Hiramine, Y.
Osaka J. Math.
20 (1983), 735-746

AUTOMORPHISMS OF p-GROUPS OF SEMIFIELD TYPE

YUTAKA HIRAMINE

(Received March 10, 1982)

1. Introduction

Let $\pi=\pi(D)$ be a finite projective plane coordinatized by a semifield D of order q. Let A be the collineation group of all elations with axis $[\infty]$ and B the collineation group of all elations with center (∞). We denote by $P(\pi)$ the collineation group generated by A and B. Set $P=P(\pi)$. Then P has the following properties:

(i) $P=AB$, $|P|=q^3$, where q is a power of a prime p, and A and B are elementary abelian normal subgroups of P of order q^2.

(ii) $ab=ba$ implies $a\in A\cap B$ or $b\in A\cap B$ for all $a\in A$ and $b\in B$.

A p-group P is called a p-group of semifield type if it satisfies (i) and (ii) as above. This is the same as a T-group satisfying that all $a\in A-A\cap B$ and all $b\in B-A\cap B$ are regular, defined in [1].

In the paper [1], A. Cronheim has proved as part of a more general theorem that a finite semifield can be constructed for the group P and the ordered pair (A, B). We denote the semifield by $D(A, B)$ and the set of all such ordered pairs (A, B) by V_P. Let W_P denote the set of all abelian subgroups of P of order q^2. Then one of the following holds (Lemma 4.1).

(i) $p=2$ and $|V_P|=2$.

(ii) $p>2$ and $V_P=\{(A, B)\,|\,A\neq B,\ A, B\in W_P\}$.

In this paper we will study the semifields constructed for all (A, B) in V_P.

Let (A, B) and (A', B') be elements in V_P. Then $D(A, B)$ and $D(A', B')$ are isotopic if and only if there exists an automorphism f of P which maps A onto A' and B onto B' (Lemma 4.2). Therefore, we will consider the action of $\mathrm{Aut}(P)$ on the set W_P and will prove the following.

Theorem 4.8. *Let P be a p-group of semifield type of order p^{3n} for an odd prime p and a positive integer n and assume $|W_P|>2$. Set $L=\mathrm{Aut}(P)$, $G=C_L(Z(P))$ and $W=W_P$. Then*

(i) *$|W|=1+p^r$ for a positive divisor r of n.*

(ii) $PSL(2, p^r) \leq G^W \leq L^W \leq P\Gamma L(2, p^r)$ *in the natural doubly transitive representation. Moreover, three-point stabilizer of* G^W *is the identity subgroup.*

As an application of the theorem, we will prove the following.

Corollary 5.2. *Let* π_1 *or* π_2 *be a non-Desarguesian semifield plane and let* P_1 *or* P_2 *be its collineation group generated by all elations, respectively. Then* P_1 *and* P_2 *are isomorphic as abstruct groups if and only if* π_1 *is isomorphic to* π_2 *or its dual.*

This implies that, as an abstruct group, the group $P\,(=P(\pi))$ characterizes the semifield plane π up to its dual.

For the most part we shall use the notation of [2] and [3]. All set, planes and groups will be finite. Throughout this paper, p will stand for a prime.

2. p-groups constructed for semifields

Let D be a set with two binary operations $+$ and $\cdot$. $D=D(+, \cdot)$ is called a finite semifield (also called a division ring, as in [3]) if the following conditions are satisfied:

(i) $D(+)$ is a group with identity element 0.

(ii) $ab=0$ implies $a=0$ or $b=0$ for all $a, b \in D$.

(iii) If $a, b, c \in D$, then $(a+b)c=ac+bc$ and $c(a+b)=ca+cb$.

(iv) There exists an element $1 \in D-\{0\}$ such that $1x=x1=x$ for all $x \in D$.

A semifield is an elementary abelian p-group for some prime p with respect to the operation $+$ (Exercise 7.2 of [3]).

Let D be a semifield of order $q\,(=p^n)$. We define $P(D)$ to be the set of all ordered triples (x, y, z) for $x, y, z \in D$. On $P(D)$, we define the multiplication

$$(x_1, y_1, z_1)(x_2, y_2, z_3) = (x_1+x_2, y_1+y_2, z_1+z_2+y_2x_1)$$

for $x_i, y_i, z_i \in D$, $1 \leq i \leq 2$.

Let $(x_i, y_i, z_i) \in P(D)$ and set $a_i=(x_i, y_i, z_i)$ for $1 \leq i \leq 3$. Then $(a_1a_2)a_3 = (x_1+x_2, y_1+y_2, z_1+z_2+y_2x_1)(x_3, y_3, z_3) = ((x_1+x_2)+x_3, (y_1+y_2)+y_3, (z_1+z_2+y_2x_1)+z_3+y_3(x_1+x_2)) = (x_1+(x_2+x_3), y_1+(y_2+y_3), z_1+(z_2+z_3+y_3x_2)+(y_2+y_3)x_1) = a_1(a_2a_3)$. Hence $(a_1a_2)a_3=a_1(a_2a_3)$. Clearly $(x, y, z)(0, 0, 0)=(0, 0, 0)(x, y, z)=(x, y, z)$ and $(x, y, z)(-x, -y, -z+yx)=(-x, -y, -z+yx)(x, y, z)=(0, 0, 0)$ for all $(x, y, z) \in P(D)$. Thus we have the following.

Lemma 2.1. *If* D *is a semifield, then* $P(D)$ *is a group of order* q^3 *with identity element* $(0, 0, 0)$.

Set $P=P(D)$, $A=\{(x, 0, z) \mid x, z \in D\}$ and $B=(0, y, z)\} \mid y, z \in D\}$. Then the following holds.

Lemma 2.2. (i) $P=AB$, $|P|=q^3$ *and* A *and* B *are elementary abelian* *normal subgroups of P of order q^2.*

(ii) *$ab=ba$ implies $a\in A\cap B$ or $b\in A\cap B$ for all $a\in A$ and $b\in B$.*

Proof. Since $(x, y, z)=(x, 0, z-yx)(0, y, 0)\in AB$ for every $(x, y, z)\in P$, we have $P=AB$. As $(x, y, z)^{-1}=(-x, -y, -z+yx)$, $[(x_1, y_1, z_1), (x_2, y_2, z_2)]=(-x_1, -y_1, -z_1+y_1x_1)(-x_2, -y_2, -z_2+y_2x_2)(x_1, y_1, z_1)(x_2, y_2, z_2)=(0, 0, y_2x_1-y_1x_2)$ and $(x_1, y_1, z_1)(x_2, y_2, z_2)^{-1}=(x_1-x_2, y_1-y_2, z_1-z_2+y_2x_2-y_2x_1)$. Hence it follows that A and B are abelian normal subgroups of P of order q^2. Moreover $(x, 0, z)^p=(px, 0, pz)=(0, 0, 0)$ and $(0, y, z)^p=(0, py, pz)=(0, 0, 0)$. Therefore (i) holds.

Let $a=(x_1, 0, z_1)\in A$, $b=(0, y_2, z_2)\in B$ and assume $ab=ba$. Then $1=a^{-1}b^{-1}ab=[(x_1, 0, z_1), (0, y_2, z_2)]=(0, 0, y_2x_1)$ and so $y_2x_1=0$, whence $x_1=0$ or $y_2=0$. Therefore $a\in A\cap B$ or $b\in A\cap B$ and so (ii) holds.

EXAMPLE 2.3. Let $D=GF(p^n)$ and let f be a mapping from $P(D)$ into $PSL(3, p^n)$ such that

$$f(x, y, z)=\begin{bmatrix}1 & 0 & 0\\ x & 1 & 0\\ z & y & 1\end{bmatrix}^{-1}. \quad \text{Then } f(ab)=f(a)f(b) \text{ for all } a,\ b\in P(D).$$

Therefore $P(D)$ is isomorphic to a Sylow p-subgroup of $PSL(3, p^n)$ in this case.

Two semifields D_1 and D_2 are said to be isotopic if there exists a triple (α, β, γ) of nonsingular additive mappings α, β, γ from D_1 onto D_2 such that $\gamma(xy)=\beta(x)\alpha(y)$ for all $x, y\in D$. Almost as an immediate consequence of the definition we have

Lemma 2.4. *Let D_1 and D_2 be semifields. If D_1 is isotopic to D_2, then $P(D_1)$ is isomorphic to $P(D_2)$.*

Proof. Let (α, β, γ) be an isotopism from D_1 to D_2. We define a mapping from $P(D_1)$ to $P(D_2)$ in such a way that $f(x, y, z)=(\alpha(x), \beta(y), \gamma(z))$ for $(x, y, z)\in P(D_1)$. Clearly f is a bijection. On the other hand, $f(x_1, y_1, z_1)\times(x_2, y_2, z_2)=(x_1+x_2, y_2+y_2, z_1+z_2+y_2x_1)=(\alpha(x_1+x_2), \beta(y_1+y_2), \gamma(z_1+z_2+y_2x_1))=(\alpha(x_1), \beta(y_1), \gamma(z_1))(\alpha(x_2), \beta(y_2), \gamma(z_2))=f(x_1, y_1, z_1)f(x_2, y_2, z_2)$. Thus $P(D_1)$ is isomorphic to $P(D_2)$.

DEFINITION 2.5. Let D be a semifield of order q and let $\pi=\pi(D)$ be a semifield plane of order q coordinatized by D as defined in [3]. We define an action of every element $(x, y, z)\in P(D)$ on $\pi(D)$ in the following way:

$$(\infty)^{(x,y,z)}=(\infty),\quad (a)^{(x,y,z)}=(a+y),\quad (a, b)^{(x,y,z)}=(a+x, b+ya+z),$$
$$[\infty]^{(x,y,z)}=[\infty],\quad [a]^{(x,y,z)}=[a+x],\quad [a, b]^{(x,y,z)}=[a-y, b+(a-y)x+z]$$
$$\text{for } a, b\in D.$$

Set $A=\{(x, 0, z)\mid x, z\in D\}$ and $B=\{(0, y, z)\mid y, z\in D\}$. Then A or B is a collineation group which consists of elations with axis $[\infty]$ or center (∞), respectively. Since $|A|=|B|=q^2$ and the order of $\pi(D)$ is q, A or B is the collineation group of all elations with axis $[\infty]$ or center (∞), respectively. If D is not a field, $P(D)=AB$ is a normal subgroup of the full collineation group of $\pi(D)$ by Lemma 8.5 of [3].

DEFINITION 2.6. A p-group $P=AB$ is called a p-group of semifield type if it satisfies the conditions of Lemma 2.2. Let V_P denote the set of all such pairs (A, B). Let W_P denote the set of all abelian subgroups of P of order q^2. Clearly $A, B\in W_P$.

3. Properties of p-groups of semifield type

Throughout this section let P be a p-group of semifield type of order q with $q=p^n$ for a prime p and let $(A, B)\in V_P$. Set $Z=A\cap B$. Since A is an elementary abelian p-group, $A=A_1\times Z$ for a subgroup A_1 of A. Similarly $B=B_1\times Z$ for a subgroup B_1 of B. By a definition, $|A_1|=|B_1|=|Z|=q$. We can then write each element x of P uniquely in the form $x=abz$ for $a\in A_1$, $b\in B_1$ and $z\in Z$.

Lemma 3.1. *The following hold.*

(i) $[P, P]=Z(P)=Z$.

(ii) $[xy, z]=[x, z][y, z]$, $[x, yz]=[x, y][x, z]$ *for* $x, y, z\in P$ *and* $[x^i, y^j]=[x, y]^{ij}$ *for all integers* i, j.

(iii) *If* $u\in P-A$ *and* $v\in P-B$, *then* $Z=\{[a_1, u]\mid a_1\in A_1\}=\{[v, b_1]\mid b_1\in B_1\}$.

(iv) *If* $x\in P-Z$, *then* $|C_P(x)|=q^2$. *Moreover* $\{g^{-1}xg\mid g\in P\}=xZ$.

Proof. Since $P=AB$ and $C_B(A)=Z$, $C_P(A)=A$. Similarly $C_P(B)=B$. Thus $Z(P)\leq C_P(A)\cap C_P(B)=A\cap B=Z$. Since P/A and P/B are abelian, $[P, P]\leq A\cap B=Z$. On the other hand, since $|\{[a, b]\mid b\in B\}|=|B/C_B(a)|=|Z|$, $[a, B]=Z$ for $a\in A-Z$. Therefore (i) holds and (ii) follows immediately from Theorem 2.2.1 and Lemma 2.2.2 of [2].

Let $v\in P-B$. Then $v=ab$ for suitable $a\in A-Z$ and $b\in B$. As above, $Z=[a, B]=[v, B]=[v, B_1]$. Similarly $Z=[A_1, u]$ for $u\in P-A$. Thus (iii) holds.

Let $x\in P-Z$. Then $x\in P-A$ or $x\in P-B$. Hence $[x, P]=Z$ by (i) and (ii), so that $|C_P(x)|=|P/[x, P|]=q^2$. Thus (iv) holds.

DEFINFTION 3.2. Let $a_0\in A_1-\{1\}$ and $b_0\in B_1-\{1\}$ and let D be any set of symbols with cardinal q such that $0, 1\in D$, $0\neq 1$. Let D^3 be the set of all ordered triples (x, y, z) with $x, y, z\in D$. We define a mapping s from D^3 onto P in the following way.

(i) $s(0, 0, 0)=1$, $s(1, 0, 0)=a_0$ and $s(0, 1, 0)=b_0$.

(ii) s maps the set $\{(x, 0, 0) \mid x \in D, x \neq 0, 1\}$ onto $A_1 - \{1, a_0\}$ in an arbitrary manner.

(iii) Let $s(0, 0, x) = [s(x, 0, 0), s(0, 1, 0)]$ (cf. Lemma 3.1 (iii)).

(iv) Let $s(0, y, 0)$ be a unique element in B_1 such that $s(0, 0, y) = [s(1, 0, 0), s(0, y, 0)]$ (cf. Lemma 3.1 (iii)).

(v) Set $s(x, y, z) = s(0, 0, z)s(0, y, 0)s(x, 0, 0)$.

We define binary operations of addition $+$ and multiplication $\cdot$ into D: For $a, b \in D$, $a+b$ and $a \cdot b$ denote elements of D such that $s(a, 0, 0)s(b, 0, 0) = s(a+b, 0, 0)$ and $s(0, 0, ba) = [s(a, 0, 0), s(0, b, 0)]$, respectively.

By definition, D(+) is isomorphic to A_1, hence it is an abelian group with identity element 0.

Lemma 3.3. *The following hold.*

(i) $s(a, 0, b)s(c, 0, d) = s(a+c, 0, b+d)$ *for* $a, b, c, d \in D$.

(ii) $s(0, a, b)s(0, c, d) = s(0, a+c, b+d)$ *for* $a, b, c, d \in D$.

Proof. $s(a, 0, b)s(c, 0, d) = s(0, 0, b)s(0, 0, d)s(a, 0, 0)s(c, 0, 0) = [s(b, 0, 0), b_0] \times [s(d, 0, 0), b_0]s(a+c, 0, 0) = [s(b+d, 0, 0), b_0]s(a+c, 0, 0)$ (cf. Lemma 3.1 (ii))$= s(0, 0, b+d)s(a+c. 0, 0) = s(a+c, 0, b+d)$. Hence (i) holds. Similarly we have (ii).

Lemma 3.4. $s(x_1, y_1, z_1)s(x_2, y_2, z_2) = s(x_1+x_2, y_1+y_2, z_1+z_2+y_2x_1)$ *for triples* $(x_1, y_1 z_1), (x_2, y_2, z_2) \in D^3$.

Proof. By definition 3.2 and Lemma 3.3, $s(x_1, y_1, z_1)s(x_2, y_2, z_2) = s(0, 0, z_1) \times s(0, y_1, 0)s(x_1, 0, 0)s(0, 0, z_2)s(0, y_2, 0)s(x_2, 0, 0) = s(0, 0, z_1+z_2)s(0, y_1+y_2, 0)$ $s(x_1, 0, 0)[s(x_1, 0, 0), s(0, y_2, 0)]s(x_2, 0, 0) = s(0, 0, z_1+z_2+y_2x_1)s(0, y_1+y_2, 0)$ $s(x_1+x_2, 0, 0) = s(x_1+x_2, y_1+y_2, z_1+z_2+y_2x_1)$. Hence the lemma holds.

We define a multiplication into D^3 in such a way that $(x_1, y_1, z_1)(x_2, y_2, z_2) = (x_1+x_2, y_1+y_2, z_1+z_2+y_2x_1)$. Then we have

Proposition 3.5. (i) $D = D(+, \cdot)$ *is a semifield.*

(ii) $D^3 = P(D)$ *and* D^3 *is isomorphic to* P.

Proof. $D(+)$ is an abelian group with identity element 0 as stated earlier.

By Definition 3.2 (iii) (iv), $1x = x$, $y1 = y$ for all $x, y \in D$. Hence 1 is identity element with respect to multiplication.

Let $a, b \in D$ and assume $ab = 0$. Then $[s(b, 0, 0), s(0, a, 0)] = s(0, 0, 0) = 1$ and so $s(b, 0, 0) \in Z \cap A_1 = 1$ or $s(0, a, 0) \in Z \cap B_1 = 1$. Thus $a = 0$ or $b = 0$.

Let $a, b, c \in D$. Then $s(0, 0, (a+b)c) = [s(c, 0, 0), s(0, a+b, 0)] = [s(c, 0, 0), s(0, a, 0)s(0, b, 0)] = [s(c, 0, 0), s(0, a, 0)][s(c, 0, 0), s(0, b, 0)] = s(0, 0, ac+bc)$ by Lemma 3.1 (ii). Hence $(a+b)c = ac+bc$. Similarly $c(a+b) = ca+cb$. Thus we have (i), and (ii) follows immediately from (i) and Lemma 3.4.

The definition of $D(+,\cdot)$ depends on the choice of the direct factors A_1, B_1 and the elements $a_0\in A_1$, $b_0\in B_1$, whence we will denote it by $D(A_1, B_1, a_0, b_0)$.

Lemma 3.6. *The definition of $D(+,\cdot)$ is independent of the choice of $A_1, B_1, a_0\in A_1-\{1\}$ and $b_0\in B_2-\{1\}$ and uniquely determined up to isotopism. (We denote $D(+,\cdot)$ by $D(A, B)$.)*

Proof. Let $A=A_i\times Z$, $B=B_i\times Z$, $a_i\in A_i-\{1\}$, $b_i\in B_i-\{1\}$, $D_i=D(A_i, B_i, a_i, b_i)$ and let s_i be the isomorphism from $P(D_i)$ onto P defined in Definition 3.2 for $i=1,2$. Set $A_1=\langle c_1, c_2, \cdots, c_n\rangle$ and $B_1=\langle d_1, d_2, \cdots, d_n\rangle$. Since $A=A_1Z=A_2Z$ and $B=B_1Z=B_2Z$, $A_2=\langle c_1u_1, c_2u_2, \cdots, c_nu_n\rangle$ and $B_2=\langle d_1v_1, d_2v_2, \cdots, d_nv_n\rangle$ for suitable elements $u_i, v_i\in Z$, $1\leq i\leq n$. Let g be a mapping from P onto itself defined by $g(\prod_i c_i^{x_i}\prod_j d_j^{y_j}z)=\prod_i c_i^{x_i}\prod_j d_j^{y_j}\prod_i u_i^{x_i}\prod_j v_j^{y_j}z$ for integers x_i, y_j, $1\leq i, j\leq n$ and $z\in Z$. It is easily verified that g is an automorphism of P. Set $h=s_2^{-1}gs_1$. Then h is an isomorphism from $P(D_1)$ to $P(D_2)$.

We now define three mappings α, β, γ in such a way that $(\alpha(x), 0, 0)=h(x, 0, 0)$, $(0, \beta(y), 0)=h(0, y, 0)$ and $(0, 0, \gamma(z))=h(0, 0, z)$. Then $h(x, y, z)=h(0, 0, z)h(0, y, 0)h(x, 0, 0)=(0, 0, \gamma(z))(0, \beta(y), 0)(\alpha(x), 0, 0)=(\alpha(x), \beta(y), \gamma(z))$. Since $h(x_1, y_1, z_1)(x_2, y_2, z_2)=h(x_1, y_1, z_1)h(x_2, y_2, z_2)$, $(\alpha(x_1+x_2), \beta(y_1+y_2), \gamma(z_1+z_2+y_2x_1))=(\alpha(x_1)+\alpha(x_2), \beta(y_1)+\beta(y_2), \gamma(z_1)+\gamma(z_2)+\beta(y_2)\alpha(x_1))$ for all $x_1, y_1, z_1, x_2, y_2, z_2\in D_1$. Therefore $\mu(x+y)=\mu(x)+\mu(y)$ for $\mu\in\{\alpha, \beta, \gamma\}$ and $\gamma(yx)=\beta(y)\alpha(x)$ for all $x, y\in D_1$. Hence (α, β, γ) is an isotopism from D_1 onto D_2 and so the lemma holds.

Lemma 3.7. *Let $P=AB$ be a p-group of semifield type with $(A, B)\in V_P$ and let x be an automorphism of P which fixes A and B and centralizes $Z=A\cap B$. If x centralizes a nontrivial element of the factor group P/Z, then x centralizes P/Z.*

Proof. Let $Z\neq uZ\in C_{P/Z}(x)$. Then $u=ab$ for suitable $a\in A$ and $b\in B$. Since $Z\neq uZ$, $a\notin Z$ or $b\notin Z$. We may assume $a\notin Z$. Then $[abZ, b_1]=[abZ, b_1]^x=[abZ, b_1]^x$ for every $b_1\in B$. Hence $[abZ, b_1^{-1}b_1^x]=1$ by Lemma 3.1 (ii), and so $b_1^{-1}b_1^x\in Z$ as $b_1^{-1}b_1^x\in B$ and $a\in A-Z$. This implies that $b_1Z\in C_{P/Z}x)$ for all $b_1\in B$. Therefore $B/Z\leq C_{P/Z}(x)$, and similarly $A/Z\leq C_{P/Z}(x)$. Thus we have the lemma.

4. The action of Aut(P) on the set W_P

Throughout this section, let $P=AB$ be a p-group of semifield type of order q^3, $q=p^n$, p a prime and let V_P and W_P be as in Definition 2.6. Clearly (A, B), $(B, A)\in V_P$ and $A, B\in W_P$. Furthermore, for each $C\in W_P$, C is a normal subgroup of P which contains $Z=A\cap B$ by Lemma 3.1 (i) (iv).

Lemma 4.1. *The following hold.*

(i) *If* $p=2$, *then* $V_P=\{(A, B), (B, A)\}$.

(ii) *If* $p>2$, *then* $V_P=\{(A', B') \mid A' \neq B', A', B' \in W_P\}$.

Proof. Set $D=D(A, B)$. By Proposition 3.5, D is a semifield and P is isomorphic to $P(D)$. Let $C \in W_P-\{A, B\}$. For $(x, y, z) \in P(D)$ and a positive integer m, $(x, y, z)^m=(mx, my, mz+(1+2+\cdots+(m-1))yx)$. Hence C is an elementary abelian p-group if $p>2$, while C is a homocyclic 2-group of exponent 4 if $p=2$. In particular $V_p=\{(A, B), (B, A)\}$ if $p=2$.

Let $A', B' \in W_P$ with $A' \neq B'$ and suppose $p>2$. Then A' and B' are elementary abelian normal p-subgroups of P of order q^2 which contain Z. By Lemma 3.1 (iv), $A' \cap B'=Z$. Therefore $A'B'=P$. Let $a' \in A'$, $b' \in B'$ and assume $a'b'=b'a'$. If $a' \notin Z$, then $b' \in C_P(a') \cap B'=A' \cap B'=Z$. Thus $(A', B') \in V_P$.

Lemma 4.2. *Let* (A, B) *and* $(A', B') \in V_P$. *Then* $D(A, B)$ *is isotopic to* $D(A', B')$ *if and only if there exists an automorphism* f *of* P *which maps* A *onto* A' *and* B *onto* B'.

Proof. Set $D_1=D(A, B)$, $D_2=D(A', B')$ and let s_i be the isomorphism from $P(D_i)$ to P defined in Definition 3.2 for $i=1, 2$.

Suppose D_1 is isotopic to D_2 and let (α, β, γ) be an isotopism from D_1 to D_2. Let h be a mapping from $P(D_1)$ onto $P(D_2)$ such that $h(x, y, z)=(\alpha(x), \beta(y), \gamma(z))$ for $x, y, z \in D_1$. For (x_1, y_1, z_1) and $(x_2, y_2, z_2) \in P(D_1)$, $h(x_1, y_1, z_1)(_2, y_?, z_2)=(\alpha(x_1+x_2), \beta(y_1+y_2), \gamma(z_1+z_2+y_2x_1))=(\alpha(x_1)+\alpha(x_2), \beta(y_1)+\beta(y_2), \gamma(z_1)+\gamma(z_2)+\beta(y_2)\alpha(x_1))=h(x_1, y_1, z_1)h(x_2, y_2, z_2)$. Hence h is an isomorphism from $P(D_1)$ onto $P(D_2)$. Set $f=s_2hs_1^{-1}$. Then f is an automorphism of P which maps A onto A' and B onto B'.

Conversely, let f be an automorphism of P which maps A onto A' and B onto B'. We set $h=s_2^{-1}fs_1$ and define three mappings α, β, γ from D_1 onto D_2 in such a way that $h(x, y, z)=(\alpha(x), \beta(y), \gamma(z))$ for $x, y, z \in D_1$. By a similar argument as in the proof of Lemma 3.6, (α, β, γ) is an isotopism from D_1 onto D_2. Thus we have the lemma.

Let D be a semifield and let N_l, N_m or N_r be its left, middle or right nucleus, respectively (cf. [3]). We note that N_l, N_m and N_r are fields and that $N_l=N_r$ if D is commutative.

Proposition 4.3. *Let* $P=AB$ *be a* p-*group of semifield type with* $(A, B) \in V_P$. *Then the following hold.*

(i) $D(A, B)$ *is isotopic to a commutative semifield if and only if* $|W_P|>2$.

(ii) *Suppose* $D(A, B)$ *is isotopic to a commutative semifield* D_0 *and set* $Q=P(D_0)$. *Then* Q *is isomorphic to* P *and* $W_Q=\{C_k \mid k \in N_m \cup \infty\}$, *where* N_m *is the middle nucleus of* D_0 *and* $C_k=\{(x, kx, z) \mid x, z \in D_0\}$, $C_\infty=\{(0, y, z) \mid y, z \in D_0\}$

for $k\in N_m$.

Proof. To prove (ii) and "only if" part of (i), we may assume that $D=D(A,B)$ is commutative and $P=P(D)$ by Lemmas 2.4, 4.2 and Proposition 3.5 (ii). Then $A=\{(x,0,z)\mid x,z\in D\}$ and $B=\{(0,y,z)\mid y,z\in D\}$. Let $k\in N_m-\{0\}$ and set $C_k=\{(x,kx,z)\mid x,z\in D\}$. Since $k\in N_m$ and D is commutative, $[(x,kx,z),(x',kx',z')]=(0,0,(kx')x-(kx)x')=1$ and so C_k is an abelian subgroup of order q^2. In particular $|W_P|>2$. Conversely, let $C\in W_P-\{A,B\}$. Since $C\cap B=\{(0,0,z)\mid z\in D\}$, there is a unique element $k\in D$ such that $(1,k,0)\in C$. By Lemma 3.1 (iv), $C=C_P(1,k,0)=\{(x,kx,z)\mid x,z\in D\}$. Therefore $1=[(x,kx,z),(x',kx',z')]=(0,0,(kx')x-(kx)x')$ and hence $(kx')x=(kx)x'$ for all $x,x'\in D$. Thus $k\in N_m$.

We now assume $|W_P|>2$ and let $C\in W_P$, $C\neq A,B$. Let $c\in C-Z$. Then there are $a_0\in A$ and $b_0\in B$ such that $c=a_0b_0$. Since $C\cap A=C\cap B=Z$, neither a_0 nor b_0 is contained in Z. Hence we can choose subgroups A_1 of A and B_1 of B such that $a_0\in A_1$, $b_0\in B_1$, $A=A_1\times Z$ and $B=B_1\times Z$. Set $D_0=D(A_1,B_1,a_0,b_0)$. By Lemma 3.6, D is isotopic to D_0. Let s be an isomorphism from $P(D_0)$ onto P defined in Definition 3.2. Since $s^{-1}(c)=s^{-1}(a_0)s^{-1}(b_0)=(1,0,0)(0,1,0)=(1,1,1)$, $s^{-1}(c)=s^{-1}(C_P(C))=C_{P(D_0)}(1,1,1)=\{(x,x,z)\mid x,z\in D_0\}$. Therefore $\{(x,x,z)\mid x,z\in D_0\}$ is abelian and so $1=[(x,x,z),(x',x',z')]=(0,0,x'x-xx')$ for all $x,x'\in D_0$. Hence $x'x=xx'$ for all $x,x'\in D_0$, so that D_0 is commutative.

Theorem 4.4. *Let D be a semifield of order q and set* $\pi=\pi(D)$, $P=P(D)$. *Then the following conditions are equivalent.*

(i) π *is a Desarguesian plane of order q.*

(ii) $|W_P|=q+1$.

(iii) $C_P(x)$ *is abelian for all* $x\in P-Z(P)$.

Proof. Suppose (i). By Lemma 2.4, we may assume that D is a field. Clearly the middle nucleus of D is equal to D. Using Proposition 4.3, $|W_P|=|N_m|+1=|D|+1=q+1$, so (i) implies (ii).

Suppose (ii). Set $Z=Z(P)$. Then $|P-Z|/|A-Z|=q+1=|W_P|$ for $A\in W_P$. By Lemma 3.1 (iv), $A\cap B=Z$ for all $A,B\in W_P$ $(A\neq B)$. Hence $\bigcup_{A\in W_P} A-Z=P-Z$. Thus (ii) implies (iii).

Suppose (iii). Then, obviously $|W_P|>2$ and so, by Proposition 4.3 (ii), D is isotopic to a commutative semifield D_0. Hence P is isomorphic to $P(D_0)$ by Lemma 2.4 and Proposition 3.5. Let k be any element in D_0. Since $(1,k,0)\notin Z(P(D_0))$, $C_{P(D_0)}(1,k,0)=\{(x,kx,z)\mid x,z\in D_0\}$ isa belian. From this, $1=[(x,kx,z),(x',kx',z')]=(0,0,(kx')x-(kx)x')$ and so $(kx')x=(kx)x'$ for all $x,x'\in D_0$. As D_0 is commutative, this implies that k is an element of the middle nucleus of D_0 for all $k\in D_0$. Therefore D_0 is a field and so $\pi=\pi(D_0)$ is a Desarguesian plane of order q. Thus (iii) implies (i).

Let $P=AB$ be a p-group of semifield type. By Proposition 4.3, $|W_P|=1+p^r$ for a non negative integer r. Since automorphic images of abelian subgroups are also abelian, the automorphism group of P induces a permutation group on W_P. We denote by Aut(P) the automorphism group of P.

Lemma 4.5. *Let D_0 be a commutative semifield of odd order and let N_m or N_r be the middle or right nucleus of D_0, respectively. For $a, b, c, d \in N_m$ with $0 \neq ad-bc \in N_r$, we define a mapping $f=f_{(a,b,c,d)}$ from $P(D_0)$ into itself in the following way:*

$$f(x, y, z) = (ax+by,\ cx+dy,\ \{x(acx)+y(bdy)\}/2+x(bc)y+(ad-bc)z)\,.$$

Then the following hold.

(i) *f is an automorphism of $P(D_0)$.*

(ii) *Let C_k, $k \in N_m \cup \infty$ be as defined in Proposition 4.3 (ii). The action of $f=f_{(a,b,c,d)}$ on $W_{P(D_0)}$ is equivalent to that of $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL(2, N_m)$ on $PG(1, N_m)=$ $\left\{\begin{bmatrix} 1 \\ k \end{bmatrix} \mid k \in N_m\right\} \cup \left\{\begin{bmatrix} 0 \\ 1 \end{bmatrix}\right\}$.*

Proof. Let $(x_1, y_1, z_1), (x_2, y_2, z_2) \in P(D_0)$ and set $x_0=x_1+x_2$, $y_0=y_1+y_2$, $z_0=z_1+z_2+y_2x_1$. Then $f(x_1, y_1, z_1)f(x_2, y_2, z_2)=(ax_0+by_0,\ cx_0+dy_0,\ z')$. Here $z'=\{x_1(acx_1)+y_1(bdy_1)\}/2+x_1(bc)y_1+(ad-bc)z_1+\{x_2(acx_2)+y_2(bdy_2)\}/2+x_2(bc)y_2+(ad-bc)z_2+(cx_2+dy_2)(ax_1+by_1)=\{x_1(acx_1)+2x_1(acx_2)+x_2(acx_2)\}/2+\{y_1(bd)y_1+2y_1(bdy_2)+y_2(bd)y_2\}/2+\{x_1(bc)y_1+x_2(bc)y_2+x_2(bc)y_1+x_1(bc)y_2\}+\{-x_1(bc)y_2+x_1(ad)y_2+(ad-bc)(z_1+z_2)\}=\{x_0(acx_0)+y_0(bdy_0)\}/2+x_0(bc)y_0+(ad-bc)z_0$ because $a, b, c, d \in N_m$ and $ad-bc \in N_r=N_l$. Hence we have $f(x_1, y_1, z_1)f(x_2, y_2, z_2)=f(x_1, y_1, z_1)(x_2, y_2, z_2)$ and so f is a homomorphism. Assume $f(x, y, z)=1$ for some $(x, y, z) \in P(D_0)$. Then $ax+by=0$ and $cx+dy=0$. Since $a, b, c, d \in N_m$ and $ad-bc \neq 0$, we have $x=y=0$ and so $(ad-bc)z=0$. Hence $(x,y,z)=(0,0,0)$. Therefore (i) holds.

Let C_k, $k \in N_m \cup \infty$ be as defined in Proposition 4.3 (ii). Then $f(x, kx, z)=((a+bk)x, (c+dk)x, z')$ and $f(0, y, z)=(by, dy, z'')$ for some $z', z'' \in D_0$. Hence $f(C_k)=C_{k'}$, $k'=(c+dk)/(a+bk)$. Here we set $(c+d\infty)/(a+b\infty)=d/b$ and $u/0=\infty$. Then (ii) holds.

Lemma 4.6. *Let p be an odd prime and let P be a p-group of semifield type of order q^3, $q=p^n$. Suppose $|W_P|>2$ and set $|W_P|=1+p^r$ $(r \geq 1)$. Then there exists an automorphism group M of P which has the following properties:*

(i) *M fixes every element of $Z(P)$.*

(ii) *The restriction of M on W_P is isomorphic to $PSL(2, p^r)$ in its natural permutation representation on $PG(1, p^r)$.*

Proof. By Propositions 3.5 and 4.3, we may assume that $P=P(D_0)$ for a commutative semifield D_0. We apply Lemma 4.5 to D_0. Let notations be as in Lemma 4.5 and let M denote the group generated by all $f_{(a,b,c,d)}$ such that $a, b, c, d\in N_m$ and $ad-bc=1$. Then M satisfies (i) and (ii) of the lemma.

Lemma 4.7. *Let P be a p-group of semifield type for an odd prime p. Let f be an autom orphism of P which fixes each element of $Z(P)$ and fixes three distinct elements of W_P. Then f acts trivially on W_P.*

Proof. Suppose $A^f=A$, $B^f=B$, $C^f=C$ for $A, B, C\in W_P$ with $A\neq B\neq C\neq A$. Let $x\in A-Z$. By Lemma 4.1, $A\cap B=B\cap C=C\cap A=Z$. Hence, there is $b\in B-Z$ such that $xb\in C-Z$. Then $1=[xb, (xb)^f]=[b, x^f][x, b^f]=[b, x^f][x, b^f]^{f^{-1}}$ and so $[b, x^f]=[b, x^{f^{-1}}]$. Hence $x^f\in x^{f^{-1}}Z$ for $x\in A-Z$. Similarly $y^f\in y^{f^{-1}}Z$ for $y\in B-Z$. Thus f^2 centralizes P/Z. By Lemma 3.7, $f=1$ or f inverts P/Z and so the lemma holds.

NOTATION: Let X be a group which acts on a set S. We denote by X^S the restriction of X on S.

Using Lemma 4.7, we now prove the following.

Theorem 4.8. *Let P be a p-group of semifield type of order p^{3n} for an odd prime p and a positive integer n and assume $|W_P|>2$. Set $L=\mathrm{Aut}(P)$, $G=C_L(Z(P))$ and $W=W_P$. Then*

(i) *$|W|=1+p^r$ for a positive divisor r of n.*

(ii) *$PSL(2,p^r)\le G^W\le L^W\le P\Gamma L(2,p^r)$ in the natural doubly transitive representation. Moreover, three-point stabilizer of G^W is the identity subgroup.*

Proof. Since $|W_P|>2$, we can apply Proposition 4.3 and Lemmas 4.6 and 4.7. Let M, D_0, N_m and C_k be as in them. Since D_0 is a vector space over N_m, $|W|=1+p^r$ for a positive divisor r of n by Proposition 4.3. By Lemma 4.6, $G^W\ge M^W=PSL(2,p^r)$ and so G^W is doubly transitive. Let H be the stabilizer of C_0 and C_1 and set $N=M\cap H$. By a property of $PSL(2,p^r)$, N has exactly two orbits on $W-\{C_0, C_1\}$. By Lemma 4.7, $|H^W: N^W|=1$ or 2, so that $|G^W: M^W|=1$ or 2. Hence $L^W\trianglerighteq[G^W, G^W]=M^W=PSL(2,p^r)$. Therefore L^W is a normal extension of $PSL(2,p^r)$. By a property of $PSL(2,p^r)$, we have the lemma.

5. Correspondence between semifields and p-groups of semifield type

Let $D=D(+,\cdot)$ be a semifield. A dual semifield $D^*=D(\tilde{+},\tilde{\cdot})$ of D is defined in such a way that

$$a\tilde{+}b = a+b\,, \quad a\cdot b = b\cdot a\,, \quad \text{for} \quad a, b\in D\,.$$

We note that the equation $ma+b=k$ is equal to $(-a)\tilde{\cdot}(-m)\tilde{+}(-k)=-b$. Let τ be a mapping from the dual plane $\pi(D)^*$ of $\pi(D)$ onto $\pi(D^*)$ defined in the following manner:

$$\tau(\infty) = [\infty]\,, \quad \tau(a) = [-a]\,, \quad \tau(a, b) = [-a, -b]\,, \quad \tau[\infty] = (\infty)\,,$$
$$\tau[m] = (-m)\,, \quad \tau[m, k] = (-m, -k)\,, \qquad \text{for} \quad a, b, m, k\in D\,.$$

Then τ is an isomorphism from $\pi(D)^*$ onto $\pi(D^*)$.

Let $P=AB$ be a p-group of semifield type and set $D=D(A, B)$. Then $\pi(D)^*$ is isomorphic to $\pi(D(B, A))$. Hence $D^*=D(A, B)^*$ is isotopic to $D(B, A)$ by Theorem 8.11 of [3]. Therefore we have the following theorem as a result of Lemma 4.2 and Theorem 4.8.

Theorem 5.1. *Let $P=AB$ and $P'=A'B'$ be p-groups of semifield type for a prime p. Then P is isomorphic to P' if and only if one of the following holds.*
(i) *$D(A, B)$ and $D(A', B')$ are isotopic.*
(ii) *$W_P=\{A, B\}$, $W'_P=\{A', B'\}$ and the dual of $D(A, B)$ is isotopic to $D(A', B')$.*

Proof. Suppose that the groups P and P' are isomorphic and deny (i). We may assume $P=P'$ and $(A, B), (A', B')\in V_P$. By Lemma 4.2 and Theorem 4.8, we have $|W_P|=2$. Then $V_P=\{(A, B), (B, A)\}$ and so $A'=B, B'=A$. Therefore the dual of $D(A, B)$ is isotopic to $D(A', B')$. It follows from Proposition 4.3 that $W_P=\{A, B\}$, for otherwise $D(A, B)$ is isotopic to its dual. Hence (ii) holds.

Conversely, suppose (i) or (ii) and set $D_1=D(A, B)$, $D_2=D(B, A)$, $D_3=D(A', B')$. Then, by Proposition 3.5 (ii), P, $P(D_1)$ and $P(D_2)$ are isomorphic. Similarly P' and $P(D_3)$ are isomorphic. Since D_3 is isotopic to D_1 or D_2, P is isomorphic to P' by Lemma 2.4.

By Theorem 5.1 and by the fact that we have seen in Definition 2.5, we obtain the following.

Corollary 5.2. *Let π_1 or π_2 be a non-Desarguesian semifield plane and let P_1 or P_2 be its collineation group generated by all elations, respectively. Then P_1 and P_2 are isomorphic as abstract groups if and only if π_1 is isomorphic to π_2 or its dual.*

Acknowledgement
The author wuold like to thank the referee for his valuable suggestions. In particular the proofs to Lemmas 3.1, 4.7 and Theorem 4.4 have been shortened by these efforts.

References

[1] A. Cronheim: *T-groups and their geometry,* Illinois J. Math. **9** (1965), 1–30.
[2] D. Gorenstein: Finite groups, Harper and Row, New York, 1968.
[3] D.R. Hughes and F.C. Piper: Projective planes, Springer-Verlag, Berlin-Heidelberg-New York, 1973.

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