

Autotopism Groups of Cyclic Semifield Planes

Ulrich Dempwolff

Abstract

In this article we investigate the autotopism group of the so-called cyclic semifield planes. We show that the group generated by the homology groups of the nuclei is already the full group of autotopisms which are linear with respect to the nuclei. The full autotopism group is also computed with the exception of one special subcase.

1 Introduction

Let V be a m -dimensional space over a field $K = \text{GF}(q^n)$, $\sigma \in \text{Aut}(K)$ an automorphism of order n , and T an irreducible σ -linear operator on V . Then

$$\mathbf{S} = \mathbf{S}(T) = \sum_{i=0}^{m-1} KT^i = \sum_{i=0}^{m-1} T^i K$$

is an additively closed spread set (see [6] but also [8]). Let $K_0 = \text{GF}(q)$ be the fixed field of σ and let ψ be an arbitrary K_0 -isomorphism from V onto \mathbf{S} . Then

$$x * y = x\psi(y)$$

determines on V a presemifield multiplication. Note that if one chooses ψ such that for $y \in V$ in addition $\psi^{-1}(\mathbf{1})\psi(y) = y$ holds one obtains even a semifield multiplication. The (pre)semifields of this isotopism class were called *cyclic semifields* in [6]. If $n = 1$ the semifield is actually a field. We say therefore that cyclic semifield is *proper* if $n > 1$.

On the other hand the spread set \mathbf{S} determines a translation plane $\mathbf{P} = \mathbf{P}(T)$ on $W = V \oplus V$, where the associated spread is

$$\Sigma = \{V(\infty)\} \cup \{V(s) \mid s \in \mathbf{S}\}$$

with

$$V(\infty) = 0 \oplus V, \quad V(s) = \{(x, xs) \mid x \in V\}.$$

Our aim is to determine the autotopism group of these planes. We will show:

Theorem 1. *Let V be a m -dimensional space over $K = \text{GF}(q^n)$, $\sigma \in \text{Aut}(K)$ an automorphism of order $n > 1$, and T an irreducible, σ -linear, operator on V . Set $K_0 = K_\sigma = \text{GF}(q)$. Then $F = C_{\text{End}_{K_0}(V)}(T)$ is a field isomorphic to $\text{GF}(q^m)$. Moreover the following holds:*

- (a) The right and middle nuclei of $\mathbf{P} = \mathbf{P}(T)$ are isomorphic to K and the left nucleus is isomorphic to F .
- (b) Denote by M the normal subgroup of autotopisms of \mathbf{P} which are linear with respect to the nuclei. Then M is the product of the homology groups associated with the nuclei. In particular

$$M \simeq (K^* \times K^* \times F^*)/K_0^*.$$

For autotopisms outside of M we state:

Theorem 2. *We assume that \mathbf{P} satisfies the assumptions of Theorem 1 and we keep the notation of this theorem. Assume further $q = p^f$, where $\text{char } K = p$, and denote by G the autotopism group of \mathbf{P} . Then n divides $|G/M|$. Moreover $|G/M|$ divides $f \cdot m \cdot n$ if $n > (m, n)$ and $|G/M|$ divides $f \cdot m \cdot n \cdot (m, n)$ if $n = (m, n)$.*

We will observe that—in contrast to Theorem 1—the quotient G/M does depend on the individual operator T and not only on the parameters m and n . In fact we will compute the group G/M except the case that n divides m and $n < m$, where we have only incomplete information.

The notation of this paper can be found in 2.1, 3.1 and in the definitions at the beginning of sections 3 and 4. Section 2 includes some auxiliary results on field extensions. Section 3 is devoted to the proof of Theorem 1 and section 4 to the proof of Theorem 2.

In section 5 we determine the full autotopism group G in the case $(m, n) = 1$. This result will be used in sections 6 and 7 where we treat the cases $n \geq m$ and $n < m$ respectively. The precise structure of G/M (excluding the case $n|m$, $n < m$) is given in Propositions 6.3 and 7.4.

The terminology on semifield planes follows standard texts like [3] or [5].

2 Semilinear operators and preliminary results

In this section we explain the description of irreducible linear operators of [4]. The work of Kantor and Liebler [9] on cyclic semifields contains a representation of such transformations too. However it seems convenient to use the very concrete description of [4]. We also collect some special results on field extensions.

2.1. Description of semilinear operators. We make the following assumptions:

V is a m -dimensional space over the field $K = \text{GF}(q^n)$.

σ is an automorphism of K of order n , i. e. $K_0 = \text{GF}(q)$ is the fixed field.

Set $F = \text{GF}(q^m)$, $d = (m, n)$, $m' = m/d$, and $L = \text{GF}(q^{m'n})$.

(I) From [4] we take:

Theorem. *Let V, K, σ , etc. satisfy the above assumptions and let T be an irreducible, σ -linear operator on V . Then:*

(a) *There is a decomposition*

$$V = U_0 \oplus \cdots \oplus U_{d-1}$$

into K -spaces such that $U_i T = U_{i-1}$ for all i (and $U_{-1} = U_{d-1}$).

(b) *T^d induces on each U_i an irreducible, σ^d -linear operator.*

(c) *Each U_i can be identified with L and T^d induces on such a space a mapping of the form $x \mapsto wx^\gamma$ with $w \in L^*$ and $\gamma \in \text{Aut}(L)$ such that $\gamma_K = \sigma^d$.*

(d) *T^n restricted to U_i has the form $\zeta \mathbf{1}$ where $F = K_0[\zeta]$.*

Using coordinates we can identify V with L^d , U_i with Le_i (e_i a standard basis vector), and the K -structure of V is given by

$$a \cdot x = (ax_0, a^\sigma x_1, \dots, a^{\sigma^{d-1}} x_{d-1}), \quad a \in K, \quad \text{where } x = (x_0, \dots, x_{d-1}) \in V.$$

The action of T is given by

$$xT = (x_1, \dots, x_{d-1}, wx_0^\gamma),$$

where $\zeta = N_{L:F}(w)$ with γ and ζ as in (d) of the Theorem. For the remainder of this paper T will usually denote a σ -linear operator and this context the symbols

$$w \quad \text{and} \quad \zeta = N_{L:F}(w)$$

will always refer to the foregoing representation. Note that any choice of w and ζ with $\zeta = N_{L:F}(w)$ and $F = K_0(\zeta)$ defines by the above equation an irreducible semilinear transformation. We also describe T formally by the matrix

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & \gamma w \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}.$$

In the sequel we will use similar matrix descriptions for other semilinear transformations too.

(II) When we will describe autotopisms the following two types of semilinear operators (acting on $V = L^d$) will be relevant:

Let $a_0, \dots, a_{d-1} \in L^*$, $\phi \in \text{Aut}(L)$, and let $P(\pi) = (\delta_{i,\pi(j)})_{0 \leq i,j < d}$ be permutation matrix associated with the permutation π which is a power of the d -cycle $(0, 1, \dots, d-1)$. The semilinear operator described formally by the matrix

- (a) $\text{diag}(\phi a_0, \dots, \phi a_{d-1})$ has *diagonal form of type ϕ* and
(b) $\text{diag}(\phi a_0, \dots, \phi a_{d-1})P(\pi)$ is an operator of *permutational form of type ϕ* .

Definition. We will call an additive endomorphism S of V *linear*, if it is a linear transformation with respect to the K - and F -structure of V , i.e. $(a \cdot x)S = a \cdot (xS)$ and $(bx)S = b(xS)$ for $a \in K$ and $b \in F$.

Lemma 2.2. *Let S be an invertible operator on V which is semilinear with respect to the F - and K -structure. Then S induces a permutation of $\{U_0, U_1, \dots, U_{d-1}\}$ which lies in the group generated by the cycle $(U_0, U_1, \dots, U_{d-1})$. If S is even linear then S fixes each U_i .*

Proof. Let ω be a generator of the field $K_1 = \text{GF}(q^d)$. When we consider ω as an element of F this element induces on V the K_0 -linear map $\omega \mathbf{1}$. Considering ω as an element of K we denote the K_0 -linear map $x \mapsto \omega \cdot x$ by $\tilde{\omega}$. In particular $\omega \mathbf{1}$ and $\tilde{\omega}$ agree on U_0 . The U_i 's are the homogeneous components of the group $\langle \omega \mathbf{1}, \tilde{\omega} \rangle$ on V . A *homogeneous component* of a G -module, G a group, is the sum of all irreducible submodules of one isomorphism type. This notion of basic representation theory is connected with Clifford's theorem (see for instance [1], (12.11-13), p. 40) which is used here in a very elementary fashion. Since S normalizes the group $\langle \omega \mathbf{1}, \tilde{\omega} \rangle$ we see that it induces a permutation on the set $\{U_0, U_1, \dots, U_{d-1}\}$. Clearly, if S is linear, then S fixes each U_i .

So assume that S is not linear. The operator T from 2.1 satisfies the assertion of the lemma. So adjusting S by a power of T we may assume wlog. that S fixes U_0 . Denote by ϕ the automorphism induced by S on F and by ψ the automorphism induced by S on K . Then for $u \in U_0$ also $uS \in U_0$ and

$$\omega^\psi(uS) = \omega^\psi \cdot (uS) = (\omega \cdot u)S = (\omega u)S = \omega^\phi(uS).$$

Hence

$$\omega^\psi = \omega^\phi.$$

Now let $u \in U_i$, $i > 0$, and assume $uS \in U_j$. Then:

$$\omega^{\psi\sigma^j}(uS) = \omega^\psi \cdot (uS) = (\omega \cdot u)S = (\omega^{\sigma^i} u)S = \omega^{\sigma^i\phi}(uS)$$

Hence $\omega^{\psi\sigma^j} = \omega^{\sigma^i\phi}$ and therefore

$$\omega^{\psi\sigma^{j-i}} = \omega^\phi \quad \text{or} \quad \omega^{\sigma^{j-i}} = \omega^{\psi\phi^{-1}\sigma^{j-i}} = \omega$$

which in turn implies $i = j$ as $|j - i| < d$. The proof is complete. \square

The next result is known (see [2]). For convenience we supply a proof.

Lemma 2.3. *Let V, W be a finite dimensional L -spaces. Let $L : K$ be a Galois extension with Galois group Γ . For $\gamma \in \Gamma$ denote by H_γ the K -subspace*

of γ -linear mappings in $\text{Hom}_K(V, W)$. Then

$$\text{Hom}_K(V, W) = \bigoplus_{\gamma \in \Gamma} H_\gamma.$$

Proof. Assume $[L : K] = \ell$, $\dim_L V = m$, and $\dim_L W = n$. Then $\dim_K \text{Hom}_L(V, W) = \ell mn$ and $\dim_K \text{Hom}_K(V, W) = \ell^2 mn$. If T is invertible and γ -linear, then $H_\gamma = T \text{Hom}_L(V, W)$, so that $\dim_K H_\gamma = \ell mn$ too. Hence it suffices to show

$$\sum_{\gamma \in \Gamma} H_\gamma = \bigoplus_{\gamma \in \Gamma} H_\gamma.$$

We proceed by induction and suppose, that for any subset $\Delta \subseteq \Gamma$ of size $< r$ we have already shown $\sum_{\delta \in \Delta} H_\delta = \bigoplus_{\delta \in \Delta} H_\delta$ and let $\Omega = \{\omega_1, \dots, \omega_r\}$ be a r -subset. Assume

$$0 = T_1 + \dots + T_r, \quad T_i \in H_{\omega_i}.$$

We have to show: $T_i = 0$ for all i .

Let $L = K[c]$. Then for $v \in V$

$$v \left(\sum_{i=2}^r T_i c^{\omega_1} \right) = c^{\omega_1} v \sum_{i=2}^r T_i = -c^{\omega_1} v T_1 = -(cv) T_1 = \sum_{i=2}^r c^{\omega_i} v T_i = v \left(\sum_{i=2}^r T_i c^{\omega_i} \right).$$

Hence $\sum_i T_i c^{\omega_1} = \sum_i T_i c^{\omega_i}$. Since each $T_i c^{\omega_1}$ and $T_i c^{\omega_i}$ is ω_i -linear induction forces $T_i c^{\omega_1} = T_i c^{\omega_i}$ and thus $T_i = 0$ for $i > 1$ by the choice of c . Then $T_1 = 0$ holds too. \square

The following result is a slight generalization of Theorem 5 of [7]. The proof is taken from this article.

Lemma 2.4. *Let $L : K$ be a field extension of degree n and let $\{u^i \mid 0 \leq i < n\}$ and $\{w^i \mid 0 \leq i < n\}$ be K -bases of L . Let k be a number between 1 and $(n-1)/2$. Set $U = \bigoplus_{i=0}^k K u^i$ and $W = \bigoplus_{i=0}^k K w^i$. Equivalent are:*

- (a) *There exists a $\lambda \in L$ with $W = \lambda U$.*
- (b) *w lies in the orbit of u under $\text{PGL}(2, K)$ (acting naturally on $\text{PG}(1, L)$).*

Moreover, if (a) and (b) hold and if

$$w = \frac{a + bu}{c + du}, \quad a, b, c, d \in K,$$

then

$$\lambda \in \frac{1}{(c + du)^k} K.$$

Proof. (a) \Rightarrow (b). There exist polynomials

$$0 \neq B_i = \sum_{j=0}^k b_j^{(i)} X^j \in K[X], \quad 0 \leq i \leq k,$$

such that

$$\lambda B_i(u) = w^i.$$

In particular

$$\lambda = \frac{1}{B_0(u)}, \quad w = \frac{B_1(u)}{B_0(u)}.$$

Assume $k = 1$, $B_1 = a + bX$, and $B_0 = c + dX$. As $w \notin K$ the pairs (a, b) and (c, d) are K -linear independent. Hence the mapping

$$x \mapsto \frac{a + bx}{c + dx}$$

lies in $\text{PGL}(2, K)$ and we are done.

So we assume $k > 1$. Substituting λ we see

$$w^i = \frac{B_i(u)}{B_0(u)}, \quad 1 \leq i \leq k.$$

For $i > 1$ we also have $w^i = w^{i-1}w = \frac{B_{i-1}(u)}{B_0(u)} \frac{B_1(u)}{B_0(u)}$ showing

$$B_i(u)B_0(u) = B_{i-1}(u)B_1(u), \quad 1 \leq i \leq k.$$

This is a polynomial equation of polynomials in u of degree $< n$. Hence we obtain even an equation of (formal) polynomials in $K[X]$

$$B_i B_0 = B_{i-1} B_1, \quad 1 \leq i \leq k.$$

In particular $B_1^2 = B_2 B_0$.

CASE 1 B_1 does not divide B_0 . Then there exists $f \in K[X]$ irreducible with $B_1 = g_1 f^t$, $(f, g_1) = 1$, and f^t does not divide B_0 . Therefore f^{t+1} divides B_2 . A straightforward induction shows

$$B_i = g_i f^{t+i-1}, \quad g_i \in K[X], 1 \leq i \leq k.$$

In particular $B_k = g_k f^{t+k-1}$. Since $\deg B_k \leq k$ we see that

$$\deg f = 1, \quad g_k \in K, \quad t = 1, \quad \text{i.e.} \quad B_k = g_k f^k.$$

Then

$$B_{k-1} = \frac{B_0 B_k}{B_1} = g_k f^{k-1} \frac{B_0}{g_1}.$$

Hence g_1 divides B_0 and as $\deg B_{k-1} \leq k$ one has

$$0 \leq \deg E \leq 1 \quad \text{for} \quad E = \frac{B_0}{g_1}.$$

Moreover

$$w = \frac{B_k(u)}{B_{k-1}(u)} = \frac{f(u)}{E(u)}.$$

Set $f = a + bX$ and $E = c + dX$. Again $w \notin K$ implies $ad - bc \neq 0$ and w has the desired form. Note that

$$\lambda = \frac{w^k}{B_k(u)} = \frac{1}{g_k E(u)^k} \in \frac{1}{E(u)^k} K.$$

CASE 2 Now we assume that B_1 divides B_0 . Since $w \notin K$, we even have $\deg B_1 < \deg B_0$ and using $B_i = B_{i-1}B_1/B_0$ we obtain

$$\deg B_i \leq k - i, \quad 0 \leq i \leq k.$$

But as $B_k \neq 0$ we have

$$B_k \in K, \quad \text{and} \quad \deg B_i = k - i, \quad 0 \leq i \leq k.$$

This shows

$$E = E(X) = \frac{B_0}{B_1} = c + dX, \quad c, d \in K, \quad d \neq 0.$$

Using again $B_i B_0 = B_{i-1} B_1$ we have

$$B_i = B_k E^{k-i}, \quad w = \frac{B_1(u)}{B_0(u)} = \frac{1}{E(u)}, \quad \lambda = \frac{1}{B_k E^k(u)},$$

and we are done.

(b) \Rightarrow (a). Assume now

$$w = \frac{F(u)}{E(u)}, \quad F = a + bX, \quad E = c + dX.$$

Then define

$$\lambda = \frac{1}{E(u)^k}$$

and inductively

$$B_0 = \frac{1}{\lambda}, \quad B_i = w B_{i-1}, \quad 1 \leq i \leq k.$$

A straightforward computation shows

$$B_i(u) = F(u)^i E(u)^{k-i} \in U, \quad 1 \leq i \leq k,$$

and then

$$B_i \lambda = \left(\frac{F(u)}{E(u)} \right)^i = w^i.$$

Now $W = \lambda U$ follows. □

Lemma 2.5. Let $L : K$ be a field extension of degree m and $L = K[u]$. For $1 \leq s < m$ set $L_s = \bigoplus_{i=0}^{s-1} Ku^i$ and let $x \in L$ satisfy $xL_s = L_s$. Then $x \in K$.

Proof. Write $E = L_s$ and $x = a_0 + a_1u + \cdots + a_tu^t$ with $a_i \in K$, $a_t \neq 0$. Since $x = x \cdot 1 \in E$ we see $t < s$. We claim $t = 0$ and thus $x \in K$.

Assume $t > 0$. Then

$$xu^{s-t} = a_0u^{s-t} + a_1u^{s+1-t} + \cdots + a_tu^s.$$

But then $xu^{s-t} \notin E$ as $u^s \in L - E$, a contradiction. \square

Lemma 2.6. Let $L : K_0$ be a field extension of degree mn , $(m, n) = 1$, and let F, K be subfields such that $[F : K_0] = m$ and $[K : K_0] = n$. Assume further that $L : F$ is a Galois extension with a cyclic Galois group $\Sigma = \langle \sigma \rangle$ and that $K : K_0$ is a Galois extension too such that the Galois group is the restriction of Σ to K . Set $Y = \{y \in L^* \mid y^\sigma y^{-1} \in K\}$. Then $Y = F^*K^*$.

Proof. For $y \in Y$ we have $y^\sigma = yv$, $v \in K$. Hence

$$y = y^{\sigma^n} = yvv^\sigma \cdots v^{\sigma^{n-1}} = yN_{K:K_0}(v),$$

i.e. $N_{K:K_0}(v) = 1$. By Hilbert's theorem 90 there exists a $u \in K$ such that $v = u^\sigma u^{-1}$. This implies $(y/u)^\sigma = y/u$, i.e. $y/u \in F$. \square

Lemma 2.7. Let $K : K_0$ be a cyclic Galois extension with Galois group $\langle \phi \rangle$ of order > 1 . Let $L : K$ be a field extension of degree ℓ and assume $L = K_0[u]$. Then $B = \{u^i \mid 0 \leq i < \ell\}$ is a K -basis of L . Write $x \in L$ as $x = \sum_{i=0}^{\ell-1} x_i u^i$, $x_i \in K$, and set $\bar{x} = \sum_{i=0}^{\ell-1} x_i^\phi u^i$. Assume $z \in L$ and that $\overline{z \cdot \bar{x}} = \bar{z} \cdot \bar{x}$ holds for all $x \in L$. Then $z \in K$.

Proof. Clearly, B is a K -basis. Let $f = X^\ell - \sum_{i=0}^{\ell-1} a_i X^i$ be the minimal polynomial of u over K and assume $z = \sum_{i=0}^k z_i u^i$, $z_i \in K$, $z_k \neq 0$, $k < \ell$.

Suppose $k > 0$. Then

$$\begin{aligned} zu^{\ell-k} &= \sum_{i=0}^k z_i u^{\ell-k+i} = \sum_{i=0}^{k-1} z_i u^{\ell-k+i} + z_k \sum_{i=0}^{\ell-1} a_i u^i \\ &= z_k \sum_{i=0}^{\ell-k-1} a_i u^i + \sum_{i=\ell-k}^{\ell-1} (z_{k-\ell+i} + z_k a_i) u^i \end{aligned}$$

i.e.

$$\overline{z \cdot u^{\ell-k}} = z_k^\phi \sum_{i=0}^{\ell-k-1} a_i^\phi u^i + \sum_{i=\ell-k}^{\ell-1} (z_{k-\ell+i}^\phi + z_k^\phi a_i^\phi) u^i.$$

Similarly

$$\bar{z} \cdot \overline{u^{\ell-k}} = \bar{z} u^{\ell-k} = z_k^\phi \sum_{i=0}^{\ell-k-1} a_i u^i + \sum_{i=\ell-k}^{\ell-1} (z_{k-\ell+i}^\phi + z_k^\phi a_i) u^i.$$

Since $z_k \neq 0$ we obtain $a_i^\phi = a_i$ for all $0 \leq i < \ell$. Hence $f \in K_0[X]$ and thus $[L : K_0] \leq \ell$, a contradiction. \square

3 Cyclic semifields and the proof of Theorem 1

We first introduce some notation 3.1 for cyclic semifield planes which will be kept fixed throughout this paper. Then we compute the nuclei (Proposition 3.3) and prove Theorem 1.

3.1. Description of cyclic semifield planes. Let V, K, F, σ, T etc. have the same meaning as in 2.1. We introduce the following notation:

$$\mathbf{S} = \mathbf{S}(T) = \bigoplus_{i=0}^{m-1} KT^i = \bigoplus_{i=0}^{m-1} T^i K$$

is the spread set of the cyclic semifield plane defined by T .

Set $W = V \oplus V$ and

$$\Sigma = \Sigma(T) = \{V(\infty)\} \cup \{V(s) \mid s \in \mathbf{S}\}$$

with $V(\infty) = 0 \times V$ and $V(s) = \{(v, vs) \mid v \in V\}$. Then Σ is the spread on W associated with \mathbf{S} .

Set $d = (m, n)$. Then

$$\mathbf{S} = \mathbf{S}_0 \oplus \cdots \oplus \mathbf{S}_{d-1}.$$

where $\mathbf{S}_0 = \{s \in \mathbf{S} \mid U_0 s \subseteq U_0\}$ and $\mathbf{S}_i = T^i \mathbf{S}_0 = \mathbf{S}_0 T^i$ for $0 \leq i < d$. Note that \mathbf{S}_i is the set of transformations in \mathbf{S} which move U_i onto U_0 .

Let \mathbf{S}^j be the set of σ^j -linear transformations in \mathbf{S} . Then (see Lemma 2.3)

$$\mathbf{S} = \mathbf{S}^0 \oplus \cdots \oplus \mathbf{S}^{\min(m,n)-1}.$$

Note that $\mathbf{S}^j = KT^j$ if $m \leq n$. If $m > n$ set $m = en + r$, $0 \leq r < n$. Then

$$\mathbf{S}^j = \bigoplus_{i=0}^{e'} K \zeta^i T^j = \bigoplus_{i=0}^{e'} \zeta^i T^j K$$

with $e' = e$ if $j < r$ and $e' = e - 1$ otherwise. Recall $T^n = \zeta \mathbf{1}$.

An autotopism α is identified with an element in $\text{GL}_{\text{GF}(p)}(W)$, $p = \text{char } K$, which stabilizes Σ and fixes the fibers $V(\infty)$ and $V(0)$. We also write $\alpha = (\alpha_1, \alpha_2)$ where α_1 is the restriction to $V(0)$ and α_2 is the restriction to $V(\infty)$. We call α *diagonal of type ϕ* , $\phi \in \text{Aut}(L)$, if both α_1 and α_2 are

diagonal of type ϕ , i.e. we have a matrix description of α_1 and α_2 in the form:

$$\alpha_1 = \text{diag}(\phi a_0, \dots, \phi a_{d-1}), \quad \alpha_2 = \text{diag}(\phi b_0, \dots, \phi b_{d-1})$$

We call α *semidiagonal of type ϕ* if α_1 is diagonal of type ϕ and α_2 is permutational of type ϕ , i.e. α_2 has a matrix description in the form

$$\text{diag}(\phi b_0, \dots, \phi b_{d-1})P(\pi)$$

with $\pi \in \langle (0, 1, \dots, d-1) \rangle$.

3.2. Some autotopisms. For $0 \neq a \in K$ the maps L_a and R_a defined by

$$(x, y)L_a = (a \cdot x, y), \quad (x, y)R_a = (x, a \cdot y)$$

are homologies and we see that middle nucleus $N_m = \{\alpha \in \text{End}_{K_0}(V) \mid \alpha \mathbf{S} \subset \mathbf{S}\}$ contains the group

$$\mathcal{L} = \{L_a \mid 0 \neq a \in K\} \simeq K^*$$

and the right nucleus $N_r = \{\alpha \in \text{End}_{K_0}(V) \mid \mathbf{S}\alpha \subset \mathbf{S}\}$ contains the group

$$\mathcal{R} = \{R_a \mid 0 \neq a \in K\} \simeq K^*.$$

For $0 \neq b \in F$ the map D_b defined by

$$(x, y)D_b = (bx, by)$$

is a kern homology. Hence the left nucleus N_ℓ contains the group

$$\mathcal{D} = \{D_b \mid 0 \neq b \in F\} \simeq F^*.$$

Finally, we observe that the transformation \overline{T} defined by $(x, y)\overline{T} = (xT, yT)$ is an autotopism.

Proposition 3.3. $N_r \simeq N_m \simeq K$ and $N_\ell \simeq F$.

Proof. Let $0 \neq \beta \in N_r$, i.e. $\mathbf{S}\beta = \mathbf{S}$. Write

$$T\beta = \sum_{i=0}^k T^i a_i, \quad k \leq m-1, \quad a_k \neq 0.$$

Assume $k \geq 1$. Then

$$T^{m-k}T\beta = \sum_{i=0}^k T^{m-k+i} a_i = T^m a_k + \sum_{i=0}^{k-1} T^{m-k+i} a_i.$$

If $k \geq 2$ then $T^m a_k$ and thus T^m lies in \mathbf{S} . This implies $\mathbf{S}T = \mathbf{S}$, a contradiction, since \mathbf{S} is proper.

Hence $k \leq 1$. If $a_0 \neq 0$ then $\beta = \mathbf{1}a_1 + T^{-1}a_0$ and $\beta = \mathbf{1}\beta \in \mathbf{S}$, i.e. $T^{-1} \in \mathbf{S}$ and $\mathbf{S}T^{-1} = \mathbf{S}$, a contradiction. We conclude $a_0 = 0$ and $\beta = \mathbf{1}a_1$. This shows $N_r \simeq K$ and by symmetry $N_m \simeq K$.

Let $0 \neq \beta \in N_\ell$, i.e. $s\beta = \beta s$ for $s \in \mathbf{S}$. Since β also commutes with K we see that

$$\beta \in C_{\text{End}_{K_0}}(\{T\} \cup K\mathbf{1}).$$

From (Theorem 2.4 in [4]) we get $\beta \in F$. The second claim follows. \square

Definition. We call an autotopism *linear* if it commutes with all elements from the nuclei.

For instance the group

$$M = \mathcal{LRD}.$$

is a group of linear autotopisms. \overline{T} is linear with respect to N_ℓ but only semi-linear respect to N_m and N_r .

Lemma 3.4. *Set $\mathcal{K} = \mathcal{D} \cap (\mathcal{L} \times \mathcal{R})$. Then $\mathcal{K} \simeq K_0^*$ and $M \simeq (\mathcal{D} \times \mathcal{L} \times \mathcal{R})/\mathcal{K}$.*

Proof. Suppose $L_a R_b = D_c \in (\mathcal{L} \times \mathcal{R}) \cap \mathcal{D}$. Then

$$V(1) = V(1)D_c = V(1)L_a R_b = V(a^{-1}b)$$

implies $a = b$. Moreover

$$V(T) = V(T)D_c = V(T)L_a R_a = V(a^{-1}a^\sigma T)$$

which shows $a^{-1}a^\sigma = 1$, i.e. $a \in K_0$. The claim follows. \square

The following observation will be used repeatedly:

Lemma 3.5. *Let i, j be numbers in $\{0, \dots, d-1\}$. Let s, s' be elements in \mathbf{S}_i and $0 \neq u \in U_j$. Then $s = s'$ if us and us' have the same image under the projection onto U_{j-i} . In particular if $s, s' \in \mathbf{S}_0$ and $s_{U_j} = s'_{U_j}$ then $s = s'$.*

Proof. We may assume that $s, s' \neq 0$. As $U_{j-i} = U_i s = U_i s'$ we see for $u \in U_i$ that $u(s - s') = 0$ and since $s - s' \in \mathbf{S}$ we obtain $s = s'$. \square

Lemma 3.6. *The claim of Theorem 1 is true if $d = 1$.*

Proof. Let α be a linear autotopism. We can make the identifications $V = L$ and $xT = wx^\sigma$. By our assumption we have

$$(x, y)\alpha = (ax, by), \quad a, b \in L.$$

Take $0 \neq s \in \mathbf{S}^0$. Then $V(s)\alpha = V(a^{-1}bs)$ and hence $a^{-1}bs \in \mathbf{S}^0$, i.e. $a^{-1}b\mathbf{S}^0 = \mathbf{S}^0$. By Lemma 2.5 (and as $m \neq n$) we get $a^{-1}b \in K$. Adjusting α by $L_{ab^{-1}} \in \mathcal{L}$ we may assume wlog. that $a = b$.

Choose now $0 \neq s \in \mathbf{S}^1$. Then $s = s_0T$, $s_0 \in \mathbf{S}^0$ and

$$V(s)\alpha = V(a^{-1}s_0Ta) = V(a^\sigma a^{-1}s_0T) = V(a^\sigma a^{-1}s)$$

and $a^\sigma a^{-1}s$ is a σ -linear operator in \mathbf{S} . Hence $a^\sigma a^{-1}s \in \mathbf{S}^1$ and $a^\sigma a^{-1}\mathbf{S}^1 = \mathbf{S}^1$. As before we deduce $a^\sigma a^{-1} \in K^*$. Apply Lemma 2.6 to conclude $a \in F^*K^*$. This shows $\alpha \in M$. \square

Lemma 3.7. *Let α be a linear autotopism. For each $i \in \{0, \dots, d-1\}$ the following holds.*

- (a) α leaves invariant $W_i = U_i \oplus U_i$.
- (b) $\alpha_1^{-1}\mathbf{S}_i\alpha_2 = \mathbf{S}_i$.
- (c) \mathbf{S}_0 induces on W_i a cyclic semifield spread which is invariant under the linear autotopism α_{W_i} .
- (d) For each i there exist a $\mu_i \in M$ such that

$$\alpha_{W_i} = (\mu_i)_{W_i}.$$

Proof. (a) By Lemma 2.2 α_1 and α_2 leave each U_i invariant. Therefore α leaves all W_i 's invariant.

(b) Let $0 \neq s$ be in \mathbf{S}_i . Then $V(s)\alpha = V(\alpha_1^{-1}s\alpha_2)$ and for $j \in \{0, \dots, d-1\}$ we have:

$$U_j\alpha_1^{-1}s\alpha_2 = U_j s\alpha_2 = U_{j-i}\alpha_2 = U_{j-i}$$

Hence $\alpha_1^{-1}s\alpha_2 \in \mathbf{S}_i$.

(c) We know that $T_i = (T^d)_{U_i}$ is an irreducible, σ^d -linear operator on the K -space U_i . Note that the fixed field of σ^d is $K_1 \simeq \text{GF}(q^d)$ and that $(T_i)^{n'}$ and K_1 induce on U_i the field F . In particular

$$K_{U_i} \cap F_{U_i} = (K_1)_{U_i}.$$

Hence (with K_1 in the role of K_0) \mathbf{S}_0 induces on W_i a cyclic semifield spread and α induces a linear autotopism.

(d) Set $m = m'd$ and $n = n'd$. By Proposition 3.3 and Lemma 3.5 the nuclei of the semifield induced by \mathbf{S}_0 on U_i coincide with the nuclei of \mathbf{S} when restricted to U_i . Moreover, $[K : K_1] = n'$, $[F : K_1] = m'$, and $(m', n') = 1$. Therefore we can apply Lemma 3.6 to W_i and α_{W_i} . Our statement on the nuclei implies assertion (d). \square

Now Theorem 1 follows from Lemma 3.6 and:

Lemma 3.8. *The claim of Theorem 1 is true if $d > 1$.*

Proof. Let α be a linear autotopism. We keep the notation of Lemma 3.7. Suppose first that \mathbf{S}_0 induces on W_0 a proper cyclic semifield spread. Then by

Lemma 3.6 the homology groups associated with the nuclei are already induced by the elements of M . Hence we find $\mu \in M$ such that

$$\mu_{W_0} = \alpha_{W_0}^{-1}.$$

Assume now that \mathbf{S}_0 is not proper, then $F = L \simeq \mathbf{S}_0$, i.e. n divides m and $L = K \oplus K\zeta \oplus \dots \oplus K\zeta^{m'-1}$. Adjusting α by a suitable element in M we can assume $(\alpha_1)_{U_0} = 1$. We identify $(\mathbf{S}_0)_{U_0}$ with L and as $(\mathbf{S}_0)_{U_0}(\alpha_2)_{U_0} = (\mathbf{S}_0)_{U_0}$ we may identify $(\alpha_2)_{U_0}$ with some $z \in L$. Apply Lemma 2.7. Hence $z \in K$ and $(\alpha_2 R_{z^{-1}})_{U_0} = 1$.

So in any case α can be replaced by some $\alpha\mu$, $\mu \in M$, such that $(\alpha\mu)_{W_0} = 1$. Then

$$(\alpha_1^{-1}\alpha_2)_{U_0} = 1.$$

Using Lemma 3.5 we deduce $\alpha_1 = \alpha_2$ and $(\alpha_1)_{U_0} = 1$. Therefore α_1 is represented in matrix form by

$$\alpha_1 = \text{diag}(1, A_2, \dots, A_d)$$

with $A_i \in L$. As

$$(\alpha_1^{-1}T^d\alpha_1)_{U_0} = T_{U_0}^d$$

we deduce from Lemma 3.5 that $T^d\alpha_1 = \alpha_1 T^d$. Hence $A_i^\gamma w = wA_i$ for $2 \leq i \leq d$, i.e. $A_i = A_i^\gamma$ or

$$A_i \in F, \quad 1 < i \leq d, \quad (1)$$

since the fixed field of γ in L is F . Moreover there exists a $T' \in \mathbf{S}_1 = T\mathbf{S}_0$ such that

$$V(T)\alpha = V(\alpha_1^{-1}T\alpha_1) = V(T')$$

with

$$T' = \begin{pmatrix} 0 & 0 & \cdots & 0 & \gamma w A_d \\ A_2^{-1} & 0 & \cdots & 0 & 0 \\ 0 & A_3^{-1}A_2 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & A_d^{-1}A_{d-1} & 0 \end{pmatrix} = T\mathcal{A}$$

and

$$\mathcal{A} = \text{diag}(A_2^{-1}, A_3^{-1}A_2, \dots, A_d^{-1}A_{d-1}, A_d) \in \mathbf{S}_0.$$

Replacing T by any element in \mathbf{S}_1 we see by the same argument that $\mathbf{S}_0\mathcal{A} = \mathbf{S}_0$ and \mathcal{A} represents an element in \mathbf{S}_0 as 1 is in \mathbf{S}_0 .

Set $x = A_2^{-1}$. Then $x_{U_0} \in (\mathbf{S}_0)_{U_0}$ and $(\mathbf{S}_0)_{U_0}x_{U_0} = (\mathbf{S}_0)_{U_0}$. Using Lemmas 3.6 and 3.7 with $(\mathbf{S}_0)_{U_0}$ in the role of \mathbf{S} , γ in the role of σ we see that $x_{U_0} \in K_{U_0}$. This shows using (1)

$$x_{U_0} \in (F \cap K)_{U_0} = (K_1)_{U_0}. \quad (2)$$

We conclude $A_2^{-1} \in K_1$. This shows (using Lemma 3.5 again)

$$\mathcal{A} = \text{diag}(a, a^\sigma, \dots, a^{\sigma^{d-1}})$$

for some $a \in K_1$. We obtain $A_2^{-1} = a$, $A_3^{-1} = a^\sigma A_2^{-1} = aa^\sigma$, \dots , $A_d^{-1} = aa^\sigma \dots a^{\sigma^{d-2}}$. Finally the equation $A_d = a^{\sigma^{d-1}}$ implies $aa^\sigma \dots a^{\sigma^{d-1}} = 1$. Hilbert's theorem 90 shows that there is a $b \in K_1$ with $a = b/b^\sigma$. We conclude

$$\alpha_1 = \text{diag}\left(1, \frac{b^\sigma}{b}, \frac{b^{\sigma^2}}{b}, \dots, \frac{b^{\sigma^{d-1}}}{b}\right)$$

and

$$\alpha = D_{b^{-1}} L_b R_b \in M$$

follows. □

4 Proof of Theorem 2

In this section we show that autotopisms of $\mathbf{P}(T)$ can be described by some kind of "normal form" (see the definition and 4.1 below). Subsequently we verify Theorem 2.

Definition. Denote by G_1 the subgroup of G (autotopism group of $\mathbf{P} = \mathbf{P}(T)$) consisting of diagonal autotopisms and by G_0 the subgroup which consists of diagonal and semidiagonal autotopisms (see 3.1).

The next result shows that the quotient G/M is determined by the subgroup G_0 :

Proposition 4.1. $M \leq G_0 \trianglelefteq G$, $G = G_0 \langle \overline{T} \rangle$, and $|G : G_0| = d$. Moreover all autotopisms in G_0 are diagonal, that is $G_0 = G_1$, if n is not a divisor of m .

We need:

Lemma 4.2. Let α be an autotopism of $\mathbf{P} = \mathbf{P}(T)$.

- (a) α_1 and α_2 are associated with the same field automorphism of F .
- (b) α_1 and α_2 are associated with the same field automorphism of K or n divides m .
- (c) α_1 and α_2 induce the same permutation on $\{U_0, \dots, U_{d-1}\}$ or n divides m .
- (d) Let α_1 and α_2 induce the trivial permutation on $\{U_0, \dots, U_{d-1}\}$. Then α_1 and α_2 are associated with the same field automorphism of K .

Proof. (a) As kernel of \mathbf{P} is F one knows that α is a semilinear map on W with respect to F . This shows the claim.

(b) Suppose that $\alpha_i, i = 1, 2$, are associated with the field automorphisms ϕ_i of K . Then $\alpha_1^{-1}\alpha_2$ is associated with the field automorphism $\tau = \phi_1^{-1}\phi_2$ of K . Hence $\alpha_1^{-1}\mathbf{S}^0\alpha_2$ is a set of τ -linear mappings on V (considered as a K -space) contained in \mathbf{S} . Therefore $\tau = \sigma^k$ for some $0 \leq k \leq \min(m-1, n-1)$.

Assume $k > 0$. Suppose first $n > m$. Then $\alpha_1^{-1}\mathbf{S}^{m-k}\alpha_2$ is a set of σ^m -linear mappings inside of \mathbf{S} , which is impossible.

Assume next $m \geq n$ and set $m = en + r, 0 \leq r < n$. Then $\dim_K \mathbf{S}^j = e + 1$ for $0 \leq j < r$ and $\dim_K \mathbf{S}^j = e$ for $r \leq j < n$. Assume $r > 0$. Then $\dim_K \mathbf{S}^k = \dim_K \mathbf{S}^0$ implies $k < r$. But then

$$e = \dim_K \mathbf{S}^r = \dim \alpha_1^{-1}\mathbf{S}^{r-k}\alpha_2 = \dim \mathbf{S}^{r-k} = e + 1,$$

a contradiction. Therefore if $\phi_1 \neq \phi_2$, i.e. $\tau \neq 1$, we see, that n divides m .

(c) Assume that $\mathbf{S}_j = \alpha_1^{-1}\mathbf{S}_0\alpha_2 \neq \mathbf{S}_0$. Then $\alpha_1^{-1}\mathbf{S}^0\alpha_2 \subseteq \mathbf{S}_j$ is a set of semilinear, but not linear mappings with respect to K . I.e. the automorphisms of K associated with α_1 and α_2 must be different. Apply (b).

(d) By (b) we only have to consider the case that n divides m ; i.e. F contains a subfield isomorphic to K and each element of K when restricted to a U_i lies in this subfield. By (a) the claim follows. \square

Proof of 4.1. By Lemma 2.2 every autotopism of G induces a permutation of the subspaces $\{U_i \times 0 \mid 0 \leq i < d\}$ and G_0 is the kernel of this permutation representation:

Let α be an element in G_0 . If n is not a divisor of m , we see by Lemma 4.2.c that α fixes all spaces $0 \times U_i$ and by Lemma 4.2.d that α_1 and α_2 induce on K the same field automorphism. As L is generated by the subfields K and F we see (using Lemma 4.2.a) that α is a diagonal autotopism. If n divides m then K is isomorphic to a subfield of $L = F$ and α is semidiagonal by Lemma 4.2.a. Moreover $G_0 \trianglelefteq G$.

Using Lemma 2.2 again we see, that we can adjust any autotopism with an element from $\langle \bar{T} \rangle$ to obtain a semi-diagonal autotopism. This implies the second assertion. Clearly, \bar{T} permutes the above subspaces transitively and again by Lemma 2.2 the permutation representation is semi-regular. Hence $|G : G_0| = d$. Moreover by Lemma 4.2.c we have $n \mid m$ if G_0 contains a semi-diagonal, but not diagonal autotopism. \square

Lemma 4.3. *Theorem 2 is true.*

Proof. By Proposition 4.1, $|G/G_0| = d$ and G_1 is the subgroup of autotopisms in G which fix $W_0 = U_0 \oplus U_0$. The mapping $G_1 \rightarrow \text{Aut}(L)$ which maps α to ϕ where ϕ is the type of α (see 3.1) is obviously a homomorphism with kernel M . Thus

$$|G_1/M| \mid |\text{Aut}(L)| = f \cdot m \cdot n/d.$$

Assume first that n does not divide m . Then by Proposition 4.1 $G_0 = G_1$ and therefore $|G/M|$ divides $f \cdot m \cdot n$.

Assume next now that n divides m . Then (using Lemma 2.2) G_0 induces a semiregular permutation representation on $\{0 \times U_i \mid 0 \leq i < d\}$ with kernel G_1 . This shows

$$|G_0/G_1| \mid d$$

Therefore $|G/M|$ divides $f \cdot m \cdot n \cdot d$. \square

5 The case $(m, n) = 1$

We assume throughout this section

$$d = (m, n) = 1.$$

In view of 3.1 we can identify $V \cong L$ and T with the mapping

$$x \mapsto wx^\sigma,$$

where $F = K_0[\zeta]$, $L = K[\zeta]$, and $\zeta = N_{L:F}(w)$. Clearly, all autotopisms are diagonal, i.e. $G_0 = G$. Therefore we may write formally (abbreviating $a_0 = e$, $b_0 = v$ in (2.1)):

$$\alpha_1 = \phi e, \quad \alpha_2 = \phi v, \quad e, v \in L.$$

Lemma 5.1. *Let $m < n$ and $\phi \in \text{Aut}(L)$. Equivalent are:*

- (a) *There exists an autotopism of type ϕ .*
- (b) *$w^{\phi^{-1}} \in (L^*)^{\sigma^{-1}} K^*$.*

Proof. Let α be an autotopism of type ϕ . Use the notation from above. Then $\alpha_1^{-1} = \phi^{-1} f$ with $f = e^{-\phi}$.

Let $x \in K^*$. Then $\alpha_1^{-1} T^k x \alpha_2$ is σ^k -linear, i.e. $\alpha_1^{-1} T^k x \alpha_2 = T^k y$ for some $y \in K^*$. On the other hand

$$\alpha_1^{-1} T^k x \alpha_2 = \sigma^k f^{\phi \sigma^k} (w w^\sigma \dots w^{\sigma^{k-1}})^\phi v x^\phi = T^k \frac{(w w^\sigma \dots w^{\sigma^{k-1}})^\phi}{w w^\sigma \dots w^{\sigma^{k-1}}} f^{\phi \sigma^k} v x^\phi$$

Hence we have for $0 \leq k < m$

$$\frac{(w w^\sigma \dots w^{\sigma^{k-1}})^\phi}{w w^\sigma \dots w^{\sigma^{k-1}}} f^{\phi \sigma^k} v \in K. \quad (1)$$

Specializing $k = 0$ we get

$$v = \frac{A}{f^\phi} \quad (2)$$

with $A \in K^*$ and specializing $k = 1$ we have

$$\frac{w^\phi}{w} \cdot \frac{(f^\phi)^\sigma}{f^\phi} \cdot A \in K^*. \quad (3)$$

Therefore the condition

$$w^{\phi-1} \in K^*(L^*)^{\sigma-1}$$

is necessary for the existence of an autotopism of type ϕ .

Suppose conversely that this condition is true. Then choose $f \in L^*$ such that (3) holds with $A = 1$ and define $v \in L^*$ by (2) and then α_1 and α_2 as above.

We claim that this defines an autotopism. The foregoing computations show that we have to verify equation (1) for all $0 \leq k < n$. We notice that the cases $k = 0, 1$, i.e. equations (2) and (3), are already true.

Assume $k \geq 2$. Then

$$\begin{aligned} \frac{(ww^\sigma \cdots w^{\sigma^{k-1}})^\phi}{ww^\sigma \cdots w^{\sigma^{k-1}}} f^{\phi\sigma^k} v &= \frac{(ww^\sigma \cdots w^{\sigma^{k-1}})^\phi}{ww^\sigma \cdots w^{\sigma^{k-1}}} \cdot \frac{f^{\phi\sigma^k}}{f^\phi} \\ &= \frac{(ww^\sigma \cdots w^{\sigma^{k-1}})^\phi}{ww^\sigma \cdots w^{\sigma^{k-1}}} \frac{(f^\sigma f^{\sigma^2} \cdots f^{\sigma^k})^\phi}{(f f^\sigma \cdots f^{\sigma^{k-1}})^\phi} \\ &= \left(\frac{w^\phi}{w} \frac{f^{\phi\sigma}}{f^\phi} \right) \left(\frac{w^\phi}{w} \frac{f^{\phi\sigma}}{f^\phi} \right)^\sigma \cdots \left(\frac{w^\phi}{w} \frac{f^{\phi\sigma}}{f^\phi} \right)^{\sigma^{k-1}} \in K^* \end{aligned}$$

by (3). The proof is complete. \square

Lemma 5.2. *Let $m > n$ and $\phi \in \text{Aut}(L)$. Equivalent are:*

- (a) *There exists an autotopism of type ϕ .*
- (b) *ζ^ϕ lies in the orbit of ζ under $\text{PGL}(2, K)$ (acting naturally on $\text{PG}(1, L)$).*
Moreover if

$$\zeta^\phi = \frac{F(\zeta)}{E(\zeta)}; \quad F(X), E(X) \in K[X], \quad 0 \leq \deg F(X), \deg E(X) \leq 1,$$

then $E(\zeta)w^{\phi-1} \in L^{\sigma-1}K$ if $n = 2$, and $E(\zeta) \in K$, $w^{\phi-1} \in L^{\sigma-1}K$ if $n > 2$.

Proof. (a) \Rightarrow (b). We choose the same notation as in the proof of Lemma 5.1. Write $m = en + r$.

Then for $0 \leq k < n$ we have $\alpha_1^{-1} \mathbf{S}^k \alpha_2 = \mathbf{S}^k$. Set $L(k) = \bigoplus_{i=0}^e K\zeta^i$ for $k < r$ and $L(k) = \bigoplus_{i=0}^{e-1} K\zeta^i$ for $r \leq k < n$. Then $\mathbf{S}^k = T^k L(k)$. Set

$$A_k = \frac{(ww^\sigma \cdots w^{\sigma^{k-1}})^\phi}{ww^\sigma \cdots w^{\sigma^{k-1}}} f^{\phi\sigma^k} v.$$

The same computation as in the proof of Lemma 5.1 shows $A_k L(k)^\phi = L(k)$ ($\Leftrightarrow A_k^{-1} L(k) = L(k)^\phi$). By Lemma 2.4 (with ζ in the role of u , ζ^ϕ in the role of w) we have

$$\zeta^\phi = \frac{F(\zeta)}{E(\zeta)}; F(X) = a + bX, E(X) = g + hX \in K[X],$$

and

$$A_k \equiv \begin{cases} E(\zeta)^e, & 0 \leq k < r, \\ E(\zeta)^{e-1}, & r \leq k < n, \end{cases} \pmod{K^*}.$$

In particular

$$E(\zeta) \equiv \frac{A_{r-1}}{A_r} = (w^{1-\phi})^{\sigma^{r-1}} (f^{1-\sigma})^{\phi\sigma^{r-1}} \pmod{K^*}.$$

This implies

$$g + h\zeta \in (w^{1-\phi})^{\sigma^{r-1}} L^{1-\sigma} K.$$

If $n = 2$ then $r = 1$ and $E(\zeta) = g + h\zeta \in (w^{1-\phi}) L^{1-\sigma} K = (w^{1-\phi}) L^{\sigma-1} K$ and we are done.

So assume $n > 2$. Then $n-1 > r$ or $r > 1$. We only treat the case $n-1 > r$, the other case is similar. In the first case $A_r \equiv A_{r+1} \pmod{K^*}$. Hence

$$\frac{A_{r+1}}{A_r} = (w^{\phi-1})^{\sigma^r} (f^{\sigma-1})^{\phi\sigma^r} \in K^*.$$

This implies

$$(w^{1-\phi})^{\sigma^{r-1}} \equiv (f^{\sigma-1})^{\phi\sigma^{r-1}} \pmod{K^*},$$

and therefore

$$E(\zeta) \equiv (w^{1-\phi})^{\sigma^{r-1}} (f^{1-\sigma})^{\phi\sigma^{r-1}} \equiv 1 \pmod{K^*}.$$

So we may assume $E(\zeta) = 1$ and $\zeta^\phi = F(\zeta) = a + b\zeta$.

The case $r > 1$ (use A_0 and A_1) leads to the same assertion. So (b) holds.

(b) \Rightarrow (a). Assume now $\zeta^\phi = \frac{F(\zeta)}{E(\zeta)}$ where $F(X), E(X) \in K[X]$ have the shape from above. Moreover assume $E(\zeta) \in (w^{1-\phi}) L^{1-\sigma} K$ if $n = 2$ and $E(\zeta) \in K$, $w^{\phi-1} \in L^{1-\sigma} K$ if $n > 2$. In both cases choose $f \in L^*$ such that

$$(f^\phi)^{1-\sigma} \equiv E(\zeta) w^{\phi-1} \pmod{K^*},$$

and define $v \in L^*$ by the equation

$$A_0 = E(\zeta)^e = f^\phi v.$$

Moreover define $A_k, L(k)$, $1 \leq k < n$ as above. Using Lemma 2.4, a straightforward computation shows

$$A_k L(k)^\phi = L(k).$$

Then $\alpha_1^{-1} = \phi^{-1} f$ and $\alpha_2 = \phi v$ define an autotopism of type ϕ . \square

Remark. The case $m > n = 2$ is implicitly contained as Theorem 5 in the article of Johnson, Polverino, Marino, and Trombetti [7].

6 The case $n \geq m$

We keep the description of V , T , and autotopisms as explained in 2.1 and 3.1. We assume throughout this section

$$n \geq m.$$

In view of the previous section we may assume

$$d = (m, n) > 1.$$

It will be convenient to write $k^{(j)}$ instead of k^{σ^j} for $k \in K$ and $j = 0, 1, \dots$

Lemma 6.1. *Assume $m = n$. Then $F \simeq K \simeq L$.*

(a) $G_1/M \simeq \{\phi \in \text{Aut}(L) \mid w^{\phi^{-1}} \in K_0\}$.

(b) $G_0/G_1 \simeq C_2$ if $m = 2$ and $G_0 = G_1$ otherwise.

Proof. We have $\mathbf{S} = \bigoplus_{i=0}^{m-1} T^i K$.

(a) Let $\alpha = (\alpha_1, \alpha_2)$ be a diagonal autotopism of type $\phi \in \text{Aut}(L)$. We write $\alpha_1^{-1} = \text{diag}(\phi^{-1}a_0, \phi^{-1}a_1, \dots)$ and $\alpha_2 = \text{diag}(\phi b_0, \phi b_1, \dots)$ as in 3.1. By adjusting α with a suitable element from M we may assume $a_0 = b_0 = 1$ and $\alpha_1 = \alpha_2$. This implies (note $d = n$)

$$b_i = \frac{1}{a_i^\phi} \quad 1 \leq i < n.$$

For $Tk \in \mathbf{S}_1 = TK$ there exists an $\ell \in K$ with

$$\alpha_1^{-1}Tk\alpha_2 = T\ell$$

and a computation leads to the equations

$$a_1^\phi = \frac{\ell^{(0)}}{k^{\phi(0)}}, \quad \frac{a_2^\phi}{a_1^\phi} = \frac{\ell^{(1)}}{k^{\phi(1)}}, \quad \frac{a_3^\phi}{a_2^\phi} = \frac{\ell^{(2)}}{k^{\phi(2)}}, \quad \dots, \quad \frac{a_{n-1}^\phi}{a_{n-2}^\phi} = \frac{\ell^{(n-2)}}{k^{\phi(n-2)}}, \quad \frac{w^{\phi^{-1}}}{a_{n-1}^\phi} = \frac{\ell^{(n-1)}}{k^{\phi(n-1)}}.$$

This implies

$$N_{K:K_0}\left(\frac{\ell^{(0)}}{k^{\phi(0)}}\right) = w^{\phi^{-1}}.$$

Therefore a necessary condition for the existence of a diagonal autotopism of type ϕ is

$$w^{\phi^{-1}} \in K_0.$$

We show that this condition is sufficient too. So take $a \in K$ such that $N_{K:K_0}(a^\phi) = w^{\phi^{-1}}$ and define:

$$a_0 = 1, \quad a_1 = a^{(0)}, \quad a_2 = a^{(0)}a^{(1)}, \quad \dots, \quad a_{n-1} = a^{(0)}a^{(1)} \dots a^{(n-2)}$$

and $\alpha_1 = \alpha_2$ as above. A computation shows

$$\alpha_1^{-1}T\alpha_2 = Ta^\phi.$$

Now $\alpha_1^{-1}T^i\alpha_2 = (\alpha_1^{-1}T\alpha_1)^i \in T^iK$ follows. Hence $\alpha = (\alpha_1, \alpha_2)$ defines a diagonal autotopism associated with ϕ .

(b) Let $\alpha = (\alpha_1, \alpha_2)$ be a proper semi-diagonal autotopism of type $\phi \in \text{Aut}(L)$. We split our argument into subcases.

(1) Let α_2 induce a permutation of order n . Then $n = 2$ and such autotopisms do exist.

We may assume wlog. that

$$x\alpha_2 = (b_1x_1^\phi, b_2x_2^\phi, \dots, b_{n-1}x_{n-1}^\phi, b_0x_0^\phi)$$

and by adjusting the autotopism with a suitable element from M we may even assume $\alpha_1^{-1}\alpha_2 = T$, $a_0 = 1$, and $b_0 = w$. This implies

$$b_i = \frac{1}{a_i^\phi}, \quad 1 \leq i < n.$$

Assume first $n = 2$. Then $\alpha_1^{-1}T\alpha_2 \in \mathbf{S}_0 = K$ which shows that there exists a $k \in K$ such that

$$k^{(0)} = \frac{w^\phi}{a_1^\phi}, \quad k^{(1)} = a_1^\phi w.$$

Choosing $\phi = \sigma$ and $a_1 = 1$ we obtain a solution.

So we assume from now on $n > 2$. Then $\alpha_1^{-1}T\alpha_2 = kT^2$ for some $k \in K$. Comparing both sides we obtain the equations

$$a_1 = k^{\varphi(1)}, a_2 = k^{\varphi(1)}k^{\varphi(2)}, \dots, a_{n-1} = k^{\varphi(1)}k^{\varphi(2)} \dots k^{\varphi(n-1)}$$

with $\varphi = \phi^{-1}$. This forces as in (a) $w^{\phi^{-1}} = N_{K:K_0}(k)$.

Finally $\alpha_1^{-1}T^{n-1}\alpha_2 \in K$, i.e. there exists $\ell \in K$ such that the equations

$$\ell^{(0)} = \frac{w^\phi}{a_1^\phi}, \ell^{(1)} = \frac{w^\phi a_1^\phi}{a_2^\phi}, \dots, \ell^{(n-2)} = \frac{w^\phi a_{n-2}^\phi}{a_{n-1}^\phi}, \ell^{(n-1)} = w a_{n-1}^\phi$$

hold. Replacing the a_i 's we get

$$\ell^{(0)} = \frac{w^\phi}{k^{(1)}}, \ell^{(1)} = \frac{w^\phi}{k^{(2)}}, \dots, \ell^{(n-2)} = \frac{w^\phi}{k^{(n-1)}},$$

and

$$\ell^{(n-1)} = w k^{(1)} k^{(2)} \dots k^{(n-1)} = \frac{w^\phi}{k^{(0)}}.$$

This shows $w^\phi = \ell^{(0)}k^{(1)} = \ell^{(n-1)}k^{(0)}$ forcing $w^\sigma = w$, a contradiction. Hence (1) is true.

(2) Let $n = 2k$, $k > 1$. Then 2 is not the order of the permutation induced by α_2 .

Assume the contrary. Then

$$x\alpha_2 = (b_k x_k^\phi, \dots, b_{n-1} x_{n-1}^\phi, b_0 x_0^\phi, \dots, b_{k-1} x_{k-1}^\phi)$$

and adjusting α with a suitable element from M we may even assume $a_0 = 1$ and $\alpha_1^{-1}\alpha_2 = T^k$. This shows

$$b_0 = w, \quad b_i = \frac{w}{a_i^\phi}, \quad 1 \leq i < k; \quad b_i = \frac{1}{a_i^\phi}, \quad k \leq i < n.$$

Also $\alpha_1^{-1}T\alpha_2 = \ell T^{k+1}$ for some $\ell \in K$. We obtain the equations

$$\begin{aligned} \ell^{(0)}w &= w^\phi b_{n-1}, \ell^{(1)}w = a_1^\phi b_0, \dots, \ell^{(k)}w = a_k^\phi b_{k-1}, \\ \ell^{(k+1)} &= a_{k+1}^\phi b_k, \dots, \ell^{(n-1)} = a_{n-1}^\phi b_{n-2}. \end{aligned}$$

This leads to

$$a_1^\phi = \ell^{(1)}, a_2^\phi = \ell^{(1)}\ell^{(2)}, \dots, a_{n-1}^\phi = \ell^{(1)}\ell^{(2)} \dots \ell^{(n-1)}$$

and

$$w^{\phi-1} = \mathbf{N}_{K:K_0}(\ell).$$

Finally we have $\alpha_1^{-1}T^k\alpha_2 = s$ with $s \in K$. One obtains the equations

$$\begin{aligned} s^{(0)} &= w^\phi b_k, s^{(1)} = w^\phi a_1^\phi b_{k+1}, \dots, s^{(k-1)} = w^\phi a_{k-1}^\phi b_{n-1}, \\ s^{(k)} &= a_k^\phi b_0, \dots, s^{(n-1)} = a_{n-1}^\phi b_{k-1}. \end{aligned}$$

We eliminate the a_i 's and the b_i 's and get

$$s^{(i)} = \frac{w^\phi}{\ell^{(i+1)} \dots \ell^{(k+i)}}, \quad s^{(k+i)} = w\ell^{(i+1)} \dots \ell^{(k+i)}, \quad 0 \leq i < k.$$

In particular

$$s^{(1)} = \frac{w^{\phi(1)}}{\ell^{(2)} \dots \ell^{(k+1)}} = \frac{w^\phi}{\ell^{(2)} \dots \ell^{(k+1)}}.$$

But then $w^{\phi(1)} = w^\phi$, a contradiction. This implies assertion (2).

Using (1) and (2) we may now assume that $n > 2$ and that the permutation induced by α_2 has an odd order r , where r is a proper divisor of n , say $n = fr$. Then α_2 leaves invariant the subspace

$$\tilde{V} = U_0 \oplus U_f \oplus \dots \oplus U_{(r-1)f}$$

and

$$\tilde{\mathbf{S}} = K \oplus KT^f \oplus \dots \oplus KT^{(r-1)f}$$

induces on $\widetilde{W} = \widetilde{V} \times \widetilde{V}$ a cyclic semifield plane and $\alpha_{\widetilde{W}}$ induces a semi-diagonal autotopism whose associated permutation has order r . This shows that we are in the situation of (1). Hence $r \leq 1$, i.e. the autotopism is diagonal. The proof is complete. \square

Lemma 6.2 *Assume $m < n$. Then G_0 is the group of diagonal autotopisms. Let ϕ be an automorphism of L . Equivalent are:*

(a) *There exists a diagonal autotopism associated with ϕ .*

(b) $w^{\phi-1} \in K^{1+\sigma+\dots+\sigma^{d-1}} L^{\gamma-1}$.

In particular $G_0/M \simeq \{\phi \in \text{Aut}(L) \mid w^{\phi-1} \in K^{1+\sigma+\dots+\sigma^{d-1}} L^{\gamma-1}\}$.

Proof. The first assertion follows from Proposition 4.1. Let $\alpha = (\alpha_1, \alpha_2)$ be a diagonal autotopism associated with $\phi \in \text{Aut}(L)$ (we represent the α_i 's as in the proof of 6.1). As $\mathbf{S}^i = T^i K$ and as \mathbf{S}^i is the set of σ^i -linear maps in \mathbf{S} we have $\alpha_1^{-1} \mathbf{S}^i \alpha_2 = \mathbf{S}^i$. In particular by adjusting α with some element from M we may assume $\alpha_1 = \alpha_2$. This implies

$$b_i = \frac{1}{a_i^\phi}, \quad 0 \leq i < d.$$

There exist some $k \in K$ such that $\alpha_1^{-1} T \alpha_2 = T k$. We obtain the equations

$$a_1^\phi b_0 = k^{(0)}, \dots, a_{d-1}^\phi b_{d-2} = k^{(d-2)}, w^\phi a_0^{\gamma\phi} b_{d-1} = w k^{(d-1)}.$$

Eliminating the b_i 's we get

$$a_1^\phi = k^{(0)} a_0^\phi, a_2^\phi = k^{(0)} k^{(1)} a_0^\phi, \dots, a_{d-1}^\phi = k^{(0)} k^{(1)} \dots k^{(d-2)} a_0^\phi$$

and

$$w^{\phi-1} a_0^{\gamma\phi} = k^{(0)} k^{(1)} \dots k^{(d-1)} a_0^\phi.$$

Therefore condition (b) is necessary for the existence of a diagonal autotopism of type ϕ .

Conversely, we assume that condition (b) holds and show the existence of an autotopism. Choose $a_0 \in L$ and $k \in K$ such that

$$w^{\phi-1} = k^{(0)} \dots k^{(d-1)} (a_0^\phi)^{1-\gamma}$$

and define a_i for $0 < i < d$ by

$$a_i^\phi = k^{(0)} k^{(1)} \dots k^{(i-1)} a_0^\phi$$

and $\alpha_1 = \alpha_2$ by

$$x \alpha_1^{-1} = (a_0 x_0^{\phi-1}, \dots, a_{d-1} x_{d-1}^{\phi-1}).$$

Then the above computations show $\alpha_1^{-1}\mathbf{S}^i\alpha_2 = \mathbf{S}^i$ for $i = 0, 1$. Now $\alpha_1^{-1}\mathbf{S}^i\alpha_2 = \alpha_1^{-1}\mathbf{S}^i\alpha_1 = \mathbf{S}^i$ follows for all $0 \leq i < m$. The proof is complete. \square

Summarizing Theorem 1, Proposition 4.1, Lemmas 5.1, 6.1, and 6.2 we have:

Proposition 6.3 *Assume $n \geq m$ and use the notation of 2.1 and 3.1. Then $M \trianglelefteq G_1 \trianglelefteq G_0 \trianglelefteq G$, $|M| = (q^n - 1)^2(q^m - 1)/(q - 1)$, and $|G : G_0| = d$. Moreover:*

- (a) $G_1/M \simeq \{\phi \in \text{Aut}(L) \mid w^{\phi-1} \in K^{1+\sigma+\dots+\sigma^{d-1}}L^{\gamma-1}\}$.
- (b) $G_0/G_1 \simeq C_2$ if $m = n = 2$ and $G_0 = G_1$ otherwise.

7 The case $m > n$

We assume throughout this section

$$m > n.$$

In view of the section 5 we may assume

$$d = (m, n) > 1.$$

We set further $m = m'd$, $n = n'd$. We recall from 2.1 and 3.1 $\gamma \in \text{Aut}(L)$ such that $\gamma_K = \sigma^d$. A K -basis for L is $\{1, \zeta, \zeta^2, \dots, \zeta^{m'-1}\}$ where

$$\zeta = N_{L:F}(w) = ww^\gamma \dots w^{\gamma^{n'-1}}.$$

If $x = \sum_{i=0}^{m'-1} x_i \zeta^i$, $x_i \in K$, we set $x^{(0)} = x$ and

$$x^{(1)} = \sum_{i=0}^{m'-1} x_i^\sigma \zeta^i$$

and define inductively $x^{(i+1)} = (x^{(i)})^{(1)}$.

Lemma 7.1. *Assume for $\phi \in \text{Aut}(L)$ that $\zeta^\phi = a + b\zeta$ with $a, b \in K_0$. Then for all $x \in L$ we have*

$$x^{(1)\phi} = x^{\phi(1)}.$$

Proof. Both mappings are additive. So it suffices to consider monomials of the form $x = k\zeta^j$, $k \in K$. We calculate

$$x^{(1)\phi} = \sum_{\ell=0}^j \binom{j}{\ell} k^{\sigma\phi} a^{j-\ell} b^\ell \zeta^\ell$$

and

$$x^{\phi(1)} = \sum_{\ell=0}^j \binom{j}{\ell} k^{\phi\sigma} (a^{j-\ell} b^\ell)^\sigma \zeta^\ell$$

and the claim follows by the assumptions. \square

Lemma 7.2. *Assume that for $\phi \in \text{Aut}(L)$ both $\zeta^\phi = a + b\zeta$; $a, b \in K_0$ and $w^{\phi^{-1}} \in K^{1+\sigma+\dots+\sigma^{d-1}}L^{\gamma^{-1}}$ hold. Then there exists a diagonal autotopism of type ϕ .*

Proof. Choose $s \in K$ and $a_0 \in L$ such that

$$w^{\phi^{-1}} = s^{(0)}s^{(1)} \dots s^{(d-1)}a_0^{\phi(\gamma^{-1})}$$

holds. Define further a_1, a_2, \dots by

$$a_1^\phi = a_0^\phi s^{(0)}, a_2^\phi = a_0^\phi s^{(0)}s^{(1)}, \dots, a_{d-1}^\phi = a_0^\phi s^{(0)} \dots s^{(d-2)}$$

and set

$$\alpha_1^{-1} = \text{diag}(\phi^{-1}a_0, \dots, \phi^{-1}a_{d-1}).$$

Then

$$\alpha_1 = \text{diag}(\phi b_0, \dots, \phi b_{d-1})$$

with $b_i = 1/a_i^\phi$. Set $\alpha_2 = \alpha_1$ and $\alpha = (\alpha_1, \alpha_2)$. Then calculations show $\alpha_1^{-1}\mathbf{S}^0\alpha_1 = \mathbf{S}^0$ and $\alpha_1^{-1}T\alpha_1 = Ts$. Then even $\alpha_1^{-1}\mathbf{S}\alpha_1 = \mathbf{S}$ and the assertion follows. \square

Lemma 7.3. *Assume $m > n > d > 1$. Then G_1/M is isomorphic to the subgroup of $\phi \in \text{Aut}(L)$ such that $\zeta^\phi = a + b\zeta$, $a, b \in K_0$, and $w^{\phi^{-1}} \in K^{1+\sigma+\dots+\sigma^{d-1}}L^{\gamma^{-1}}$.*

Proof. Let $m' = en' + r'$, $r' < n'$. Then $m = en + r$, $r = r'd < n$. For $0 \leq k < n$ set (as in the proof of Lemma 5.2)

$$L(k) = \begin{cases} \bigoplus_{i=0}^e K\zeta^i, & 0 \leq k < r, \\ \bigoplus_{i=0}^{e-1} K\zeta^i, & r \leq k < n. \end{cases}$$

Also set $L_j = \bigoplus_{i=0}^j K\zeta^i$, i.e. $L(k) = L_e$ if $k < r$ and $L(k) = L_{e-1}$ if $r \leq k < n$. Then

$$\mathbf{S}^k = L(k)T^k = T^k L(k).$$

Moreover $\mathbf{S} = \mathbf{S}_0 \oplus \dots \oplus \mathbf{S}_{d-1}$ with $\mathbf{S}_0 = \bigoplus_{d|j} \mathbf{S}^j = \bigoplus_{i=0}^{m'-1} KT^{di}$ and $\mathbf{S}_k = T^k \mathbf{S}_0$, $0 \leq k < d$. Let $\alpha = (\alpha_1, \alpha_2)$ be a diagonal autotopism of type $\phi \in \text{Aut}(L)$. We represent α_1^{-1} and α_2 as in the proof of 6.1. We verify the assertion of the lemma by splitting the proof into intermediate steps.

STEP 1. The restriction of \mathbf{S}_0 on $W_i = U_i \oplus U_i$, $0 \leq i < d$, defines with respect to the γ -linear operator T^d a cyclic semifield plane.

Since $\dim_F L = n'$ (we identify U_i with L) the γ -linear operator $(T^d)_{U_i}$ is irreducible (see [4], Cor. 2.5). Also $\dim_K L = m'$ and the assertion follows from

[6].

STEP 2. We have:

(a) $\zeta^\phi = \frac{F(\zeta)}{E(\zeta)}$, $F(X), E(X) \in K[X]$, $0 \leq \deg F(X), \deg E(X) \leq 1$. Moreover $E(\zeta) \equiv (w^{1-\phi})^{\gamma^{r'-1}} a_i^{(1-\gamma)\phi\gamma^{r'-1}} \pmod{K^*}$ if $n' = 2$ and $w^{\phi-1} \in KL^{\gamma-1}$, $E(\zeta) \in K$ if $n' > 2$.

(b) For $0 \leq i < d$ and $0 \leq k < n'$ set

$$A_k^i = \frac{(ww^\gamma \cdots w^{\gamma^{k-1}})^\phi}{ww^\gamma \cdots w^{\gamma^{k-1}}} a_i^{\phi\gamma^k} b_i.$$

Then $A_k^i L(k)^\phi = L(k)$ and $A_k^i \equiv E(\zeta)^{e'}$ mod K^* , where $e' = e$ if $k < r$ and $e' = e - 1$ if $k \geq r$. In particular $A_0^i = a_i^\phi b_i \equiv E(\zeta)^e$ mod K^* .

Apply step 1 and Lemma 5.2 onto the restriction of \mathbf{S}_0 and α to W_0 . Assertion (a) follows. From the proof of this lemma and the restriction of \mathbf{S}_0 and α to W_i we obtain the assertions from (b) too (the pair (f, v) of the proof of Lemma 5.2 is replaced by (a_i, b_i)).

Set $F = a + bX$ and $E = g + hX$. We can adjust the nominator and denominator of the rational function F/E by some element from K^* , i.e. we can and do assume that one of the coefficients a, b, g, h is 1.

STEP 3. The element $E(\zeta)$ lies in K^* even if $n' = 2$.

A typical element s in \mathbf{S}^0 has the form $s = \text{diag}(x^{(0)}, x^{(1)}, \dots, x^{(d-1)})$ with $x \in L(0) = L_e$. For $0 \leq i < d$ we have

$$\phi^{-1} a_i x^{(i)} \phi b_i = a_i^\phi b_i x^{(i)\phi} = A_0^i x^{(i)\phi}$$

which shows

$$\alpha_1^{-1} s \alpha_2 = \text{diag}(A_0^0 x^{(0)\phi}, A_0^1 x^{(1)\phi}, \dots, A_0^{d-1} x^{(d-1)\phi}) \in \mathbf{S}^0.$$

This implies for $1 \leq i < d$ and $x \in L_e$

$$(A_0^{i-1} x^{(i-1)\phi})^{(1)} = A_0^i x^{(i)\phi}.$$

By step 2 we have $A_0^i = k_i E(\zeta)^e$ with some $k_i \in K$. We specialize $x = \zeta^j$. Then $x^{(i)\phi} = x^{(i)}$ and $A_0^i x^{(i)\phi} = k_i E(\zeta)^e (F(\zeta)/(\zeta))^j = k_i E(\zeta)^{e-j} F(\zeta)^j$ and we obtain:

$$k_{i-1}^\sigma (E(\zeta)^{e-j} F(\zeta)^j)^{(1)} = k_i E(\zeta)^{e-j} F(\zeta)^j \quad (1)$$

Set $m_i = \frac{k_i}{k_{i-1}^\sigma}$. Then specializing $j = e$ we get for $1 \leq i < d$

$$\sum_{j=0}^e \binom{e}{j} (b^\sigma)^j (a^\sigma)^{e-j} \zeta^j = m_i \sum_{j=0}^e \binom{e}{j} (b^j a^{e-j}) \zeta^j$$

and specializing $j = 0$ we obtain

$$\sum_{j=0}^e \binom{e}{j} (h^\sigma)^j (g^\sigma)^{e-j} \zeta^j = m_i \sum_{j=0}^e \binom{e}{j} (h^j g^{e-j}) \zeta^j.$$

This shows

$$(a^\sigma)^e = m_i a^e, \quad (b^\sigma)^e = m_i b^e, \quad (g^\sigma)^e = m_i g^e, \quad (h^\sigma)^e = m_i h^e.$$

In particular $m_1 = m_2 = \dots = m_{d-1}$. A typical element in \mathbf{S}^d has the form

$$s = \text{diag}(\gamma w x^{(0)}, \dots, \gamma w x^{(d-1)})$$

where $x \in L_d$. Then a similar computation as above shows

$$\alpha_1^{-1} s \alpha_2 = \text{diag}(\gamma w A_1^0 x^{(0)\phi}, \gamma w A_1^1 x^{(1)\phi}, \dots, \gamma w A_1^{d-1} x^{(d-1)\phi}) \in \mathbf{S}^d.$$

We deduce for $1 \leq i < d$ and $x \in L(d) = L_{e-1}$ (note that $r' = 1$ as $n' = 2$)

$$(A_1^{i-1} x^{(i-1)\phi})^{(1)} = A_1^i x^{(i)\phi}.$$

Specializing $x = \zeta^j$ we obtain similar as before

$$\ell_{i-1}^\sigma (E(\zeta)^{e-1-j} F(\zeta)^j)^{(1)} = \ell_i E(\zeta)^{e-1-j} F(\zeta)^j \quad (2)$$

with some $\ell_i \in K$. Now choosing $j = 0$ and $j = e - 1$ we obtain

$$(a^\sigma)^{e-1} = n_i a^{e-1}, \quad (b^\sigma)^{e-1} = n_i b^{e-1}, \quad (g^\sigma)^{e-1} = n_i g^{e-1}, \quad (h^\sigma)^{e-1} = n_i h^{e-1}.$$

where $n_i = \frac{\ell_i}{\ell_{i-1}^\sigma}$. Again $n_1 = n_2 = \dots = n_{d-1}$. Set $z = \frac{m_1}{n_1}$. Then

$$a^\sigma = za, \quad b^\sigma = zb, \quad g^\sigma = zg, \quad h^\sigma = zh.$$

As one of the coefficient a, b, \dots is 1 we conclude $z = 1$ and $a, b, g, h \in K_0$. This shows for $j < m'$ that

$$(E(\zeta)^j)^{(1)} = E(\zeta)^j. \quad (3)$$

Finally, $\alpha_1^{-1} \mathbf{S}^1 \alpha_2 = \mathbf{S}^1$. For $s \in L(1)$ there exist $s' \in L(1)$ such that the equation $\alpha_1^{-1} T s \alpha_2 = T s'$ holds. Computing the left hand side and comparing both sides we see

$$a_i^\phi b_{i-1} L(1)^\phi = L(1), \quad 1 \leq i < d.$$

Since $L(1) = L_e$ we deduce from Lemma 2.4 that $a_i^\phi b_{i-1} \equiv E(\zeta)^e \pmod{K^*}$ for all i . This implies (as $a_i^\phi b_i \equiv E(\zeta)^e \pmod{K^*}$)

$$a_0 \equiv a_1 \equiv \dots \equiv a_{d-1}, \quad b_0 \equiv b_1 \equiv \dots \equiv b_{d-1} \pmod{K^*}.$$

Let $z = a_1^\phi b_0 = k E(\zeta)^e$ with $k \in K$. Then

$$\alpha_1^{-1} T \alpha_2 = T \text{diag}(z^{(0)}, \dots, z^{(d-1)})$$

which shows

$$z^{(d-1)} = w^{\phi-1} a_0^{\gamma\phi} b_{d-1}.$$

Also

$$z^{(d-1)} = w^{\phi-1} (a_0^{\gamma-1})^\phi a_0^\phi b_{d-1} \equiv w^{\phi-1} (a_0^{\gamma-1})^\phi a_0^\phi b_0 \equiv w^{\phi-1} (a_0^{\gamma-1})^\phi E(\zeta)^e \pmod{K^*}.$$

We know by step 2 and as $r' = 1$ that $E(\zeta) \equiv w^{1-\phi} (a_0^{1-\gamma})^\phi \pmod{K^*}$. Using (3) this yields

$$E(\zeta)^{e-1} \equiv z^{(d-1)} \equiv E(\zeta)^e \pmod{K^*}.$$

But then $E(\zeta) \in K$ and the assertion of step 3 follows.

STEP 4. The assertion of the lemma holds.

By step 3 we have $E(\zeta) \in K$ which implies $A_0^i \in K$ for $0 \leq i < d$. Hence we may adjust α by some element of M such that we even can assume $A_0^0 = 1$. As

$$\alpha_1^{-1} \mathbf{1} \alpha_2 = \text{diag}(1, A_0^1, \dots, A_0^{d-1}) \in \mathbf{S}$$

we deduce from Lemma 3.5 that all $A_0^i = 1$ for all i , i.e. $\alpha_1 = \alpha_2$. Then for $s = \text{diag}(x^{(0)}, x^{(1)}, \dots, x^{(d-1)}) \in \mathbf{S}^0$ we obtain

$$\alpha_1^{-1} s \alpha_1 = \text{diag}(x^{(0)\phi}, x^{(1)\phi}, \dots, x^{(d-1)\phi})$$

which in turn implies that the equation

$$x^{(1)\phi} = x^{\phi(1)}$$

must hold for all $x \in L(0) = L_e$. In particular

$$a + b\zeta = \zeta^{(1)\phi} = \zeta^{\phi(1)} = a^\sigma + b^\sigma \zeta$$

which forces

$$a, b \in K_0. \tag{4}$$

Conversely, this condition implies by Lemma 7.1 that our equation $x^{(1)\phi} = x^{\phi(1)}$ holds even for $x \in L$. Moreover $L(k)^\phi = L(k)$ for all k . We have $\alpha_1^{-1} T \alpha_1 = Ts$ with $s \in L(1) = L_e$. Also $\alpha_1^{-1} T t \alpha_1 = \alpha_1^{-1} T \alpha_1 \alpha_1^{-1} t \alpha_1 = T \alpha_1^{-1} t \alpha_1 s$ for $t \in L_e$ which implies $L_e s = L_e$. So by Lemma 2.5

$$s \in K.$$

We already have seen in step 3 that $\alpha_1^{-1} T \alpha_1 = Ts$ leads to the equations

$$s^{(0)} = a_1^\phi b_0, \dots, s^{(d-2)} = a_{d-1}^\phi b_{d-2}, s^{(d-1)} w = a_0^{\gamma\phi} b_{d-1} w^\phi.$$

This shows (using $b_i = a_i^{-\phi}$)

$$w^{\phi-1} = s^{(0)} s^{(1)} \dots s^{(d-1)} a_0^{\phi(1-\gamma)} = s^{1+\sigma+\dots+\sigma^{d-1}} b_0^{\gamma-1}.$$

Therefore the condition

$$w^{\phi-1} \in K^{1+\sigma+\dots+\sigma^{d-1}} L^{\gamma-1} \quad (5)$$

is necessary for the existence of a diagonal autotopism of type ϕ . However we see by Lemma 7.2 that conditions (4) and (5) are even sufficient for the existence of the autotopism. The proof is complete. \square

Summarizing Theorem 1, Proposition 4.1, and Lemmas 5.2, 7.2, and 7.3 we obtain:

Proposition 7.4. *Assume $m > n$ and use the notation of 2.1 and 3.1. Denote by G_1 the subgroup of diagonal autotopisms. Then $M \trianglelefteq G_1 \trianglelefteq G_0 \trianglelefteq G$, $|M| = (q^n - 1)^2(q^m - 1)/(q - 1)$, and $|G : G_0| = d$. Moreover:*

(a) *Assume $n > d > 1$. Then $G_0 = G_1$ and*

$$G_0/M \simeq \{\phi \in \text{Aut}(L) \mid w^{\phi-1} \in K^{1+\sigma+\dots+\sigma^{d-1}} L^{\gamma-1}, \zeta^\phi = a+b\zeta, a, b \in K_0\}.$$

(b) *Assume $n = d$. Then $[G_0 : G_1]$ divides n and G_1/M contains a subgroup isomorphic to*

$$\{\phi \in \text{Aut}(L) \mid w^{\phi-1} \in K^{1+\sigma+\dots+\sigma^{d-1}} L^{\gamma-1}, \zeta^\phi = a + b\zeta, a, b \in K_0\}.$$

Example 7.5. Assume $n = d < m$. For $\phi \in \text{Aut}(L)$ define a K -subspace of L by

$$L_\phi = \{c \in L \mid (cx^\phi)^{(1)} = c^{(1)}x^{(1)\phi}, x \in L\}.$$

Computations like the previous ones show that a necessary condition for the existence of a diagonal or semidiagonal autotopism of type ϕ is that

$$L_\phi \neq 0.$$

Suppose now $n = 2$, $m = 4$, and $L_\phi \neq 0$. Computations show that a diagonal autotopism of type ϕ exists iff $w^{\phi-1} \in K^{1+\sigma}$ and that a semidiagonal autotopism of type ϕ exists iff $w^{\phi+1} \in K^{1+\sigma}$. In the special case $K = \text{GF}(4)$, $L = F = \text{GF}(16)$, a computer calculation shows $L_\phi \neq 0$ iff $|\phi| = 2$. Also $|w|$ is divisible by 5. Therefore no diagonal autotopism of type ϕ do exist. A semidiagonal autotopism of type ϕ exists iff $|w| = 5$.

Final remarks. (a) Assume the notation of Section 7. A complete treatment of the case $n = d$, $n < m$, would require a characterization of the sets L_ϕ for $\phi \in \text{Aut}(L)$, where L_ϕ is defined as in the previous example. We do not have such a characterization.

(b) Let V be a m -dimensional vector space over the not necessarily finite field K . Let $\sigma \in \text{Aut}(K)$ be of order n and let T be an irreducible, σ -linear

operator on V . It is easy to see that $\mathbf{S} = \sum_{i=0}^{m-1} KT^i$ still defines a semifield. Let $F = C_{\text{End}_{\kappa_0}(V)}(T)$ be a field (not merely a skew field), i.e. T is separable in the sense of [4]. Then Theorem 1 is still true: by [4] the description of T is completely analogous as in the case $|K| < \infty$ and it is not hard to see all arguments of the proof of Theorem 1 carry over to our more general situation.

References

- [1] M. Aschbacher: *Finite Group Theory*, 2-nd ed., Cambridge Univ. Press, 2000.
- [2] G. Bell: Cohomology of degree 0,1 and 2 of $\text{SL}_m(q)$ I-II, J. Algebra 54(1978), 216-238, 239-259.
- [3] P. Dembowski: *Finite Geometries*, Springer, 1968.
- [4] U. Dempwolff: On irreducible semilinear transformations, to appear in Forum Mathematicum.
- [5] D.Hughes, F. Piper: *Projective Planes*, Springer 1973.
- [6] V. Jha, N. Johnson: An analog of the Albert-Knuth theorem on the orders of finite semifields, ans a complete solution to Cofman's subplane problem, Algebras, Groups, Geom. 6(1989), 1-35.
- [7] N. Johnson, G. Marino, O. Polverino, R. Trombetti: On a generalization of cyclic semifields, J. Algebr. Comb., 29(2009), 1-34.
- [8] W. Kantor: Finite semifields, in: *Finite Geometries, Groups, and Computation*, A. Hulpke, R. Liebler, T. Penttila, A. Seress Eds., Pingree Park, Col. USA, Sept. 4-9, 2004, W. de Gruyter, 2006, pp. 103-114.
- [9] W. Kantor, R. Liebler: Semifields arising from irreducible semilinear transformations, J. Austr. Math. Soc., 85(2008), 351-363.