JOURNAL OF ALGEBRA 133, 103–110 (1990)

On Planar Functions

YUTAKA HIRAMINE

Department of Mathematics, College of General Education, Osaka University, Toyonaka, Osaka, Japan

Communicated by Walter Feit

Received February 10, 1989

DEDICATED TO PROFESSOR TOSIRO TSUZUKU ON HIS 60TH BIRTHDAY

1. INTRODUCTION

Let n be an arbitrary positive integer and let G and H be groups of the same order n. Given a function f from G into H and a nontrivial element $u \in G^* = G - \{1\}$, we define a *mapping* f_u from G into H as

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

f is said to be a planar function of degree n if f_u is bijective for all $u \in G^*$. P. Dembowski and T. G. Ostrom studied such functions [2, Sect. 5; 3, p. 227] and showed that every planar function from G into H gives rise to an affine plane $S(G, H, f)$ of order n, which is defined in the following way (cf. [3, 5.1.12]).

Points: the elements of the direct product $G \times H$.
Lines: $L(a, b) = \{(x, f(xa^{-1})b) \mid x \in G\}$, $a \in G$, $b \subset H$,
$L(c) = \{(c, y) \mid y \in H\}$, $c \in G$. (*)
Incidence: set theoretic inclusion.

It is an open problem to decide the possible degrees of planar functions. For example, every degree must be odd by Lemma 9 of [2] (cf. Remark 2.3). Furthermore, in all the known examples both G and H are elementary abelian p-groups for some odd prime p and the resulting planes are all the semifield planes of odd order coordinatized by commutative semifields (Remark 3.2). In particular the known examples of planar functions have prime power degrees.

The purpose of this paper is to study planar functions. In Section 2 we will show that each planar function f from G into H corresponds to a partition of $G \times G$ (Lemma 2.1). From this we have a system of diophantine

0021-8693/90 $3.00

equations that has at least one solution (Lemma 2.2). As an application, we will give a result that rules out some possibilities for the degrees of planar functions (Section 4). The terminology we use is standard and can be found in [4] or [6].

2. Some Partition Given by a Planar Function

Let G and H be groups of the same order n. Throughout the section elements of G will be denoted by small Roman letters and elements of H by small Greek letters: $G=\{a, b, c, \ldots\}$, $H=\{\alpha, \beta, \gamma, \ldots\}$.

Let f be a function from G into H and set $S_\alpha=\{x\in G \mid f(x)=\alpha\}$, $\alpha\in H$. Further set $T(\alpha, \eta)=S_\alpha\times S_{\eta\alpha}-T_\infty$, where $T_\infty=\{(x, x)\mid x\in G\}$. Clearly $T_\infty\cup\bigcup_{\alpha,\eta\in H} T(\alpha, \eta)$ is a partition of $G\times G$. Let $T_\eta=\bigcup_{\alpha\in H} T(\alpha, \eta)$, $\eta\in H$.

An action of G on $G\times G$ is defined by $(a, b)c=(ac, bc)$ for $(a, b)\in G\times G$ and $c\in G$. Every planar function can be interpreted in the following way.

Lemma 2.1. *The following three conditions are equivalent.*

(i) *f is planar.*

(ii) *$T(\alpha, \eta)\cap T(\beta, \eta)u\neq\varnothing$ implies $u=1$ $(\alpha, \beta, \eta\in H, u\in G)$.*

(iii) *$G^*=\{ab^{-1}\mid (a, b)\in T_\eta\}$ for every $\eta\in H$. (If this is the case, $|T_\eta|=n-1$.)*

Proof. Assume that f is planar. Let $(a, b)\in T(\alpha, \eta)$, $(c, d)\in T(\beta, \eta)$ and assume that $(a, b)=(c, d)u$ for some $u\in G$. Then, as $f(a)=\alpha$, $f(b)=\eta\alpha$, $f(c)=\beta$, and $f(d)=\eta\beta$, we have $f(a)f(b)^{-1}=f(c)f(d)^{-1}$. From this $f_{ab^{-1}}(b)=f_{cd^{-1}}(d)$. On the other hand, $1\neq ab^{-1}=(cu)(du)^{-1}=cd^{-1}$. By the definition of a planar function, $b=d$. Hence $u=d^{-1}b=1$. Thus (i) implies (ii).

Assume (ii) and deny (iii). Since $\bigcup_{\eta\in H} T_\eta=\{(x, y)\in G\times G\mid x\neq y\}$ and $T_\tau\cap T_\mu=\varnothing$ for any distinct τ and μ in H, there exists an $\eta\in H$ such that $|T_\eta|>(n^2-n)/n=n-1$. Hence $ab^{-1}=cd^{-1}$ for some distinct (a, b), $(c, d)\in T_\eta$. Set $u=c^{-1}a$ $(=d^{-1}b)$ and $\alpha=f(a)$, $\beta=f(c)$. Then $(a, b)=(c, d)u$ and $(a, b)\in T(\alpha, \eta)$, $(c, d)\in T(\beta, \eta)$. By (ii), $u=1$, contrary to $(a, b)\neq(c, d)$. Thus (ii) implies (iii).

Assume (iii). If $f_u(a)=f_u(b)$ for some a, b, $u\in G$, $u\neq 1$, we have $f(ua)\alpha^{-1}=f(ub)\beta^{-1}=\eta$ for some $\eta\in H$, where $\alpha=f(a)$ and $\beta=f(b)$. Then, as $u\neq 1$, $(a, ua)\in T(\alpha, \eta)$ and $(b, ub)\in T(\beta, \eta)$. Hence (a, ua), $(b, ub)\in T_\eta$. Since $a(ua)^{-1}=b(ub)^{-1}$, we have $a=b$ by (iii). Thus (iii) implies (i).

In the rest of the paper we assume that f is planar. Let x_α be the number of elements of S_α. Clearly x_α is a nonnegative integer.

LEMMA 2.2. *The following hold.*

(i) $\sum_{\alpha \in H} x_\alpha = n$.

(ii) $\sum_{\alpha \in H} x_\alpha^2 = 2n - 1$.

(iii) *If* $\eta \in H$ *and* $\eta \neq 1$, *then* $\sum_{\alpha \in H} x_\alpha x_{\eta\alpha} = n - 1$.

Proof. Since $G = \bigcup_{\alpha \in H} S_\alpha$ and $S_\alpha \cap S_\beta = \varnothing$ for any distinct $\alpha, \beta \in H$, (i) holds.

By Lemma 2.1, $|T_\eta| = n - 1$. Put $\eta = 1$. Then $T_1 = \bigcup_{\alpha \in H} T(\alpha, 1)$ and $|T(\alpha, 1)| = |S_\alpha \times S_\alpha - T_\infty| = x_\alpha^2 - x_\alpha$. Hence $\sum_{\alpha \in H} (x_\alpha^2 - x_\alpha) = |T_1| = n - 1$. It follows from (i) that $\sum_{\alpha \in H} x_\alpha^2 = \sum_{\alpha \in H} x_\alpha + n - 1 = 2n - 1$. Thus (ii) holds.

If $\eta \neq 1$, then $S_\alpha \times S_{\eta\alpha} \cap T_\infty = \varnothing$ and so $|T(\alpha, \eta)| = |S_\alpha \times S_{\eta\alpha}| = x_\alpha x_{\eta\alpha}$. Hence $\sum_{\alpha \in H} x_\alpha x_{\eta\alpha} = |T_\eta| = n - 1$. Thus (iii) holds.

Remark 2.3. By the above lemma, $\sum_{\alpha \in H} x_\alpha (x_\alpha - 1) = n - 1$ and so n must be odd (cf. Lemma 9 of [2]).

DEFINITION 2.4. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be a labelling of the elements of H. A matrix $M = (m_{\alpha_i, \alpha_j})$ relative to f is defined to be an $n \times n$ matrix of nonnegative integers such that $m_{\alpha_i, \alpha_j} = x_{\alpha_i^{-1}\alpha_j}$.

LEMMA 2.5. *Let* M *be a matrix relative to* f. *Then* $M \cdot M^t = M^t \cdot M = (n-1)J + nI$, *where* J *is the* $n \times n$ *matrix with a* 1 *in every position and* I *is then identity matrix.* (M^t *is the transposed matrix of* M.)

Proof. Let $M \cdot M^t = (a_{\alpha,\beta})$. Then $a_{\alpha,\beta} = \sum_{\gamma \in H} m_{\alpha,\gamma} m_{\beta,\gamma} = \sum_{\gamma \in H} x_{\alpha^{-1}\gamma} x_{\beta^{-1}\gamma}$ $= \sum_{\gamma \in H} x_{\alpha^{-1}\gamma} x_{\beta^{-1}\alpha\alpha^{-1}\gamma} = \sum_{\delta \in H} x_\delta x_{\beta^{-1}\alpha \cdot \delta}$. Hence, by Lemma 2.2, $M \cdot M^t = (n-1)J + nI$. In particular $|M \cdot M^t| = n^{n+1}$ and so M is a nonsingular matrix.

Since $MJ = JM$ $(= nJ)$ by Lemma 2.2(i), $(M \cdot M^t)M = ((n-1)J + nI)M$ $= M((n-1)J + nI)$. Thus $M^t \cdot M = (n-1)J + nI$.

LEMMA 2.6. *There exists an* $n \times n$ *unitary matrix* U *such that*

$$U^{-1}MU = \begin{pmatrix} z_1 & & 0 \\ & \ddots & \\ 0 & & z_n \end{pmatrix}, \qquad \text{where } z_1 = n \text{ and } z_j \bar{z}_j = n \text{ for } j > 1.$$

Proof. By Lemma 2.5, there exists a unitary matrix U such that $U^{-1}MU$ is a diagonal matrix. Set

$$U^{-1}MU = \begin{pmatrix} z_1 & & 0 \\ & \ddots & \\ 0 & & z_n \end{pmatrix}.$$

By Lemma 2.2(i),

$$M\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix}=n\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix}.$$

Hence we may assume $z_1=n$. Since U is a unitary matrix,

$$(U^{-1}MU)(\overline{U^{-1}MU})^{t}=U^{-1}MM^{t}U=\begin{pmatrix}z_1\bar{z}_1 & & 0\\ & \ddots & \\ 0 & & z_n\bar{z}_n\end{pmatrix}.$$

By Lemma 2.5, the eigenvalues of $M\cdot M^{t}$ are n^2 (with multiplicity 1) and n (with multiplicity $n-1$). Thus $z_j\bar{z}_j=n$ for every $j>1$.

Since n is odd, G and H are solvable groups by the Feit–Thompson theorem. In particular $H/[H,H]\neq 1$ and so there exists a nontrivial linear character of H.

LEMMA 2.7. *Let λ be a nontrivial linear character of H. Set $z=\sum_{\alpha\in H}x_\alpha\lambda(\alpha)$. Then $z\bar{z}=n$.*

Proof. Since

$$M\begin{pmatrix}\lambda(\alpha_1)\\ \vdots\\ \lambda(\alpha_n)\end{pmatrix}=\begin{pmatrix}\sum_j x_{\alpha_1^{-1}\alpha_j}\lambda(\alpha_j)\\ \vdots\\ \sum_j x_{\alpha_n^{-1}\alpha_j}\lambda(\alpha_j)\end{pmatrix}$$

$$=\begin{pmatrix}\sum_j x_{\alpha_1^{-1}\alpha_j}\lambda(\alpha_1^{-1}\alpha_j)\,\lambda(\alpha_1)\\ \vdots\\ \sum_j x_{\alpha_n^{-1}\alpha_j}\lambda(\alpha_n^{-1}\alpha_j)\,\lambda(\alpha_n)\end{pmatrix}$$

$$=z\begin{pmatrix}\lambda(\alpha_1)\\ \vdots\\ \lambda(\alpha_n)\end{pmatrix},$$

$$\begin{pmatrix}\lambda(\alpha_1)\\ \vdots\\ \lambda(\alpha_n)\end{pmatrix}\neq\begin{pmatrix}t\\ \vdots\\ t\end{pmatrix}$$

for any $t\in\mathbb{C}$, $z\bar{z}=n$ by Lemma 2.6.

3. Planar Functions Corresponding to Semifield Planes

All the known planar functions are constructed from semifield planes. In this section we will determine their general form.

Let q be a power of an odd prime and D a semifield of order q. The semifield plane $\pi(D)$ is defined as follows [6].

Points: the elements of the direct product $D \times D$.

Lines: $(y = mx + b) = \{(x, y) \mid y = mx + b,\ x \in D\}$, $m, b \in D$,
$(x = k) = \{(k, y) \mid y \in D\}$, $k \in D$.

Incidence: set theoretic inclusion.

Given a semifield D, a p-group $P = D \times D \times D$ of order q^3 ($q = |D|$) is defined by the rule

$$(x_1, y_1, z_1)(x_2, y_2, z_2) = (x_1 + x_2,\ y_1 + y_2,\ z_1 + z_2 + y_2 x_1)$$

for all (x_1, y_1, z_1), $(x_2, y_2, z_2) \in P$. Then P acts on $\pi(D)$ as a collineation group in such a way that

$$(a, b)^{(x, y, z)} = (a + x,\ b + ya + z)$$

for a point $(a, b) \in D \times D$ and an element $(x, y, z) \in P$ (cf. [5, Sect. 2]).

Set $A = \{(x, 0, z) \mid x, z \in D\}$ and $B = \{(0, y, z) \mid y, z \in D\}$. Then A is the group of (l_∞, l_∞)-elations and B is the group of (∞, ∞)-elations. Moreover A and B are elementary abelian normal subgroups of P of order q^2. Set $Z = A \cap B$. Then $P = AB$, and Z is the group of all (∞, l_∞)-elations of order q.

Assume $\pi(D) \simeq S(G, H, f)$ for suitable collineation groups G and H of $\pi(D)$ and a planar function f from G into H. Here H is the group of (Q, l_∞)-elations for some point $Q \in l_\infty$ and $G \times H$ acts transitively on the affine points and also on $l_\infty - \{Q\}$. (See [2, Sect. 5].) If $Q \neq (\infty)$, then the dual plane of $\pi(D)$ must be desarguesian by Theorem 6.18 of [6]. Therefore, without loss of generality we may assume that $Q = (\infty)$. Therefore $H = Z$ and G normalizes P. Clearly Z is in the center of GP. Let l be an affine line through (∞) and V an affine point on it. Let L be the stabilizer of V in the group GP. Since Z centralizes L and Z acts transitively on the the set of affine points on l, L must be a group of (∞, l)-elations. Hence $|L| \leqslant q$ and so $|GP| = |GP : L| \times |L| \leqslant q^2 q = q^3 = |P|$. Thus $G \leqslant P$.

Lemma 3.1. *GH is isomorphic to an elementary abelian group of order q^2 and $GH \neq A, B$.*

Proof. Since $H=Z$, G acts transitively on $l_\infty-\{(\infty)\}$. Hence $G\cap A=1$ and so $P=GA$. From this $G\simeq GA/A=P/A$. Thus the lemma holds.

Remark 3.2. By Proposition 4.3 of [5] and the lemma above, D is isotopic to a commutative semifield.

LEMMA 3.3. *There exists an element* $0\neq a\in D$ *such that* $GH=\{(x, ax, z)\mid x, z\in D\}$ *and* $(ax)y=(ay)x$ *for all* $x, y\in D$.

Proof. Since $GH\cap B=H$, $(1, a, a')\in GH$ for some elements $a, a'\in D$. Then $GH\leqslant\{(x, y, z)\in P\mid (x, y, z)(1, a, a')=(1, a, a')(x, y, z)\}=\{(x, ax, z)\in P\mid x, z\in D\}$. Hence $GH=\{(x, ax, z)\in P\mid x, z\in D\}$.

Let x and y be any two elements of D. Then $(x, ax, 0)$, $(y, ay, 0)\in GH$ as $GH\geqslant H=Z$. Therefore $(x, ax, 0)(y, ay, 0)=(y, ay, 0)(x, ax, 0)$ and so $(ay)x=(ax)y$.

LEMMA 3.4. *There exists a mapping* g *from* D *into* D *such that*

(i) $G=\{(x, ax, g(x))\mid x\in D\}$ *and*

(ii) $g(x+y)=g(x)+g(y)+(ay)x$ *for all* $x, y\in D$.

Proof. Since $G\cap Z=G\cap H=1$, G can be represented in the form stated in (i). Since $(x, ax, g(x))(y, ay, g(y))=(x+y, a(x+y), g(x)+g(y)+(ay)x)$, we have (ii).

LEMMA 3.5. *Put* $F(x)=g(x)-\frac{1}{2}(ax)x$. *Then* $F(x+y)=F(x)+F(y)$ *for* $x, y\in D$.

Proof. Since $(ax)y=(ay)x$, we can verify the lemma by direct calculation.

LEMMA 3.6. *Let* (c, d) *be an affine point of* $\pi(D)$, $c, d\in D$, *and* (x, ax, z) *an element of* GH. *If we identify each affine point* $(c, d)^{(x, ax, z)}$ *with* (x, ax, z), *the set* $\mathscr{P}$ *of affine points on a line* $(y=mx+b)$ *is*

$$\mathscr{P}=\{(x, ax, mx-(ax)c+s)\mid x\in D\},\qquad \text{where}\quad s=mc+b-d.$$

Proof. Since $(c, d)^{(x, ax, z)}=(c+x, d+(ax)c+z)$, each point $(t, mt+b)$ corresponds to (x, ax, z), where $c+x=t$ and $d+(ax)c+z=mt+b$. Hence $\mathscr{P}=\{(t-c, a(t-c), mt+b-d-(a(t-c))c)\mid t\in D\}=\{(x, ax, mx-(ax)c+s)\mid x\in D\}$, where $s=mc+b-d$.

PROPOSITION 3.7. *Let D, G, H, and f be as stated above. If we identify G and H with the additive group D^+, the planar function f corresponding to the group GH has the form*

$$f(x) = (x^\tau + (rx^\theta)x^\theta + s)^\mu.$$

Here $s \in D$, θ, τ, $\mu \in \mathrm{Hom}(D^+, D^+)$, and θ and μ are nonsingular. Moreover $0 \neq r \in D$ and $(rx)y = (ry)x$ for all $x, y \in D$.

Proof. By Lemma 3.6, $\mathscr{P} = \{w\rho \mid w = (x, ax, g(x)) \in G, \rho = (0, 0, N(x)), x \in D\}$, where $N(x) = mx - (ax)c + s - g(x)$. Hence, by $(*)$ in Section 1

$$f(x) = (mx^\theta - (ax^\theta)c + s - g(x^\theta))^\mu$$

for some nonsingular θ, $\mu \in \mathrm{Hom}(D^+, D^+)$. Set $x^\tau = mx^\theta - (ax^\theta)c - F(x^\theta)$ and $r = -\frac{1}{2}a$. Then $\tau \in \mathrm{Hom}(D^+, D^+)$ and so we have the proposition.

4. A NONEXISTENCE THEOREM

In this section we present a theorem on planar functions as an application of the results obtained in Section 2. Throughout the section let n (>0) be an odd integer and f a planar function of degree n from G into H. Given two primes p and q, $\mathrm{ord}_p(q)$ denotes the order of q in the multiplicative group of Z/pZ.

THEOREM 4.1. *Let f be a planar function of degree n from G into H and p and q prime divisors of n such that $\mathrm{ord}_p(q)$ is even. If p divides $|H/[H, H]|$, then the square free part of n is not divisible by q.*

Proof. Since p divides $|H/[H, H]|$, there exists a nontrivial linear character λ of H such that λ^p is the trivial character. Hence $\lambda(\alpha)$ is an algebraic integer of the p-cyclotomic field $\mathbb{Q}(\zeta_p)$ for each $\alpha \in H$. It follows that $z = \sum_{\alpha \in H} x_\alpha \lambda(\alpha) \in \mathbb{Q}(\zeta_p)$ and that z is an algebraic integer, where $x_\alpha = |S_\alpha|$ (see Section 2). By Lemma 2.7, $z\bar{z} = n$.

Set $r = \mathrm{ord}_p(q)$, $g = (p-1)/r$ and let $\mathbb{G}$ be the Galois group of $\mathbb{Q}(\zeta_p)$ over $\mathbb{Q}$. By a theorem of number theory (cf. Theorem 5.2.2 of [1]), q has the factorization

$$q = \mathfrak{Q}_1 \mathfrak{Q}_2 \cdots \mathfrak{Q}_g \tag{1}$$

in $\mathbb{Q}(\zeta_p)$, where $\mathfrak{Q}_1$, $\mathfrak{Q}_2$, ... and $\mathfrak{Q}_g$ are distinct prime ideals. Moreover $\mathbb{G}$ is isomorphic to a cyclic group of order $p-1$ and acts transitively on $\Delta = \{\mathfrak{Q}_1, \mathfrak{Q}_2, ..., \mathfrak{Q}_g\}$. Hence, the unique subgroup $\mathbb{G}_0$ of $\mathbb{G}$ of order r fixes Δ elementwise. By assumption, r is even. Therefore $\mathfrak{Q}_i^\tau = \mathfrak{Q}_i$ $(1 \leqslant i \leqslant g)$, where

τ is the unique element of $\mathbb{G}_0$ of order 2. Since $\zeta_p^{\tau} = \zeta_p^{-1} = \bar{\zeta}_p$, $\xi^{\tau} = \bar{\xi}$ for any $\xi \in \mathbb{Q}(\zeta_p)$. Thus

$$\bar{\mathfrak{Q}}_i = \mathfrak{Q}_i, \qquad 1 \leqslant i \leqslant g. \tag{ii}$$

Set $n = q^e m$, where e and m are some positive integers such that $(q^e, m) = 1$. Then, by (i), n has the following factorization in $\mathbb{Q}(\zeta_p)$:

$$n = \mathfrak{Q}_1^e \mathfrak{Q}_2^e \cdots \mathfrak{Q}_g^e \mathscr{A}. \tag{iii}$$

Here $\mathfrak{Q}_i$ and $\mathscr{A}$ are relatively prime for each $i \in \{1, 2, ..., g\}$.

Set $z = \mathfrak{Q}_1^{e_1} \mathfrak{Q}_2^{e_2} \cdots \mathfrak{Q}_g^{e_g} \mathscr{B}$, where $\mathfrak{Q}_i$ and $\mathscr{B}$ are relatively prime for each $i \in \{1, 2, ..., g\}$. Then $\bar{z} = (\bar{\mathfrak{Q}}_1)^{e_1} (\bar{\mathfrak{Q}}_2)^{e_2} \cdots (\bar{\mathfrak{Q}}_g)^{e_g} \bar{\mathscr{B}}$. However, it follows from (ii) that $\bar{z} = \mathfrak{Q}_1^{e_1} \mathfrak{Q}_2^{e_2} \cdots \mathfrak{Q}_g^{e_g} \bar{\mathscr{B}}$. Therefore $n = z\bar{z} = \mathfrak{Q}_1^{2e_1} \mathfrak{Q}_2^{2e_2} \cdots \mathfrak{Q}_g^{2e_g} \mathscr{B}\bar{\mathscr{B}}$. Since $\mathfrak{Q}_i$ and $\mathscr{B}\bar{\mathscr{B}}$ are relatively prime, we have $e = 2e_i$ for each $i \in \{1, 2, ..., g\}$. Thus e is even and the theorem holds.

COROLLARY 4.2. *Let f be a planar function of degree n from a group G into an abelian group H. Let p and q be primes such that pq divides n. If* $\mathrm{ord}_p(q)$ *is even, then the square free part of n is not divisible by q.*

COROLLARY 4.3. *Let p and q be primes such that $p < q$ and p divides $q^m + 1$ for some positive integer m. Then there exists no planar function of degree pq.*

REFERENCES

1. Z. I. BOREVICH AND I. R. SHAFAREVICH, "Number Theory," Academic Press, San Diego, CA/New York/London, 1966.
2. P. DEMBOWSKI AND T. G. OSTROM, Planes of order n with collineation groups of order n^2, *Math. Z.* **103** (1968), 239–258.
3. P. DEMBOWSKI, "Finite Geometries," Springer-Verlag, Berlin/Heidelberg/New York, 1968.
4. D. GORENSTEIN, "Finite Groups," Harper & Row, New York, 1968.
5. Y. HIRAMINE, Automorphisms of p-groups of semifield type, *Osaka J. Math.* **20** (1983), 735–746.
6. D. R. HUGHES AND F. C. PIPER, "Projective Planes," Springer-Verlag, New York/Heidelberg/Berlin, 1970.