Innovations in Incidence Geometry
Volume 4 (2006), Pages 103–108
ISSN 1781-6475

ACADEMIA PRESS

On finite projective planes defined by planar monomials

Ulrich Dempwolff   Marc Röder

Abstract

In this note we determine the automorphism groups of finite projective planes defined by monomial planar functions. We also decide the isomorphism problem for such planes.

Keywords: planar polynomials, projective planes, automorphism groups

MSC 2000: 51E35,51A40

1 Introduction

Let M, N be finite groups. A map $f\colon M \to N$ is called a *planar function* [6], [7] if for every $1 \neq a \in M$ the mapping $\Delta_{f,a}\colon M \to N,\ x \mapsto f(ax)f(x)^{-1}$ is a bijection. One can define an affine plane $\mathbf{A}(f)$ by taking as points the elements of the group $M \times N$. The lines are defined by:

$$L_0(a,b) = \{(x,y) \mid x \in M,\ y = f(xa^{-1})b\},\ (a,b) \in M \times N,$$
$$L_0(c) = \{(c,y) \mid y \in N\},\ c \in M.$$

The projective completion $\mathbf{P}(f)$ is obtained by adding the symbols $(\infty), (a)$; $a \in M$, to the point set and adding a new line $L_\infty = \{(\infty), (a) \mid a \in M\}$. The old lines are extended by $L(a,b) = L_0(a,b) \cup \{(a)\}$ and $L(c) = L_0(c) \cup \{(\infty)\}$. The natural action of the group $M \times N$ induces a group of collineations which is faithful and regular on the affine points $M \times N$ and has on L_∞ the orbits $L_\infty - \{(\infty)\}$ and $\{(\infty)\}$. The group N induces the full group of translations with axis L_∞ and center (∞).

In [5] Coulter and Matthews consider the special case where $M \simeq N \simeq F$ is the additive group of $F = \mathrm{GF}(p^n)$ for an odd prime p. A mapping on F can be described uniquely by a polynomial $f \in F[X]$ of degree $< p^n$. Note that $\mathbf{P}(f) \simeq \mathbf{P}(g)$ if $g = f^{p^k}$, k arbitrary. It is known [7] that $\mathbf{P}(X^2)$ is desarguesian and $\mathbf{P}(X^{p^a+1})$, $0 < a < n$, is a commutative twisted semifield plane if $n/(n,a)$ is odd. Coulter and Matthews show that for $p = 3$ and α odd the planes $\mathbf{P}(X^{(3^\alpha+1)/2})$, with $(\alpha, n) = 1$ and $\alpha \not\equiv \pm 1 \pmod{2n}$, are not translation planes. We extend these investigations on monomial planar functions and show:

Theorem 1.1. *Let X^m and $X^{m'}$ be planar functions on $F \simeq \mathrm{GF}(p^n)$.*

(a) *$\mathbf{P}(X^m)$ and $\mathbf{P}(X^{m'})$ are isomorphic iff $m' \equiv mp^k \pmod{p^n}$ for a suitable k.*

(b) *$\mathbf{P}(X^m)$ is a translation plane or a dual translation plane iff this plane is desarguesian with $m \equiv 2p^k \pmod{p^n}$ or a commutative twisted semifield plane with $m \equiv (p^a+1)p^k \pmod{p^n}$, $0 < a < n$, and $n/(n,a)$ odd.*

The automorphism groups of the desarguesian planes and the twisted semifield planes are known [1], [2], [3]. For the remaining cases we have:

Theorem 1.2. *Assume that $\mathbf{P}(X^m)$ is not a translation plane. Then*

$$\mathrm{Aut}(\mathbf{P}(X^m)) \simeq \Gamma \cdot (F \times F),\ \Gamma \simeq \Gamma\mathrm{L}(1, p^n).$$

This theorem shows that in the case of a non translation plane the "obvious" automorphisms comprise the full automorphism group. Note that $F \times F$ corresponds to the group $M \times N$. An element $a \in F^*$ induces the automorphism $\varepsilon_a \colon (x, y) \mapsto (ax, a^m y)$ and the Frobenius automorphism induces the collineation $\delta \colon (x, y) \mapsto (x^p, y^p)$.

2 The proofs

The following lemma is well known:

Lemma 2.1. *Let Z be a cyclic group of order $p^n - 1$, V an n-dimensional $\mathrm{GF}(p)$-space and $D \colon Z \to \mathrm{GL}(V)$ a faithful representation.*

(a) *Let $D' \colon Z \to \mathrm{GL}(V)$ be an irreducible representation. Then D' is equivalent to a representation $D^k \colon Z \to \mathrm{GL}(V)$ for a suitable value $k \in \{0, \ldots, p^n - 1\}$ where D^k is defined by $D^k(x) = D(x)^k$.*

(b) *Two irreducible representations D^k and D^ℓ are equivalent if and only if $\ell \equiv kp^a \pmod{p^n}$ with $0 \leq a < n$ suitable.*

Let $\mathbf{P} = \mathbf{P}(X^m)$ be a projective plane as defined in the introduction with respect to the group $M \times N \simeq F \times F$. Use the notation from the end of the introduction and denote by $Z \simeq F^*$ the cyclic group generated by the mappings $\varepsilon_a \colon (x, y) \mapsto (ax, a^m y)$ and by $D \simeq C_n$ the group generated by $\delta \colon (x, y) \mapsto (x^p, y^p)$. Set further $A = \mathrm{Aut}(\mathbf{P}(X^m))$ and $A_0 = DZMN$.

Lemma 2.2. *Assume that* $\mathbf{P}$ *is not a translation plane or a dual translation plane.*

(a) *A leaves L_∞ and (∞) fixed.*

(b) *N is the group of all central collineations with axis L_∞. In particular $N \trianglelefteq A$.*

(c) *$C_A(N) = \langle z_0 \rangle MN$, where z_0 is the involution in Z. In particular $M = [C_A(N), C_A(N)] \trianglelefteq A$.*

Proof. (a) If L_∞ or (∞) are not fixed by A, suitable conjugates of N would form the translation group with respect to a translation line or a translation point. This contradicts the assumption.

(b) Let K be the group of central collineations with axis L_∞. Assume that $K - N$ contains a translation. Using the action of M we even find a translation $1 \neq \tau$ with center (0). But then $\langle \tau^Z \rangle$ is the full elation group with respect to the flag $((0), L_\infty)$ and $\mathbf{P}$ is a translation plane, a contradiction. Therefore $K - N$ is a set of homologies. If this set is not empty we get (using the group action as before) a homology $1 \neq \kappa$ with center $(0,0)$. The involution z_0 is a homology with axis $L(0)$ and center (0) since m is even [5, Prop. 2.4]. Thus $z_0\kappa = \kappa z_0$. Moreover $[M \times N, \kappa] \leq C_A(N) \cap K = N$ and $[M \times N, z_0] = M$ which shows $[M, \kappa] = 1$. But then M fixes the center $(0,0)$ of κ, a contradiction.

(c) Take $\gamma \in C_A(N)$. Replacing γ by a suitable element from γM we may assume that γ fixes the line $L(0)$. Again replacing γ by a suitable element from γN we may even assume that γ is a central collineation with axis $L(0)$. Assume $\gamma \neq 1$. As γ fixes L_∞ the center of γ lies on this line. If γ is an elation with center (∞) then $\langle \gamma^Z \rangle$ is the full elation group with respect to the flag $((\infty), L(0))$ and $\mathbf{P}$ is a dual translation plane, a contradiction. Thus γ is a homology. If the center of γ is not (0) then $\beta = z_0 z_0^\gamma$ is a central collineation with axis $L(0)$ which is inverted by z_0 and z_0^γ. Hence β is an elation with center (∞). But this case is ruled out already.
So (0) is the center of γ and $C_A(N) = CMN$ with a group C of homologies with respect to the anti flag $((0), L(0))$. The group $C_A(N)/N$ is represented faithfully as a permutation group on $L_\infty - \{(\infty)\}$ and $CN/N \cap (CN/N)^{xN} = 1$ for $xN \in C_A(N)/N - CN/N$. Hence $C_A(N)/N$ is a Frobenius group with Frobenius kernel MN/N. This implies that C normalizes $M = [MN, z_0]$ as

$\langle z_0 \rangle \leq Z(C)$. If $\langle z_0 \rangle < C$ this group has on $L(0,0)$ an orbit containing (at least) three points of the form $(a_1, b), (a_2, b), (a_3, b)$, a contradiction to [5, Prop. 2.4]. □

Proof of Theorem 1.2. Use the bar convention for homomorphic images modulo N. The group $\overline{A}_0$ has a 2-transitive, faithful action on $L_\infty - \{(\infty)\}$. By Lemma 2.2 the group $\overline{M}$ is normal. Hence $\overline{A}/\overline{M}$ is isomorphic to a subgroup of $\mathrm{GL}(\overline{M}_{\mathrm{GF}(p)})$ which contains $\overline{A}_0/\overline{M} \simeq \Gamma\mathrm{L}(1, p^n)$. By [9] we have $\overline{A} \simeq \mathrm{A}\Gamma\mathrm{L}(a, p^b)$ with $ab = n$ (one can also use the classification of the 2-transitive groups, but [9] is more elementary). If $a = 1$ we are done.

So assume $a > 1$. If $a > 2$ then $\overline{A}$ contains an involution xN such that $|C_{L_\infty}(xN)| \neq 1,\ 2,\ p^{n/2}+1,\ p^n+1$. As the coset xN contains an involution this involution is neither a homology nor planar, a contradiction.

Thus $a = 2$. By Lemma 2.2 $A/C_A(N) \simeq \Gamma\mathrm{L}(2, p^{n/2})/\langle -\mathbf{1} \rangle$. Choose $B < A$ such that $B/C_A(N) \simeq \mathrm{PSL}(2, p^{n/2})$. Then $z_0MN \in B/MN \simeq \mathrm{SL}(2, p^{n/2})$. Set $B_0 = C_B(z_0)$. As $M = [M, z_0]$ a Frattini argument shows $B = B_0M,\ B_0 \cap M = 1$. Moreover B_0 induces the group $\mathrm{PSL}(2, p^{n/2})$ on N by conjugation . Choose $u \in B_0$ of order 4 such that $u^2 = z_0$. Then $|C_N(u)| > 1$ as the involutions in $\mathrm{PSL}(2, p^{n/2})$ are conjugate. As u normalizes M we see that $\langle u \rangle$ has on $L(0,0)$ an orbit of length 4 of the form $\{(a_1, b), \ldots, (a_4, b)\}$, a contradiction. □

Proof of Theorem 1.1. If $\mathbf{P}(X^m)$ is a translation plane or a dual translation plane it follows from [5, Cor. 5.12] that $\mathbf{P}$ is a semifield-plane. Using [8] we see that $\mathbf{P}$ is a twisted field plane which is even commutative by [7]. This shows part (b) of Theorem 1.1.

For the nontrivial implication of (a) we assume that $\varphi\colon \mathbf{P} = \mathbf{P}(X^m) \to \mathbf{P}' = \mathbf{P}(X^{m'})$ is an isomorphism. Using the transitivity properties of $A' = \mathrm{Aut}(\mathbf{P}')$ we can assume that (using the notation of the definition) $L_\infty\varphi = L'_\infty$ and the points $(\infty), (0), (0,0)$ of $\mathbf{P}$ are mapped on the corresponding points in $\mathbf{P}'$.

The isomorphism φ induces an isomorphism $\tau\colon A \to A'$ by $\alpha\tau = \varphi^{-1}\alpha\varphi,\ \alpha \in A$. Set $M' = M\tau, N' = N\tau$ etc. The group Z acts on the module $M \times N$ and via τ on the module $M' \times N'$. We denote by $D_M, D_N, D_{M'}, D_{N'}$ the representations on the respective submodules. As τ is an isomorphism of ZMN onto $Z'M'N'$ we have $D_M \sim D_{M'}$ and $D_N \sim D_{N'}$.

Case 1. $\mathbf{P}'$ is not a translation plane. $M \times N$ is characteristic in A by Theorem 2 and therefore $(M \times N)^\tau = M' \times N'$. Moreover Z is characterized as the centralizer in DZ of the commutator subgroup of DZ. Hence $Z' \leq D'Z'$ is precisely the cyclic subgroup of order $p^n - 1$ which induces collineations of type

ε_a on $M' \times N'$. Thus $D_N \sim D_M^m$ and $D_{N'} \sim D_{M'}^{m'}$. This implies $D_M^m \sim D_M^{m'}$. By Lemma 2.1 we have $m' \equiv mp^k \pmod{p^n}$ with a suitable k.

Case 2. $\mathbf{P}'$ is a translation plane. Then both planes are isomorphic semifield planes (desarguesian or commutative twisted semifield planes). Use the notation of the introduction with $M = N = \mathrm{GF}(q)$ and assume that $\mathbf{P}(f)$ is a semifield plane.

Then by [10, 3.4] the multiplication on M defined by $x \circ y = f(x+y) - f(x) - f(y)$ is distributive. By the proof of Theorem 3.5 in [10] one has $f = D + L + c$ where D is a Dembowski-Ostrom polynomial, L is a linearized polynomial, and c is a constant.

This shows that $m = p^a + p^b, a \geq b$, and $m' = p^{a'} + p^{b'}, a' \geq b'$. So $\mathbf{P}(X^m) \simeq \mathbf{P}(X^{p^\ell+1})$ with $\ell = a - b$, and $\mathbf{P}(X^{m'}) \simeq \mathbf{P}(X^{p^{\ell'}+1})$ for $\ell' = a' - b'$. The pigeon hole principle shows $(p^\ell + 1) \equiv (p^{\ell'} + 1)p^c \pmod{p^n}$ or $m' \equiv mp^d \pmod{p^n}$ respectively (c, d suitable). All assertions of Theorem 1.1 are proved. $\square$

Remarks

1. It is easy to see that a commutative semifield plane $\mathbf{P}(F, p^a, p^{-a}, -1)$ is isomorphic to $\mathbf{P}(X^{p^a+1})$, i.e. the automorphism group contains a subgroup $M \times N$ which induces the planar function X^{p^a+1}.

2. The only planes of type $\mathbf{P}(X^m)$ known to the authors are the desarguesian planes, twisted semifield planes and the planes of Coulter and Matthews. See also the discussion in [4].

3. Parts of the proof of Lemma 2.2 apply to any plane $\mathbf{P} = \mathbf{P}(f)$ (f a planar function): If $\mathbf{P}$ is not a translation plane or a dual translation plane then $N \trianglelefteq A = \mathrm{Aut}(\mathbf{P})$, $MN \trianglelefteq A$, and $C_A(N) = HMN$ with a group H of central collineations.

Acknowledgment

The authors would like to thank one of the referees for pointing out reference [10]. This lead to a shorter proof of Theorem 1.1. Remark 3 was prompted by an observation of the other referee.

References

[1] **A. A. Albert**, Isotopy for generalized twisted fields, *Anais Acad. Brasil. Ci.* **33** (1961), 265–275.

[2] ———, On the collineation groups associated with twisted fields, *Calcutta Math. Soc., Golden Jubilee Commem. Vol.* (1958–59), Part 2, (1959), 485–497.

[3] **M. Biliotti**, **V. Jha** and **N. Johnson**, The collineation groups of the generalized twisted field planes, *Geom. Dedicata* **76** (1999), 97–126.

[4] **R. Coulter**, The classification of planar monomials over fields of prime square order, *Proc. Amer. Math. Soc.* **134** (2006), 3373–3378.

[5] **R. Coulter** and **R. Matthews**, Planar functions and planes of Lenz-Barlotti Class II, *Des. Codes Cryptogr.* **10** (1997), 167–184.

[6] **P. Dembowski**, *Finite Geometries*, Springer, 1968.

[7] **P. Dembowski** and **T.G. Ostrom**, Planes of order n with collineation groups of order n^2, *Math. Z.* **103** (1968), 239–258.

[8] **U. Dempwolff**, A characterization of the generalized twisted field planes, *Arch. Math.* **50** (1988), 477–480.

[9] **W. Kantor**, Linear groups containing a Singer cycle, *J. Algebra* **62** (1980), 232–234.

[10] **D. Pierce** and **M. Kallaher,** A note on planar functions and their planes, *Bull. Inst. Combin. Applications* **42** (2004), 53–75.

Ulrich Dempwolff

FACHBEREICH MATHEMATIK, TECHNISCHE UNVERSITÄT KAISERSLAUTERN, GOTTLIEB-DAIMLER-STRASSE, 67663 KAISERSLAUTERN, DEUTSCHLAND

e-mail: `dempw@mathematik.uni-kl.de`

Marc Röder

DEPARTMENT OF MATHEMATICS, NATIONAL UNIVERSITY OF IRELAND, GALWAY, IRELAND

e-mail: `marc.roeder@nuigalway.ie`