Can. J. Math., Vol. XXXIX, No. 4, 1987, pp. 784-793

THE MULTIPLICATIVE GROUPS OF QUASIFIELDS

MICHAEL J. KALLAHER

1. Introduction Let $(Q, +, \cdot)$ be a finite quasifield of dimension d over its kernel $K = GF(q)$, where $q = p^k$ with p a prime and $k \geqq 1$. (See p. 18-22 and p. 74 of [7] or Section 5 of [9] for the definition of quasifield.) For the remainder of this article we will follow standard conventions and omit, whenever possible, the binary operations $+$ and $\cdot$ in discussing a quasifield. For example, the notation Q will be used in place of the triple $(Q, +, \cdot)$ and Q^* will be used to represent the multiplicative loop $(Q - \{0\}, \cdot)$.

Let m be a non-zero element of the quasifield Q; the *right multiplicative mapping* $\rho_m: Q \to Q$ is defined by

$$(1) \quad x\rho_m \equiv xm, \quad x \in Q.$$

This mapping is an element of the group of all mappings on Q with composition as the binary operation. The *multiplicative group* of Q is the subgroup $\mathfrak{M}(Q)$ generated by the mappings ρ_m, where $m \in Q^*$. That is,

$$(2) \quad \mathfrak{M}(Q) \equiv \langle \rho_m | m \in Q^* \rangle.$$

The purpose of this article is to investigate the possibilities for Q given that $\mathfrak{M}(Q)$ satisfies certain properties. Apparently, this problem has not been considered before. Albert in his work on semifields used the mappings ρ_m, but he did not investigate the relationship between Q and $\mathfrak{M}(Q)$. (See [1] and others to which he refers in the footnotes.) From one viewpoint this neglect is justified. As we shall see, distinct non-isomorphic quasifields of the same order can have the same multiplicative group. On the other hand, we shall show that the multiplicative group $\mathfrak{M}(Q)$ does influence the nature of Q.

In Section 2 some basic known facts about the groups $\mathfrak{M}(Q)$ are given, and some examples are considered. In Section 3 one of the principal results of this article is proven; namely, it is shown that the group $\mathfrak{M}(Q)$ is solvable if and only if the quasifield is a generalized André system or one of twelve exceptions. This result has its origins in [8]. Using this result, in Section 4 there is presented a generalization of Rao's characterization of generalized André systems.

The reader is assumed to be familiar with the basic results on quasifields and translation planes, as given in either of the monograms [3], [7], or [9].

Received March 24, 1983.

Is is also assumed that the reader knows the basic facts concerning permutation groups as given in [**11**], for example.

2. Basic facts. In this section some simple facts about the groups $\mathfrak{M}(Q)$ are derived and some examples are given. Most of the facts are well-known; see, for example, 5.1.2 in [**3**].

LEMMA 2.1. *Let Q be a quasifield of finite dimension d over its kernel $K = GF(q)$, where $q = p^k$ with p a prime and $k \geqq 1$. The group $\mathfrak{M}(Q)$ is a transitive group of linear transformations on Q as a vector space over K.*

Proof. Let $x, y, m \in Q$ and let $k \in K$. Then

$$(x + y)m = xm + ym$$

or

$$(x + y)\rho_m = x\rho_m + y\rho_m;$$

also

$$(kx)m = k(xm)$$

or

$$(kx)\rho_m = k(x\rho_m).$$

Hence, $\mathfrak{M}(Q)$ is a group of linear transformations on Q. It is also transitive since, given $x, z \in Q^* = Q - \{0\}$ there exists $m \in Q^*$ with $xm = z$, or $x\rho_m = z$.

LEMMA 2.2. *Under the hypothesis of Lemma* 2.1 *the following statements hold*:

(i) *For every $m \in Q^* = Q - \{0\}$ with $m \neq 1$ the right multiplication ρ_m is fixed-point-free on Q^*.*

(ii) *If $m \in Q^*$ then $|\rho_m| \mid |Q^*|$.*

Proof. Under multiplication the set Q^* forms a loop. Hence, for $x \in Q^*$ the equation $x\rho_m = x$, or $xm = x \cdot 1$, holds if and only if $m = 1$. This gives statement (i). Statement (ii) follows from statement (i).

The next two lemmas describe some conditions on (Q) which force the quasifield Q to be a nearfield or a semifield.

LEMMA 2.3. *Let Q be a quasifield of dimension d over its kernel $K = GF(q)$, where $q = p^k$ with p a prime and $k \geqq 1$. The following statements are equivalent*:

(i) *The quasifield Q is a nearfield; that is, the multiplication in Q is associative.*

(ii) $(Q) = \{\rho_m | m \in Q^*\}$.

(iii) *The group (Q) has size $q^d - 1$.*

https://doi.org/10.4153/CJM-1987-038-x Published online by Cambridge University Press

Proof. The multiplication in Q is associative if and only if for all $x, m, n \in Q$

$$(xm)n = x(mn);$$

that is, if and only if for all $m, n \in Q^*$

$$\rho_m\rho_n = \rho_{mn}.$$

The lemma easily follows.

LEMMA 2.4. *Let Q be a quasifield of dimension d over its kernel $K = GF(q)$ where $q = p^k$ with p a prime and $k \geqq 1$. The quasifield Q is a semifield if and only if for all $m, n \in Q^*$,*

$$\rho_m + \rho_n = \rho_{m+n}.$$

Proof. This lemma follows easily from the definitions.

Lemmas 2.3 and 2.4 are originally due to Bruck and Bose [**2**, Section 11].

We close this section with a few examples. The Hall quasifields are defined as follows. Let $K = GF(q)$ with $q = p^k \geqq 2$ and p a prime, and let $f(x) = x^2 - rx - s$ be an irreducible polynomial over K. If H is the set of ordered pairs (a, b) with $a, b \in K$, a multiplication $\cdot$ is defined by

$$(a, b) \cdot (c, d) \equiv \begin{cases} (ad, bd) & \text{if } c = 0 \\ (bc - ad + ra, bd - ac^{-1}f(d)) & \text{if } c \neq 0. \end{cases}$$

Addition in H is the usual coordinate addition. This gives a quasifield $H(q)$ of order q^2 and kernel $K \cong \{(0, d) \mid d \in K\}$. Different polynomials may give rise to nonisomorphic Hall quasifields. Using the standard basis, the right multiplicative mappings have the matrix representation

$$\rho_{(c,d)} \equiv \begin{cases} \begin{bmatrix} d & 0 \\ 0 & d \end{bmatrix} & \text{if } c = 0 \\ \begin{bmatrix} -d + r & -c^{-1}(d^2 - rd - s) \\ c & d \end{bmatrix} & \text{if } c \neq 0. \end{cases}$$

Consider first the case $q = p = 3$. There are two nonisomorphic Hall quasifields. One, $H_1(3)$, results by taking $f(x) = x^2 + 1$. This is the nearfield of order 9, and the multiplicative group $\mathfrak{M}(H_1(3))$ is the quaternion group of order 8. The second, $H_2(3)$, results by taking $f(x) = x^2 + x + 2$. For this quasifield the product of the right multiplicative mappings $\rho_{(1,1)}$ and $\rho_{(1,0)}$ is the 3-element

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

in $GL(2, 3)$. It follows that $\mathfrak{M}(H_2(q)) = GL(2, 3)$. If $q > 3$ then the

results of the next section show that $\mathfrak{M}(H(q)) = GL(2, q)$. If $q = 2$ then $H(2) = GF(4)$ and $\mathfrak{M}(H(2)) = GF(4)^*$.

Another example is the class of Walker quasifields. Let $K = GF(q)$ with $q = p^k \equiv -1 \pmod 6$, and p a prime. On W, the set of ordered pairs of elements in K, a new multiplication $\cdot$ is defined by

$$(a, b) \cdot (c, d) = \left(a(d - c^2) + bc, -\frac{1}{3}ac^3 + bd\right).$$

(The element $1/3$ exists in K since $q \equiv -1 \pmod 6$.) As with the Hall quasifields, addition in W is the usual coordinate addition. This gives a quasifield $W(q)$ of order q^2 and kernel K. Using the standard basis, the right multiplicative mappings have the matrix representation

$$\rho_{(c,d)} = \begin{bmatrix} d - c^2 & -\frac{1}{3}c^3 \\ c & d \end{bmatrix}.$$

The results of the next section show that $\mathfrak{M}(W(q)) = GL(2, q)$. Thus, the groups $\mathfrak{M}(Q)$ will not in general distinguish between different types of quasifields.

3. Quasifields Q with $\mathfrak{M}(Q)$ solvable. This section considers quasifields Q whose multiplicative group $\mathfrak{M}(Q)$ is solvable. As opposed to the general situation where $\mathfrak{M}(Q)$ appears to have little influence on Q (see the previous section) solvability of $\mathfrak{M}(Q)$ severely restricts the possible structures for Q.

One class of quasifields with solvable multiplicative group is the class of generalized André systems, first defined by Foulser [**4**]. The description given here is due to Ostrom [**10**]. Consider the finite field $GF(q^d)$, where d is a positive integer and $q = p^k$ with p a prime and $k \geqq 1$. Associate with each $m \in GF(q^d) - \{0\}$ an automorphism $\alpha(m)$ of $GF(q^d)$ fixing $GF(q)$ pointwise. Define on $GF(q)$ a new multiplication $\circ$ by

$$X \circ m \equiv x^{\alpha(m)}m.$$

Then $(GF(a^d), +, \circ)$, where $+$ is the usual field addition, is a quasifield called a generalized André system. Furthermore, for each $m \in GF(q^d) - \{0\}$ the mapping

$$\rho_m : x \to x \circ m = x^{\alpha(m)}m$$

is an element of $\Gamma L(1, q^d)$. Hence the multiplicative group is solvable. Note that every finite field is a generalized André system, as is every regular nearfield. (See [**9**; p. 41].)

Other quasifields with solvable multiplicative groups include four irregular nearfields as well as the quasifields coordinatizing the planes of

type $F * p$. where $p = 7$ or 11, described in [**9**; Section 19]. The following theorem indicates that there are only a few others. (See the remark after the theorem.)

THEOREM 3.1. *Let Q be a finite quasifield of dimension d over its kernel $K = GF(q)$, where $q = p^k$ with p a prime and $k \geqq 1$. If the multiplicative group $\mathfrak{M}(Q)$ is solvable, then one of the following statements holds*:

(i) *The quasifield Q is a generalized André system.*

(ii) *The quasifield Q is the nonassociative quasifield of order* 9 *and* $\mathfrak{M}(Q) = GL(2, 3)$.

(iii) *The quasifield Q is a solvable irregular nearfield N_p of order* $p^2 = 5^2, 7^2, 11^2,$ *or* 23^2.

(iv) *The quasifield Q coordinatizes the Lüneburg translation plane $F * p$, where $p = 7$ or* 11.

(v) *One of the following holds*:

(a) *The dimension $d = 2$ and $q = 5$, and the group $\mathfrak{M}(Q)$ is one of two groups having order* 48 *and* 96 *respectively.*

(b) *The dimension $d = 2$ and $q = 7$, and the group $\mathfrak{M}(Q) = \langle \mathfrak{M}(N_7), 2I_2 \rangle$ of order* 144.

(c) *The dimension $d = 2$ and $q = 11$, and the group $\mathfrak{M}(Q) = \langle \mathfrak{M}(N_{11}), C \rangle$ of order* 240, *where*

$$C = \begin{bmatrix} 9 & 1 \\ 1 & 4 \end{bmatrix}.$$

(d) *The dimension $d = 4$ and $q = 3$, and $\mathfrak{M}(Q)$ is one of three groups having order* 160, 320, *and* 640 *respectively.*

Proof. By Lemma 2.1 the group $\mathfrak{M}(Q)$ is a solvable transitive group of linear transformations on Q as a vector space of dimension d over K. Thus, Huppert's theorem on such groups can be applied. (See [**6**] or [**11**; p. 246].) Hence, either $\mathfrak{M}(Q) \leqq \Gamma L(1, p^{kd})$ or $\mathfrak{M}(Q)$ is one of thirteen exceptions.

First, if $\mathfrak{M}(Q) \leqq \Gamma L(1, p^{kd})$ then every mapping in $\mathfrak{M}(Q)$ has the form

$$x \to x^{p^s} a, \quad 1 \leqq s \leqq kd, \quad a \in GF(q^d)^*.$$

In particular, this must be the form of the right multiplicative mappings ρ_m with $m \in Q^*$. If follows that Q is a generalized André system. Hence, in this case statement (i) holds.

We turn now to the thirteen exceptions of Huppert's theorem. Two exceptions occur with $d = 2$ and $q = p = 3$. They are $SL(2, 3)$ and $GL(2, 3)$. The group $SL(2, 3)$ cannot occur. The group $SL(2, 3)$ has a normal Sylow 2-subgroup S. By statement (ii) of Lemma 2.2 each ρ_m has order dividing $|Q^*| = 8$. It follows that

$$\langle \rho_m | m \in Q^* \rangle = S \neq SL(2, 3).$$

The group $GL(2, 3)$ does occur; it is $\mathfrak{M}(Q)$ for the nonassociative quasifield Q of order 9. (See Section 2.)

Three exceptions occur when $q = p = 5$ and $d = 2$. The groups are: a group $G_1 = \langle A, B\rangle$ of order 24, a group $G_2 = \langle A, B, 2I\rangle$ of order 48, and a group $G_3 = \langle A, B, C\rangle$ of order 96. Here I is the 2 by 2 identity matrix and

$$A = \begin{bmatrix} 0 & 4 \\ 1 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 3 \\ 4 & 3 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}.$$

(These are taken over $GF(5)$.) The group G_1 is the multiplicative group of the irregular nearfield N_5 of order 25. (See [**6**; p. 126-128] and [**3**; p. 230-231].) The group

$$G_2 = \langle \mathfrak{M}(N_5), 2I\rangle$$

is the multiplicative group of the quasifield Q_2 of order 25 defined as follows. Let 1, t be a basis for Q_2 over its kernel $GF(5)$. Addition is as usual, and multiplication is given by

$$(\alpha + \beta t)(\gamma + \delta t) = \begin{cases} \alpha\gamma + \beta\gamma^{-1}t & \text{if } \gamma \neq 0, \delta = 0 \\ 4\beta\delta^{-1} + \alpha\delta t & \text{if } \gamma = 0, \delta \neq 0 \\ (\alpha\gamma + 2\beta\gamma^2\delta) + (\alpha\delta + 3\beta\gamma\delta^2)t & \text{if } \gamma\delta \neq 0. \end{cases}$$

Similarly, the group

$$G_3 = \langle \mathfrak{M}(N_5), C\rangle$$

is the multiplicative group of a quasifield Q_3 of order 25.

Two exceptions occur when $q = p = 7$ and $d = 2$. The groups are: a group $G_4 = \langle A, B\rangle$ of order 48 and a group $G_5 = \langle A, B, 2I\rangle$ of order 144. Here

$$A = \begin{bmatrix} 0 & 6 \\ 1 & 0 \end{bmatrix} \quad B = \begin{bmatrix} 1 & 3 \\ 6 & 5 \end{bmatrix}.$$

The group G_4 is the multiplicative group of the irregular nearfield N_7 of order 49. (See [**6**; p. 126-128] and [**3**, p. 230-231].) The group G_5 is the multiplicative group of the quasifield Q_5 defined as follows. Let 1, t be a basis for Q_5 over its kernel $GF(7)$. Addition is as usual, and multiplication is given by the rule:

$$(\alpha + \beta t)(\gamma + \delta t) = \begin{cases} \alpha\gamma + \beta\gamma^{-1}t & \text{if } \gamma \neq 0, \delta = 0 \\ 3\beta\delta^{-1} + \alpha\delta t & \text{if } \gamma = 0, \delta \neq 0 \\ (\alpha\gamma + \beta[2\delta^2\gamma^3 + 6\delta^5]) + (\alpha\delta + 5\beta\gamma^5)t & \text{if } \gamma\delta \neq 0. \end{cases}$$

The quasifield Q_5 coordinatizes the Lüneburg translation plane $F * 7$. (See Theorem 19.10 in [**9**].)

Two exceptions occur when $q = p = 11$ and $d = 2$. The groups are: a group $G_6 = \langle A, B, 4I \rangle$ of order 120 and a group $G_7 = \langle A, B, 4I, C \rangle$ of order 240. Here

$$A = \begin{bmatrix} 0 & 10 \\ 1 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 5 \\ 6 & 9 \end{bmatrix}, \quad C = \begin{bmatrix} 9 & 1 \\ 1 & 4 \end{bmatrix}.$$

The group G_6 is the multiplicative group of the irregular nearfield N_{11} of order 121 with solvable multiplicative group. (There is a second irregular nearfield or order 121 whose multiplicative group is $SL(2, 5)$. See [**6**; p. 126-128] and [**3**; p. 230-231].) The second group G_7 is also the multiplicative group of a quasifield Q_7 of order 121 which coordinatizes the Lüneburg translation plane $F * 11$.

One exception occurs for $q = 23$ and $d = 2$. It is the group $G_8 = \langle A, B, 2I \rangle$, where

$$A = \begin{bmatrix} 0 & 22 \\ 1 & 0 \end{bmatrix} \quad B = \begin{bmatrix} 1 & 17 \\ 12 & 19 \end{bmatrix},$$

and it has order 528. This is the multiplicative group of the irregular nearfield N_{23} of order 529. (See [**6**; p. 126-128] and [**3**; p. 230-231].)

Finally, three exceptions occur when $p = 3$ and $kd = 4$. These have orders 160, 320, and 640, respectively.

Remark. Using an Apple II+ microcomputer, the groups G_2, G_3, G_5 were investigated, and in each group a spread was found, from which the quasifields Q_2, Q_3, Q_5, Q_7 were calculated. However there may be other spreads associated with these groups giving rise to distinct planes. Finally, it is not known whether or not the three exceptional groups in the case $p = 3$ and $kd = 4$ are multiplicative groups of quasifields of order 81.

Theorem 3.1 shows that the generalized André systems (which include the finite fields and the regular nearfields), the irregular nearfields N_5, N_7, N_{11}, and N_{23} and the quasifields coordinatizing the translation planes of type $F * p$ do, modulo possibly one or two others, have a common characterization: solvable multiplicative group.

We close this section with a corollary to Theorem 3.1 showing that the only finite semifields Q with $\mathfrak{M}(Q)$ solvable are the Galois fields.

COROLLARY 3.1.1. *Let Q be a finite semifield of dimension d over its kernel $K = GF(q)$, where $q = p^k$ with p a prime and $k \geqq 1$. If $\mathfrak{M}(Q)$ is solvable then Q is the Galois field $GF(q^d)$.*

Proof. By Theorem 3.1 the semifield Q is either a generalized André system, or $q = p$ and $d = 2$, or $a^d = 3^4$. If the first possibility holds then Theorem 9.11 in [**9**; p. 45] says Q is a field. If $d = 2$ and $q = p$ then Q is a

field by 5.3.10 of [**3**; p. 244]. For the case $q^d = 3^4$, a computer search shows that none of the three groups given by Huppert [**6**] for this case can be the multiplicative group of a semifield.

4. Rao's theorem. In the article [**12**] Rao gave necessary and sufficient conditions for a quasifield Q to be a generalized André system. The conditions involved the quasifield Q having an element $a \in Q$ belonging to both the middle and right nuclei of Q and having order u, a prime q-primitive divisor of $q^d - 1$. Here Q has dimension d over its kernel $K = GF(q)$. (Rao [**12**] uses the left distributive law in his definition of quasifield, and not the right as we do.) Rao also assumes the group $\langle a \rangle$ is normal in $\mathfrak{M}(Q)$, although he does not state it in these terms.

The purpose of this section is to generalize Rao's result using the last two properties mentioned in the preceding paragraph. For the definition of q-primitive divisor, see [**9**; p. 28]. We note here that a prime q-primitive divisor exists except in the two cases: (1) $d = 2$ and $q + 1 = 2^s$ with $s \geqq 1$, and (2) $d = 6$ and $q = 2$. (See Theorem 6.2 in [**9**].)

THEOREM 4.1. *Let Q be a finite quasifield of dimension d over its kernel $K = GF(q)$, where $q = p^k$ with p a prime and $k \geqq 1$. If $\mathfrak{M}(Q)$ has a normal subgroup U of order u^l, where $l \geqq 1$ and u is a prime q-primitive divisor of $q^d - 1$, then $\mathfrak{M}(Q)$ is solvable and Q is a generalized André system.*

Proof. The group $\mathfrak{M}(Q)$ is a subgroup of $GL(d, q)$. Then $U \leqq GL(d, q)$. By Korollar 1 of [**5**] the normalizer of U in $GL(d, q)$ is solvable. Hence $\mathfrak{M}(Q)$ is solvable. Thus Theorem 3.1 can be applied. Case (ii) of Theorem 3.1 does not apply since $3^2 - 1$ has no 3-primitive divisors. In each of the cases (iii)-(vi) the only prime q-primitive divisor is 3, and the groups in each case do not have a normal subgroup U of order 3^l. In case (vii) the only prime q-primitive divisor is 5, and the groups do not have a normal subgroup of order 5. Thus only case (i) of Theorem 3.1 holds, and the theorem follows.

The situation in which $q^d - 1$ has no prime q-primitive divisor will now be considered. The case in which $q = 2$ and $d = 6$ does not need to be considered since there is no generalized André system of dimension 6 over $GF(2)$. (See [**9**; p. 48].) The second case in which $q = p = 2^l - 1$ and $d = 2$ is handled by the following theorem.

THEOREM 4.2. *Let p be a prime of the form $2^l - 1$ and $l \geqq 2$, and let Q be a finite quasifield of dimension 2 over its kernel $K = GF(p)$. If $\mathfrak{M}(Q)$ has a normal subgroup U of order 2^l, then $\mathfrak{M}(Q)$ is solvable and Q is either a generalized André system, the quasifield in case* (ii) *of Theorem* 3.1, *or one of the quasifields in case* (iv) *of Theorem* 3.1. *If U is cyclic then Q is a generalized André system.*

Proof. Without loss of generality, assume $p > 3$; for if $p = 3$ then either Q is a generalized André system or the quasifield in case (ii) of Theorem 3.1. Then $l \geqq 5$. Assume $\mathfrak{M}(Q)$ is non-solvable. Consider the subgroup

$$T = \mathfrak{M}(Q) \cap SL(2, p).$$

Since $\mathfrak{M}(Q)SL(2, p)/SL(2, p)$ is a subgroup of $GL(2, p)/SL(2, p)$, the group T is a non-solvable group and $|\mathfrak{M}(Q)/T|$ divides $p - 1$. By Lemma 2.1 the integer $|\mathfrak{M}(Q)|$ is divisible by $p^2 - 1$ and hence 2^{l+1} divides $|\mathfrak{M}(Q)|$. Thus, 2^l divides $|T|$. Since $l \geqq 5$, the integer 32 divides $|T|$. It follows that under the natural homomorphism the group T induces a subgroup $\bar{T}$ whose order is divisible by 16. By Theorem 14.1 in [**9**] it follows that

$$\bar{T} = PSL(2, p).$$

Hence $T = SL(2, p)$.

But then $U \cap SL(2, p)$ must be a normal subgroup of $SL(2, p)$ having order at least $2^{l-1} \geqq 16$. This is a contradiction. Thus $\mathfrak{M}(Q)$ is solvable. Theorem 3.1 gives the first part of the theorem.

If the group U is in addition cyclic then the only possibility is that Q is a generalized André system. since in the three other possibilities the group $\mathfrak{M}(Q)$ does not have a normal cyclic subgroup of order 2^l.

Rao's theorem now follows immediately from the previous two theorems.

THEOREM 4.3. (Rao) *Let Q be a quasifield of dimension d over its kernel $K = GF(q)$, where $q = p^k$ with p a prime and $k \geqq 1$. Assume $d \neq 6$ if $q = 2$. If Q contains an element $a \neq 0$ such that*

(i) *for all $x, y \in Q$,*

$$x \cdot ay = xa \cdot y$$

$$x \cdot ya = xy \cdot a$$

(ii) *the element a has multiplicative order v where either v is a prime q-primitive divisor of $q^d - 1$ or $v = 2^l$ in the case $d = 2$ and $q = p = 2^l - 1$,*

(iii) *for each $x \in Q$ with $x \neq 0$,*

$$xa = a^{t(x)}x,$$

where $t(x)$ *is a positive integer depending on x, then Q is a generalized André system.*

Proof. Consider the set

$$U = \{\rho_a^i | i = 0, 1, \ldots, v-1\}.$$

https://doi.org/10.4153/CJM-1987-038-x Published online by Cambridge University Press

It is easily seen that $\rho_a^i = \rho_b$, where $b = a^i$, using (i). Thus U is a subgroup of $\mathfrak{M}(Q)$. For $c \in Q^* = Q - \{0\}$,

$$\rho_a\rho_c = \rho_{ac};$$

also

$$ca = a^{t(c)}c$$

implies

$$\rho_c\rho_a = \rho_a^{t(c)}\rho_c,$$

or

$$\rho_c\rho_a\rho_c^{-1} = \rho_a^{t(c)}.$$

Hence, the group U is normal in $\mathfrak{M}(Q)$. Theorem 4.1 and 4.2 then give the theorem.

Remark. The converse of Theorem 4.3 is also true. See [**12**].

References

1. A. A. Albert, *On the collineation groups of certain non-desarguesian planes*, Portugal. Math. *18* (1959), 207-224.
2. R. H. Bruck and R. C. Bose, *Linear representations of projective planes in projective spaces*, J. Algebra *4* (1966), 117-172.
3. P. Dembowski, *Finite geometries* (Springer-Verlag, Berlin-Heidelberg-New York, 1968).
4. D. A. Foulser, *A generalization of André's systems*, Math. Z. *100* (1967), 380-395.
5. C. Hering, *Zweifach transitive Permutationsgruppen in denen* 2 *die maximale Anzahl von Fixpunkten von Involutionen ist*, Math. Z. *104* (1968), 150-174.
6. B. Huppert, *Zweifach transitive auflösbare Permutationsgruppen*, Math. Z. *68* (1957), 126-150.
7. M. J. Kallaher, *Affine planes with transitive collineation groups*, (North Holland, New York-Amsterdam-Oxford, 1982).
8. M. J. Kallaher and T. G. Ostrom, *Fixed point free linear groups, rank three planes, and Bol quasifields*, J. Algebra *18* (1971), 159-178.
9. H. Lüneburg, *Translation planes* (Springer-Verlag, Berlin-Heidelberg-New York, 1980).
10. T. G. Ostrom, *A characterization of generalized André planes*, Math. Z. *110* (1969), 1-9.
11. D. S. Passman, *Permutation groups*, (Benjamin, New York-Amsterdam, 1968).
12. M. L. N. Rao, *Characterization of Foulser's* λ*-systems*, Proc. Amer. Math. Soc. *24* (1970), 538-544.

Washington State University,
Pullman, Washington