Internat. J. Math. & Math. Sci.
Vol. 3 No. 1 (1980) 29-45

ON THE KNUTH SEMI-FIELDS

D.R. HUGHES

Department of Mathematics
Westfield College
University of London
London

M.J. KALLAHER

Department of Mathematics
Washington State University
Pullman, Washington 99163
U. S. A.

(Received May 28, 1979 and in revised form October 22, 1979)

ABSTRACT: We consider three of Knuth's four classes of semi-fields - Knuth [11] - namely, those having dimension 2 over a nucleus and show that the autotopism group is solvable (Corollary 4.12). This generalizes a result of Hughes [5]. We also show that for semi-fields of dimension 2 over a nucleus, the number of pairwise non-isomorphic isotopic images is at least 5 (Corollary 5.1.1). This generalizes a result in [10].

KEY WORDS AND PHRASES : *Semi-fields, autotopism, determinant group, Knuth semi-fields.*

1980 MATHEMATICS SUBJECT CLASSIFICATION CODES: *50D05, 05B25, 17E05.*

1. INTRODUCTION.

The central purpose of this article is to investigate the autotopism groups of one class of Knuth semi-fields. These semi-fields are defined as follows. Let F be a finite field, let $S = F \times F$, let σ be a non-identity automorphism of F, let $\tau = \sigma^{-1}$, and choose $f,g \in F$ such that $y^{\sigma+1} + gy - f \neq 0$ for all $y \in F$. (If F is not a prime field, then there always exists σ,f,g such that $y^{\sigma+1} + gy - f \neq 0$ for all $y \in F$. See Knuth [11,p. 214].) Taking componentwise addition, the set S is a semi-field under any one of the following multiplications:

$K(u)$: $(a,b)(c,d) \equiv (ac + b^{\sigma}d^{\tau^2}f,\ bc + a^{\sigma}d + b^{\sigma}d^{\sigma}g)$

$K(\ell)$: $(a,b)(c,d) \equiv (ac + b^{\sigma}df,\ bc + a^{\sigma}d + b^{\sigma}dg)$

$K(r)$: $(a,b)(c,d) \equiv (ac + b^{\tau}d^{\tau^2}f,\ bc + a^{\sigma}d + bd^{\tau}g)$

$K(m)$: $(a,b)(c,d) \equiv (ac + b^{\tau}df,\ bc + a^{\sigma}d + bdg)$

If N_r, N_m, N_ℓ are the right, middle, and left nuclei, respectively, of S then the classes $K(\ell)$, $K(r)$, $K(m)$ are characterized by the following statement: A semi-field S is of type $K(i)$ over the field F if and only if (a) $N_j = F$ for $j \in \{r,m,\ell\} - \{i\}$ and (b) S has (vector space) dimension 2 over F. (See Knuth [11].) The class $K(\ell)$ was discovered by Hughes and Kleinfeld [6] and Hughes [5] investigated the autotopism groups of such semi-fields with the principal result being that they are solvable. The semi-fields in $K(r)$ are obtained from the semi-fields of $K(\ell)$ by duality. As of yet the semi-fields in $K(m)$ have not been investigated. We do so in this article and show that Hughes's result for the class $K(\ell)$ essentially holds also for the class $K(m)$. (See Corollary 4.1.2)

Our proof of Corollary 4.1.2 is based upon the work of section 3. This section is based upon unpublished work of M. V. D. Burmeister, and the main result (Theorem 3.4) is a generalization of his techniques. In section 5, we extend a result of the article [10] to semi-fields having dimension 2 over one of their nuclei. Specifically, we show that such semi-fields must have at least 5 isotopic, but pairwise non-isomorphic, images.

We assume the reader is familiar with the theory of projective and affine planes as exhibited in [7].

2. PRELIMINARIES.

Throughout this section $S = \langle S, t, \cdot \rangle$ will be a finite semi-field of order p^s, where p is a prime, and N_r, N_m, N_ℓ are respectively, the right, middle, and left nucleus of S. Furthermore, G is the group of autotopisms of the semi-field S; thus G consists of all triples $\varphi = (\varphi_1, \varphi_2, \varphi_3)$ of bijective additive mappings of S with

$$(x\varphi_1)(y\varphi_2) = (xy)\varphi_3 \quad \text{for all } x, y \in S,$$

and the operation in G is componentwise composition. We have the following information.

LEMMA 2.1: Let S be a finite semi-field of order p^s, where p is a prime, and let N_m be the middle nucleus of S having order p^{t_m}, and let G be the autotopism group of S. The following statements hold:

(i) The semi-field S is both a left and right vector space over N_m having dimension $d = st_m^{-1}$.

(ii) If $\varphi = (\varphi_1, \varphi_2, \varphi_3) \in G$, then the mapping $\varphi_m : N_m \to N_m$ given by $n\varphi_m \equiv (a_\varphi n b_\varphi)\varphi_3$, when a_φ and b_φ are defined by $a_\varphi \varphi_1 = b_\varphi \varphi_2 = 1$, is an automorphism of N_m.

(iii) If $\varphi = (\varphi_1, \varphi_2, \varphi_3) \in G$ then φ_1 is a semi-linear transformation on S as a right vector space over N_m (with companion automorphism φ_m) and φ_2 is a semi-linear transformation on S as a left vector space over N_m (with companion automorphism φ_m).

PROOF: See [7; p. 170 and 179]

REMARKS:

(1) It might be helpful to consider the situation from a geometrical point of view. If $\mathfrak{A}$ is the affine plane coordinatized by S then an autotopism is a collineation of $\mathfrak{A}$ fixing the coordinate axes with φ_1 describing the action on the x-axis, φ_2 the action on the line at infinity, and φ_3 the action on the y-axis. Thus in statement (iii) above we are on the one-hand -- when considering φ_1 -- looking at the x-axis of and on the other -- when considering φ_2 -- looking at the line at infinity of $\mathfrak{A}$.

(2) There are lemmas corresponding to Lemma 2.1 for both the right nucleus N_r and the left nucleus N_ℓ of S. However, there are some slight differences. The semi-field S is a right vector space over N_r and for $\varphi = (\varphi_1,\varphi_2,\varphi_3) \in G$ the components φ_2 and φ_3 of φ are semi-linear transformations on S over N_r. The companion automorphism in both cases is $\varphi_r{:}N_r \to N_r$ given by $n\varphi_r \equiv (a_\varphi b_\varphi n)\varphi_3$. Similarly, the semi-field S is a left vector space over N_ℓ and the components φ_1 and φ_3 are semi-linear transformations on S over N_ℓ with companion automorphism φ_ℓ: $N_\ell \to N_\ell$, where $n\varphi_\ell \equiv (na_\varphi b_\varphi)\varphi_3$. (See [7; p.170 and 179].)

DEFINITION 2.1: Let S be a finite semi-field of order p^s with middle nucleus N_m of order p^{t_m} and let G be the autotopism group of S. The <u>middle linear autotopism group</u> of S is the subgroup $\underline{LG_m}$ $(\underline{S})$ of G consisting of all autotopisms $\varphi = (\varphi_1,\varphi_2,\varphi_3)$ with φ_1 and φ_2 linear transformations on S as a vector space over N_m. The <u>middle homomorphisms</u> of S are the homomorphisms Π_{mj}: $LG_m(S) \to GL(d_m,N_m)$, where $d_m = st_m^{-1}$ and $d = 1,2$ defined by

$$(\varphi_1,\varphi_2,\varphi_3)\Pi_{mj} = \varphi_j \ .$$

LEMMA 2.2: Let S be a finite semi-field of order p^s, where p is a prime, let N_m be the middle nucleus of S having order p^{t_m}, and let G be the autotopism group of S. The following statements hold:

(i) The middle linear autotopism group $LG_m(S)$ is the kernel of the homomorphism $\Sigma_m : G \to Aut(N_m)$ given by $\varphi\Sigma_m \equiv \varphi_m$.

(ii) The integer $[G : LG_m(S)]$ divides t_m.

(iii) The kernel of the homomorphism Π_{m1} is the group $N_r^* \equiv \{\rho_n | n \in N_r - \{0\}\}$, where $\rho_n = (1,\rho,\rho)$ with $\rho : S \to S$ given by $x\rho \equiv xn$. The group N_r^* is isomorphic to the multiplicative group $N_r - \{0\}$.

(iv) The kernel of the homomorphism Π_{m2} is the group $N_\ell^* \equiv \{\lambda_n | n \in N_\ell - \{0\}\}$ where $\lambda_n = (\lambda,1,\lambda)$ with $\lambda : S \to S$ given by $x\lambda \equiv nx$. The group N_ℓ^* is isomorphic to the multiplicative group $N_\ell - \{0\}$.

PROOF: Statement (i) is obvious and statement (ii) follows from (i). For statement (iii) note first that $N_r^* \leq \ker \Pi_{m1}$. For given $\rho_n = (1,\rho,\rho)$ we have $a_{\rho n} = 1$ and $b_{\rho n} = n^{-1}$; thus for $x \in N_m$ we have $x(\rho_n)_m = (xn^{-1})\rho = (xn^{-1})\,n = x$. Assume now that $\varphi = (\varphi_1,\varphi_2,\varphi_3) \in \ker \Pi_{m1}$. Then $\varphi_1 = 1$; hence for all $x,y \in S$ we have $x(y\varphi_2) = (xy)\varphi_3$. Letting $x = 1$ gives $\varphi_2 = \varphi_3$. If $n \equiv 1\varphi_2$ then $x\varphi_3 = xn$ for all $x \in S$. Thus $x(yn) = (xy)n$ for all $x,y \in S$. Hence $n \in N_r - \{0\}$ and $\varphi = (1,\rho,\rho)$ with $\rho : x \to xn$ for all $x \in S$. This proves (iii). The proof of statement (iv) is similar.

REMARKS:

(1) Analogous to the group $LG_m(S)$ we have a <u>right linear autotopism group</u> <u>$LG_r(S)$</u> - consisting of all $\varphi = (\varphi_1,\varphi_2,\varphi_3)$ with φ_2 and φ_3 linear transformations over N_r - and a <u>left linear autotopism group</u> <u>$LG_\ell(S)$</u> - consisting of all $\varphi = (\varphi_1,\varphi_2,\varphi_3)$ with φ_1 and φ_2 linear transformations over N_ℓ. In turn these groups have associated with them mappings $\Pi_{ri} : LG_r(S) \to GL(d_r,N_r)$ and $\Pi_{\ell i} : LG_\ell(S) \to GL(d_\ell,N_\ell)$ - here d_α is the dimension of S over N_α - where

$$(\varphi_1,\varphi_2,\varphi_3)\Pi_{ri} \equiv \varphi_i \quad i = 2,3$$

$$(\varphi_1,\varphi_2,\varphi_3)\Pi_{\ell i} \quad \varphi_i \quad i = 1,3$$

Results similar to the statements of Lemma 2.2 are true. In particular, $\ker \Pi_{r1} = N_{\ell}^{*}$, $\ker \Pi_{\ell 1} = N_{r}^{*}$, and $\ker \Pi_{r2} = \ker \Pi_{\ell 2} = N_{m}^{*} \equiv \{\mu_n \mid n \in N_m - \{0\}\}$ where $\mu_n = (\mu_1, \mu_2, 1)$ is given by

$$x\mu_1 \equiv xn, \quad x\mu_2 \equiv n^{-1}x$$

for $x \in S$. We can then define

$$\underline{LG(S)} \equiv \bigcap_{\alpha} LG_{\alpha}(S)$$

where α runs over $\{r,m,\ell\}$. This is called the linear autotopism group of S. The mappings $\Pi_{\alpha i}$ could then be restricted to the group LG(S).

(2) In the remainder of this article, whenever we consider the group $LG_m(S)$ we will frequently restrict ourselves to one of the groups $G_{mi} = \{\varphi_1 \mid \varphi = (\varphi_1, \varphi_2, \varphi_3) \in LG_m(S)\}$ for $i = 1$ or 2. These groups are really homomorphic images of $LG_m(S)$ and the purpose of the above lemma is to make this clear. Similar statements hold for the groups $LG_r(S)$ and $LG_{\ell}(S)$.

LEMMA 2.3: Let S be a finite semi-field of order p^r, where p is a prime, and let G be the autotopism group of S. The group G is solvable if and only if the subgroup $LG_m(S)$ is solvable.

PROOF: This follows from the fact the $G/LG_m(S)$ is a subgroup of $\mathrm{Aut}(N_m)$.

REMARK: In Lemma 2.3, the group $LG_m(S)$ can be replaced with any of the groups $LG_r(S)$, and $LG_{\ell}(S)$. The last group is permissible because its definition implies that the factor group $G/LG(S)$ is a subgroup of the direct product $\otimes G/LG_{\alpha}(S)$, where $\alpha = r,m,\ell$. (See [8; 1.9.6].).

DEFINITION 2.2: Let S be a finite semi-field of order p^s, where p is a prime. For $i = 1,2$ we define $\underline{D_{mi}}$ to be the group of all $\varphi = (\varphi_1, \varphi_2, \varphi_3)$ in $LG_m(S)$ with $\det \varphi_i = 1$, and we define $\underline{D_m} = \underline{D_m(S)}$ to be the group $D_{m1} \cap D_{m2}$. The group D_m is the <u>middle determinant group</u> of S.

LEMMA 2.4: Let S be a finite semi-field of order p^s with p a prime and let G be the autotopism group of S. The following statements hold:

(i) The subgroups D_{m1}, D_{m2}, and D_m are normal in $LG_m(S)$.

(ii) The group G is solvable if and only if one (and hence all) of the groups D_{m1}, D_{m2}, and D_m is solvable.

(iii) The integers $|LG_m(S)||D_{m1}|^{-1}$ and $|LG_m(S)||D_{m2}|^{-1}$ divide $p^{t_m} - L$.

PROOF: Statements (i) and (ii) follow from the fact that D_{mi} is the kernel of the homomorphism $\overline{\Pi}_{mi} : LG_m(S) \to N_m - \{0\}$ given by $(\varphi_1,\varphi_2,\varphi_3)\overline{\Pi}_{mi} = \det \varphi_i$. The proof of statement (iii) is similar to the proof of Lemma 2.3.

REMARK: We can also define subgroups D_{r2}, D_{r3}, D_r of $LG_r(S)$ and $D_{\ell 1}$, $D_{\ell 3}$, D_ℓ of $LG_\ell(S)$. Lemma similar to Lemma 2.4 can then be proven. Thus for each such group $D_{\alpha j}$, we have

$$|G| = u_\alpha v_{\alpha j}|D_{\alpha j}|$$

with $u_\alpha | t_\alpha$ and $v_{\alpha j} | (p^{t\alpha} - 1)$. Also, the group G is solvable if and only if one (and hence all) of the $D_{\alpha j}$ is solvable.

DEFINITION 2.3: Let S be a finite semi-field of order p^s with autotopism group G. The <u>determinant group</u> of S is the subgroup $\underline{D} = \underline{D(S)} = D_r \cap D_m \cap D_\ell$ of G.

We close this section with a lemma that plays a role similar to the role of Lemma 2.3.

LEMMA 2.5: Let S be a finite semi-field of order p^s with p a prime and let its middle nucleus N_m have order p^{t_m}. For $i = 1$ or 2 the homomorphism Π_{mi} induces by restriction a homomorphism $\Pi^*_{mi} : D_{mi} \to SL(d_m, N_m)$, where $d_m = st_m^{-1}$, and $\ker \Pi^*_{m1} = D_{m1} \cap N^*_r$ and $\ker \Pi^*_{m2} = D_{m2} \cap N^*_\ell$.

3. <u>THE DIMENSION 2 CASE.</u>

In this section we restrict ourselves to semi-fields S which have dimension 2 over one of their nuclei. Without loss of generality, we shall assume the nucleus is N_m. (By this we mean that similar arguments apply for either of the other two nuclei. Thus, in the notation of the previous section, we have

$$d_m = \dim_{N_m} S = st_m^{-1} = 2$$

$$s = 2t_m \quad .$$

Consider first the group $LG_m(S)$. The following result is important in the analysis of the structure of $LG_m(S)$ and the subgroups D_{mj} .

THEOREM 3.1: Let S be a finite semi-field of order p^s where p is a prime and assume that S has dimension 2 over its middle nucleus N_m. If $p > 2$ then the group $LG_m(S)$ contains no elements of order p.

PROOF: Assume $\varphi = (\varphi_1,\varphi_2,\varphi_3)$ is an element of order p in $LG_m(S)$. Consider the projective plane $\mathcal{P}(S)$ coordinatized by S. Then φ induces a collineation $\bar{\varphi}$ on $\mathcal{P}(S)$ fixing the points (0,0), (0), and (∞). (See Remark (1) after Lemma 2.1.) Because $\bar{\varphi}$ has order p, it fixes other points in each of the three lines determined by these points, hence it fixes a subplane $\mathcal{P}_0$ pointwise. Consider the action of $\bar{\varphi}$ on the line (0,0)(0); this is given by

$$(x,0)\bar{\varphi} = (x\varphi_1,0).$$

Since $\bar{\varphi}$ cannot be an elation, we must have $\varphi_1 \neq 1$. Thus, φ_1 is a linear transformation of order p; that is, $\varphi_1 \in GL(2,N_m)$. An element of order p in $GL(2,N_m)$ fixes exactly $|N_m| = p^{t_m}$ points. It follows that $\bar{\varphi}$ fixes pointwise a subplane $\mathcal{P}_0$ of order p^{t_m} and thus $\bar{\varphi}$ is a Baer collineation. By Foulser [1; Theorem 4.3], this gives a collineation. Hence the theorem holds.

For later reference, we state a result, due to Ganley [2], for the case $p = 2$.

THEOREM 3.2: GANLEY: Let S be a finite semi-field of order 2^s. If S has dimension 2 over one of its nuclei then its autotopism group is solvable.

Consider now the subgroup D_{m1} of $LG_m(S)$. Since D_{m1} is the kernel of the homomorphism $\bar{\Pi}_{m1} : LG_m(S) \to GL((2,N_m)/SL(2,N_m)$, the homomorphism Π_{m1} maps D_{m1} onto a subgroup D^*_{m1} of $SL(2,N_m)$ with kernel $D_{m1} \cap N^*_r$. (See Lemma 2.4.)

We will use this fact repeatedly.

THEOREM 3.3: Let S be a semi-field of order p^s, where p is a prime, and having dimension 2 over its middle nucleus N_m, let G be its autotopism group, let $D^*_{ml} = D_{ml}/(D_{ml} \cap N^*_r)$, let $|N_m| = p^{t_m}$, and let $|N_r| = p^{t_r}$. One and only one of the following statements holds:

(i) The autotopism group G is non-solvable with $D^*_{ml} = SL(2,5)$ and $|G|$ divides $t_m(p^{t_m} - 1)(p^{t_r} - 1) \cdot 120 = 60s(p^{\frac{1}{2}s}-1)(p^{t_r} - 1)$. Furthermore, $p \geq 7$ and $p^s-1 \equiv 0 \pmod 5$.

(ii) The autotopism group G is solvable with D^*_{ml} a solvable subgroup of $SL(2,N_m)$ such that $(p,|D^*_{ml}|) = 1$ and $|G|$ divides $t_m(p^{t_m} -1)(p^{t_r} - 1)k = \frac{1}{2}s(p^{\frac{1}{2}s} - 1)(p^{t_r} - 1)$ where either $k|2(p^{\frac{1}{2}s} \pm 1)$, $k = 24$, or $k = 48$.

PROOF: By the Remark after Lemma 2.3, the integer $|G||D_{ml}|^{-1}$ divides $t_m(p^{t_m} - 1)$. Consider the group d_{ml}. The group $D^*_{ml} = D_{ml}/(D_{ml} \cap N^*_r)$ is a subgroup of $SL(2,N_m) = SL(2,p^{t_m})$ containing no p-elements (Theorem 3.1). If G is non-solvable, then D_{ml} is non-solvable and so is D^*_{ml}. It follows that $D^*_{ml} = SL(2,5)$. (See Huppert [8; Hauptsatz II.8.27].)

If G is solvable, then D^*_{ml} must be a solvable subgroup of $SL(2,p^{t_m})$ having no p-elements; then D^*_{ml} must either have order dividing $2(p^{t_m} \pm 1)$ or its image in $PSL(2,p^{t_m})$ is either A_4 or S_4. (Again, see Hauptsatz II.8.27 of [8].

REMARK: Note that Theorem 3.3 has analogies with N_m and D_{ml} replaced by N_α and $D_{\alpha j}$, where $\alpha \in \{r,m,\ell\}$ and $j \in \{1,2,3\}$.

We investigate further statement (i) above by means of a sequence of lemmas.

LEMMA 3.1: Let S be a semi-field of order p^s, where p is an odd prime and having dimension 2 over its middle nucleus N_m, let G be its autotopism group, and let $D^*_{ml} = D_{ml}/(D_m \cap N^*_r)$. If G is non-solvable, then the following statements hold:

(i) $D^*_{ml} = SL(2,5)$

(ii) $|D_{m1} \cap N_m^*| = 2 = |D_{m1} \cap N_\ell^*|$

PROOF: Statement (i) follows from statement (i) of Theorem 3.3. For statement (ii) note that $E = D_{m1} \cap N_m^*$ and $F = D_{m1} \cap N_\ell^*$ are normal cyclic subgroups of D_{m1}. Since $N_m^* \cap N_r^* = N_m^* \cap N^* = 1$, it follows that E and F yield cyclic normal subgroups E^* and F^* of D_{m1}^* with $E^* \simeq E$ and $F^* \simeq F$. Now D_{m1}^* has exactly two such subgroups; namely, 1 and its center Z of order 2. Since the autotopisms $\sigma_m = (\varepsilon,\varepsilon,1)$ and $\sigma_\ell = (\varepsilon,1,\varepsilon)$, where $\varepsilon : x \to (-1)x = x(-1) = -x$, are in E and F, respectively, we have $E^* = Z = F^*$.

Under the hypothesis of Lemma 3.1, consider the group $D_{m2}^{**} = D_{m2}/(D_{m2} \cap N_\ell^*)$. By arguments similar to those given in the first paragraph of the proof of Theorem 3.3 and in the proof of Lemma 3.1, we have the following Lemma.

LEMMA 3.2: Under the hypothesis of Lemma 3.1 the following statements hold for the group $D_{m2}^* = D_{m2}/(D_{m2} \cap N_\ell^*)$:

(i) $D_{m2}^{**} = SL(2,5)$

(ii) $|D_{m2} \cap N_m^*| = |D_{m2} \cap N_r^*| = 2$

Consider now the group $D_m = D_{m1} \cap D_{m2}$. Under the hypothesis of Lemma 3.1, the group D_m is non-solvable (Lemma 2.4). Hence D_m yields a non-solvable normal subgroup D_m^* of $D_{m1}^* = SL(2,5)$. It follows that $D_m^* = D_{m1}^*$. Since $|D_{m1} \cap N_r^*| = 2$, we have $D_m = D_{m1}$. Similarly, $D_m = D_{m2}$. Thus $D_m = D_{m1} = D_{m2}$ and in the last two lemmas D_m can replace D_{m1} and D_{m2}.

Let $\sigma = (\sigma_1,\sigma_2,\sigma_3)$ be an involution in D_m. If σ is a Baer involution (that is, if each σ_i fixes pointwise a subspace S_i of S having dimension ½s over GF(p)), then its image σ^* in $D_m^* = D_{m1}^*$ must be a non-trivial involution in $D_m^* = SL(2,5)$ fixing a non-trivial subspace pointwise. But $D_m^* = SL(2,5)$ has a unique involution and, since $\sigma_m = (\varepsilon,\varepsilon,1)$ is D_m^*, the unique involution of D_m^* is ε which has no fixed points. Thus we have a contradiction and hence

D_m has no Baer involution.

If $\sigma = (\sigma_1, \sigma_2, \sigma_3)$ is an involution in D_m, then each σ_1 is either the identity 1 or the mapping ε. Since at most one σ_i can be 1, the group D_m has exactly three involutions -namely,

$$\sigma_r \equiv (1,\varepsilon,\varepsilon), \qquad \sigma_m \equiv (\varepsilon,\varepsilon,1), \quad \text{and} \quad \sigma_\ell \equiv (\varepsilon,1,\varepsilon). \tag{3.1}$$

Note that $D_m \cap N_\alpha^* = \langle\sigma_\alpha\rangle$ for $\alpha = r,m,\ell$. Furthermore, direct calculation shows that for all $\tau \in D_m$, we have $\sigma_\alpha \tau = \tau\sigma_\alpha$ for $\alpha = r,m,\ell$. Hence $Z = \{1,\sigma_r,\sigma_m,\sigma_\ell\}$ is a subgroup of $Z(D_m)$. Since $D_m^* = D_m/\langle\sigma_r\rangle$ has a center of order 2, it follows that $Z(D_m) = Z$.

We have proven the following lemma.

LEMMA 3.3: Under the hypothesis of Lemma 3.1, the following statements hold:

(i) $D_m = D_{m1} = D_{m2}$

(ii) $|D_m| = 240$

(iii) D_m contains exactly three involutions; namely
$\sigma_r = (1,\varepsilon,\varepsilon)$, $\sigma_m = (\varepsilon,\varepsilon,1)$, and $\sigma_\ell = (\varepsilon,1,\varepsilon)$ where $\varepsilon : S \to S$ is given by $\varepsilon : x \to (-1)x = x(-1) = -x$.

(iv) $Z(D_m) = \{1,\sigma_r,\sigma_m,\sigma_\ell\}$

(v) $D_m \cap N_\alpha^* = \langle\sigma_\alpha\rangle$ for all $\sigma \in \{r,m,\ell\}$

We turn to investigating the Sylow 2-subgroups of D_m. Assume $\tau \in D_m$ is an element of order 8. Then τ^4 is an involution in D_m and hence $\tau^4 = \sigma_\alpha$ for some $\alpha \in \{r,m,\ell\}$. If $\alpha \neq r$ then τ induces an element τ^* of order 8 in $D_m^* = D_m/\langle\sigma_\ell\rangle = SL(2,5)$. If $\alpha = r$ then τ induces an element τ^{**} of order 8 in $D_m^{**} = D_m/\langle\sigma_\ell\rangle = SL(2,5)$. Since $SL(2,5)$ has no element of order 8, in both cases we have a contradiction. Thus, D_m has no elements of order 8.

Let T be a Sylow 2-subgroup of D_m. The group T contains the center $Z = Z(D_m)$ of D_m. Furthermore, the image T^* of T in the factor group

$D_m^* = SL(2,5)$ is a quaternion group of order 8. The normalizer of T^* in D^* contains an element τ^* of order 3 that does not centralize T^*. (This follows from Hauptsatz II.8.27 of [8] as applied to $PSL(2,5)$.) If $\tau \in D_m$ is a pre-image in D_m of τ^* with $|\tau| = 3$, then τ normalizes T but does not centralize T. Hence the group T has a non-trivial automorphism of order 3.

Thus, T is a group of order 16 having exactly 3 involutions, no elements of order 8, and an automorphism of order 3. Consulting the list in [3] of the 14 groups of order 16, we see that there is exactly one such group - namely, $Q \otimes Z_2$ - having these three properties.

Consider the group $D_m \cap D_r$. Since G is non-solvable and $G/(D_m \cap D_r)$ is isomorphic to a subgroup of $G/D_m \otimes G/D_r$, by Lemma 2.4 and the Remark following, we have $D_m \cap D_r$ is non-solvable. Hence its image $(D_m \cap D_r)^*$ in D_m^* is a non-solvable normal subgroup of $D_m^* = SL(2,5)$. It follows that $(D_m \cap D_r)^* = D_m^*$. Since $D_m^* = D_m/<\sigma_r>$ and $<\sigma_r> \leq D_m \cap D_r$, we have that $D_m \cap D_r = D_m$ or $D_m \leq D_r$. A similar proof shows that $D_m \leq D$. Thus, $D(S) = D_m$. (See Definition 2.3.)

Now the group $T = Q \otimes Z_2$ has the property that for one of its involutions - in this case σ_m - the factor group $T/<\sigma_m>$ is elementary abelian. Since $D_m/<\sigma_m>$ is a homomorphic pre-image of $D_m/Z(D_m) = PSL(2,5)$, it follows that $D_m/<\sigma_m> = PSL(2,5) \otimes Z_2$.

We have proven the following lemma.

LEMMA 3.4: Under the hypothesis of Lemma 3.1, the following statements hold:

(i) The Sylow 2-subgroups of D_m are isomorphic to $Q \otimes Z_2$.

(ii) $D(S) = D_m$

(iii) $D_m/<\sigma_m> = PSL(2,5) \otimes Z_2$

It follows from the various Remarks made in Section 2 that the proof of Lemmas 3.1 - 3.4 can be applied when N_m is replaced by N_α, and thus D_m by D_α, for $\alpha \in \{r,m,\ell\}$. Thus Lemmas 3.1 and 3.4 can be combined to give the following theorem.

THEOREM 3.4: Let S be a finite semi-field of order p^s, where p is an odd prime, and dimension 2 over one of its nuclei $N_\alpha (\alpha \in \{r,m,\ell\})$. Let G be the autotopism group of S, let $D_\alpha = D_\alpha(S)$ be the determinant group of S associated with N_α, and let $D(S) \equiv D_r \cap D_m \cap D_\ell$. If G is nonsolvable then the following statements hold:

(i) $|D_\alpha| = 240$

(ii) D_α has exactly three involutions; namely, σ_r, σ_m, and σ_ℓ. (See (3.1))

(iii) $Z(D_\alpha) = \{1,\sigma_r,\sigma_m,\sigma_\ell\}$

(iv) $D_\alpha \cap N^*_\beta = \langle\sigma_\beta\rangle$ for all $\beta \in \{r,m,\ell\}$

(v) $D(S) = D_\alpha$

(vi) $D_\alpha / \langle\sigma_\beta\rangle = SL(2,5)$ for $\beta \in \{r,m,\ell\} - \{\alpha\}$

(vii) $D_\alpha / \langle\sigma_\alpha\rangle = PSL(2,5) \otimes Z_2$

We close this section with an interesting relationship among the nuclei when the group SL(2,5) occurs.

COROLLARY 3.4.1: Under the hypothesis of Theorem 3.4, if β, $\gamma \in \{r,m,\ell\} - \{\alpha\}$ then $N_\beta = N_\gamma \subseteq N_\alpha$.

PROOF: We prove this theorem for $\alpha = m$. Let $n \in N_r - \{0\}$ and consider the associated autotopism $\rho_n = (1,\rho,\rho)$, where $\rho\colon x \to xn$. Consider $D_m / \langle\sigma_\ell\rangle$ and G/N^*_ℓ. Such $\langle\sigma_\ell\rangle = D_m \cap N^*_\ell$, we have $D_m / \langle\sigma_\ell\rangle = SL(2,5)$ normal in G/N^* which in turn is a subgroup of $GL(2,N_m)$. If $\sigma = (\sigma_1,\sigma_2,\sigma_3)$ is in D_m then its image in $D_m / \langle\sigma_\ell\rangle$ is just σ_2. Furthermore, the image of ρ_n in G/N^* is just ρ. Since τ_2 is a linear transformation over N_r (Remark (2) after Lemma 2.1 and the Remark after Lemma 2.4), we must have $\rho\sigma_2 = \sigma_2\rho$. Thus ρ is in the centralizer of SL(2,5) in $GL(2,N_m)$. Since the centralizer of SL(2,5) in $GL(2,N_m)$ is the center of $GL(2,N_m)$ - See Huppert [8; Sec. II.7 and II.8] - the mapping ρ is in the center of $GL(2,N_m)$. Thus, $\rho : x \to \bar{n}x$ with $\bar{n} \in N_m$. Since $1\rho = n$ we have $\bar{n} = n$. Therefore, $N_r \subseteq N_m$. Note also that this implies for all $n \in N_r$ we have $nx = xn$ for all $x \in S$. Thus, if $n \in N_r$ and $x,y \in S$, then

$$n(xy) = (xy)n = x(yn) = x(ny) = (xn)y = (nx)y$$

This says that $n \in N_\ell$. Hence $N_r \subseteq N$ also.

To show that $N_\ell \subseteq N_r \subseteq N_m$, consider the mapping λ_n, where $n \in N$ (Lemma 2.2(iv)), and the groups $D_m / < \sigma_r >$ and G/N_r^*. Proceeding as in the preceding paragraph, we obtain the desired result.

REMARK: Note that we have actually shown in the proof of Corollary 3.4.1 that $N_\sigma = N_\beta$ is the center of S.

4. THE KNUTH SEMI-FIELDS

In this section we consider the last three classes of Knuth's semi-fields defined in Section 1. These semi-fields are characterized by the following two properties: (a) Two of the nuclei are equal, and (b) the semi-field has dimension 2 over the nuclei of (a). The following result is then applicable.

THEOREM 4.1: Let S be a finite semi-field of order p^s, where p is a prime, with the following properties:

(i) Two of the nuclei of S are equal

(ii) S has dimension 2 over the nuclei of (a).

The autotopism group G of S is solvable.

PROOF: If $p = 2$ the theorem follows from Theorem 3.2. Assume $p > 2$ and that G is non-solvable. Without loss of generality, assume that the nuclei in (i) are N_m and N_r. By Theorem 3.4, we have $D(S) = D_m = D_r$. Applying Theorem 3.4 with $\alpha = m$ and $\beta = r$ gives $D(S)/< \sigma_m > = PSL(2,5) \otimes Z_2 = SL(2,5)$, a contradiction. Thus, for $p > 2$ the group G is solvable.

COROLLARY 4.1.1: If S is a finite semi-field of dimension 2 over two of its nuclei then the autotopism group G of S is solvable.

PROOF: If G is non-solvable then Corollary 3.4.1 implies that the three nuclei of S are equal. Theorem 4.1 now implies G is solvable. This contradiction implies that G is solvable.

COROLLARY 4.1.2: If S is a finite Knuth semi-field of type $K(\ell)$, $K(r)$, or $K(m)$ having order $p^s = p^{2t}$ then the autotopism group G of S is solvable and G has the following normal series

$$G \trianglerighteq L \trianglerighteq D \trianglerighteq \overline{D} \trianglerighteq 1 \qquad (4.1)$$

with $|G/L|$ dividing t, both $|L/D|$ and $|D/\overline{D}|$ dividing $p^t - 1$, and the group $\overline{D}$ a solvable subgroup of $SL(2,p^t)$ having no p-elements. Thus $|G|$ divides $t(p^t - 1)^2 k$ where either $k = 24$ or 48 or k divides $2(p^t \pm 1)$.

PROOF: The fact that G is solvable follows from Theorem 4.1. The existence of the normal series (4.1) follows from the appropriate version of Theorem 3.3. (See the Remark after Theorem 3.3.) If $p = 2$ then a derivation similar to that in the proof of Theorem 3.3 gives the normal series (4.1).

5. THE INVARIANT u

In [10] the following problem was investigated: Given a finite semi-field plane $\mathfrak{A}$ coordinatized by the semi-field S with autotopism group G, let $u = u(\mathfrak{A})$ be the number of orbits of G not on one of the three axes of $\mathfrak{A}$. What is the lower bound for u? In [9] it was proven that $u = 1$ if and only if is desarguesian (i.e., S is a field). In [10] the authors proved that for non-desarguesian semi-field planes $u \geq 5$ when G is solvable and the order of S is not 2^6. This latter condition holds if S has non-square order (i.e., if $s \neq 2$) or if S has odd dimension over one of its nuclei. (See Theorem 8.18 in [7] and Ganley [2].) We show now that $u \geq 5$ if S has dimension 2 over one of its nuclei.

In [10] it was shown that $u \leq 4$ implies that the integer $|G|$ is divisible by either $p^s - 1$ or $\frac{1}{4}(p^s - 1)$ where p^s is the order of S. We show first that this implies G is solvable when S has dimension 2 over one of its nuclei.

THEOREM 5.1: Let S be a finite semi-field of order p^s and having dimension 2 over one of its nuclei, and let G be the autotopism group. If $|G|$ is divisible by either $p^s - 1$ or $\frac{1}{4}(p^s - 1)$, then G is solvable.

PROOF: Without loss of generality, we may assume S has dimension 2 over its middle nucleus $N_m = GF(p^t m)$. Assume G is non-solvable. Then $s \geq 4$. (See [11; p. 208] and [7; Theorem 8.18].) By Theorem 3.3(i) the integer $|G|$ divides $60s(p^t m - 1)(p^t r - 1)$, where $N_r = GF(p^t r)$, and $p \geq 7$. Since $s \geq 4$ the integer $p^s - 1$ has a prime division v that does not divide $p^a - 1$ for any positive integer a less than s. (See [4; Theorems 3.3, 3.5, and 3.9].) By hypothesis $v \,\big|\, |G|$; thus $v \,\big|\, 60$. (The prime v does not divide s; because if $v|s$ and $v|(p^s - 1)$ then $v|p^{\frac{s}{r}} -1)$ since $b^v \equiv b \pmod v$ for all integers $b \geq 1$.) Since $s \geq 4$ and $p^2 \equiv 1$ mod 3) for all $p > 3$, we must have $v = 5$. Hence the prime division v is unique; also, if 5^i is the highest power of 5 dividing $p^s - 1$ then we must have $i = 1$. Since $p^4 \equiv 1 \pmod 5$ for all primes, it follows that $s = 4$. Theorem 3.5 and 3.9 in [4] imply that $p = 3$, contradicting the fact that $p \geq 7$. Hence G is solvable.

COROLLARY 5.1.1: Let $\mathfrak{A}$ be a finite semi-field plane coordinatized by a semi-field S of order p^s with $p^s \neq 2^6$. If S has dimension 2 over one of its nuclei, then $\mu(\mathfrak{A}) \geq 5$.

PROOF: Assume $u(\mathfrak{A}) \leq 4$. It follows from [10] that either $(p^s - 1)$ or $\frac{1}{4}(p^s - 1)$ divides $|G|$, where G is the autotopism group of S. Theorem 5.1 implies G is solvable. Theorem 6.3 of [10] implies $u \geq 5$, a contradiction. Hence $u \geq 5$.

REMARK: The invariant u also has the interpretation that it is the number of pairwise non-isomorphic semi-fields isotopic to the semi-field S. The semi-field of order 16 and dimension 2 over its kernel has exactly five non-isomorphic isotopic images.

ACKNOWLEDGMENT: The second author was supported in part by the National Science Foundation.

REFERENCES

1. Foulser, D. A. Baer p-elements in translation planes, J. Algebra 31(1974) 354-366.

2. Ganley, M. J. Baer involutions in semi-field planes of even order, Geom. Dedi. 2(1974) 499-508.

3. Hall, Marshall and J. K. Senior. The Groups of Order $2^n (N \geq 6)$. Macmillan, New York, 1964.

4. Hering, C. Transitive linear groups and linear groups which contain irreducible subgroups of prime order, Geom. Dedi. 2(1974) 425-460.

5. Hughes, D. R. Collineation groups of non-desarguesian planes II. Some semi-nuclear division algebras, Amer. J. Math. 82(1960) 113-119.

6. Hughes, D. R. and E. Kleinfeld, Semi-nuclear extensions of Galois fields, Amer. J. Math. 82(1960) 389-392.

7. Hughes, D. R. and F. Piper. Projective Planes, Springer-Verlag, Berlin-Heidelberg-New York, 1973.

8. Huppert, B. Endliche Gruppen I, Springer-Verlag, Berlin-Heidelberg-New York, 1976.

9. Kallaher, M. J. A conjecture on semi-field planes, Archiv der Math. 26(1975) 436-440.

10. Kallaher, M. J. and R. A. Liebler. A conjecture on semi-field planes II, Geom. Dedi, to appear.

11. Knuth, D. E. Finite Semi-fields and projective planes, J. Algebra 2(1965) 182-217.