

On Irreducible Semilinear Transformations

Ulrich Dempwolff

Abstract

In this note irreducible, semilinear transformations on finite dimensional vector spaces are studied. We assume that the field automorphism associated with the operator has finite order and that the centralizer ring of the operator is a field. We characterize and classify these operators and describe them concretely. These results are applied to semilinear transformations on finite dimensional vector spaces over finite fields.

1 Introduction

Jacobson [9] seems to be the first one who studied semilinear operators thoroughly. Using a theory of noncommutative polynomial rings, he determined the module structure induced by a semilinear operator on a finite dimensional vector space. More standard methods lead in [5] and [6] to the same results. However none of these papers contains a description and classification of irreducible operators.

In their course of studying finite semifields, Kantor and Liebler [10] were lead to the investigation of irreducible, semilinear transformations on *finite vector spaces*, i.e. finite dimensional vector spaces over finite fields. They give a first description and a rough classification of such operators. Our intention is to extend their result. The final remark (b) gives a precise statement of their theorem and discusses the relation with our results.

In the next section we consider irreducible, semilinear operators T over a finite dimensional K -spaces V such that the skew field S of endomorphisms commuting with T and K is a field. We call such operators separable and note that this class includes irreducible, semilinear transformations on finite spaces. The key observation is that the dimension of V over S is the order

of the field automorphism associated with this operator (see Theorem 2.4). For applications an explicit description of such operators is desirable. A first concrete construction of separable transformations is given in 2.8. We reduce the classification problem to the classification of irreducible, *linear* operators (Theorem 2.10). A main consequence of Theorems 2.4 and 2.10 is:

Theorem *Let V be a finite dimensional K -space, σ a field automorphism of K of order n , and T an irreducible, σ -linear operator on V . Assume that the skew field S of endomorphisms commuting with T and K is a field. Then:*

(a) $\dim_S V = n$.

(b) *Let T' be an irreducible, σ -linear operator such that T^n and $(T')^n$ are conjugate in $\text{GL}(V)$. Then T and T' are conjugate under $\text{GL}(V)$.*

In the last section we consider the special case of finite vector spaces. This includes a second construction of irreducible, semilinear operators (see 3.3) and the classification of irreducible, semilinear operators (Theorem 3.4).

2 Separable irreducible, semilinear transformations

The following notation will be fixed throughout this paper. Let K be a field with an automorphism σ . Set $K_0 = C_K(\sigma)$. Let V be a K -space. We also will consider V as a M -space for various other fields M and we write

V_M if we consider V as a M -space.

Let T a σ -semilinear operator on V . Then $\alpha \in K$ defines a K_0 -linear operator $R(\alpha)$ by

$$vR(\alpha) = \alpha v.$$

We have

$$R(\alpha)T = TR(\alpha^\sigma) \tag{*}$$

as $vTR(\alpha^\sigma) = \alpha^\sigma(vT) = (\alpha v)T = vR(\alpha)T$. Define a set

$$\mathcal{I} = \{R(\alpha) \mid \alpha \in K\} \cup \{T\}$$

of K_0 -linear operators. The following Lemma is obvious:

Lemma 2.1

- (a) $\dim V = 1$ and $T = 0$ iff T is irreducible and singular.
- (b) Let T be non-singular. T is irreducible iff the set \mathcal{I} is irreducible on V_{K_0} .

From now on we assume that T is non-singular and irreducible, σ has the finite order n , and that V is a finite dimensional K -space. If we define the semi-direct product

$$\mathcal{G} = R(K^*)\langle T \rangle$$

we may also consider V_{K_0} as an irreducible \mathcal{G} -module. This view point is taken in Corollary 2.6 and 3.2 below. By [1], Satz 14, [4], Theorem 3.4.1 $K : K_0$ is a Galois extension with Galois group

$$\text{Gal}(K : K_0) = \langle \sigma \rangle.$$

Schur's Lemma shows that

$$S = C_{\text{End}_{K_0}(V)}(\mathcal{I})$$

is a skew field. It's center contains K_0 and T^n . The following notion is essential for the remainder of this note.

DEFINITION We call the irreducible, σ -linear operator T *separable* if S is commutative, i.e. a field.

Lemma 2.2 *The minimal polynomial f_0 of T^n over K_0 is irreducible and $K_0[T^n]$ is a subfield of $\text{End}_{K_0}(V)$ (even of the center of S).*

Proof. Let f_0 be an irreducible divisor of the minimal polynomial. Then $\ker f_0(T^n)$ is invariant under \mathcal{I} . Hence $V = \ker f_0(T^n)$ and f_0 is the minimal polynomial of T^n . The assertion follows. \square

Use the notation of Lemma 2.2. Then

$$F = K_0[T^n] \simeq K_0[X]/(f_0)$$

is an extension field of K_0 of degree $[F : K_0] = \deg f_0$. We consider $V = V_F$ as an F -space by defining ($a_i \in K_0$)

$$\left(\sum_i a_i (T^n)^i \right) v = \sum_i a_i v (T^n)^i.$$

Note that the operators in \mathcal{I} are F -linear. Let $K = K_0[\omega]$ and f be the minimal polynomial of ω over K_0 . Denote by

L the splitting field of f over F .

We call L the *composite field* of K and F . Then by the Translation Theorem ([1], Satz 34, [4], Proposition 3.4.7) a root $\tilde{\omega}$ of f in L can be chosen such that $L = F[\tilde{\omega}]$ and we have a K_0 -linear embedding $\tilde{\cdot} : K \rightarrow \tilde{K} = K_0[\tilde{\omega}] \subseteq L$ with $\omega \mapsto \tilde{\omega}$ (which depends on the choice of $\tilde{\omega}$). For convenience we summarize this situation in:

HYPOTHESIS I $K = K_0[\omega]$ is a Galois extension of K_0 of degree n with a cyclic Galois group $\langle \sigma \rangle$. V is an m -dimensional K -space and T an irreducible, σ -linear operator on V . The composite field of K and $F = K_0[T^n]$ is L and $\tilde{\cdot} : K \rightarrow \tilde{K} = K_0[\tilde{\omega}] \subseteq L$, $\omega \mapsto \tilde{\omega}$ is a K_0 -linear embedding.

We start with a general lemma on irreducible, semilinear operators (without assuming separability).

Lemma 2.3 *Assume hypothesis I. Set $[\tilde{K} \cap F : K_0] = d$, $\tilde{K} \cap F = K_0[\tilde{\omega}_0]$, and let ω_0 be the counter image of $\tilde{\omega}_0$ in K .*

(a) *We have a decomposition*

$$V_F = U_0 \oplus U_1 \oplus \cdots \oplus U_{d-1},$$

where U_i is the eigenspace to the eigenvalue $\tilde{\omega}_0^{\sigma^i}$ for $R(\omega_0)$. The group $\langle T \rangle / \langle T^d \rangle$ induces a regular action on the U_i 's.

(b) *Consider U_0 as a K -space. The operator T^d is an irreducible, σ^d -linear operator on U_0 and $S = C_{\text{End}_{K_0}(V)}(\mathcal{I}) \simeq C_{\text{End}_{K_0}(U_0)}(\mathcal{I}_0) = S_0$ where $\mathcal{I}_0 = \{R(\alpha)_{U_0} \mid \alpha \in K\} \cup \{T_{U_0}^d\}$.*

(c) *Denote by $R_i(\alpha)$ the restriction of $R(\alpha)$ to U_i , $0 \leq i < d$. Then $L_i = F[R_i(\omega)] \simeq L$ is an extension field of F of degree $n' = n/d$. Consider U_i as an L_i -space. T^d induces on U_i a γ_i -linear operator, where γ_i is a field automorphism of L_i of order n' .*

Proof. (a) $\widetilde{\omega}_0$, the counter image ω_0 , and $R(\omega_0)$ have the same minimal polynomial over K_0 . By our assumptions $K_0[\omega_0] : K_0$ is a Galois extension, i.e. $K_0[\widetilde{\omega}_0] \subseteq F$ contains all roots $\widetilde{\omega}_0, \widetilde{\omega}_0^\sigma, \dots, \widetilde{\omega}_0^{\sigma^{d-1}}$ of this polynomial.

Denote by U_i , the eigenspace for the eigenvalue $\widetilde{\omega}_0^{\sigma^i}$ of $R(\omega_0)$. Clearly, the U_i 's are K -spaces. Let $g \in K_0[X]$ be a polynomial such that $\omega_0^\sigma = g(\omega_0)$. Let u be in U_i . Then

$$uR(\omega_0^\sigma) = ug(R(\omega_0)) = g(\widetilde{\omega}_0^{\sigma^i})u = \widetilde{g(\omega_0)^{\sigma^i}}u = \widetilde{\omega_0^{\sigma^{i+1}}}u.$$

Hence U_i is the eigenspace for the eigenvalue $\widetilde{\omega_0^{\sigma^{i+1}}}$ of $R(\omega_0^\sigma)$ and therefore $U_i T = U_{i-1}$ for $0 \leq i < d$ (and $U_{-1} = U_{d-1}$) by (*). Then $U_0 \oplus \dots \oplus U_{d-1}$ is a T -invariant K -space. Therefore V is equal to this sum. All assertions of (a) follow.

(b) The K -space U_0 is irreducible under the σ^d -linear operator T^d : Suppose $0 \neq U \subseteq U_0$ is a K -space invariant under T^d . Then the K -space

$$W = U \oplus UT^{-1} \oplus \dots \oplus UT^{1-d}$$

is invariant under T . We conclude $V = W$ and $U = U_0$.

Then $\mathcal{I}_0 = \{R(\alpha), \mid \alpha \in K\} \cup \{T^d\}$ induces on U_0 an irreducible set of K_0 -linear operators. We claim $S_0 \simeq S$:

By definition $s \in S$ fixes U_0 , so that s_{U_0} lies in S_0 . As S is a skew field the restriction map $S \ni s \mapsto s_{U_0} \in S_0$ is a ring monomorphism.

Take now $t \in S_0$ and define $\widehat{t} \in \text{End}_{K_0}(V)$ by $uT^{-k}\widehat{t} = utT^{-k}$ for $u \in U_0$ and $0 \leq k < d$. It is easy to see that \widehat{t} commutes with the $R(\alpha)$'s and that for $k > 0$ one has $uT^{-k}\widehat{t}T = uT^{-k}T\widehat{t}$. Moreover

$$u\widehat{t}T = utT = utT^d T^{-d+1} = uT^d t T^{-d+1} = uT^d T^{-d+1} \widehat{t} = uT\widehat{t}.$$

Hence $t \mapsto \widehat{t}$ is an embedding of S_0 into S and this map is the inverse of the map $s \mapsto s_{U_0}$.

(c) Let $g = X^{n'} - \sum_{j=0}^{n'-1} m_j X^j$ be the minimal polynomial of ω over $K_0[\omega_0]$. For $m_j \in K_0[\omega_0]$ there exist a $\widetilde{m}_j \in K_0[\widetilde{\omega}_0] \subseteq F$ with $R_i(m_j) = \widetilde{m}_j|_{U_i}$. This shows that $\widetilde{g} = X^{n'} - \sum_{j=0}^{n'-1} \widetilde{m}_j X^j \in F[X]$ annihilates $R_i(\omega)$ and therefore divides the minimal polynomial f of ω over K_0 . We know that the polynomial f splits over F into d irreducible factors of degree n' since it's splitting field L has degree n' over F . As \widetilde{g} has degree n' it is an irreducible polynomial over F . Hence $L \simeq L_i = F[R_i(\omega)] \subseteq \text{End}_F(U_i)$. An element

$y \in L_i$ is uniquely represented as $y = \sum_{k=0}^{n'-1} y_k R_i(\omega)^k$ with $y_k \in F$. By the Translation Theorem the map $\gamma_i : y \mapsto y^{\gamma_i} = \sum_{k=0}^{n'-1} y_k R_i(\omega^{\sigma^d})^k$ is a field automorphism of L_i of order n' . We have

$$yT^d = T^d \sum_{k=0}^{n'-1} y_k (R_i(\omega)^k)^{T^d} = T^d \sum_{k=0}^{n'-1} y_k R_i(\omega^{\sigma^d})^k = T^d y^{\gamma_i}.$$

So $T_{U_i}^d$ is a γ_i -semilinear map when we consider U_i as a L_i -space. \square

The following characterization of separable operators has various consequences.

Theorem 2.4 *Assume hypothesis I. The following are equivalent:*

- (a) T is separable.
- (b) $\dim_F V_F = n$.
- (c) $F = S = C_{\text{End}(V_{K_0})}(\mathcal{I})$.

Proof. We use the notation of Lemma 2.3. (c) \Rightarrow (a) follows from the definition of separability.

(a) \Rightarrow (b). We use induction on n . If $d > 1$ we know by induction (applied to the pair $U_0, T_{U_0}^d$) that $\dim_F U_0 = n'$. Then $\dim_F V = d \cdot \dim_F U_0 = n$.

So assume now $d = 1$, i.e. $\tilde{K} \cap F = K_0$. Then by the Translation Theorem $L = F[\tilde{\omega}]$ is an extension field of F of degree n with a cyclic Galois group $\langle \gamma \rangle$. Choosing the notation of the embedding $K = K_0[\omega] \rightarrow K_0[\tilde{\omega}] \subseteq L$ suitably we may assume $\tilde{\omega}^\sigma = \tilde{\omega}^\gamma$. Set $V^L := L \otimes_F V_F$. The action of \mathcal{I} extends naturally to V^L (if $y \in L$, $v \in V_F$ one has $(y \otimes v)X = y \otimes vX$ for $X = R(\alpha)$ or T). Then $R(\omega)$ has as a L -linear map the eigenvalues $\tilde{\omega}, \tilde{\omega}^\sigma, \dots, \tilde{\omega}^{\sigma^{n-1}}$. Let $V(\tilde{\omega}), V(\tilde{\omega}^\sigma), \dots$ be the respective eigenspaces. Then $V(\tilde{\omega}^{\sigma^j})T^{-1} = V(\tilde{\omega}^{\sigma^{j+1}})$ by a similar argument as in the proof of Lemma 2.3.a. Let t be any element in $\text{End}_L(V(\tilde{\omega}))$ and $v \in V(\tilde{\omega})$. We define $\hat{t} \in \text{End}_L(V^L)$ by $vT^{-k}\hat{t} = vtT^{-k}$. Arguing as in the proof of Lemma 2.3.b we see that \hat{t} commutes with \mathcal{I} . Set $r = \dim_L V(\tilde{\omega})$. Then $C_{\text{End}_L(V^L)}(\mathcal{I})$ contains a subring isomorphic to $L^{r \times r}$. On the other hand by [8], V, 11.9 we have (as $S = C_{\text{End}_F(V_F)}(\mathcal{I})$ by Lemma 2.2)

$$C_{\text{End}_L(V^L)}(\mathcal{I}) \simeq L \otimes_F C_{\text{End}_F(V_F)}(\mathcal{I}) \simeq L \otimes_F S.$$

Actually, the quoted result is stated for the centralizer ring of a representation of a finite group. However the formal proof can be extended without any changes to the centralizer ring of a set of linear operators. The right hand side is abelian which implies $r = 1$. Therefore $n = \dim_L V^L = \dim_F V_F$.

(b) \Rightarrow (c). We have $S_0 = C_{\text{End}_{K_0}(U_0)}(\mathcal{I}_0) = C_{\text{End}_F(U_0)}(\mathcal{I}_0)$ again by Lemma 2.2. By assumption $\dim_F U_0 = \frac{n}{d} = n' = [L : F]$ holds. $\omega, \tilde{\omega}$, and $R(\omega)$ have the same minimal polynomial over K_0 and over F this polynomial splits into d irreducible factors of degree n' . Therefore U_0 as an F -space is irreducible under $R(\omega)$. We conclude $L_0 = \langle R_0(K) \rangle_F = C_{\text{End}_F(U_0)}(R_0(K))$ as $\dim_F C_{\text{End}_F(U_0)}(R_0(K)) \leq n' = \dim_F U_0$. Hence $S_0 \subseteq L_0$. Since $t \in S_0$ commutes with T^d we see that $t \in C_{L_0}(T^d) = \langle R_0(K_0[\omega_0]) \rangle_F$. This shows that $t = \lambda \mathbf{1}_{U_0}$ with a scalar λ in F and $S_0 = F_{U_0}$ follows. The proof is complete. \square

Remark In the next section we outline in the case of finite vector spaces an alternative proof of Theorem 2.4.

Example Set $K = \mathbf{C}$ and $K_0 = \mathbf{R}$. Consider the quaternions $\mathbf{H} = K \oplus K\mathbf{j}$ where $K = K_0 \oplus K_0\mathbf{i}$ and $\mathbf{H} = K_0 \oplus K_0\mathbf{i} \oplus K_0\mathbf{j} \oplus K_0\mathbf{k}$, $\mathbf{k} = \mathbf{ij}$. The left multiplication by \mathbf{j} defines a σ -semilinear operator T , σ being the conjugation of the complex numbers. It is easy to see that this operator is irreducible. As $T^2 = -\mathbf{1}$ we have $F = K_0$ but $\dim_{K_0} \mathbf{H} = 4 \neq 2 = |\sigma|$. This shows that the Theorem does not hold if T is not separable, i.e. S is not a field. Indeed it is easy to see that $S \simeq \mathbf{H}$.

We note that separability can be detected by the minimal polynomial of the *linear part* of a semilinear transformation:

Corollary 2.5 *Let K be a field with an automorphism σ of order n . Set $K_0 = C_K(\sigma)$. Let T' be a σ -linear operator on the finite dimensional K -space W . Assume that $F = K_0[(T')^n]$ is a field (i.e. the minimal polynomial of $(T')^n$ over K_0 is irreducible) and that W has dimension n as a F -space. Then T' is irreducible and separable.*

Proof. Let V be an irreducible T' -subspace of W . Consider $T = T'_V$. By Lemma 2.3.a (and with its notation) we have $\dim V_F = d \cdot \dim_F U_0$ and Lemma 2.3.c shows $\dim_F U_0 = [L : F] \dim_L U_0 \geq n'$. Hence $V = W$ and we can apply the Theorem. \square

We consider V_F as a \mathcal{G} -module. The resulting matrix representation is given by:

Corollary 2.6 *Assume hypothesis I and that T is separable. Suppose further $[\tilde{K} \cap F : K_0] = d$ and $n = dn'$. The module V_F induces a matrix representation $D : \mathcal{G} \rightarrow \mathrm{GL}(n, F)$ in block form (with blocks $X, Y(\alpha^{\sigma^i})$ of size $n' \times n'$) such that*

$$D(T) = \begin{pmatrix} 0 & 0 & \cdots & 0 & X \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}, \quad D(R(\alpha)) = \mathrm{diag}(Y(\alpha), Y(\alpha^\sigma), \dots, Y(\alpha^{\sigma^{d-1}})),$$

for $\alpha \in K$. Moreover $X^{-1}Y(\alpha)X = Y(\alpha^{\sigma^d})$.

Proof. Use the notation of Lemma 2.3. Let $\mathcal{B} = \{v_1, \dots, v_{n'}\}$ be a F -basis of U_0 . Take $\mathcal{C} = \mathcal{B} \cup \mathcal{B}T^{-1} \cup \dots \cup \mathcal{B}T^{1-d}$ as a basis of V_F . By the choice of the basis T is represented by a matrix of the form $D(T)$. As $T^{-1}R(\alpha) = R(\alpha^\sigma)T^{-1}$ the matrix of $R(\alpha)$ with respect to \mathcal{C} has the form $D(R(\alpha))$ with $Y(\alpha) \in \mathrm{GL}(n', F)$. Moreover

$$R(\alpha^\sigma) = T^{-1}R(\alpha)T = \mathrm{diag}(Y(\alpha^\sigma), Y(\alpha^{\sigma^2}), \dots, Y(\alpha^{\sigma^{d-1}}), X^{-1}Y(\alpha)X)$$

which implies $X^{-1}Y(\alpha)X = Y(\alpha^{\sigma^d})$. \square

As we have seen a separable, σ -linear operator T on an m -dimensional K -space is associated with a field extension $F : K_0$, $F = K_0[T^n]$, of degree m . Starting with a field extension $F : K_0$ of degree m we ask which generators of F can take the role of T^n . The next result shows that the generator can not be arbitrary.

Corollary 2.7 *Assume hypothesis I and that T is separable. Then T^n is a value of the norm map $N_{L:F} : L \rightarrow F$.*

Proof. To see this we use the notation of the proofs of 2.3 and 2.4. The field $L_i \simeq L$ acts regularly on U_i as $\dim_F L_i = \dim_F U_i = n'$. In particular L_i is self-centralizing in $\mathrm{End}_F(U_i)$. Pick $0 \neq u \in U_i$. The automorphism γ_i defines a F -linear operator $\bar{\gamma}_i$ by $(uy)\bar{\gamma}_i = uy^{\gamma_i}$, $y \in L_i$. Then

$\overline{\gamma}_i^{-1}y\overline{\gamma}_i = T^{-d}yT^d = y^{\gamma_i}$. We deduce $T_{U_i}^d = w\overline{\gamma}_i$ for some $w \in L_i$. This implies $(T^n)_{U_i} = (T_{U_i}^d)^{n'} = ww^{\gamma_i} \cdots w^{\gamma_i^{n'-1}} = N_{L_i:F}(w)$ and the claim follows. \square

2.8 FIRST CONSTRUCTION OF IRREDUCIBLE, SEMILINEAR TRANSFORMATIONS Let $K = K_0[\omega]$, K_0 , n , and σ have the usual meaning. For a given $0 < m \in \mathbf{Z}$ we construct all separable, σ -linear operators on a m -dimensional K -space. The construction is based on Corollary 2.6.

For this purpose we take any field extension $F : K_0$ of degree m and denote by L the composite field of F and K . By Corollary 2.7 a candidate for T^n is any element $u \in F$ such that u lies in the image of the norm map from L into F and which generates F , i.e. $F = K_0[u]$. We know that $[L : F] = n'$ divides n , say $n = dn'$. Moreover $\text{Gal}(L : F) = \langle \gamma \rangle \simeq C_{n'}$ and we have an embedding $\widetilde{\cdot} : K \rightarrow L$, $\alpha \mapsto \widetilde{\alpha}$ such that $\widetilde{\alpha^{\sigma^d}} = \widetilde{\alpha}^\gamma$. Choose $w \in L$ such that $N_{L:F}(w) = u$. Set $V = L^d$. First we turn V into a K -space and define for $\alpha \in K$

$$\alpha \cdot x = (\widetilde{\alpha}x_0, \widetilde{\alpha}^\sigma x_1, \dots, \widetilde{\alpha^{\sigma^{d-1}}} x_{d-1}).$$

Then V_K has dimension

$$\dim_K V = [L : \widetilde{K}] \dim_L V = \frac{[L : K_0]}{[K : K_0]} d = m.$$

We define the operator T by

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

for $x = (x_0, \dots, x_{d-1}) \in V$. One checks immediately that T is σ -linear. Finally

$$xT^d = (wx_0^\gamma, \dots, wx_{d-1}^\gamma), \quad xT^n = N_{L:F}(w)x = ux.$$

By Corollary 2.5 T is a separable operator. Theorem 2.4 and Theorem 2.10 below show that all separable, σ -linear operators are covered by this construction. The drawback of this construction is the rather artificial definition of the K -structure. Under 3.3 in the next chapter we give for finite fields K an alternative construction with a more natural action of this field on the underlying vector space.

The most natural groups under which one can consider the conjugacy problem of irreducible, σ -linear operators are the groups $\text{GL}(V_K)$ and $\Gamma\text{L}(V_K)$.

The next two results address this question.

Lemma 2.9 *Let E be a field, W be an E -space of dimension m , and $M \subseteq \text{End}_E(W)$ a field such that $M : E$ is a Galois extension with $\text{Gal}(M : E) = \langle \gamma \rangle \simeq \mathbb{C}_m$. Let $m = ab$ and $X, X' \in \text{GL}(W_E)$ such that $X^a = (X')^a$ and $\beta^X = \beta^{X'} = \beta^{\gamma^b}$ for $\beta \in M$. Then there exists a $\rho \in M$ such that $X' = X^\rho$.*

Proof. One has $C_{\text{End}_E(W)}(M) = M$ as $\dim_E M = \dim_E W = m$. This shows $X^{-1}X' \in M$, i.e. $X' = X\rho_0$ for some $\rho_0 \in M$. Set $\tau = \gamma^b$ and let N be the fixed field of τ . Then $M : N$ is a Galois extension and a computation shows

$$X^a = (X')^a = X^a \rho_0 \rho_0^\tau \cdots \rho_0^{\tau^{a-1}} = X^a N_{M:N}(\rho_0).$$

Therefore $N_{M:N}(\rho_0) = 1$. By Hilbert's Theorem 90 ([1], Satz 30, [4], 3.9.3) there exists a $\rho \in M$ such that $\rho_0 = \rho^{1-\tau}$. Hence $X^\rho = X'$. \square

Theorem 2.10 *Assume hypothesis I and separability of the operator T . Let T' be a second irreducible, σ -linear operator.*

(a) *The following are equivalent:*

- (1) *T and T' are conjugate by an element from $\text{GL}(V_K)$.*
- (2) *T^n and $(T')^n$ are conjugate in $\text{GL}(V_K)$.*
- (3) *T^n and $(T')^n$ have the same minimal polynomials over K_0 .*

(b) *Assume that σ lies in the center of $\text{Aut}(K)$. The following are equivalent:*

- (1) *T and T' are conjugate in $\Gamma\text{L}(V_K)$.*
- (2) *T^n and $(T')^n$ are conjugate in $\Gamma\text{L}(V_K)$.*
- (3) *The minimal polynomials of T^n and $(T')^n$ over K_0 are conjugate under $\text{Aut}(K)$.*

Proof. (a) The implications (1) \Rightarrow (2) \Rightarrow (3) are obvious.

(3) \Rightarrow (1): First, by Corollary 2.5 T' is separable too. Let f_0 be the (irreducible) minimal polynomial of T^n over K_0 and $g \in K[X]$ be an irreducible divisor of f_0 . Then $f_0 = \prod_{k=0}^{r-1} g^{\sigma^k}$ (where $g^{\sigma^r} = g$) and as $\sum_k \ker g^{\sigma^k}(T^n)$

is T -invariant we have even $V = \bigoplus_{k=0}^{r-1} \ker g^{\sigma^k}(T^n)$. Also $\ker g(T^n)T = \ker g^\sigma(T^n)$ by (*), i.e. all subspaces of the decomposition have the same dimension. A similar decomposition is induced by $(T')^n$. Therefore T^n and $(T')^n$ are conjugate in $\text{GL}(V_K)$ and we can assume $T^n = (T')^n$.

Let $d, n',$ etc. have the same meaning (with respect to T) as in Lemma 2.3. So for a fixed k the operator $T_{U_k}^d$ is a γ_k -semilinear map when we consider U_k as a L_k -space. Also $(T'_{U_k})^d$ is semilinear associated with the same automorphism. Set $X_k = T_{U_k}^d$ and $X'_k = (T'_{U_k})^d$ which are F -linear maps. By Lemma 2.9 applied to $M = L_k$ and $E = F$ there are $\rho_k \in L_k$, $0 \leq k < d$, such that $X'_k = X_k^{\rho_k}$. Set $P = \text{diag}(\rho_0, \dots, \rho_{d-1})$. Then P is a K -linear map (as it is a K_0 -linear map which commutes with $R(\omega)$) with $(T^d)^P = (T')^d$.

So we assume from now on

$$T^d = (T')^d.$$

We choose as in Corollary 2.6 a basis of V_F which induces the matrix representation D . Since T' permutes the spaces U_0, U_1, \dots in the same way as the operator T we get

$$D(T') = \begin{pmatrix} 0 & 0 & \cdots & 0 & A_d \\ A_1 & 0 & \cdots & 0 & 0 \\ 0 & A_2 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & A_{d-1} & 0 \end{pmatrix}.$$

The relation $R(\alpha)T' = T'R(\alpha^\sigma)$ implies $A_i Y(\alpha) = Y(\alpha)A_i$ for $1 \leq i < d$ and $A_d Y(\alpha^{\sigma^d}) = Y(\alpha)A_d$. This shows that the operator Δ defined by

$$D(\Delta) = \text{diag}(1, A_1, A_2 A_1, \dots, A_{d-1} \cdots A_2 A_1)$$

induces an K -linear map. Since $T^d = (T')^d$ we have $X = A_d A_{d-1} \cdots A_2 A_1$ ($= A_{d-1} A_{d-2} \cdots A_1 A_d = \dots$) with X defined as in Corollary 2.6. Then

$$D(T')^{D(\Delta)} = D(T)$$

and the proof of (a) is complete.

(b) Again the implications (1) \Rightarrow (2) \Rightarrow (3) are trivial.

(3) \Rightarrow (1): By assumption the field K_0 is invariant under $\text{Aut}(K)$. Assume $\tau \in \text{Aut}(K)$ and that f_0 (f_0^τ) is the minimal polynomial of T^n ($(T')^n$)

over K_0 . Pick $X \in \Gamma(V_K)$ such that τ is the associated automorphism. Then $0 = X^{-1}f_0(T^n)X = f_0^\tau((T^X)^n)$, i.e. the minimal polynomial of $(T^X)^n$ is f_0^τ . By assumption T^X is σ -linear. By (a) we have a $Y \in \text{GL}(V_K)$ such that $T' = (T^X)^Y = T^{XY}$ and the assertion follows. \square

3 Finite vector spaces

Wedderburn's Theorem on finite division rings implies that the results of the previous section apply to finite vector spaces:

Proposition 3.1 *Every irreducible, semilinear operator on a finite vector space is separable.*

3.2 PROOF OF THEOREM 2.4 FOR FINITE VECTOR SPACES We show that Theorem 2.4 for finite vector spaces is a direct consequence of results from representation theory.

Assume hypothesis I. Then T is separable by the proposition. We consider V_{K_0} as a \mathcal{G} -module (\mathcal{G} defined as in the beginning of section 2) and show (a) $\dim_S V = n$, $S = \text{End}_{\mathcal{G}}(V_{K_0}) = C_{\text{End}_{K_0}(V)}(\mathcal{I})$, and (b) $F = S$. Thus hypothesis I implies all three assertions of Theorem 2.4. We fix some notation and set $K_0 = \text{GF}(q)$, $K = \text{GF}(q^n)$, and $K^* = \langle \omega \rangle$.

To (a): We verify the assertion in five steps.

(1) V_S is an absolutely irreducible $S\mathcal{G}$ -module: By definition $S = \text{End}_{\mathcal{G}}(V_S)$. Then [2], (25.8) implies the assertion.

(2) The only maximal abelian normal subgroup of \mathcal{G} which contains the commutator group is $A = R(K^*)\langle T^n \rangle$: The routine verification is left to the reader.

(3) Let W be an irreducible $\mathbf{C}\mathcal{G}$ -module, $\dim W > 1$. Then $W = U^{\mathcal{G}}$ with a 1-dimensional $\mathbf{C}A$ -module U : By a Theorem of Shoda (see for instance [3] or [8], p. 585) the module W has the form $U^{\mathcal{G}}$ where $W = U^{\mathcal{G}}$ with a 1-dimensional $\mathbf{C}B$ -module U and B a maximal abelian normal subgroup of \mathcal{G} which contains the commutator group. Apply (2).

Let p be the characteristic of K_0 and $\overline{K_0}$ be the algebraic closure of K_0 .

(4) Let W be an irreducible $\overline{K_0}\mathcal{G}$ -module, $\dim W > 1$. Then $W = U^{\mathcal{G}}$ with a 1-dimensional $\overline{K_0}A$ -module U : This follows from (3) and a Theorem of Richen [7], Theorem 1.7, p. 417, which states that in our situation every

irreducible character of \mathcal{G} is irreducible as a Brauer character in characteristic p .

(5) Assertion (a) holds: By (1) V_S is absolutely irreducible. Then $\overline{V} := \overline{K}_0 \otimes_S V_S$ is irreducible and has dimension $|\mathcal{G} : A| = n$ by (2), (3), and (4).

To (b): We already know $S = \text{End}_{\mathcal{G}}(V_F)$. As V_F is an irreducible $F\mathcal{G}$ -module, [2], (26.2.1) implies

$$(V_F)^S := S \otimes_F V_F = \bigoplus W^a,$$

where W is an irreducible $S\mathcal{G}$ -module and a ranges over a set of coset representatives of $N_{\Gamma}(W)$ in $\Gamma = \text{Gal}(S : F)$. Clearly, V_F is a $F\mathcal{G}$ -submodule of $(V_F)^S$ and hence a submodule of some W^a . But then V_F is even a $F\mathcal{G}$ -submodule of every W^a . By [2], (26.2.2) $W^a \simeq W^{a'}$ as $S\mathcal{G}$ -modules for all coset representatives a, a' . This implies $N_{\Gamma}(W) = \Gamma$ so that V_F is absolutely irreducible. $S = F$ follows. \square

Remark Assume hypothesis I with $K_0 = \text{GF}(q)$, $K = \text{GF}(q^n)$, and $F \simeq \text{GF}(q^m)$. Set $d = (m, n)$ and $m' = m/d$. By the structure of Galois fields we see that $\tilde{K} \cap F \simeq \text{GF}(q^d)$ and $L \simeq \text{GF}(q^{m'n})$. In particular our numbers m' and n' are coprime.

3.3 SECOND CONSTRUCTION OF IRREDUCIBLE, SEMILINEAR TRANSFORMATIONS Let $K = \text{GF}(q^n)$ and σ be an automorphism of order n , for convenience we assume $x^\sigma = x^q$ (the adjustments for an arbitrary automorphism of order n are straightforward). For $0 < m \in \mathbf{Z}$ we will define σ -linear, irreducible operators on a K -space V of dimension m .

We define $d = (m, n)$, $m' = m/d$, $n' = n/d$, $L = \text{GF}(q^{m'n})$, and $F = \text{GF}(q^m)$. Finally let $V = U_0 \oplus \cdots \oplus U_{d-1}$, $U_i = Le_i$, be a d -dimensional L -space, which we consider in the obvious fashion as a K -space. There exists a $0 < c \in \mathbf{Z}$, $(c, n') = 1$, such that $x^{q^{cm}} = x^{q^d}$ for $x \in K$. We define $\gamma \in \text{Aut}(L)$ by $x^\gamma = x^{q^{cm}}$. As $x \mapsto x^{q^d}$ is an automorphism of K of order n' and as γ acts trivially on F we conclude $|\gamma| = |\gamma_K| = n'$, i.e. $\text{Gal}(L : F) = \langle \gamma \rangle$. Define an extension $\bar{\sigma} \in \text{Aut}(L)$ of σ by $x^{\bar{\sigma}} = x^q$ and a second automorphism $\rho = \gamma\bar{\sigma}^{-d+1}$. Note that $\rho_K = \sigma = \bar{\sigma}_K$.

For $w \in L^*$ we define $T = T_{w, \sigma} : V \rightarrow V$ by

$$xT = (wx_{d-1}^\rho, x_0^{\bar{\sigma}}, \dots, x_{d-2}^{\bar{\sigma}})$$

where $x = (x_0, x_1, \dots, x_{d-1})$ is identified with $x_0e_0 + \dots + x_{d-1}e_{d-1}$. Then $T_{w,\sigma}$ is a σ -linear operator on V_K . A computation shows

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

and

$$xT^n = x(T^d)^{n'} = (ux_0, u^\sigma x_1, \dots, u^{\sigma^{d-1}} x_{d-1})$$

with $u = ww^\gamma \dots w^{\gamma^{n'-1}} = N_{L:F}(w)$. As a consequence of Corollary 2.5 we note:

Proposition *Choose $w \in L$ such that $F = \text{GF}(q)[N_{L:F}(w)]$. Then $T = T_{w,\sigma}$ is irreducible.*

We have already described all irreducible, semilinear transformations on finite vector spaces:

Theorem 3.4 *Let V be a finite dimensional vector space over the finite field K . Using the notation of 3.3 the following holds.*

- (a) *Any irreducible, semilinear transformation on V_K is conjugate under $\text{GL}(V_K)$ to some operator $T_{w,\sigma}$.*
- (b) *Assume from now on that $K = \text{GF}(q^n)$ and $\dim_K V = m$. Let σ be an automorphism of order n . Set $F = \text{GF}(q^m)$ and $L = \text{GF}(q^{m'n})$ where $m' = m/d$, $d = (m, n)$. The following are equivalent:*
 - (1) *The irreducible, σ -linear operators $T_{w,\sigma}$ and $T_{w',\sigma}$ are conjugate under $\text{GL}(V_K)$.*
 - (2) *The linear operators $T_{w,\sigma}^n$ and $T_{w',\sigma}^n$ are conjugate in $\text{GL}(V_K)$.*
 - (3) *$N_{L:F}(w)$ and $N_{L:F}(w')$ are conjugate under $\text{Gal}(F : K_0)$ where $K_0 = \text{GF}(q)$.*
- (c) *The following are equivalent:*
 - (1) *The irreducible, σ -linear operators $T_{w,\sigma}$ and $T_{w',\sigma}$ are conjugate under in $\Gamma\text{L}(V_K)$.*
 - (2) *The linear operators $T_{w,\sigma}^n$ and $T_{w',\sigma}^n$ are conjugate in $\Gamma\text{L}(V_K)$.*
 - (3) *$N_{L:F}(w)$ and $N_{L:F}(w')$ are conjugate under $\text{Aut}(F)$.*

Proof. In order to be specific we use the notation of (b).

(a) Let T be an irreducible, σ -linear operator. By Theorem 2.4 the minimal polynomial f_0 of T^n over K_0 is irreducible and has degree m . Choose $w \in L$ such that $u = N_{L:F}(w)$ (the norm map is surjective) has the same minimal polynomial over K_0 . As we have seen in 3.3 the operator $T_{w,\sigma}^n$ has also the minimal polynomial f_0 over K_0 . By Theorem 2.10.a T and $T_{w,\sigma}$ are conjugate.

(b) Set $T = T_{w,\sigma}$ and $T' = T_{w,\sigma'}$. According to Theorem 2.10 the assertions (1) and (2) are equivalent. Set $u = N_{L:F}(w)$ and $u' = N_{L:F}(w')$. By Theorem 2.10 we have to show that T^n and $(T')^n$ are conjugate if u and u' are conjugate under $\text{Gal}(F : K_0)$. But in the latter case the minimal polynomial of u over K_0 is also the minimal polynomial of u' over K_0 . Then the minimal polynomials of T^n and $(T')^n$ over K_0 agree and we can apply Theorem 2.10.a. The equivalence of (2) and (3) follows.

(c) Again (1) \Leftrightarrow (2) follows from Theorem 2.10. Satz II.7.3 of [8], implies that the maps $x\phi = u^{\bar{\sigma}}x$ and $x\psi = (u')^{\bar{\sigma}}x$ in $\text{GL}(L_K)$ are conjugate under $\Gamma(L_K)$ iff u and u' are conjugate under $\text{Aut}(L)$. Using the notation of (b) we see that T^n and $(T')^n$ are conjugate in $\Gamma(V_K)$ iff u and u' are conjugate under $\text{Aut}(L)$. The image of the restriction of $\text{Aut}(L)$ to F is $\text{Aut}(F)$. The proof is complete. \square

We illustrate the previous results with some small examples.

Example Let V be a vector space of size 2^{12} . We consider V as a K -space, $K = \text{GF}(2^a)$, $1 < a < 12$, and determine all irreducible, semilinear operators with the help of Theorem 3.4. We set $m = \dim V_K$, $n = |\sigma|$, and $T = T_{w,\sigma}$ denotes a semilinear operator, such that $F = K_0[u]$, $u = N_{L:F}(w)$ and F , L , and K_0 as usual. The $\Gamma(L_K)$ -classes are determined by the action of $\text{Aut}(F)$ on the elements $u \in F$ which generate together with K_0 the field F . The action of the group $\text{Gal}(F : K_0)$ on such an orbit splits this orbit into suborbits. The collection of all suborbits corresponds to $\text{GL}(V_K)$ -orbits of semilinear operators.

CASE $K = \text{GF}(2^2)$, $m = 6$: Then $n = 2$, $F = L = \text{GF}(2^6)$, $K_0 = \text{GF}(2)$, and $d = 2$. Hence $N_{L:F}(w) = w$ has order 9, 21 or 63. We have one $\Gamma(L_K)$ -class with $|T| = 18$, two classes with $|T| = 42$, and 6 classes with $|T| = 126$. Each $\Gamma(L_K)$ -class is also an $\text{GL}(V_K)$ -orbit.

CASE $K = \text{GF}(2^3)$, $m = 4$: Then $n = 3$, $F = \text{GF}(2^4)$, $L = \text{GF}(2^{12})$, $K_0 = \text{GF}(2)$, and $d = 1$. Hence $N_{L:F}(w) = w^{273}$ has order 5 or 15. We have two field automorphisms and for each automorphism one class with $|T| = 15$ and two classes with $|T| = 45$. Each $\Gamma\text{L}(V_K)$ -class is also an $\text{GL}(V_K)$ -orbit.

CASE $K = \text{GF}(2^4)$, $m = 3$: If $n = 4$ then $F = \text{GF}(2^3)$, $L = \text{GF}(2^{12})$, $K_0 = \text{GF}(2)$, and $d = 1$. Hence $N_{L:F}(w) = w^{585}$ has order 7. We have two field automorphisms and for each field automorphism two $\Gamma\text{L}(V_K)$ -classes with $|T| = 28$. These classes are also $\text{GL}(V_K)$ -orbits.

If $n = 2$ then $F = \text{GF}(2^6)$, $L = \text{GF}(2^{12})$, $K_0 = \text{GF}(2^2)$, and $d = 1$. Hence $N_{L:F}(w) = w^{65}$ has order 7, 9, 21 or 63. We have two $\Gamma\text{L}(V_K)$ -classes with $|T| = 14$, one class with $|T| = 18$, two classes with $|T| = 42$, and 6 classes with $|T| = 126$. The classes with $|T| = 14$ are also $\text{GL}(V_K)$ -orbits while each the other $\Gamma\text{L}(V_K)$ -class splits into two $\text{GL}(V_K)$ -orbits.

CASE $K = \text{GF}(2^6)$, $m = 2$: If $n = 6$ then $F = \text{GF}(2^2)$, $L = K$, $K_0 = \text{GF}(2)$, and $d = 2$. Hence $N_{L:F}(w) = w^{21}$ has order 3. We have two field automorphisms and for each automorphism we have one $\Gamma\text{L}(V_K)$ -class which is also an $\text{GL}(V_K)$ -orbit and $|T| = 18$.

If $n = 3$ then $F = \text{GF}(2^4)$, $L = \text{GF}(2^{12})$, $K_0 = \text{GF}(2^2)$, and $d = 1$. Hence $N_{L:F}(w) = w^{273}$ has order 5 or 15. We have two field automorphisms and for each field automorphisms we have one $\Gamma\text{L}(V_K)$ -class with $|T| = 15$ and two classes with $|T| = 45$. Each $\Gamma\text{L}(V_K)$ -class splits into two $\text{GL}(V_K)$ -orbits.

If $n = 2$ then $F = L = \text{GF}(2^6)$, $K_0 = \text{GF}(2^3)$, and $d = 2$. Hence $N_{L:F}(w) = w$ has order 3, 9, 21 or 63. We have one $\Gamma\text{L}(V_K)$ -class with $|T| = 6$, one with $|T| = 18$, two with $|T| = 42$, and 6 with $|T| = 126$. The class with $|T| = 6$ is also an $\text{GL}(V_K)$ -orbit. Any other $\Gamma\text{L}(V_K)$ -class splits into three $\text{GL}(V_K)$ -orbits.

Example In the previous example the σ -linear operator $T = T_{w,\sigma}$ is represented as $xT = wx^{2^b}$ (with a suitable b) if $d = 1$ and $V = L = \text{GF}(2^{12})$ and as $(x, y)T = (wy^{2^a}, x^{2^a})$ (with a suitable a) if $d = 2$, $V = L^2$, and $L = \text{GF}(2^6)$. Therefore it may be tempting to assume that an irreducible, σ -linear operator on a finite vector space V_K , $K = \text{GF}(q^n)$, can be represented in a simpler form than 3.3:

$$xT = (wx_{d-1}^{\bar{\sigma}}, x_0^{\bar{\sigma}}, \dots, x_{d-2}^{\bar{\sigma}}) \quad (+)$$

where $\bar{\sigma}$ is an extension of σ to a field $M \subseteq \text{End}_K(V)$, $w \in M$, and where $V = \bigoplus_i M e_i$.

However this assumption is false: Let $K = \text{GF}(2^6)$, $L = \text{GF}(2^{12})$, $V = L^2$, and let σ be the Frobenius automorphism of K . Choose $w \in L$ such that $N_{L:F}(w) \in F = \text{GF}(2^4)$ has order 15. Then $T = T_{w,\sigma}$ defined by $(x, y)T = (wy^{2^7}, x^2)$ is an irreducible, σ -linear operator of order 90 on V_K . On the other hand it is easy to see that any operator of the form (+) has an order which is coprime to 5.

Remarks (a) Let T be an arbitrary semilinear operator on a finite vector space V . By [5], [6], or [9], V is the direct sum of indecomposable, uniserial T -spaces and all composition factors of an indecomposable summand are isomorphic. More precisely, the semilinear operator operator is characterized by the number of indecomposable summands, the isomorphism types of irreducible composition factors (precisely one type for each indecomposable space), and the lengths (number of composition factors) of the indecomposable summands. Therefore Theorem 3.4 implies the enumeration of the equivalence classes of semilinear operators on a finite vector space.

(b) Kantor and Liebler show in [10]:

Theorem *Let T be an irreducible, σ -semilinear transformation on a finite vector space V over a finite field K . Then there is a decomposition*

$$V = V_1 \oplus \cdots \oplus V_t$$

of V into subspaces V_i permuted cyclically by T such that $T^t|_{V_1}$ is a 1-dimensional affine map over an extension field of K . Moreover, t divides the order of σ , and the map $T^t|_{V_1}$ uniquely determines T up to $\text{GL}(V)$ -conjugacy.

This result can be regarded as an intermediate step towards Theorem 3.4: Kantor and Liebler show that an irreducible, σ -semilinear transformation T is characterized by T^d (d with its usual meaning). Our theorem shows that T^n already characterizes T .

ACKNOWLEDGMENT I like to thank W. Kantor. His comments lead to an improvement of the readability of this paper.

NOTE. After the submission of this article the author became aware of "Über halbeinfache Transformationen" Math. Annalen 115(1938), 87-144 by K. Asano and T. Nakayama. Using the theory of non-commutative

polynomial rings the validity of part (b) of the theorem is shown even in the non-separable case.

References

- [1] E. Artin: Galoissche Theorie, Harri Deutsch, 1968.
- [2] M. Aschbacher: Finite Group Theory, Cambridge University Press, 2000.
- [3] B. G. Basmaji: Monomial representations and metabelian groups, Nagoya Mat. J. 35(1969), 99-107.
- [4] J. R. Bastida: Field extensions and Galois theory, Addison-Wesley, 1984.
- [5] U. Dempwolff: Normal forms and fixed subspaces of semilinear maps, Boll. UMI 4-A(1990), 209-218.
- [6] U. Dempwolff: Normalformen semilinearer Operatoren, Math. Semesterber. 46(1999), 205-214.
- [7] W. Feit: The Representation Theory of Finite Groups, North-Holland, 1982.
- [8] B. Huppert, N. Blackburn: Endliche Gruppen I, Finite Groups II, Springer, 1973, 1982.
- [9] N. Jacobson: Pseudo-linear transformations, Ann. of Math. 38(1937), 484-507.
- [10] W. Kantor, R. Liebler: Semifields arising from irreducible semilinear transformations, to appear in J. Austr. Math. Soc.