

## QUASIFIELDS WITH IRREDUCIBLE NUCLEI

MICHAEL J. KALLAHER

Department of Pure and Applied Mathematics  
Washington State University  
Pullman, Washington 99164-2930

(Received January 22, 1984)

ABSTRACT. This article considers finite quasifields having a subgroup  $N$  of either the right or middle nucleus of  $Q$  which acts irreducibly as a group of linear transformations on  $Q$  as a vector space over its kernel. It is shown that  $Q$  is a generalized André system, an irregular nearfield, a Lüneburg exceptional quasifield of type  $R * p$  or type  $F * p$ , or one of four other possibilities having order  $5^2$ ,  $5^2$ ,  $7^2$ , or  $11^2$ , respectively. This result generalizes earlier work of Lüneburg and Ostrom characterizing generalized André systems, and it demonstrates the close similarity of the Lüneburg exceptional quasifields to the generalized André system.

KEY WORDS AND PHRASES. *Quasifields, type L quasifields, irreducibility, nucleus.*  
1980 MATHEMATICS SUBJECT CLASSIFICATION CODES: 51A40

### 1. INTRODUCTION

This article is a continuation of Kallaher [1]. 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  $k \geq 1$ . For the rest of this article we will use  $Q$  in place of the triple  $(Q, +, \cdot)$ , thereby suppressing the two operations  $+$  and  $\cdot$  whenever it is feasible; furthermore, the symbol  $Q^*$  will denote the multiplicative loop  $(Q - \{0\}, \cdot)$  of  $Q$ , and  $K^*$  will have the same relationship to the field  $K$ . If  $m \in Q^*$  the right multiplicative mapping  $\rho_m: Q \rightarrow Q$  is defined as follows:

$$x\rho_m \equiv xm \quad \text{for } x \in Q. \quad (1.1)$$

The multiplicative group of  $Q$  is the group  $\mathfrak{M}(Q)$  generated by the mappings  $\rho_m$ , where  $m \in Q^*$ ; that is,

$$\mathfrak{M}(Q) \equiv \langle \rho_m \mid m \in Q^* \rangle. \quad (1.2)$$

One of the principal results in [1] is a description of the possibilities for  $Q$  and  $\mathfrak{M}(Q)$  when  $\mathfrak{M}(Q)$  is solvable. A second principal result deals with type L quasifields; these are quasifields  $Q$  with a non-trivial subgroup  $N$  of either the middle nucleus  $M$  of  $Q$  or the right nucleus  $R$  of  $Q$  such that  $\mathfrak{M}(N) = N$  is normal in  $\mathfrak{M}(Q)$ . The subgroup  $N$  is called a type L subgroup.

The purpose of this article is to prove the following theorem.

**THEOREM 1.** Let  $Q$  be a finite type L quasifield of dimension  $d$  over its kernel  $K = GF(q)$ , where  $q = p^k$  with  $p$  a prime and  $k \geq 1$ , and let  $N$  be a type L subgroup of  $Q$ . Assume that  $d \neq 6$  if  $q = 2$ . If  $\mathfrak{M}(N)$  acts irreducibly on  $Q$  then one of the following statements holds:

- (i) The quasifield  $Q$  is a generalized André system, and  $\mathfrak{M}(Q) \leq \Gamma L(1, q^d)$ .
- (ii) The quasifield  $Q$  is an irregular nearfield.
- (iii) The quasifield  $Q$  is a Lüneburg exceptional quasifield of type  $F * p$ , where  $d = 2$  and  $q = p = 7$  or  $11$ .
- (iv) The quasifield  $Q$  is a Lüneburg exceptional quasifield of type  $R * p$ , where  $d = 2$  and  $q = p = 19$  or  $29$ .
- (v) The dimension  $d = 2$  and  $q = p = 5$ . Furthermore, if  $N_5$  is the irregular nearfield of order 25 then either  $\mathfrak{M}(Q) = \langle \mathfrak{M}N_5^*, 2I \rangle$  of order 48 or  $\mathfrak{M}(Q) = \langle \mathfrak{M}(N_5), C \rangle$  of order 96. Here  $I$  is the 2 by 2 identity matrix and

$$C = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}.$$

- (vi) The dimension  $d = 2$  and  $q = p = 7$ . Furthermore,  $\mathfrak{M}(Q) = \langle \mathfrak{M}N_7^*, 2I \rangle$  of order 144, where  $N_7$  is the irregular nearfield of order 49.
- (vii) The dimension  $d = 2$  and  $q = p = 11$ . Furthermore,  $\mathfrak{M}(Q) = \langle \mathfrak{M}N_{11}^*, D \rangle$  of order 240, where  $N_{11}$  is the irregular nearfield of order 121 with solvable multiplicative group and

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

The above theorem is a generalization of the Lüneburg-Ostrom characterization of generalized André systems. (See Theorem 9.2 and Corollary 9.3 on p. 42 of Lüneburg [2].) Their characterization involves collineation groups and their action on each of the components of the associated translation plane, while the above characterization involves only the quasifield and its multiplication. Theorem 1 also shows that the Lüneburg exceptional quasifields are very much similar to the generalized André systems. This observation has not been made until now. There are also connections between the above Theorem and recent work (as yet unpublished) by Geoffrey Mason and T. G. Ostrom on translation planes of order  $p^2$  having an extra-special group of collineations.

Note also that statements (i) to (vii) are not completely disjoint. For example, if  $Q$  is a Lüneburg exceptional quasifield of type  $F * 7$ , then  $\mathfrak{M}(Q) = \langle \mathbb{M}_7^*, 2I \rangle$ , the group of statement (vi). Similarly, a Lüneburg exceptional quasifield of type  $F * 11$  satisfies statement (vii). These are the only overlaps.

The proof of Theorem 1 will be given by means of a sequence of Lemmas and Theorems. Section 2 will list background material and some results on type L quasifields and type L subgroups; these will be used in Sections 3 and 4. Section 3 will prove Theorem 1 in the case where  $q^d - 1$  has no prime  $q$ -primitive divisor, and Section 4 will prove Theorem 1 in the case where  $q^d - 1$  has a prime  $q$ -primitive divisor. (See Theorems 3 and 4.)

We will assume the reader is familiar with the subject of quasifields and the associated translation planes as given, for example, in Kallaher [3] and Lüneburg [2]. Also, information concerning Frobenius complements will be used frequently; this can be found in Passman [4].

2. BACKGROUND MATERIAL.

In this section we collect together material which will be referred to frequently in proving Theorem 1. Proofs are omitted as they appear elsewhere.

THEOREM 2. Let  $Q$  be a quasifield of finite dimension  $d$  over its kernel  $K = GF(q)$ , where  $q = p^k$  with  $p$  a prime and  $k \geq 1$ . The group  $\mathfrak{M}(Q)$  is a transitive group of linear transformations on  $Q$  as a (right) vector space over  $K$ . Furthermore, if  $\mathfrak{M}(Q)$  is solvable, then  $Q$  and  $\mathfrak{M}(Q)$  satisfy statements (i), (ii), (iii), (v), (vi), or (vii) of Theorem 1, or they satisfy one of the following two statements:

- (viii) The dimension  $d = 2$  and  $q = 3$ ; the quasifield  $Q$  is the non-associative quasifield of order 9, and  $\mathfrak{M}(Q) = GL(2,3)$ .
- (ix) The dimension  $d = 4$  and  $q = 3$ , and  $\mathfrak{M}(Q)$  is one of three groups having orders 160, 320, 640, respectively.

PROOF. See Lemma 2.1 and Theorem 3.1 of Kallaher [1].

LEMMA 1. Let  $Q$  be a type L quasifield with type L subgroup  $N$ , and assume  $Q$  has dimension  $d$  over its kernel  $K = GF(q)$ , where  $q = p^k$  with  $k \geq 1$ . The following statements hold:

- (i)  $\mathfrak{M}(N) \cong N$
- (ii) The type L subgroup  $N$  is contained in both the middle nucleus and the right nucleus of  $Q$ .
- (iii) The type L subgroup  $N \cong \mathfrak{M}(N)$  acts fixed-point-free on  $Q$ , and

$$|N| \mid |Q^* - \{0\}|.$$

PROOF. See Lemma 5.1 of Kallaher [1].

One implication of statement (iii) in the last Lemma is that the type L subgroup  $N$  is a Frobenius complement. This means that the group structure of  $N$  is essentially determined. It is given in the next Lemma. A Z-group is a (finite) group in which every Sylow subgroup is cyclic. Such a group is solvable.

LEMMA 2. Let  $N$  be as in Lemma 1. One and only one of the following statements holds:

- (i) The group  $N$  is solvable, and  $N$  contains a normal subgroup  $N_0$  such that  $N_0$  is a  $Z$ -group and  $N/N_0$  is a subgroup of  $S_4$ .
- (ii) The group  $N$  is non-solvable, and  $N$  contains a normal subgroup  $N_1$  with  $[N:N_1] \leq 2$  such that  $N_1 = \text{SL}(2,5) \times N_0$  with  $N_0$   $Z$ -group of order prime to 30.

PROOF. See Passman [4], Theorem 18.2 on p. 196 and Theorem 18.6 on p. 204. This yields the following important information.

LEMMA 3. Let  $N$  be as in Lemma 1. If  $N_0$  is the subgroup of  $N$  described in statement (i), respectively statement (ii), of Lemma 2, then  $N_0$  is normal in  $N$ . Furthermore, if  $U_0$  is a subgroup of prime order  $u$  in  $N_0$ , then  $U_0$  is normal and unique in  $N_0$ , and hence  $U_0$  is normal in  $\mathbb{M}(Q)$ .

PROOF. For the first statement we need only consider the subgroup  $N_0$  of statement (ii) in Lemma 2. Since clearly  $N_0$  is generated by all elements of  $N_1$  whose order is prime to 30, the subgroup  $N_0$  is characteristic in  $N_1$  and hence  $N_0 \leq N$ . The first part of the second statement is proven in the first paragraph of the proof of Theorem 18.2 on pp. 196-197 of Passman [4]. (In the proof it is essential that  $N_0$  is a Frobenius complement.) The second part of the second statement is proven as follows. If  $u = 2$  then  $U_0$  is unique in  $N$  by Theorem 18.1 on pp. 193-194 of Passman [4]. Assume  $u$  is odd. Again by Theorem 18.1 of Passman [4] the Sylow  $u$ -subgroups of  $N$  are cyclic. Since  $U_0$  is characteristic in  $N_0$  it is normal in  $N$ , for  $N_0$  is normal in  $N$ . It follows that  $U_0$  is contained in every Sylow  $u$ -subgroup of  $N$ ; thus  $U_0$  is the only subgroup of order  $u$  in  $N$ , and hence  $U_0$  is characteristic in  $N$ . Since  $N \trianglelefteq \mathbb{M}(Q)$ , it follows that  $U_0 \trianglelefteq \mathbb{M}(Q)$ .

LEMMA 4. Assume the hypothesis of Lemma 1. If the group  $N$  is cyclic then the quasifield  $Q$  is a generalized André system.

PROOF. By Proposition 19.8 on p. 244 of Passman [4], we must have  $\mathbb{M}(Q) \leq \Gamma L(1, q^d)$ . It is well known that this implies  $Q$  is a generalized André system. (See, for example, Kallaher [3; p. 70], or Kallaher [1; Section 3].)

We close this section with some definitions and a few remarks that will be used frequently. A group  $G$  of linear transformations on a vector space  $V$  is irreducible, or acts irreducibly, if the only subspaces of  $V$  fixed by  $G$  are the trivial subspaces  $V$  and the zero subspace  $\emptyset$ . Otherwise,  $G$  is reducible on  $V$ .

In the finite case there is a nice number-theoretic condition that ensures irreducibility. Assume the vector space  $V$  has dimension  $d$  over the field  $F = \text{GF}(q)$ . A  $q$ -primitive divisor of  $q^d - 1$  is a positive integer  $v$  such that  $v \mid (q^d - 1)$  and  $(v, q^i - 1) = 1$  for all  $i$  with  $1 \leq i < d$ . The number  $q^d - 1$  always has a prime  $q$ -primitive divisor except in the two cases: (1)  $d = 2$  and  $q$  is an odd prime where  $q + 1$  is a power of 2, or (2)  $d = 6$  and  $q = 2$ . (See Theorem 6.2 on p. 27 of Lüneburg [2].) If  $|G|$  is divisible by a prime  $q$ -primitive divisor, then  $G$  acts irreducibly on  $V$ . Note that under the hypothesis of Theorem 1 we have  $q^d - 1$  divides  $|\mathbb{M}(Q)|$ , and hence every  $q$ -primitive divisor of  $q^d - 1$  must divide  $|\mathbb{M}(Q)|$ .

LEMMA 5. Assume the hypothesis of Lemma 1. Assume further that  $u$  is a prime  $q$ -primitive divisor of  $q^d - 1$  and  $U$  is a Sylow  $u$ -subgroup of  $\mathbb{M}(Q)$ . If  $U \not\leq N$ , then one of the following statements holds:

- (i) The group  $N$  is cyclic,  $[N, U] = 1$ , and  $Q$  is a generalized André system.
- (ii) The group  $N$  is solvable,  $p > 2$ ,  $|U| = u = d + 1 = 2^i + 1$  for some integer  $i \geq 1$ , and  $2^{2i+1} \mid |N|$ .

PROOF. This follows from Satz 2 of Hering [5] and Lemma 4.

3. NONEXISTENCE OF  $q$ -PRIMITIVE DIVISORS.

In this section Theorem 1 is proven in the case where  $q^d - 1$  has no  $q$ -primitive divisor. It then follows that  $d = 2$  and  $q + 1 = 2^t$  for some integer  $t \geq 2$ . Another observation is: The subgroup  $K^*$  induces the full group of scalar transformations in  $\mathbb{M}(Q)$ . We will use the symbol  $K^*$  to also denote this group of scalar transformations.

We start with the following Lemma.

LEMMA 6. Assume the hypothesis of Theorem 1 and assume  $q = p$  is odd and  $d = 2$ . One of the following statements holds:

- (i) The group  $\mathbb{M}(Q)$  is solvable.
- (ii) The group  $\mathbb{M}(Q)$  contains  $SL(2, 5)$  as a type L subgroup of  $Q$ .

PROOF. Assume the group  $\mathbb{M}(Q)$  is nonsolvable. Let  $\bar{\mathbb{M}} = \mathbb{M}(Q) \cap SL(2, p)$ , and let  $\mathbb{M}'$  be the image of  $\bar{\mathbb{M}}$  in  $PSL(2, p)$ . The only nonsolvable subgroups of  $PSL(2, p)$  are  $PSL(2, p)$  and  $PSL(2, 5)$ . Thus,  $\mathbb{M}' = PSL(2, p)$  or  $\mathbb{M}' = PSL(2, 5)$ . Since  $K^*$ , the full group of scalar transformations, is contained in  $\mathbb{M}(Q)$ , it follows that  $\bar{\mathbb{M}}$  contains the center of  $SL(2, p)$ ; hence  $\bar{\mathbb{M}} = SL(2, p)$  or  $\bar{\mathbb{M}} = SL(2, 5)$ .

Assume  $\bar{\mathbb{M}} = SL(2, p)$ . Since  $K^* \leq \mathbb{M}(Q)$  it follows that  $SL(2, p) < \mathbb{M}(Q) \leq GL(2, p)$ . The group  $N$  irreducible on  $Q$  implies  $N \not\leq K^*$  and thus  $N/N \cap K^*$  is a nontrivial normal subgroup of  $\mathbb{M}(Q)/K^* \leq PGL(2, p)$ . Note that  $PSL(2, p) \leq \mathbb{M}(Q)/K^* \leq PGL(2, p)$ . The only nontrivial normal subgroups of  $PGL(2, p)$  are  $PGL(2, p)$  and  $PSL(2, p)$ , both of which have elements of order  $p$ . Since  $p \nmid |N|$ , this gives a contradiction. Thus  $\bar{\mathbb{M}} \neq SL(2, p)$ .

It follows that  $\bar{\mathbb{M}} = SL(2, 5)$ . Then  $\mathbb{M}(Q)/K^*$  is a subgroup of  $PGL(2, p)$  containing  $PSL(2, 5)$  as a normal subgroup. Since the normalizer of  $PSL(2, 5)$  in  $PGL(2, p)$  is itself—Theorem 14.6 of Lüneburg [2]—it follows that  $\mathbb{M}(Q)/K^* = PSL(2, 5)$ . Since  $N \not\leq K^*$  it follows that  $N/N \cap K^* = PSL(2, 5)$ . Thus  $N$  is nonsolvable, and Lemma 2 implies  $N$  contains  $SL(2, 5)$  as a normal subgroup. In fact,  $SL(2, 5)$  is characteristic in  $N$ , and thus  $SL(2, 5)$  is normal in  $\mathbb{M}(Q)$ . Hence  $SL(2, 5)$  is a type L subgroup of  $Q$ .

LEMMA 7. Assume the hypotheses of Lemma 6. The quasifield  $Q$  and its multiplicative group  $\mathbb{M}(Q)$  satisfies one of the statements in the conclusion of Theorem 1.

PROOF. Assume  $\mathbb{M}(Q)$  is solvable. We can then apply Theorem 2. Statement (ix) of Theorem 2 cannot hold since  $d = 2$ . Statement (viii) is also not possible since the quasifield of that statement has a trivial right nucleus and a trivial middle nucleus. Hence, if  $\mathbb{M}(Q)$  is solvable one of the statements (i), (ii), (iii), (v), (vi), or (vii) of Theorem 1 holds.

Assume  $\mathbb{M}(Q)$  contains  $SL(2, 5)$  as a type L subgroup of  $Q$ . Statement (ii) of Theorem 5.1 in Kallaher [1] implies that  $Q$  is a Lüneburg exceptional quasifield of

type  $R * p$  with  $p = 11, 19, 29,$  or  $59$ . A Lüneburg exceptional quasifield of type  $R * p$  with  $p = 11$  or  $p = 59$  is the irregular nearfield of that order. (In the case  $p = 11$  it is the irregular nearfield with  $Q^*$  nonsolvable.) Thus either statement (ii) or statement (iv) of Theorem 1 holds.

The following is the object of this section.

**THEOREM 3.** Assume the hypothesis of Theorem 1. If  $q^d - 1$  does not have a prime  $q$ -primitive divisor, then the conclusion of Theorem 1 holds.

**PROOF.** Since  $d \neq 6$  if  $q = 2$  the hypothesis about the nonexistence of  $q$ -primitive divisors implies  $d = 2$  and  $q = p$ , an odd prime, with  $p + 1$  a power of 2. Thus the Theorem follows from Lemmas 6 and 7.

#### 4. EXISTENCE OF $q$ -PRIMITIVE DIVISORS

In this section we prove Theorem 1 in the case where  $q^d - 1$  has a (prime)  $q$ -primitive divisor  $u$ .

**LEMMA 8.** Assume the hypothesis of Theorem 1, and let  $N_0$  be the subgroup of  $N$  described in statement (i), respectively statement (ii), of Lemma 2. If there exists a prime  $q$ -primitive divisor  $u$  of  $q^d - 1$  such that  $u \mid |N_0|$ , then  $Q$  is a generalized André system.

**PROOF.** Let  $U_0$  be a subgroup of order  $u$  in  $N_0$ . By Lemma 3 the group  $U_0$  is normal in  $\mathbb{M}(Q)$ . Since  $u$  is a  $q$ -primitive divisor of  $q^d - 1$  the group  $U_0$  is irreducible on  $Q$  as a vector space over  $K$ . Thus  $U_0$  is itself a cyclic irreducible type L subgroup of  $Q$ . By Lemma 4 the quasifield  $Q$  is a generalized André system.

**LEMMA 9.** Assume the hypothesis of Theorem 1. If there exists a prime  $q$ -primitive divisor  $u$  of  $q^d - 1$  such that  $u \mid |N|$ , then one of the following statements holds:

- (i) The quasifield  $Q$  is a generalized André system.
- (ii) The quasifield  $Q$  is a Lüneburg exceptional quasifield of type  $F * p$ , where  $d = 2$  and  $q = p = 5, 11,$  or  $23$ .
- (iii) The quasifield  $Q$  is a Lüneburg exceptional quasifield of type  $R * p$ , where  $d = 2$  and  $q = p = 11, 19, 29,$  or  $59$ .

**PROOF.** If  $u$  divides the order of the subgroup  $N_0$  of  $N$  then Lemma 8 implies statement (i) holds. Hence we may assume  $u \nmid |N_0|$ . It follows that either  $u = 3$  or  $u = 5$  by Lemma 2. We now break the proof into two cases: (1) The group  $N$  is solvable, and (2) the group  $N$  is nonsolvable.

Assume  $N$  is solvable. By Lemma 2 the prime  $u = 3$ . Since  $q^2 \equiv 1 \pmod{3}$  for all  $q$  not divisible by 3, it follows that  $d = 2$ . By statement (i) of Lemma 2 a Sylow 3-subgroup  $U$  of  $N$  is cyclic of order 3. If  $U$  is normal in  $N$  then  $U$  is characteristic in  $N$ , and hence  $U$  is normal in  $\mathbb{M}(Q)$ . Then  $U$  is itself an irreducible cyclic type L subgroup of  $Q$ , and thus by Lemma 4 statement (i) of the present Lemma holds. Assume  $U$  is not normal, i.e., assume  $N$  has more than one Sylow 3-subgroup. Let  $N_1$  be the (normal) subgroup of  $N$  generated by the Sylow 3-subgroups of  $N$ .

Recall that  $\mathbb{M}(Q) \leq GL(2, q)$ , and let  $\bar{\mathbb{M}}$  be the subgroup induced in  $PGL(2, q)$  by  $\mathbb{M}(Q)$ . Since  $\mathbb{M}(Q)$  is transitive on  $Q^*$  the group  $\bar{\mathbb{M}}$  acts transitively on the set of

points of the projective line over  $K^* = GF(q)$ . Thus  $(q + 1) \mid |\overline{M}|$ . The group  $N$  induces in  $\overline{M}$  a normal subgroup  $\overline{N}$ . Since  $N$  is solvable and contains more than one Sylow 3-subgroup, by Theorem 14.1 of Lüneburg [2] the group  $\overline{N}$  contains a subgroup  $\overline{A} \cong A_4$  and  $[\overline{N} : \overline{A}] \leq 2$ . (Here the fact that  $p \nmid |N|$  is used.) Since  $\overline{A}$  is generated by its Sylow 3-subgroups it is characteristic in  $\overline{N}$ , and thus  $\overline{A}$  is normal in  $\overline{M}$ .

By Theorems 14.4 and 14.5 of Lüneburg [2] the index  $[\overline{M} : \overline{A}] \leq 2$ . Thus  $(q + 1) \mid 24$ , which in turn implies  $q = 2, 3, 5, 11, \text{ or } 23$ . Since  $12 \mid (q^2 - 1)$ , it follows that  $q = 5, 11, \text{ or } 23$ . By Corollary 3.4 of Lüneburg [2] the group  $N$  has a unique involution which is in  $Z(N)$ . The group  $N_1$  is a pre-image of the group  $\overline{A}$  since  $N_1$  is generated by the Sylow 3-subgroups of  $N$ . It follows that  $N_1 = SL(2,3)$ . The group  $N_1$  is characteristic in  $N$  and thus  $N_1$  is a type L subgroup of  $Q$ . By statement (i) of Theorem 5.1 in Kallaher [1] statement (ii) of the present Lemma holds.

Assume now that the group  $N$  is nonsolvable. Then  $u = 3$  or  $u = 5$ . If  $u = 3$  then as before  $d = 2$ . Assume  $u = 5$ ; then either  $d = 2$  or  $d = 4$  since  $q^4 \equiv 1 \pmod{5}$  for all  $q$  not divisible by 5. We want to prove  $d = 2$ . Thus we may assume 3 is not a  $q$ -primitive divisor of  $q^d - 1$ . Assume there exists a prime  $q$ -primitive divisor  $v > 5$ . If  $v \mid |N|$  then  $v \mid |N_0|$  and Lemma 8 implies  $Q$  is a generalized André system. But then  $\mathbb{M}(Q)$  is solvable, contradicting the assumption that  $N$  is nonsolvable. If  $v \nmid |N|$  then Lemma 5 implies  $N$  is solvable, again a contradiction. Thus 5 is the only prime  $q$ -primitive divisor of  $q^d - 1$ . Furthermore, Lemma 5 implies  $5 \mid (q^d - 1)$ . Assume  $d = 4$ . Since 5 is the only prime  $q$ -primitive divisor of  $q^4 - 1$ , it follows that  $q^2 + 1 = 2^t \cdot 5$  for some  $t \geq 1$ . On the other hand, by Lemma 2 we have  $120 \mid (q^4 - 1)$ . Thus  $q$  is odd and  $q > 3$ . But then  $q^2 + 1 \equiv 2 \pmod{4}$ . Hence  $q^2 + 1 = 2 \cdot 5 = 10$ ; this implies  $q = 3$ , a contradiction. Thus  $d = 2$ .

We have shown that  $d = 2$  when  $N$  is nonsolvable. Statement (ii) of Lemma 2 applies and shows that  $N$  contains  $SL(2,5)$  as a characteristic subgroup of  $N$ . It follows that  $SL(2,5)$  is a type L subgroup of  $Q$ . Statement (ii) of Theorem 5.1 in Kallaher [1] then implies statement (iii) of the present Lemma holds. This proves Lemma 9.

Consider statements (ii) or (iii) of the conclusion of Lemma 9. A Lüneburg exceptional quasifield of type  $F * p$ , where  $p = 5$  or  $23$ , is the irregular nearfield of that order. Similarly, a Lüneburg exceptional quasifield of type  $R * p$ , where  $p = 11$  or  $59$ , is an irregular nearfield. Thus the conclusion of Lemma 9 could read as follows: Statements (i), (ii), (iii), or (iv) of Theorem 1 holds.

LEMMA 10. Assume the hypothesis of Theorem 1, and assume  $q^d - 1$  has a prime  $q$ -primitive divisor  $u$ . If  $u \nmid |N|$  then the quasifield  $Q$  and its multiplicative group  $\mathbb{M}(Q)$  satisfies one of the statements in the conclusion of Theorem 1.

PROOF. If  $|N|$  is divisible by a prime  $q$ -primitive divisor of  $q^d - 1$ , then Lemma 9 and the comments after it prove the present Lemma. Thus we may assume no prime  $q$ -primitive divisor of  $q^d - 1$  divides  $|N|$ . Lemma 5 then applies; it says that for every prime  $q$ -primitive divisor of  $q^d - 1$  either statement (i) or statement (ii)

holds. We may assume statement (ii) of Lemma 5 holds for every prime  $q$ -primitive divisor of  $q^d - 1$ . It follows that  $u$  is the only prime  $q$ -primitive divisor of  $q^d - 1$  and  $u \mid (q^d - 1)$ . Furthermore,  $u = d + 1 = 2^i + 1$  for some integer  $i \geq 1$ , and  $2^{2i+1} \mid |N|$ . Using the notation of Hering [6] we have  $\Phi_d^*(q) = u = d + 1$ . By statement (b) of Theorem 3.9 in Hering [6] it follows that either  $d = 4$ ,  $q = 2$ , or  $d = 4$ ,  $q = 3$ , or  $d = 2$ ,  $q = p$ .

If  $d = 4$  then  $2^5 \mid |N|$ . Since  $|N| \mid (q^d - 1)$ , in each of the first two possibilities it follows that  $2^5 \mid (q^d - 1)$ , a contradiction. Thus  $d = 2$  and  $q = p$ . The present Lemma then follows from Lemma 7. (If  $q = 2$ ,  $d = 2$  then  $Q$  must be  $GF(4)$ , which is a generalized André system.)

Lemmas 9 and 10 give the following result.

**THEOREM 4.** Assume the hypothesis of Theorem 1. If  $q^d - 1$  has a prime  $q$ -primitive divisor then the conclusion of Theorem 1 holds.

This Theorem together with Theorem 3 proves Theorem 1.

#### REFERENCES

1. KALLAHER, M. J. The multiplicative groups of quasifields, to appear.
2. LÜNEBURG, H. Translation Planes, Springer-Verlag, Berlin-Heidelberg-New York, 1980.
3. KALLAHER, M. J. Affine Planes with Transitive Collineation Groups, North Holland, New York-Amsterdam-Oxford, 1982.
4. PASSMAN, D. S. Permutation Groups, Benjamin, New York-Amsterdam, 1968.
5. HERING, C. Zweifach transitive Permutationsgruppen, in denen 2 die maximale Anzahl von Fixpunkten von Involutionen ist, Math. Z. 104 (1968), 150-174.
6. HERING, C. Transitive linear groups and linear groups which contain irreducible subgroups of prime order, Geom. Dedi. 2 (1974), 425-460.





# Hindawi

Submit your manuscripts at  
<http://www.hindawi.com>

