数理解析研究所講究録
1063 巻 1998 年 30-40

A 72-arc associated with the A_6-invariant sextic

岡山大学理学部　　兼田　均　(Hitoshi Kaneta)

0 Introduction

We shall show that some highly symmetric curves give highly symmetric arcs. Let C be a compact Riemann surface with genus g. If $g \geq 2$, then the order of the automorphism group $G(C)$ of C is bounded by $84(g-1)$(Hurwitz inequality). If $g=3$, a compact Riemann surface attains the upper bound if and only if C is isomorphic to the Klein quartic $x^3y+y^3z+z^3x$. As is well known, the automorphism group of the curve is isomorphic to $PSL(2,7)$. If $g=10$, the maximum order of the automorphim groups is not known. A. Wiman [3], however, has shown that the Wiman sextic $F_6=10x^3y^3+9(x^5+y^5)z-45x^2y^2z^2-135xyz^4+27z^6$ has the automorphim group isomorphic to $A_6 \simeq PSL(2,9)$, and that the group acts transitively on the set of flexes. Recall that an automorphim of a non-singular plane curve (defined over $\mathbf{C}$) of degree $n \geq 4$ is given by a projective transformation [2, theorem 5.3.17(3)].

An n-point set K_n in the r-dimensional projective space $PG(r,k)$ defined over a field k is called an n-arc, if any $r+1$ points of them are linearly independent. We write $PG(r,q)$ for $PG(r,GF(q))$, where $GF(q)$ is the finte field of q elements.

Following theorems are our main results.

Theorem 1 *Let k be an algebraically closed field with* char $k \neq 7$. *Then the 24-point set $\mathcal{F}_{24}$ of flexes of the Klein quartic is a 24-arc in $PG(2,k)$ if and only if* char $k \neq 2$. *$\mathcal{F}_{24}$ lies in $PG(2,q)$ if and only if $7 \mid (q-1)$.*

Theorem 2 *Let k be an algebraically closed field with* char $k \neq 2,3,5$. *Then*
(1) *The 72-point set $\mathcal{F}_{72}$ of flexes of the Wiman sextic F_6 is a 72-arc in $PG(2,k)$ if and only if* char $k \neq 11,19,31,61$.
(2) *$\mathcal{F}_{72}$ lies in $PG(2,q)$,if $30 \mid (q-1)$.*

More detailed results on the Klein quartic and the Wiman sextic are summarized in the follwoing §1 and §2 respectively without proof in principle.

These results were obtained in collabration with F. Pambianco and S. Marcugini who are combinatorial geometers at Department of Mathematics of Perugia University, Perugia, Italy.

Definition. Let B, $C \in PGL(3,k)$, and let $f \in k[x,y,z]$. Then the map $f \to f_B$ is a ring-isomorohism of $k[x,y,z]$, where $f_B(x,y,z) = f(B^{-1}(x,y,z))$. To be precise $f(B^{-1}(x,y,z)) = f({}^t\{B^{-1}\,{}^t(x,y,z)\})$. It is known that $(f_B)_C = f_{CB}$. Let $f \in k[x,y,z]$ be a homogeneous polynomial of degree n (or a plane curve f of degree n). The curve f is said to be invariant under a projectivity (B) if $f_B \sim f$. More generally let G be a subset of $PGL(3,k)$. Then a homogeneous polynomial f (or a curve f) is called G-invariant if f is invariant under every $(B) \in G$. Aut(f) is the set of projectivities (B) such that $f_B \sim f$.

1 The Klein quartic

Obviously $\xi = 5$ is a primitive element of the Galois field $GF(7)$. A representaionφ of $PSL(2,7)$ in the projective plane $PG(2,k)$ over k(i.e. group homomorphism of $PSL(2,7)$ into the projective transformation group $PGL(3,k)$) is completely determined by the images $\varphi((u))$, $\varphi((v))$, and $\varphi((w))$, where matrices u, v, and w take the following forms:

$$u = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad v = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad \text{and } w = \begin{bmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{bmatrix}.$$

An $A \in GL(3,k)$ gives a projective transformation (A) of $PG(2,k)$ in the usual manner:

$$(A)\left(\begin{bmatrix} x \\ y \\ z \end{bmatrix}\right) = \left(A\begin{bmatrix} x \\ y \\ z \end{bmatrix}\right).$$

We shall describe all injective homomorphisms φ of $PSL(2,7)$ into $PGL(3,k)$. To this end it suffices to define matrices U, V, and W such that

$$\varphi((u)) = (U), \quad \varphi((v)) = (V), \quad \text{and } \varphi((w)) = (W).$$

Let ε be a primitive 7-th root of 1, and let

$$\begin{aligned} U &= \operatorname{diag}[\epsilon, \epsilon^4, \epsilon^2] \text{ and} \\ V &= \begin{bmatrix} \alpha & \beta & \gamma \\ \beta & \gamma & \alpha \\ \gamma & \alpha & \beta \end{bmatrix}, \text{where } \alpha = \varepsilon + \varepsilon^6, \ \beta = -1 - \varepsilon^2 - \varepsilon^5, \ \text{and}\gamma = 1 \\ W &= [e_3, e_1, e_2], \text{ where } E_3 = [e_1, e_2, e_3]. \end{aligned}$$

If $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL(2,7)$, then we define $\varphi((M))$ as follows:

$$\begin{aligned} \varphi((M)) &= (U^{\frac{a}{c}} V U^{cd} W^{\log c}) \text{ if } c \neq 0 \\ \varphi((M)) &= (U^{\frac{b}{d}} V U^{-cd} W^{-\log d}) \text{ if } d \neq 0. \end{aligned}$$

Theorem 1. 1 *Assume that the field k is algebraically closed and* char$k \neq 7$.
(1) *The map φ defined above is an isomorphism of $PSL(2,7)$ into $PGL(3,k)$.*
(2) *Any automorphism τ of the field k fixes $\varphi(PSL(2,7))$.*
(3) *Let ψ be an isomorphism of $PSL(2,7)$ into $PGL(3,k)$. Then there exists an automorphism σ of k and a $T' \in GL(3,k)$ such that $\psi((g)) = \sigma((T')^{-1}\varphi((g))(T'))$ for any $(g) \in PSL(2,7)$. In particular the groups $\varphi(PSL(2,7))$ and $\psi(PSL(2,7))$ are conjugate in $PGL(3,k)$.*

The plane cueve $f = x^3y + y^3z + z^3x$ is called the Klein quartic, which we denote by C.

Lemma 1. 2 *The curve C defined over an algebraically closed field k is non-singular if and only if* char$k \neq 7$.

It is a classical result that a non-singular plane quartic with the projective automorphism group Aut(f) such that $7|\ |\mathrm{Aut}(f)|$ is projectively equaivalent to the the Klein quartic. Consider the following curve or polynomial called Hessian of f;

$$h(x,y,z) = \det \begin{bmatrix} f_{xx} & f_{xy} & f_{xz} \\ f_{yx} & f_{yy} & f_{yz} \\ f_{zx} & f_{zy} & f_{zz} \end{bmatrix} = \det \begin{bmatrix} 6xy & 3x^2 & 3z^2 \\ 3x^2 & 6yz & 3y^2 \\ 3z^2 & 3y^2 & 6xz \end{bmatrix} = -54h_0(x,y,z),$$

where $h_0(x,y,z) = xy^5 + yz^5 + zx^5 - 5x^2y^2z^2$. Let $A = [a_{ij}] \in GL(3,k)$. The matrix A induces a ring automorphism R_A of the polynomial ring $k[x,y,z]$ as follows; $(R_A\, p)(x,y,z) = p_A(x,y,z) = p(A^{-1}[x,y,z])$, where $p \in k[x,y,z]$. It is known that $R_{AB} = R_A R_B$, that is, $p_{AB} = (p_B)_A$. We say that a homogeneous polynomial $p \in k[x,y,z]$(or a curve p) is invariant under a projectivity (A) if $p_A \sim p$, in other words, if there exists a constant $\lambda \in k$ such that $p_A = \lambda p$.

Proposition 1. 3 *Assume that* char$k \neq 7$. *The polynomials f and h_0 defined above are invariant under every element of $\varphi(SL(2,7))$, where φ is the group isomorphism defined in the previous section.*

A point $(x,y,1)$ lies on the Klein quartic C if and only if $x^3y + y^3 + x = 0$. Therefore $(0,0,1)$ is a flex of C. If char$k \neq 2,3,7$, then the set of flexes is the intersection of f and h_0, and $|f \cap h_0| \leq 4 \times 6$.

Lemma 1. 4 *The orbit $\mathcal{F}_{24}$ of $(0,0,1)$ under the group $\varphi(PSL(2,7))$ consisits of 24 points, and $\mathcal{F}_{24} = f \cap h_0$.*

Theorem 1. 5 *The 24-point set $\mathcal{F}_{24}$ in* Lemma 2,3 *is an arc if* char$k \neq 2,7$, *and not an arc if* char =2.

Proof. Let $P_1 = (1,0,0)$, $P_2 = (0,1,0)$, $P_3 = (0,0,1)$ and $\mathcal{F}' = \mathcal{F} \backslash \{P_3\}$. Since $P_3 \in f \cap h_0$, and both f and h_0 is invariant under $\varphi(PSL(2,7)$, $\mathcal{F} \subset f \cap h_0$. By Bezous's theorem $\mathcal{F} = f \cap h_0$. We shall show that there exist non lines L through P_3 such that $|L \cap \mathcal{F}'| \geq 2$. Since the line x and y do not satisfy the condition, we will show that there exist no lines $L : y = ax$ $(a \neq 0)$ through P_3 such that $|L \cap \mathcal{F}'| \geq 2$. Clearly $f \cap z = \{P_1, P_2\}$. So L passes through a point $(x,y,1) \neq (0,0,1)$ such that $f(x,y,1) = h_0(x,y,1) = 0$. Hence the following two polynomials in x must have at least two common roots, which are evidently non-zero:

$$p = ax^3 + a^3x^2 + 1, \quad q = a^5x^5 + x^4 - 5a^2x^3 + a$$

Conversely, if p and q have at least two common roots x, then $x \neq 0$, and $a \neq 0$ so that the line $y = ax$ satisfies the condition $|L \cap \mathcal{F}'| \geq 2$. We have

$$q = (a^4x^2 + a)p + x^2r, \quad \text{where} \quad r = (1 - a^7)x^2 - 6a^2x - 2a^4.$$

This implies that if char $k = 2$, then p divides q for a such that $a^7 = 1$. In other words, the $|\mathcal{F} \cap y - ax| = 3 + 1$, for p has no multiple roots, and $\mathcal{F}$ is not an arc, provided char$k = 2$. If $a^7 = 1$, then p and q have at most one root in common. We may assume $a^7 \neq 1$. The common roots of p and q are those of p and r. We may assume that r has no multiple roots, namely $2a^7 \neq 11$. Hence r must divide p. Thus, by simple calculation we conclude that a polynomial $a^5(44 - 8a^7)x + (1 - a^7)^2 + 2a^7(7 - a^7)$ must vanish. However the coefficient of x cannot vanish. We have shown that there does not exist an $a \neq 0$ such that p and q have at least two roots in common.

Theorem 1. 6 *If the projective automorphims group Aut($\mathcal{K}$) of a 24-point set $\mathcal{K}$ in $PG(2,k)$ has a subgroup isomorphic to $PSL(2,7)$, then $\mathcal{K}$ is projectively equivalent to $\mathcal{F}_{24}$.*

2 The Wiman sextic

Let F_6 be the Wiman sextic:

$$F_6 = 10x^3y^3 + 9(x^5+y^5)z - 45x^2y^2z^2 - 135xyz^4 + 27z^6.$$

Lemma 2. 1 *F_6 is non-singular if and only if* char $k \notin \{2,3,5\}$.

From now on we asssume that char $k \notin \{2,3,5\}$. Wiman has shown that $\mathrm{Aut}(F_6)$ is isomorphic to A_6 and that $\mathrm{Aut}(F_6)$ acts transitively on the set $\mathcal{F}_{72}$ of flexes of the curve (defined over $\mathbf{C}$). One can verify the latter assertion immediately by the following Lemma 2.2, provided $|\mathrm{Aut}(F_6)| \geq 360$, because we know that there are at most 72 flexes for a plane sextic.

Lemma 2. 2 (1) *$P_1 = (1,0,0)$ and $P_2 = (0,1,0)$ are flexes of F_6.*
(2) *A projectivity (B) $\in Aut(F_6)$ fixes $P_2 = (1,0,0)$, if and only if $B \sim \mathrm{diag}[1,\beta,\beta^3]$ where $\beta^5 = 1$.*
(3) *An involutive projectivity (C) fixes $P_3 = (0,0,1)$ and F_6, if and only if*

$$C \sim \begin{bmatrix} 0 & \beta & 0 \\ \beta^4 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Theorem 2. 3 *Assume that* char $k \notin \{2,3,5\}$. *$\mathcal{F}_{72}$ is an arc in $PG(2,k)$ if and only if* char $k \notin \{11,19,31,61\}$.

Proof. Note that $P_1=(1,0,0) \in \mathcal{F}_{72}$. We use the fact that $\mathrm{Aut}(F_6) \cong A_6$, hence it acts transitively on $\mathcal{F}_{72}$ by Lemma 1.2. This has been proved by Wiman in the case $k = \mathbf{C}$, and will be proved in §3 for any algebraically closed field k with char $k \notin \{2,3,5\}$. Consequently $\mathcal{F}_{72}$ is an arc if and only if there pass 71 lines ℓ through P_1 such that $|\ell \cap F_{72}| \geq 2$. A line through P_1 takes the form $by + cz = 0$. Note that if $c = 0$, then P_1 is the only point both on the line and $\mathcal{F}_{72}$. Other lines take the form $z = ay$. It can be easily seen that the line $z = 0$ intersects K_{72} at P_1 and $P_2 = (0,1,0)$. Now $\mathcal{F}_{72}$ is an arc if and only if there exist 70 lines ℓ: $z = ay (a \neq 0)$ satisfying $|\ell \cap \mathcal{F}_{72}| \geq 2$. Recall that $P \in \mathcal{F}_{72}$ if and only if $F_6(P) = H_{12}(P) = 0$, where H_{12} is the Hessian of F_6[1, p.116(see the proof given there)]:
$F_6 = 10x^3y^3 + 9(x^5+y^5)z - 45x^2y^2z^2 - 135xyz^4 + 27z^6$
$H_{12} = 2 \cdot 3^4 \cdot 5^3$

$$\times \begin{bmatrix} -6(x^{11}y+xy^{11}) + 38x^6y^6 & -90(x^8y^3+x^3y^8)z & +\{9(x^{10}+y^{10}) + 468x^5y^5\}z^2 \\ -1080(x^7y^2+x^2y^7)z^3 & -3375x^4y^4z^4 & +324(x^6y+xy^6)z^5 \\ +1080x^3y^3z^6 & -2916(x^5+y^5)z^7 & -1215x^2y^2z^8 \\ -4374xyz^{10} & -729z^{12} & \end{bmatrix}.$$

We define polynomials f_5 and h_{11} by

$$F_6(1,y,ay) = yf_5(y), \quad H_{12}(1,y,ay) = 2 \cdot 3^4 \cdot 5^3\ yh_{11}(y):$$

$f_5 = 27y^5a^6 + 9y^5a - 135y^4a^4 - 45y^3a^2 + 10y^2 + 9a$
$h_{11} = -729y^{11}a^{12} - 2916y^{11}a^7 + 9y^{11}a^2 - 4373y^{10}a^{10} + 324y^{10}a^5 - 6y^{10}$
$- 6y^{10} - 1215y^9a^8 - 1080y^9a^3 + 1080y^8a^6 - 90y^8a$
$- 3375y^7a^4 - 2196y^6a^7 + 468y^6a^2 + 324y^5a^5 + 38y^5$
$- 1080y^4a^3 - 90y^3a + 9ya^2 - 6.$
It is obvious that a point P=(x, y, z) on the line ℓ: $z = ay(a \neq 0)$ coincides with P_1, if and only if $y = 0$. So the line ℓ: $z = ay(a \neq 0)$ satisfies $|\ell \cap F_{72}| \geq 2$ if and only if there exists a solution y to the equations

$$f_5(y) = 0, \quad h_{11}(y) = 0.$$

The latter condition holds if and only if the resultant $R(f_5, h_{11})$ is equal to zero. Indeed, the coefficients $27a^6$ and $-729a^{12}$ of the leading terms are not equal to zero, because char $k \neq 3$ and $a \neq 0$. By computer we get
$R(f_5, h_{11}) = 10^5 \cdot 25^2 \cdot 5 \cdot 3^7 a\, r(a^5)$, where the polynomial $r(b)$ in b takes the form

$-16010094431679906 24b^{14}$
$-800806578572759276898 9b^{13}$
$-35220078835389935057 34b^{12}$
$-1075449394283195028547 89b^{11}$
$-2225677590261675159296 49b^{10}$
$+914627058057499275964 98b^{9}$
$+156260591347850873457 03b^{8}$
$+5027576633722185810 93b^{7}$
$+193529026780405284 78b^{6}$
$+3169967197928921 73b^{5}$
$+126821594856500 1b^{4}$
$+4040019551028 6b^{3}$
$-13463272359b^{2}$
$-371960 64b$
$-1024.$

Note that the coefficient of b^{14} is equal to $-2^5 \cdot 3^{35} (\neq 0)$. Now $\mathcal{F}_{72}$ is an arc if and only if the polynomial $r(b)$ of degree 14 has no multiple roots. Again by computer we get the value of the resultant $R(b, b')$. It has 503 decimal digits, and its prime factors are 2,3,5,11,19,31, and 61.

The alternating group A_6 of order 6 is known to be isomorphic to $PSL(2, 3^2)$. We turn to the problem to describe all non-trivial representaions of $PSL(2, 3^2)$ in $PGL(3, k)$ up to equivalence . Two representaions of ψ and φ is said to be equivalent, if there exists an $S \in GL(3, k)$ such that $\psi(g)$=$(S^{-1})\psi(g)(S)$ for every $g \in PSL(2, 3^2)$, where (S) is a projective transformation of $PG(2, k)$ such that $(S)([x])$=(Sx). Here $x \in k^3$ is a homogeneous coordinates of a point $([x]) \in PG(2, k)$. $GF(3^2)$ is the finite field of characteristic 3, which has a primitive element η satisfying η^2=$\eta + 1$. For our later use, we note that

$$\eta^2 = \eta + 1, \quad \eta^3 = 2\eta + 1, \quad \eta^4 = -1, \quad \eta^5 = 2\eta, \quad \eta^6 = 2\eta + 2, \quad \eta^7 = \eta + 2.$$

A representaion(i.e. group homomorphism)φ of $PSL(2,3^2)$ is completely determined by the images $\varphi((g_1))$, $\varphi((g_2))$, $\varphi((g_3))$, and $\varphi((g_4))$, where

$$g_1 = \begin{bmatrix} \eta & 0 \\ 0 & \eta^{-1} \end{bmatrix}, \quad g_2 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad g_3 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad \text{and} \quad g_4 = \begin{bmatrix} 1 & \eta \\ 0 & 1 \end{bmatrix},$$

and $(g_i)\in PSL(2,3^2)$ for $g_i \in SL(2,3^2)$. In other words it suffices to specify matrices A, V, Ω and W in $GL(3,k)$ such that

$$\varphi((g_1)) = (A), \quad \varphi((g_2)) = (V), \quad \varphi((g_3)) = (\Omega), \quad \text{and} \quad \varphi((g_4)) = (W).$$

Let ω(resp. i) be a primitive 3-th(resp. 4-th) root of $1\in k$, and $\sqrt{5}$ be a square root of $5\in k$.

Theorem 2. 4 (1) *Under the above notation there exists a homomorhism φ of $PSL(2,3^2)$ into $PGL(3,k)$ such that*

$$A = \begin{bmatrix} \omega & 1 & \omega \\ 1 & \omega & \omega \\ 1 & 1 & \omega^2 \end{bmatrix}, \quad V = \begin{bmatrix} 2 & -4 & -\omega^2+\sqrt{5}(\omega-1) \\ -4 & 2 & -\omega^2+\sqrt{5}(\omega-1) \\ -\omega+\sqrt{5}(\omega^2-1) & -\omega+\sqrt{5}(\omega^2-1) & 2 \end{bmatrix},$$

$$\Omega = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{bmatrix}, \quad \text{and} \quad W = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

(2) *Any injective homomorphism ψ of $PSL(2,3^2)$ into $PGL(3,k)$ is equivalent to this φ.*

Remark 2. 5 (1) Note that ω and $\sqrt{5}$ have two possible values. So φ gives rise to four representaions. However, it turns out that these four groups $\varphi(PSL(2,3^2))$ are cunjugate in $PGL(3,k)$(*Corollary* 2.14).
(2) Clearly $\Omega^3 = W = E_3$ and $\Omega W \sim W\Omega$. Furthermore, let

$$T = \begin{bmatrix} 1 & 1+\omega i & 1-\omega i \\ -1 & 1+\omega i & 1-\omega i \\ 0 & 1-i & 1-i \end{bmatrix}, \text{ so } T^{-1} = \frac{1}{4i(\omega-1)} \begin{bmatrix} 2(\omega-1)i & -2(\omega-1) & 0 \\ 1-i & 1-i & 2(-1+\omega i) \\ -1-i & -1-i & 2(1+\omega i) \end{bmatrix}.$$

Here i is a primitive 4-th root of $1 \in k$. Then it holds that

$$T^{-1}AT = (\omega-1)\begin{bmatrix} 1 & 0 & 0 \\ 0 & i & 0 \\ 0 & 0 & i^3 \end{bmatrix}, \quad \text{and} \quad T^{-1}VT = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & c \\ 0 & b & 0 \end{bmatrix},$$

where $bc = 1$, and

$$b^2 + \frac{\omega^2-\omega+3i}{3}b + \{-2+(\omega^2-\omega)i\} = 0,$$

hence

$$c^2 + \frac{\omega^2-\omega-3i}{3}b + \{-2-(\omega^2-\omega)i\} = 0.$$

In other words, $b = (-\omega+\omega^2+3i)(1\pm\sqrt{5}i)$ and $c = (-\omega+\omega^2-3i)(1\mp\sqrt{5}i)$.

We will search for a plane sextic which is invariant under the projective transformations $\varphi(PSL(2,3^2))$.

Theorem 2. 6 *Let φ be the representation of $PSL(2,3^2)$ given by Theorem 2.2. Then the following homogeneous polynomial is $\varphi(PSL(2,3^2))$-invariant:*

$$\begin{aligned} f_6 &= (x^6+y^6+z^6)\frac{\omega}{30}\{-5-\sqrt{5}(\omega-\omega^2)\} \\ &+x^4yz+xy^4z+xyz^4 \\ &+(x^3y^3+y^3z^3+z^3x^3)\frac{\omega}{3}\{-1+\sqrt{5}(\omega-\omega^2)\} \\ &+x^2y^2z^2 3\omega^2. \end{aligned}$$

A few lemmas preceed the proof of Theorem 2.6

Lemma 2. 7 *Let $B, C, T \in GL(3,k)$ with $C = T^{-1}BT$, and $f \in k[x,y,z]$. If $f_B = \lambda f$, then $(f_{T^{-1}})_C = f_{T^{-1}}$.*

Lemma 2. 8 *Let*

$$f = (x^6+y^6+z^6)C_6 + (x^4ys+xy^4z+xyz^4)C_4 + (x^3y^3+y^3z^3+z^3x^3)C_3 + x^2y^2z^2C_2,$$

where $C_6, C_4, C_3, C_2 \in k$, and let $A \in GL(3,k)$ be as in Theorem 2.4. Then $f_\Omega = f_W = f$, and f is invariant under (A) if and only if one of the following two cases holds.
1) $C_3 = -10C_6 - 2\omega C_4$ *and* $C_2 = 3\omega^2 C_4$.
2) $C_4 = 6\omega^2 C_6$, $C_3 = 2C_6$ *and* $C_2 = 0$.

Lemma 2. 9 *Let f be as in Lemma 2.8. Then f is invariant under (A) and (V)(see Theorem 2.4 for the definition of A and V), if and only if f is proportional to the polynomial f_6 in Theorem 2.6.*

Proof. Assume that f satisfies the invaraince condition. f takes the form given in the previous lemma. Let h be as in the proof of the lemma. We will first show that 2) of Lemma 2.8 does not hold. Let $C_6 = 1$, $C_4 = 6\omega^2$, $C_3 = 2$ and $C_2 = 0$. Then

$$\begin{aligned} h &= 36\{2(1-\omega^2)+3i\omega\}u^4v^2 + 36\{2(1-\omega^2)-3i\omega\}u^2v^4 \\ &+ 144\{1-\omega-3i\omega^2\}u^2v^3w + 144\{1-\omega+3i\omega^2\}u^2vw^3 \\ &+ 36\{3(\omega^2-\omega)+3i\}v^6 + 36\{3(\omega^2-\omega)-3i\}w^6 \\ &+ 108\{2(\omega^2-\omega)+5i\}v^4w2 + 108\{2(\omega^2-\omega)-5i\}v^2w^4 \end{aligned}$$

Since $h_{V'^{-1}} \sim h$, the firsr two terms give

$$b^2 = \frac{2(1-\omega^2)+3i\omega}{2(1-\omega^2)-3i\omega} \text{ and } b^2 = \frac{1-\omega-3i\omega^2}{1-\omega+3i\omega^2}.$$

As one can see easily, these two equalities are not compatible.

By Lemma 2.8 1) h takes the following form:

$$\begin{aligned} h &= u^2v^4\{C_6(-540\omega^2+360\omega i-360i)+C_4(24\omega^2-24\omega i-18)\} \\ &+ u^2w^4\{C_6(-540\omega^2-360\omega i+360i)+C_4(-24\omega^2 i+24\omega i-18\} \\ &+ v^5w\{C_6(-432\omega^2 i-432\omega i-864)+C_4(-144\omega^2 i+-253\omega+144i)\} \\ &+ vw^5\{C_6(-432\omega^2 i+432\omega i-864)+C_4(144\omega^2 i-252\omega-144i)\} \\ &+ u^6\{C_6(12)+C_4(12\omega)\}+u^2v^2w^2\{C_6(1080\omega^2)+C_4(180)\}+v^3w^3\{C_4(-72\omega)\} \end{aligned}$$

Denote by α, β, γ and δ the coefficients of u^2v^4, u^2w^4, v^5w and vw^5 respectively. Since at least one of the coefficients of u^6 and v^3w^3 does not vanish, we must have $h_{V'^{-1}}=h$. The equality $h_{V'^{-1}}=h$ holds if and only if the following two conditions are satisfied.
i) $\alpha=\beta b^4$, ii) $\gamma=\delta b^4$
(recall that $bc=1$). The condition i) is equivalent to

$$\frac{C_6}{C_4}=\frac{(-24\omega^2 i+24\omega i-18)b^4-24\omega^2 i+24\omega i+18}{(360\omega i-360i+540\omega^2)b^4+360\omega i-360i-540\omega^2}.$$

Making use of the equalities

$$b^2+c^2=\frac{8}{3}+\frac{2\sqrt{5}}{3}(\omega-\omega^2) \text{ and } b^2-c^2=\frac{4}{3}i(\omega-\omega^2)+\frac{\sqrt{5}}{3}(-4i),$$

we get $C_6/C_4=-\omega\{5+\sqrt{5}(\omega-\omega^2)\}/30$. Similarly the condition ii) is equivalent $C_6/C_4=-\omega\{5+\sqrt{5}(\omega-\omega^2)\}/30$. Thus f is invariant under (A) and (V) if and only if the coefficeints C_j satisfy the condition (1) of Lemma 2.8 and the ratio C_6/C_4 is equal to $-\omega\{5+\sqrt{5}(\omega-\omega^2)\}/30$.

Proof of Theorem 2.6. Since the sextic f_6 is invariant also under (Ω) and W by Lemma 2.8, it is $PSL(2,3^2)$-invariant by Lemma 2.9.

We proceed to show that the sextic f_6 in Theorem 2.6 is projectively equivalent to the Wiman sextic F_6.

Lemma 2. 10 *Let* $X=\begin{bmatrix} a & b \\ c & d \end{bmatrix}\in SL(2,3^2)\setminus\{\pm E_2\}$. *Then* $(X)\in PSL(2,3^2)$ *has order 5 if and only if* $\mathrm{Tr}X=-1$ *in* $GF(3^2)$.

As a result of Lemma 2.10, $\varphi((g_4g_2))=(WV)$ has order 5. Note that $WV\sim D$, where

$$D=\begin{bmatrix} -\omega+\sqrt{5}(\omega^2-1) & -\omega+\sqrt{5}(\omega^2-1) & 2 \\ 2 & -4 & -\omega^2+\sqrt{5}(\omega-1) \\ -4 & 2 & -\omega^2+\sqrt{5}(\omega-1) \end{bmatrix},$$

and that

$$\det(D-\lambda E_3)=-(\lambda+6)(\lambda^2+3(-1+\sqrt{5})\lambda+36)=-6(\delta+1)(\delta^2-\frac{-1+\sqrt{5}}{2}\delta+1),$$

where $\lambda = -6\delta$. Let δ be a solution to $t^2 - \frac{-1+\sqrt{5}}{2}t + 1 = 0$. The another solution δ' to this quardratic equation is $-\delta + \frac{-1+\sqrt{5}}{2}$. Let e_1, e_2 and e_3 be eigenvectors of D for eigenvalues -6δ, $-6\delta'$ and -6 respectively;

$$e_1 = \begin{bmatrix} 6 - \omega^2 + \sqrt{5}(\omega - 1) + \delta\{6 - \omega + \sqrt{5}(-\omega - 2)\} \\ -\omega^2 + \sqrt{5}(\omega - 1) + 2\delta \\ 2 - 4\delta \end{bmatrix},$$

$$e_2 = \begin{bmatrix} \omega^2 + \sqrt{5}(\omega + 3) + \delta\{-6 + \omega + \sqrt{5}(\omega + 2)\} \\ \omega + \sqrt{5}\omega - 2\delta \\ 4 - 2\sqrt{5} + 4\delta \end{bmatrix},$$

$$e_3 = \begin{bmatrix} 2 \\ -2 + \omega^2 - \sqrt{5}(\omega - 1) \\ 2 \end{bmatrix}.$$

The following matrix

$$I = \begin{bmatrix} -4 & 2 & -\omega^2 + \sqrt{5}(\omega - 1) \\ 2 & -4 & -\omega^2 + \sqrt{5}(\omega - 1) \\ -\omega + \sqrt{5}(\omega^2 - 1) & -\omega + \sqrt{5}(\omega^2 - 1) & 2 \end{bmatrix}$$

satisfies $I^2 = 36E_3$,$Ie_1 = -6\alpha e_2$, $Ie_2 = -6\beta e_1$ and $Ie_3 = -6e_3$ for some constants α and β. $\alpha\beta = 1$, because $I^2 = 36E_3$. Consequently $Q = 6[\beta e_1, e_2, e_3]$ diagonalizes I as

$$Q^{-1}IQ = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \text{because} \quad IQ = Q\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad (= 6[e_2, \beta e_1, e_3]).$$

In terms of $\lambda = -6\delta$ satisfying $\lambda^2 = 3(1 - \sqrt{5})\lambda - 36$ the matrix Q takes the following form:

$$\begin{bmatrix} 6(-3 + 3\sqrt{5}) + \lambda(4 - 2\sqrt{5}) & 6\{\omega^2 + \sqrt{5}(\omega + 3)\} + \lambda\{6 - \omega - \sqrt{5}(\omega + 2)\} & Q_{13} \\ 12(\omega - 1) + \lambda(\omega + \sqrt{5}) & 6(\omega + \sqrt{5}\omega) + 2\lambda & Q_{23} \\ 12(\omega - \omega^2) + \lambda\{\omega^2 + \sqrt{5}(2 - \omega^2)\} & 6(4 - 2\sqrt{5}) - 4\lambda & Q_{33} \end{bmatrix},$$

where $Q_{13} = 12$, $Q_{23} = 6\{-2 + \omega^2 - \sqrt{5}(\omega - 1)\}$, $Q_{33} = 12$.

Since $(\sqrt{5})^2 = 5$, $\omega^2 = -\omega - 1$, and $\lambda^2 = 3(1 - \sqrt{5})\lambda - 36$, the coefficients of the polynomial $(f_6)_{Q^{-1}}$ take the form

$$n_0 + (n_{11}\omega + n_{12}\lambda + n_{13}\sqrt{5}) + (n_{21}\omega\lambda + n_{22}\omega\lambda\sqrt{5} + n_{23}\lambda\sqrt{5}) + n_3\omega\lambda\sqrt{5},$$

where $n_0, n_{11}, n_{12}, n_{13}, n_{21}, n22, n_{23}$, and n_3 are integers(to be precise, we interprete them as elements of the prime field $\mathbf{Z}_p = GF(p)$ of k if char $k{=}p > 0$). Using computer, we get $(f_6)_{Q^{-1}} = (6^6 10)(12^2 3)f$, where

$$\begin{aligned} f &= x^3y^3\{9360 + 900\omega - 80\lambda + 230\omega\lambda + \sqrt{5}(-120 + 1020\omega + 140\lambda - 650\omega\lambda)\} \\ &+ z(x^5 + y^5)\{-2862 - 216\omega + 450\lambda + 90\omega\lambda + \sqrt{5}(1026 + 648\omega - 90\lambda + 90\omega\lambda\} \end{aligned}$$

$$
\begin{aligned}
&+ \quad z^2x^2y^2\{-2160-1620\omega+660\lambda+15\omega\lambda+\sqrt{5}(1620+1620\omega-150\lambda+15\omega\lambda\}\\
&+ \quad z^4xy\{270^1080\omega+135\lambda+90\omega\lambda+\sqrt{5}(-90+360\omega-75\lambda-60\omega\lambda\}\\
&+ \quad z^6\{-48-24\omega+\sqrt{5}(24+12\omega)\}\\
&= \quad 10x^3y^3\{936+90\omega+48\delta-138\omega\delta+\sqrt{5}(-12+102\omega-84\delta+390\omega\delta)\}\\
&+ \quad 9z(x^5+y^5)\{-318-24\omega-300\delta-60\omega\delta+\sqrt{5}(114+72\omega+60\delta-60\omega\delta)\}\\
&- \quad 45z^2x^2y^2\{48+36\omega+88\delta+2\omega\delta+\sqrt{5}(-36-36\omega-20\delta+2\omega\delta)\}\\
&- \quad 135z^4xy\{-2+8\omega+6\delta+4\omega\delta+\sqrt{5}(2-8\omega-10\delta-8\omega\delta)/3\}\\
&+ \quad z^6\{-48-24\omega+\sqrt{5}(24+12\omega)\}\\
&= \quad 10x^3y^3a+9z(x^5+y^5)b-45z^2x^2y^2c-135z^4xyd+z^6e.
\end{aligned}
$$

We will show that there exists an $r \in k$ such that

$$
\begin{aligned}
f(x,y,rz) &= a[10x^3y^3+9z(x^5+y^5)\frac{rb}{a}-45z^2x^2y^2\frac{r^2c}{a}-135z^4xy\frac{r^4d}{a}+z^6\frac{r^6e}{a}\\
&= aF_6
\end{aligned}
$$

The following lemma is easy to prove.

Lemma 2. 11 *The following conditions* (1) *and* (2) *are equivalent.*
(1) $rb/a = f^2c/a = r^4d/a = r^6e/(27a) = 1$.
(2) $r = a/b, b^2 = ac, 27d/e = (a/b)^2, ce = 27d^2$.

Now we are in a position to prove the following

Theorem 2. 12 *The curve*

$$
\begin{aligned}
f_6 &= (x^6+y^6+z^6)\omega\{-5-\sqrt{5}(\omega-\omega^2)\}+xyz(x^3+y^3+z^3)30\\
&+ (x^3y^3+y^3z^3+z^3x^3)10\omega\{-1+\sqrt{5}(\omega-\omega^2\}+x^2y^2z^290\omega^2
\end{aligned}
$$

is projectively equivalent to the Wiman sextic

$$F_6 = 10x^3y^3+9(x^5+y^5)z-45x^2y^2z^2-135xyz^4+27z^6.$$

Proof. Let a, b, c, d, and e be as in Lemma 2.11, and let $r = a/b$, and R=Qdiag$[1,1,r]$. We will show that $(f_6)_{R^{-1}} = aF_6$. Careful calculation shows that

$$
\begin{aligned}
b^2 &= 6^22\{739+1284\omega+2060\delta+1840\omega\delta+\sqrt{5}(-359-964\omega-500\delta-520\omega\delta)\} = ac\\
b^2\frac{27d}{c} &= 3\{14432+11264\omega+3212\delta+2090\omega\delta+\sqrt{5}(-1300+20\omega-5752\delta+386\omega\delta\} = a^2\\
ce &= 24\{-150-264\omega-279\delta-135\omega\delta+\sqrt{5}(66+114\omega+129\delta+63\omega\delta\} = 27d^2.
\end{aligned}
$$

In verifying the second equality above we make use of the equality $1/e = (2+\sqrt{5})(1-\omega)/36$.

Corollary 2. 13 (1) *The projective automorohism group* Aut(F_6) *of* F_6 *has order* 360, *and* Aut(F_6) *acts transitively on the set* $\mathcal{F}_{72}$ *of flexes.*
(2) *If* σ *is an automorphism of* k, *and* $(T) \in$ Aut(F_6), *then* $(\sigma T) \in$ Aut(F_6), *namely* σAut(F_6)=Auf (F_6).

Corollary 2. 14 *Let $R \in PG(3,k)$ be as in the proof of Theorem* 2.12, *and let φ be the representaion of $PSL(2,3^2)$ in Theorem* 2.4.
(1) $\mathrm{Aut}(F_6)$ *is* $(R)^{-1}\varphi(PSL(2,3^2))(R)$. *In particular a subgroup G of $PGL(3,k)$ is isomorphic to $PSL(2,3^2)$, if and only if G is conjugate to* $\mathrm{Aut}(F_6)$ *in $PGL(3,k)$.*
(2) *The set of flexes $\mathcal{F}_{72}$ of F_6 lies in $PG(2,k_1)$, where $k_1 = k_0(\omega,\delta)$, k_0 being the prime field of k. If char $k = p > 0$, then $GF(q)$ contains k_1 if and only if* $30|(q-1)$.

Theorem 2. 15 *Let* char $k \notin \{2,3,5\}$. *An A_6-invariant sextic in $PG(2,k)$ is projectively equivalent to the Wiman sextic F_6.*

Theorem 2. 16 *Let* char $k \notin \{2,3,5\}$. *If the projective automorphims group* $\mathrm{Aut}(K)$ *of a 72-point set K in $PG(2,k)$ has a subgroup G which is isomorphic to A_6, and acts transitively on K, then K and $\mathcal{F}_{72}$ are projectively equivalent.*

References

[1] W. Fulton: Algebraic Curves, Addison-Wesley, 1989.

[2] M. Namba: Geometry of Projective Algebraic Curves, Marcel Dekker, INC, 1984.

[3] A. Wiman: Ueber eine einfache Gruppe von 360 ebenen Collineationen, Math. Annal. bd. **47**(1896).

現在の所属機関　大阪府立大学工学部数理工学科