元ベクトル空間の分割である spread を考えて多くの射影平面が得られた ([7][38] 参照). quasifield の 4 条件において, (q2) を "$\overline{\text{(q2)}}$ $Q^*(\cdot)$ は群 " でおきかえたものは *nearfield* とよばれ, これは完全に分類されている ([38] 参照). また, quasifield の条件 (q3) を "$\overline{\text{(q3)}}$ 左右分配律 " でおきかえたものは *semifield* とよばれ多くの例が知られている ([7][32]). 有限体は semifield の特別な場合である. よく知られているように有限体の全自己同型群は巡回群であるが, semifield に関しては次の予想がある.

予想 7 : semifield の全自己同型群は可解群である.

この予想については R. Liebler の結果がある ([37] 参照). また, semifield の定義から位数 p^2 の semifield は有限体となることが容易にわかる. 有限体でない位数 p^3 の semifields が知られているが p^3 の semifields はまだ分類されていない.

4. 可移平面

π を位数 n の射影平面とする. π の自己同型群 G が π の点上可移であるとき π を可移平面 (*transitive plane*) という. この場合 G が正則に作用 (したがって $|G|=n^2+n+1$) するときには Dembowski の分類定理の Case (a) に相当し, G を Singer 群という. デザルグ平面は可移平面で *Singer* 群をもつことが知られているが, これ以外には例が見つかっていない. また, アフィン平面に対しても"可移平面"を同様に定義する. この両者を特に区別する場合にはそれぞれ *transitive projective plane*, *transitive affine plane* のようにいう. (注 6) でのべたように translation plane は可移アフィン平面である.

次は可移射影平面に関する最も基本的な予想である.

予想 8 可移射影平面はデザルグ平面に限る.

この予想に関しては次が示されている.

◇ (U. Ott,1975 [47], C. Ho, 1998 [22]) G が射影平面 π の可換な Singer 群であるとすると π はデザルグ平面かまたは $Aut(\pi) \triangleright G$ である.

直線 ℓ とその上の点 P の組 (P,ℓ) は *flag* と呼ばれる. 位数 n の射影平面にはちょうど $(n+1)(n^2+n+1)$ 個の flags がある. この flags 全体の集合に可移に作用する π の自己同型群 G が存在するとき π は *flag-transitive* であるという.

◇ (W. Feit, 1990 [8]) flag-transitive な位数 n の射影平面はデザルグ平面かまたは $8|n$ で n は 2 べきでなくかつ n^2+n+1 は素数である.

可移アフィン平面については次の予想がある.

予想 9: 可移アフィン平面の位数は素数べきである.

この予想は可移群がアーベル群のときもまだ未解決ではあるが, 可移群の位数が n^2 で割れることから, 群の情報が直接 n に関する情報となるので特に非可解群の場合は解決出来てもよいように思う.

点 P と直線 g に対して (P,g)-perspectivities の全体 G は自己同型群となる. この群が P を通る直線 ℓ に対して $\ell \setminus \{P\}$ 上可移となるとき (P,ℓ_∞)-可移であるという. (P,ℓ_∞)-可移性に関して次の予想がある.

予想 10: 可移アフィン平面は ℓ_∞ 上のある点 P に対して (P,ℓ_∞)-可移である.

上の予想は可換な可移群の場合は正しいことが証明されている ([30]). また, 可移アフィン平面については次のことが分かっている.

◇ (J. Andre, 1954 [30] 参照) 可移アフィン平面が中心を無限遠直線外にもつ homology ($\neq 1$) をもてば translation plane であり特に位数は素数べきとなる.

◇ (Ostrom-Wagner, 1959 [30] 参照) アフィン平面の自己同型群が点上 2 重可移ならば translation plane である.

◇ (Wagner, 1965 [30] 参照) アフィン平面の自己同型群が直線全体上可移ならば translation plane である.

◇ (Kallaher-Libler, 1970 [30] 参照) アフィン平面の自己同型群が置換群として点上 rank 3 に作用すれば translation plane である.

◇ (Hiramine, 1990 [18]) アフィン平面の自己同型群が点上原始的に作用すれば translation plane である.

5. 射影平面の部分構造

Subplanes

位数 n の射影平面 π の部分構造でそれ自身が射影平面となっているものを $\pi = (\mathbb{P},\mathbb{L})$ の部分平面 (*subplane*) という. $\mathbb{P}$ の部分集合 S を部分平面ということがあるがこれは $B = \{g \cap S \mid g \in \mathbb{L},\ g \cap S \neq \phi\}$ とおくとき (S,B) が部分平面である場合をいう. 部分平面 $S(\neq \mathbb{P})$ の可能な位数 m には次の制限がある.

◇ (R. H. Bruck [26], [7]) $n = m^2$ かまたは $n \geq m^2+m$ である.

位数 n の射影平面 $\pi = (\mathbb{P}, \mathbb{L})$ に対して $\mathbb{P} \subset S$, $\mathbb{L} \subset B$ とする．結合構造 (S, B) が *closed configulation* であるとは次の 2 条件がみたされることをいう．

(1) $P_1, P_2 \in S$ $(P_1 \neq P_2) \implies P_1P_2 \in B$

(2) $g_1, g_2 \in B$ $(g_1 \neq g_2) \implies g_1 \cap g_2 \in S$

π の部分平面はすべて closed configulation である．

次は明らかである．◇ 射影平面 $\pi = (\mathbb{P}, \mathbb{L})$ の任意の自己同型を σ とする．σ が固定する点集合 $\mathrm{Fix}_{\mathbb{P}}(\sigma)$ と直線集合 $\mathrm{Fix}_{\mathbb{L}}(\sigma)$ に対して $(\mathrm{Fix}_{\mathbb{P}}(\sigma), \mathrm{Fix}_{\mathbb{L}}(\sigma))$ は closed configulation である．

自己同型 σ の固定集合が部分平面になるとき σ は *planar* であるという．

◇ (R. Roth [7] 第 4 章参照) 射影平面 $\pi = (\mathbb{P}, \mathbb{L})$ の自己同型 σ が planar で固定集合が位数 m の部分平面ならば $n = m^2$ または $n \geq m^2 + m + 2$ が成り立つ．

部分平面については次の予想がある．

予想 11： デザルグ平面でない任意の射影平面は位数 2 の部分平面をもつ．

Blocking Sets

定義 $\pi = (\mathbb{P}, \mathbb{L})$ を位数 n の射影平面とする．$\mathbb{P}$ の部分集合 S が *blocking set* であるとは任意の直線 $g \in \mathbb{L}$ が S および S の補集合と交わることすなわち $S \cap g \neq \phi$, $S^c \cap g \neq \phi$ が成り立つことをいう． blocking set S が *minimal* であるとは S の任意の真部分集合が blocking set でないことをいう．

blocking set については詳細な研究が行われているが詳細は [20] を参照されたい．いくつかの結果を紹介する．

◇ (Von Neumann-Morgenstern [20]) 位数が 2 より大きな射影平面は blocking set をもつ．

また位数 n の射影平面 π の blocking set の可能な大きさについては次の制限がある．

◇ (A. A. Bruen, 1980 [5]+ Hirschfeld's book [20])

$$n + \sqrt{n} + 1 \leq |S| \leq n\sqrt{n} + 1.$$

上二つの不等号で最初の等号が成り立つのは S が Baer subplane のときで 2 番目の等号が成り立つのは π の部分構造として S が unital ($(\sqrt{n^3} + 1, \sqrt{n} + 1, 1)$-design) になるときである．

アフィン平面における blocking set も同様に定義してこれを *affine blocking set* という．これについては次が成り立つ．([20] 参照)

$$|S| \geq 2n - 1$$

この射影平面に関する講演は世話人である吉荒聡氏から特に"総括と展望"ということで準備するように依頼を受けました．総括の部分はある程度は書かせていただきましたが展望がないのではないかとお叱りを受けそうです．そこで独断と偏見を許していただくことにしてこの稿で挙げた予想 1〜予想 11 について 21 世紀中に解決するであろう (=解けそうな) 予想を書かせていただいて"展望"に代えさせていただきたいと思います．

予想 5, 予想 9, 予想 6, 予想 10

参考文献

[1] K.T. Arasu, A. Pott, On quasiregular collineation grouos of projective planes, Designs, Codes and Cryptography Vol.1 (1991) 83-92.

[2] K.T. Arasu, A. Pott, Cyclic affine planes and Paley difference sets, Discrete Math. 106/107 (1992), 19-23.

[3] T. Beth, D. Jungnickel and H. Lenz, *Design Theory*, Cambridge University Press, Cambridge, 1995

[4] D.P. Brozovic, C. Ho and A. Munemasa, A note on incidence matrices of finite cyclic projective planes, preprint

[5] A. A. Bruen, Blocking sets and skew subspaces of projective space, Can.J. Math. **32** (1980) 628-630.

[6] J.A. Davis, An exponent bound for relative difference sets in p-groups, Ars Combinatoria **34** (1992) 318-320.

[7] P. Dembowski, *Finite Geometries*, Berlin-Heidelbelg-New York, Springer, 1968

[8] W. Feit, Finite projective planes and a question about primes, Proc. Amer. Math. Soc. **108** (1990) 561–564.

[9] C.I. Fung, M.K. Siu and S.L. Ma, On arrays with small off-phase binary auto-correlation, Ars Comb. **29A** (1990) 189-192.

[10] M.J. Ganley and E. Spence, Relative difference sets and quasiregular collineation groups, J. of Combin. Ser. A **19**(1975) 134-153

[11] M.J. Ganley and R.L. McFarland, On quasiregular collineation groups, Arch. Math. **56** (1975) 327-331.

[12] M.J. Ganley, On a paper of Dembowski and Ostrom, Arch. Math. **27** (1976) 93-98.

[13] A.D. Garciano and Y. Hiramine, On Sylow subgroups of abelian affine difference sets, Designs, Codes and Cryptography Vol. 22 (2001) 157-163

[14] D. Gluck, A note on permutation polynomials and finite geometries, Discrete Math. **80** (1990) 97-100.

[15] D. Gorenstein, *Finite Groups*, Harper and Row, New Yor, 1968

[16] M. Hall, Jr and R. Roth, On a conjecture of R.H. , J. of Combin. Ser. A **37** (1984) 22-31.

[17] Y. Hiramine, A conjecture on affine planes of prime order, J. of Combin. Ser. A **52**(1989) 44-50.

[18] Y. Hiramine, Affine planes with primitive collineation groups. J. Algebra **128** (1990) 366–

[19] Y. Hiramine, Planar functions and related group algebras, J. of Algebra **152**(1992) 135-145

[20] J.W. Hirschfeld, *Projective Geometries over Finite Fields (Second Edition)*, Clarendon Press, Oxford, 1998.

[21] C. Ho, Projective Planes of order 15 and other odd composite orders, Geom. Ded. **27**(1988) 49-64

[22] C. Ho, Finite projective planes with abelian transitive collineation groups, J. Algebra **208** (1998) 533-550

[23] C. Ho and G. E. Moorhouse, A new characterization of the Desarguesian plane of order 11, Algebras Groups Geom. **2** (1985) 428-435

[24] K. Horvatic-Baldasar, E. Kramer, I. and Matulic-Bedenic, On the full collineation group of projective planes of order 12. Punime Mat. No.2 (1987) 9-11.

[25] K. Horvatic-Baldasar, E. Kramer, I. and Matulic-Bedenic, On a projective plane of order 11 with Frobenius group of order 21, Rad. Mat. **6** (1990) 71-76.

[26] D.R. Hughes and F.C. Piper , *Projective Planes*, Berlin-Heidelbelg-New York, Springer, 1973

[27] B. Huppert, *Endliche Gruppen Bd. 1*, Springer-Verlag, Berlin, 1067.

[28] Z.Janko and T. van Trung, Projective plane of order 12 do not have a four group as a collineation group , J. of Combin. Ser. A **32** (1982), 401-404.

[29] M. Kallaher, Translation Planes *Handbook of Incidence Geometry*, ed. F. Buekenhout, Elsevier Science B. V. , 1995

[30] M. Kallaher, *Affine Planes with Transitive Collineation Groups*, North-Holland, New York/ Amsterdam/Oxford, 1982.

[31] W. M. Kantor, Projective planes of type I-4, Geom. Ded. **3** (1974), 335-346.

[32] D. E. Knuth, Finite semifields and projective planes, J. of Algebra **2** (1965) 182-217

[33] P.V. Kumar, On the existence of square dot-matrix patterns having a specified three-valued periodic correlation function, IEEE Trans. Inf. Th. **34** (1988), 271-277.

[34] C.W.H Lam, L. Thiel and S. Swiercz, The nonexistence of finite projective plane of order 10, Canad. J. **41** (1989), 1117-1123.

[35] C.W.H Lam, G. Kolesva and L. Thiel, A computer search for finite projective plane of order 9, Discrete Math. **92** (1991), 187-195.

[36] E.S. Lander, *Symmetric Designs: An Algebraic Approach*, Cambridge Univ. Press, New York, Springer, 1983

[37] R. A. Liebler, Autotopism group representations, J. London Math. Soc. **23** (1981), 85-91.

[38] H. Luneburg, *Translation planes*, Berlin-Heidelbelg-New York, Springer, 1980

[39] K.H. Leung, S.L. Ma and V. Tan, Planar functions from $\mathbb{Z}_n$ to $\mathbb{Z}_n$, preprint.

[40] S.L. Ma and A. Pott, Relative difference sets, planar functions, and generalizes Hadamard matrices, J. Algebra **175** (1995), 505-525.

[41] S.L. Ma, Planar functions, relative difference sets and character theory, J. Algebra **185** (1996), 342-356.

[42] H. B. Mann, *Addition Theorems*, Wiley, New York, 1965.

[43] I. Matulic-Bedenic, Projective planes of order 11 with a collineation group of order 5, Rad. Jugoslav. Akad. Znan. Umjet. **413** (1984) 39-43.

[44] I. Matulic-Bedenic, A new characterization of the Desarguesian plane of order 11, Algebras Groups Geom. **2** (1985) 428-435.

[45] I. Matulic-Bedenic, The classification of projective planes of order 11 which possess an involution, Rad. Mat. **1** (1985) 149-157.

[46] Ida Matulic-Bedenic, The classification of projective planes of order 13 which possess an involution, Rad Hrvatske akad. znan. umj. mat. **10** (1991), 9-13.

[47] U. Ott, Endliche zyklische Ebenen, Math. Z. **144** (1975) 195-215.

[48] A. Pott, On the structure of abelian groups admitting divisible difference sets, J. of combin. Ser. A **65** (1994), 202-213.

[49] A. Pott, On projective planes admitting elations and homologies, Geom. Ded.**52** (1994), 181-193.

[50] L. Ronayi and T. Szonyi, Planar functions over finite fields, Combinatorica **9** (1989), 315-320.

[51] H. J. Ryser, Matrices with integer elements in combinatorial investigations, Amer. J. Math. **74** (1952) 769-773.

[52] C. Suetake, On projective planes of order 15 admitting a collineation of order 7, Geom. Dedicata **81** (2000), 61-86.

[53] J. G. Thompson, Incidence matrices of finiteprojective planes and their eigenvalues, J. Algebra **191** (1997), 265-278.

[54] H. A. Wilbrink, A note on planar difference sets, J. of Combin. Ser. A **38** (1985) 94-95.