Hiramine, Y.
Osaka J. Math.
22 (1985), 61-69

A GENERALIZATION OF HALL QUASIFIELDS

YUTAKA HIRAMINE

(Received March 26, 1984)

1. Introduction

Let $Q=Q(+, \circ)$ be a right quasifield which satisfies the following conditions:

(1.1) Q is a two dimensional left vector space over its kernel K with a basis $\{1, \lambda\}$.

(1.2) There exist two mappings r and s from $K^{\sharp}=K-\{0\}$ into K such that every element $\xi=a+b\lambda$ of Q not in K satisfies the equation $\xi^2-r(b)\xi-s(b)=0$.

(1.3) Each element of K commutes with all the elements of Q.

Several examples of such Q are known. For example, the Hall quasifields satisfy the conditions above, where r and s are constant functions and the quadratic polynomial x^2-rx-s is irreducible over K. Moreover, the quasifields which correspond to the spread sets constructed by Narayana Rao and Satyanarayana [3] also satisfy the conditions above, where $r(x)=3x^{-1}$, $s(x)=2x^{-2}$ and $K=GF(5^{2^n-1})$.

The purpose of this paper is to study the quasifields satisfying the conditions (1.1)–(1.3). In §2 we prove the following theorem which gives a condition for $Q(+, \circ)$ to be a quasifield.

Theorem 1. *Let K be a field and let r and s be mappings from $K^{\sharp}$ into K such that* (i) *$x^2-r(u)x-s(u)$ is irreducible over K for each $u\in K^{\sharp}$ and* (ii) *$v^2-r(x)v-s(x)=wx$ has a unique solution in $K^{\sharp}$ for each $v\in K$, $w\in K^{\sharp}$. Let $Q=\{x+y\lambda \mid x, y\in K\}$ be a left vector space over K. If a multiplication $\circ$ on Q is defined by*

$$(z+t\lambda)\circ(x+y\lambda)=\begin{cases} zx-ty^{-1}F(x, y)+(zy-tx+t\,r(y))\lambda & \text{if } y\neq 0\,, \\ zx+tx\lambda & \text{if } y=0\,, \end{cases}$$

where $F(x, y)=x^2-r(y)x-s(y)$, then $Q(+, \circ)$ is a quasifield which satisfies (1.1)–(1.3).

Let $K=GF(q)$ and let Φ_K be the set of the ordered pairs (r, s) such that r and s satisfy (i) and (ii) of Theorem 1. The spread set $\Sigma_{r,s}$ which corresponds to $(r, s)\in\Phi_K$ is defined as follows: $\Sigma_{r,s}=\{M(x, y)\mid x, y\in K\}$, where $M(x, 0)=\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$ for $x\in K$ and $M(x, y)=\begin{pmatrix} x & y \\ f(x, y) & g(x, y) \end{pmatrix}$ for $x\in K$ and $y\in K^{\sharp}$. Here $f(x, y)=-y^{-1}(x^2-r(y)x-s(y))$ and $g(x, y)=-x+r(y)$.

Let $\pi_{r,s}$ be the translation plane constructed by $\Sigma_{r,s}$ and set $L(x, y)=\{(v, vM(x, y))\mid v\in K\times K\}$ for $x, y\in K$, $L(\infty)=\{(0, 0, v)\mid v\in K\times K\}$. Let G be the linear translation complement of $\pi_{r,s}$ and set $\Delta=\{L(x, 0)\mid x\in K\}\cup\{L(\infty)\}$ and $\Omega=\{L(x, y)\mid x\in K, y\in K^{\sharp}\}$. In §3 we prove the following theorem.

Theorem 2. *If $G_{L(\infty),L(0,0)}$ is transitive on Ω, then $r(x)=ax^n$ and $s(x)=bx^{2n}$ for some $a, b\in K$ and n with $0\leq n\leq q-2$.*

The Hall planes and the planes of Narayana Rao and Satyanarayana satisfy the condition of this theorem. But an element of Φ_K is not always represented in this form (Remark 3.6.).

Throughout the paper notations are standard and taken from [1] and [2]. All sets and groups are finite except in §2.

2. Proof of Theorem 1

Let Q be a set with two binary operations $+$, $\circ$ satisfying the assumption of Theorem 1. Since Q is a left vector space, the following holds.

Lemma 2.1. *$(Q, +)$ is an abelian group.*

Lemma 2.2. *Let $a, b, c, d\in K$ and assume $a+b\lambda\neq 0$ and $c+d\lambda\neq 0$. Then the equation* $(a+b\lambda)(x+y\lambda)=c+d\lambda$ (2.1)
has a unique solution for $x+y\lambda$ in $Q^{\sharp}=Q-\{0\}$.

Proof. (2.1) is equivalent to

$$ax-by^{-1}(x^2-r(y)x-s(y)) = c\,, \tag{2.2}$$

$$b\,r(y)+ay-bx = d \text{ if } y\neq 0$$

or

$$ax = c,\ bx = d \quad \text{if } y = 0\,. \tag{2.3}$$

By the second equation of (2.2),

$$b\,r(y) = bx-ay+d \tag{2.4}$$

Substituting this into the first equation of (2.2), we have

$$y^{-1}(dx+b\,s(y)) = c\,. \tag{2.5}$$

Hence $b\,s(y)+dx=cy$. By this and the second equation of (2.2),

$$d^2-bd\,r(y)-b^2\,s(y) = (ad-bc)\,y\,. \tag{2.6}$$

Therefore (2.2) is equivalent to (2.4) and (2.6) when $b \neq 0$.

Assume $b=0$ and $d=0$. Then $a \neq 0$ and $c \neq 0$. Hence (2.1) has no solution in $Q-K$ and has a unique solution $a^{-1}c+0\lambda$ in $K^{\sharp}$

Assume $b=0$ and $d \neq 0$. Then $a \neq 0$. By (2.3), (2.1) has no solution in K and by (2.2) it has a unique solution $a^{-1}c+a^{-1}d\lambda$ in $Q-K$.

Assume $b \neq 0$ and $ad-bc=0$. Then (2.6) is equivalent to $(b^{-1}d)^2-r(y)(b^{-1}d)-s(y)=0$. By the assumption (i) of Theorem 1, (2.1) has no solution in $Q-K$. Therefore it has a unique solution $b^{-1}d+0\lambda$ in $K^{\sharp}$.

Assume $b \neq 0$ and $ad-bc \neq 0$. Then (2.1) has no solution in K by (2.3). Since $b \neq 0$, (2.6) is equivalent to $(b^{-1}d)^2-r(y)(b^{-1}d)-s(y)=b^{-2}(ad-bc)y$ and hence (2.6) has a unique solution y' in $K^{\sharp}$ by the assumption (ii) of Theorem 1. Let x' be the unique solution of $b\,r(y')=bx-ay'+d$. Then $x'+y'\lambda$ is a unique solution of (2.1).

Lemma 2.3. *Let $a, b, c, d \in K$ and assume $a+b\lambda \neq 0$, $c+d\lambda \neq 0$. Then the equation*

$$(x+y\lambda)(a+b\lambda) = c+d\lambda \tag{2.7}$$

has a unique solution for $x+y\lambda$ in $Q^{\sharp}$.

Proof. If $b=0$, (2.7) has a unique solution $a^{-1}c+a^{-1}d\lambda$. Assume $b \neq 0$. Then (2.7) is equivalent to linear equations

$$\begin{aligned} xa-yb^{-1}(a^2-r(b)a-s(b)) &= c\,, \\ xb+y(r(b)-a) &= d\,. \end{aligned} \tag{2.8}$$

Since $a(r(b)-a)-b(-b^{-1}(a^2-r(b)a-s(b)))=-s(b) \neq 0$ by the assumption (i) of Theorem 1, (2.8) has a unique solution $(x, y) \neq (0, 0)$. Thus (2.7) has a unique solution in $Q^{\sharp}$.

Proof of Theorem 1.

It follows immediately from the definition that $Q(+, \circ)$ satisfies the following.

$$\xi 1 = 1\xi = \xi \text{ for all } \xi \in Q\,. \tag{2.9}$$

$$(\xi+\eta)\mu = \xi\mu+\eta\mu \quad \text{for all } \xi, \eta, \mu \in Q\,. \tag{2.10}$$

$$\xi 0 = 0 \quad \text{for all } \xi \in Q\,. \tag{2.11}$$

By Lemmas 2.1–2.3 and (2.9)–(2.11), Q is a weak quasifield. Since Q is a finite dimensional vector space over K, it is a quasifield by Theorem 7.3 of [1]. Thus we have the theorem.

Suppose $|K|<\infty$. The spread set $\Sigma_{r,s}=\{M(x, y)\,|\,x, y \in K\}$ which corresponds to the above quasifield is defined as follows: Let $K=GF(q)$ and let $M(x, y)=\begin{pmatrix} x & y \\ f(x, y) & g(x, y)\end{pmatrix}$ be a 2×2 matrix over K. Define $M(x, y)\in\Sigma_{r,s}$ if and only if $\lambda\circ(x+y\lambda)=f(x, y)+g(x, y)\lambda$. Then we have $M(x, 0)=\begin{pmatrix} x & 0 \\ 0 & x\end{pmatrix}$ for $x\in K$ and $M(x, y)=\begin{pmatrix} x & y \\ f(x, y) & g(x, y)\end{pmatrix}$, where $f(x, y)=-y^{-1}(x^2-r(y)x-s(y))$ and $g(x, y)=-x+r(y)$ for $x\in K$ and $y\in K^\sharp$.

3. The proof of Theorem 2

Throughout this section let p be a prime and $K=GF(q)$, $q=p^m$. We use the following notations.

$K^2 = \{k^2 \mid k\in K\}$

Φ_K the set of ordered pairs (r, s) of r and s which satisfy the conditions (i) and (ii) of Theorem 1

$M_2(K)$ the set of 2×2 matrices over K

$tr(M)$ the trace of a matrix M of $M_2(K)$

$\det(M)$ the determinant of a matrix M of $M_2(K)$

Let $(r, s)\in\Phi_K$ and $\Sigma_{r,s}$ the corresponding spread set defined in the last paragraph of §2. Let $\pi_{r,s}$ be the translation plane of order q^2 constructed from $\Sigma_{r,s}$.

Lemma 3.1. (i) *Let* $M(x, y)\in\Sigma_{r,s}$. *If* $y\neq 0$, *then* $r(y)=tr(M(x, y))$ *and* $s(y)=-\det(M(x, y))$.

(ii) *Let* $P, M\in M_2(K)$ *with* $\det(P)\neq 0$ *and set* $P^{-1}MP=\begin{pmatrix} * & y \\ * & *\end{pmatrix}$. *Assume* $y\neq 0$. *Then* $P^{-1}MP\in\Sigma_{r,s}$ *if and only if* $r(y)=tr(P^{-1}MP)$ *and* $s(y)=-\det(P^{-1}MP)$.

Proof. By an easy computation we have (i).

The "only if" part of (ii) is an immediate consequence of (i). Assume $r(y)=tr(P^{-1}MP)$ and $s(y)=-\det(P^{-1}MP)$ and set $P^{-1}MP=\begin{pmatrix} x & y \\ z & u\end{pmatrix}$. Since $tr(P^{-1}MP)=tr(M)$ and $\det(P^{-1}MP)=det(M)$, we have

$$r(y) = tr(M) = x+u \tag{3.1}$$

and

$$s(y) = -\det(M) = -xu+yz\,. \tag{3.2}$$

By (3.1), $u=-x+r(y)$. Substituting this into (3.2) gives $s(y)=x^2-r(y)x+yz$. As $y\neq 0$, $z=-y^{-1}(x^2-r(y)x-s(y))$. Hence $\begin{pmatrix} x & y \\ z & u\end{pmatrix}=\begin{pmatrix} x & y \\ f(x, y) & g(x, y)\end{pmatrix}\in\Sigma_{r,s}$ by what we have mentioned in the last paragraph of §2.

Lemma 3.2. (i) *The equation* $v^2-r(x)v-s(x)=wx$ *has a unique solution* *in* $K^{\sharp}$ *for any* $v\in K$, $w\in K^{\sharp}$ *if and only if* $(x-y)v^2-(xr(y)-yr(x))v-(xs(y)-ys(x))\neq 0$ *for any* $v\in K$ *and* $x, y\in K^{\sharp}$, $x\neq y$.

(ii) *Assume* $p>2$. *Then* $(r, s)\in\Phi_K$ *if and only if the following two conditions are satisfied.*

(a) $(r(y))^2+4s(y)\notin K^2$ *for any* $y\in K^{\sharp}$.

(b) $(xr(y)-yr(x))^2+4(x-y)(xs(y)-ys(x))\notin K^2$ *for any* $x, y\in K^{\sharp}$, $x\neq y$.

Proof. Assume $(x-y)v^2-(xr(y)-yr(x))v-(xs(y)-ys(x))=0$ for some $V\in K$ and $x, y\in K^{\sharp}$, $x\neq y$. Thdn $x(v^2-r(y)v-s(y))=y(v^2-r(x)v-s(x))$. Hence $(v^2-r(y)v-s(y))/y=(v^2-r(x)v-s(x))/x$. Put $w=(v^2-r(x)v-s(x))/x$. Then $w\neq 0$ as $v^2-r(x)v-s(x)\neq 0$ by the assumption (i) of Theorem 1 and the equation $v^2-r(\xi)v-s(\xi)=w\xi$ has at least two solutions for ξ.

Conversely, assume $v^2-r(x)v-s(x)=wx$ and $v^2-r(y)v-s(y)=wy$ for some $x, y\in K^{\sharp}$, $x\neq y$. Then $wxy=y(v^2-r(x)v-s(x))=x(v^2-r(y)v-s(y))$. This gives $(x-y)v^2-(xr(y)-yr(x))v-(xs(y)-ys(x))=0$. Therefore (i) holds.

Assume $p>2$. Then it is well known that a quadratic equation $ax^2+bx+c=0$ over K has no solution in K if and only if $b^2-4ac\notin K^2$. Hence (ii) follows immediately from (i).

Lemma 3.3. *Assume* $|K|>3$ *and let* $P, Q\in M_2(K)$. *If* $P+xQ\in\Sigma_{r,s}$ *for any* $x\in K$, *then either* (i) $Q=\begin{pmatrix}0&0\\0&0\end{pmatrix}$ *and* $P\in\Sigma_{r,s}$ or (ii) *P and Q are scalar matrices.*

Proof. Set $\Sigma=\Sigma_{r,s}$, $P=\begin{pmatrix}i&j\\k&l\end{pmatrix}$, $i, j, k, l\in K$ and $Q=\begin{pmatrix}a&b\\c&d\end{pmatrix}$, $a, b, c, d\in K$. Then $P+xQ=\begin{pmatrix}i+ax&j+bx\\k+cx&l+dx\end{pmatrix}$.

Assume $j=b=0$. Then $P+xQ\in\Sigma$ if and only if $P+xQ$ is a scalar matrix. Hence $i+ax=l+dx$ and $k+cx=0$. Since x is arbitrary, it follows that $i=l$, $a=d$ and $k=c=0$. Thus (ii) holds when $j=b=0$.

Assume $j\neq 0$ and $b=0$. By Lemma 3.1, $P+xQ\in\Sigma$ if and only if $r(j)=tr(P+xQ)$ and $s(j)=-\det(P+xQ)$. Hence

$$r(j) = i+l+(a+d)x \tag{3.3}$$

and

$$s(j)=-adx^2+(jc-al-id)x+jk-il\,. \tag{3.4}$$

Since (3.3) and (3.4) hold for all $x\in K$, we have

$$r(j) = i+l\,,\quad a+d = 0 \tag{3.5}$$

and

$$s(j) = jk-il\,,\quad jc-al-id = 0\,,\ ad = 0 \tag{3.6}$$

Hence $a=d=0$ so $jc=0$. As $j\neq 0$, $c=0$. Therefore $\begin{pmatrix}a&b\\c&d\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}$. Thus (i) holds when $j\neq 0$ and $b=0$.

Assume $b\neq 0$. Set $x=-b^{-1}j$. Then $j+bx=0$ and so $P+xQ$ is a scalar matrix. Hence $k-cb^{-1}j=0$ and $i-ab^{-1}j=l-db^{-1}j$. Setting $w=-b^{-1}j$, we have $j=-bw$, $k=-cw$ and $l=i+aw-dw$. Putting $y=j+bx$ gives $P+xQ=\begin{pmatrix} ab^{-1}y+aw+i & y \\ b^{-1}cy & b^{-1}dy+aw+i \end{pmatrix}$. By Lemma 3.1, we have $r(y)=b^{-1}(a+d)y+2(aw+i)$ and $s(y)=-b^{-2}(ad-bc)y^2-b^{-1}(a+d)(aw+i)y-(aw+i)^2$. In particular

$$xr(y)-yr(x) = 2(i+aw)(x-y)$$

and

$$xs(y)-ys(x)=(x-y)(b^{-2}(ad-bc)xy-(aw+i)^2). \tag{3.7}$$

If $p=2$, then $xr(y)-yr(x)=0$ by (3.7). Hence we have a contradiction by Lemma 3.2 (i).

If $p>2$, then $(xr(y)-yr(x))^2+4(x-y)(xs(y)-ys(x))=4(x-y)^2b^{-2}(ad-bc)xy\notin K^2$ by Lemma 3.2 (ii). Let x be any element of $K^2-\{0\}$ and let y be any element of $K-K^2$. Then clearly $4(x-y)^2b^{-2}xy\notin K^2$. Hence $ad-bc$ must be an element of K^2. From this $x'y'\notin K^2$ for any x', $y'\in K^*$, $x'\neq y'$. In particular $K^2=\{0, 1\}$, which implies $K=GF(3)$. This contradicts the assumption.

Set $L(x, y)=\{(v, vM(x, y))\,|\,v\in K\times K\}$ for x, $y\in K$, $L(\infty)=\{(0, 0, v)\,|\,v\in K\times K\}$ and $\Delta=\{L(x, 0)\,|\,x\in K\}\cup\{L(\infty)\}$, $\Omega=\{L(x, y)\,|\,x\in K,\ y\in K^*\}$. Then $\Delta\cup\Omega$ is the set of lines of $\pi_{r,s}$ through $(0, 0, 0, 0)$. Let G be the linear translation complement of $\pi_{r,s}$ and set $H=G_{L(\infty),L(0,0)}$, the stabilizer of the lines $L(\infty)$ and $L(0, 0)$ in G. Let $\sigma=\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ be a nonsingular 4×4 matrix, where A, B, C, $D\in M_2(K)$. Then the following criterion is well known: σ is an element of G if and only if the following conditions are satisfied.

(1) If C is nonsingular, then $C^{-1}D\in\Sigma_{r,s}$. (In this case $L(\infty)\sigma=L(u, v)$, where $C^{-1}D=M(u, v)\in\Sigma_{r,s}$.)

(2) If C is singular, then $C=\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ and D is nonsingular. (In this case $L(\infty)\sigma=L(\infty)$.)

(3) If $A+M(x, y)C$ is nonsingular, then $(A+M(x, y)C)^{-1}(B+M(x, y)D)\in\Sigma_{r,s}$. (In this case $L(x, y)\sigma=L(u, v)$, where $(A+M(x, y)C)^{-1}(B+M(x, y)D)=M(u, v)\in\Sigma_{r,s}$.)

(4) If $A+M(x, y)C$ is singular, then $A+M(x, y)C=\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. (In this case $L(x, y)\sigma=L(\infty)$.)

Lemma 3.4. *Assume either r or s is not a constant function. Let A, B, C and D be elements of $M_2(K)$ and set $\sigma=\begin{pmatrix} A & B \\ C & D \end{pmatrix}$. If $\sigma\in H$, then the following hold.*

(i) $B=C=\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ *and* $A=\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}$, $D=kA$ *for some* a, d, $k\in K^*$ *and* $c\in K$.

(ii) $r(a^{-1}dky)=kr(y)$, $s(a^{-1}dky)=k^2s(y)$. *Moreover* $L(x, y)=L(k(x+a^{-1}cy), ka^{-1}dy)$ *for all* x, $y\in K$, $y\neq 0$.

Proof. Since σ fixes $L(\infty)$ and $L(0, 0)$, $B=D=\begin{pmatrix}0&0\\0&0\end{pmatrix}$. Hence $\sigma=\begin{pmatrix}A&O\\O&D\end{pmatrix}$ and $A^{-1}MD\in\Sigma$ for any $M\in\Sigma$. In particular $A^{-1}M(x, 0)D=xA^{-1}D\in\Sigma$ for each $x\in K$. If $K=GF(3)$, $s(1)=s(-1)\neq 0$ and $(r(1)+r(-1))^2=(r(1))^2=(r(-1))^2=-(s(\pm 1))-1$ by Lemma 3.2 (ii). Hence r and s are constant functions. Applying Lemma 3.3 we have $A^{-1}D=k$ for some $k\in K^*$. Hence $A^{-1}MD=kA^{-1}MA\in\Sigma$ for any $M\in\Sigma$. Put $A=\begin{pmatrix}a&b\\c&d\end{pmatrix}$ and let $x\in K$, $y\in K^*$. Then $kA^{-1}M(x, y)A=M(u, v)$ for some $u\in K$ and $v\in K^*$. Set $M(x, y)=\begin{pmatrix}x&y\\f&g\end{pmatrix}$ and $M(u, v)=\begin{pmatrix}u&v\\f'&g'\end{pmatrix}$. Since $\begin{pmatrix}kx&ky\\kf&kg\end{pmatrix}\begin{pmatrix}a&b\\c&d\end{pmatrix}=\begin{pmatrix}a&b\\c&d\end{pmatrix}\begin{pmatrix}u&v\\f'&g'\end{pmatrix}$, we have

$$bkx+dky = av+bg' , \tag{3.8}$$

$$bkf+dkg = cv+dg' \tag{3.9}$$

and

$$akx+cky = au+bf' . \tag{3.10}$$

Hence $d(av)-b(cv)=d(bkx+dky)-b(bkf+dkg)$ by (3.8) and (3.9). From this we have

$$(ad-bc)v=k((b^2y^{-1})x^2+(2bd-b^2y^{-1}r(y))x+(d^2y-b^2y^{-1}s(y)-bdr(y)) . \tag{3.11}$$

On the other hand, by Lemma 3.1 (i), we have

$$kr(y) = r(v)$$

and

$$k^2s(y) = s(v) \tag{3.12}$$

We argue $b=0$. Suppose $b\neq 0$ and set $\Psi_y=\{v\,|\,r(v)=kr(y)\}$ for $y\in K^*$. By (3.11), $|\Psi_y|\geq(q+1)/2$ if $p>2$ and $|\Psi_y|\geq q/2$ if $p=2$ for any $y\in K^*$. Thus $|\Psi_y|>|K^*|/2$ for any $y\in K^*$ so we have $\Psi_y\cap\Psi_z\neq\phi$ for all y, $z\in K^*$. This implies that r is a constant function. Similarly s is also a constant function. This contradicts the assumption. Therefore $b=0$.

From (3.8) and (3.10), $v=a^{-1}dky$ and $u=kx+a^{-1}cky$. Hence $r(a^{-1}dky)=kr(y)$, $s(a^{-1}dky)=k^2s(y)$ by (3.12) and $L(x, y)\sigma=L(u, v)=L(kx+a^{-1}cky, a^{-1}dky)$. Thus lemma holds.

Lemma 3.5. *Set* $\Omega_y=\{L(x, y)\,|\,x\in K\}$ *for* $y\in K^*$ *and* $H_1=\{\begin{pmatrix}A&O\\O&A\end{pmatrix}\,|\,A=\begin{pmatrix}a&0\\c&a\end{pmatrix}, a\in K^*, c\in K\}$. *Then* $H_1\subset H$. *Moreover* H_1 *acts on* Ω_y *and is transitive on* Ω_y *for each* $y\in K^*$.

Proof. Let $\sigma=\begin{pmatrix}A&O\\O&A\end{pmatrix}\in H_1$. Since $A^{-1}M(x, y)A=\begin{pmatrix}x+a^{-1}cy&y\\ *&*\end{pmatrix}$, $A^{-1}M(x, y)A\in\Sigma$ by Lemma 3.1 (ii) so $\sigma\in H$. Moreover $L(x, y)\,\sigma=L(x+a^{-1}cy, y)$. Since $a\in K^*$ and $c\in K$ are arbitrary, we have the lemma.

Proof of Theorem 2.

Any mapping from $K^\sharp$ into K can be uniquely written in the form $\sum_{i=0}^{q-2} c_i x^i$, $c_i \in K$, $0 \leq i \leq q-2$. Set $r(y)=\sum_{i=0}^{q-2} c_i y^i$ and $s(y)=\sum_{i=0}^{q-2} d_i y^i$. We may assume that r or s is not a constant function. By Lemma 3.4 (ii), $L(0, 1)\sigma=L(a^{-1}ck, a^{-1}dk)$, where $\sigma=\begin{pmatrix} A & O \\ O & kA \end{pmatrix}$, $A=\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}$. By Lemma 3.5, H is transitive on Ω if and only if $K^\sharp=\{a^{-1}dk \mid \begin{pmatrix} A & O \\ O & kA \end{pmatrix} \in H,\ A=\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}\}$. Set $h=a^{-1}dk$. Then, by Lemma 3.4,

$$r(hy) = ad^{-1}hr(y) \tag{3.13}$$

and

$$s(hy) = (ad^{-1})^2 h^2 s(y) \tag{3.14}$$

Suppose H is transitive on Ω. Then, for any $h \in K^\sharp$, there exist a and d in $K^\sharp$ which satisfy (3.13) and (3.14) simultaneously. Hence $\sum_{i=0}^{q-1} c_i h^i y^i = \sum_{i=0}^{q-2} c_i a d^{-1} h y^i$ and $\sum_{i=0}^{q-2} d_i h^i y^i = \sum_{i=0}^{q-2} d_i (ad^{-1})^2 h^2 y^i$. Therefore $c_i h^i = c_i a d^{-1} h$ and $d_i h^i = d_i (ad^{-1})^2 h^2$ for all i with $0 \leq i \leq q-2$. If $c_m \neq 0$ and $c_n \neq 0$ for some m, n with $0 \leq m$, $n \leq q-2$, then $h^{m-1}=h^{n-1}=ad^{-1}$ and so $h^{m-n}=1$ for any $h \in K^\sharp$. Thus $m=n$, so that we have $r(y)=c_n y^n$. By a similar argument above, we have $s(y)=d_t y^t$ for some t with $0 \leq t \leq q-2$.

Since $(r(hy))^2/(r(y))^2 = s(hy)/s(y)$ by (3.13) and (3.14), $c_n^2 h^{2n} y^{2n} / c_n^2 y^{2n} = d_t h^t y^t / d_t y^t$. From this $h^{2n-t}=1$ for any $h \in K^\sharp$. Thus $t \equiv 2n \pmod{q-1}$.

REMARK 3.6. An element of Φ_K is not always represented in the form $(r(x), s(x))$, $r(x)=ax^n$, $s(x)=bx^{2n}$. We list some of such examples below, which were obtained by a computer search using Lemma 3.2.

(i) $K=GF(7)$, $r(x)=4x^5+6x^4$, $s(x)=6x^5+3x^4+6x^3+4x^2+3$.

(ii) $K=GF(11)$, $r(x)=5x^9+6x^7+9x^6+2$, $s(x)=3x^9+5x^8+6x^7+9x^6+4x^5+10x^4+9x^3+2x^2+9$.

(iii) $K=GF(11)$, $r(x)=2x^9+6x^8+4x^7+3x^6+8$, $s(x)=5x^9+x^8+8x^6+10x^5+x^4+2x^3+10x^2+10$.

References

[1] D.R. Hugese and F.C. Piper: Projedtive planes, Springer-Verlag, Berlin-Heidelberg-New York, 1973.

[2] H. Lüneburg: Translation planes, Springer-Verlag, Berlin-Heidelberg-New York, 1980.

[3] M.L. Narayana Rao and K. Satyanarayana: *A new class of square order planes,* J. Combin. Theory Ser. A **35** (1983), 33–42.

Department of Mathematics
College of General Education
Osaka University
Toyonaka, Osaka 560
Japan