Glasgow Math. J. **42** (2000) 289–295.

SEMILINEAR TRANSFORMATIONS OVER FINITE FIELDS ARE FROBENIUS MAPS

U. DEMPWOLFF

FB Mathematik, Universität Kaiserslautern, Postfach 3049, D-67653 Kaiserslautern, Germany
e-mail:dempwolff@mathematik.uni-kl.de

J. CHRIS FISHER and ALLEN HERMAN

Department of Mathematics and Statistics, University of Regina, Regina, SK, Canada, S4S 0A2
e-mail:fisher@math.uregina.ca, aherman@math.uregina.ca

(Received 27 October, 1998)

Abstract. In its original formulation Lang's theorem referred to a semilinear map on an n-dimensional vector space over the algebraic closure of $GF(p)$: it fixes the vectors of a copy of $V(n, p^h)$. In other words, every semilinear map defined over a finite field is equivalent by change of coordinates to a map induced by a field automorphism. We provide an elementary proof of the theorem independent of the theory of algebraic groups and, as a by-product of our investigation, obtain a convenient normal form for semilinear maps. We apply our theorem to classical groups and to projective geometry. In the latter application we uncover three simple yet surprising results.

1991 *Mathematics Subject Classification.* Primary 20G40; secondary 15A21, 51A10.

§**1. Introduction.** Let $V = V(n, F)$ be an n-dimensional vector space over a field F, and let $B = \{v_1, \ldots, v_n\}$ be a basis of V. Any automorphism σ of F induces a bijection from V to V by acting on the coordinates with respect to this basis; i.e. $(\sum x_i v_i)^\sigma = \sum x_i{}^\sigma v_i$. This bijection will also be referred to as σ. A σ-*semilinear* map T is the composition of this σ with an F-linear transformation M; i.e. $T(v) = M(v^\sigma)$, for all $v \in V$. In the case where F is a finite field, σ will be called a *Frobenius map*; it is induced by a Frobenius automorphism $a \mapsto a^q$ of F, where q is a fixed power of the characteristic of F. In this case $|F| = q^h$, for some $h \geq 1$, and we shall write $V = V(n, q^h)$. We shall also write $\sigma(v) = v^q$ for $v \in V$, and call a corresponding σ-semilinear map a q-*semilinear* map. It is easy to see that any q-semilinear map T on $V(n, q^h)$ extends to a q-semilinear map on $V(n, K)$, where K denotes the algebraic closure of $GF(q)$.

Main theorem. *Any q-semilinear map T on $V(n, K)$ fixes the vectors of a copy of $V(n, q)$.*

By choosing a new basis from among these fixed vectors we deduce the following result.

Every q-semilinear map defined over a finite field is equivalent by change of coordinates to a Frobenius map.

The latter statement is equivalent to a special case of a theorem of Lang [**5**] in the theory of algebraic groups. According to Lang's result, if K is the algebraic closure of $GF(q)$, then any matrix $M \in GL(n, K)$ can be written as $M = PP^{-(q)}$, for

https://doi.org/10.1017/S0017089500020164 Published online by Cambridge University Press

some $P \in GL(n, K)$, where $P^{-(q)}$ is the matrix obtained by applying the Frobenius automorphism $x \mapsto x^q$ to each entry of P^{-1}. If T is the q-semilinear map having matrix M with respect to the basis B, and we change coordinates using the matrix P, then the matrix corresponding to T with respect to the new basis is $P^{-1}MP^{(q)}$. With the choice of P as in Lang's theorem, we find that T has the identity matrix with respect to the new basis, so the new basis consists of fixed vectors for T. The $GF(q)$-span of this basis is the copy of $V(n, q)$ that is fixed by T as required by our result. Conversely, if there is a basis of $V(n, K)$ consisting of fixed vectors for T, then $P^{-1}MP^{(q)}$ is the identity matrix, from which Lang's theorem follows.

In Sections 2 and 3 we provide an elementary proof of this theorem independent of the theory of algebraic groups. We then show how our result can be used to extend Lang's theorem to classical groups. In Section 5 we interpret the main theorem in the language of projective geometry, revealing three simple yet surprising results.

§**2. A normal form for a semilinear transformation.** We start with an elementary deduction of a normal form for semilinear maps by achieving a decomposition of V as a direct sum of cyclic subspaces. This has to be done in a manner that avoids the characteristic equation; indeed, any *eigenvector* for an invertible semilinear map will generate many eigenvalues, since $T(v) = \lambda v$ implies that $T(\alpha v) = \alpha^q \lambda v = \alpha^{q-1}\lambda(\alpha v)$, for any $\alpha \in F$. We assume that F is commutative in order to simplify notation: by using the dual space instead of the transpose, the argument shown here can be adapted to obtain a normal form for semilinear maps of vector spaces over skew-fields (cf. [**4**, p. 496]). Our method also does not require that the field automorphism have finite order, and so we cannot obtain results regarding the isomorphism types of indecomposable summands as in [**1**].

For any $v \in V$ and transformation T of V, let $[v]$ denote the T-cyclic subspace of V spanned by $\{v, T(v), T^2(v), \ldots\}$.

THEOREM 1. *Let V be an n-dimensional vector space over the field F, σ an automorphism of F, and T a σ-semilinear map on V. Then*

$$V = [u_1] \oplus \ldots \oplus [u_r]$$

for T-cyclic subspaces satisfying $\dim[u_1] \geq \dim[u_2] \geq \ldots \geq \dim[u_r]$. *Moreover,* $\dim[u_i]$ *is maximal among the dimensions of the T-cyclic subspaces of $[u_i] \oplus \ldots \oplus [u_r]$, for each i.*

Proof. Let B be a basis of V, and suppose that T has the matrix M with respect to this basis. Let T' be the σ^{-1}-semilinear map on V that has the transpose matrix M^t with respect to the basis B.

The definition of T' depends on B but the next claim does not.

(1) *Let $[w]$ be a T-cyclic space of dimension m. Then there is a T'-invariant space W with* $\dim(V/W) = m$ *and V/W is T'-cyclic. The dual statement is also true.*

To prove (1), choose a basis $B_1 = \{w_1, \ldots, w_m, w_{m+1}, \ldots, w_n\}$ with $w = w_1$, $T(w_i) = w_{i+1}$ for $1 \leq i < m$, and

$$T(w_m) = \sum_{i=1}^{m} a_i w_i.$$

Let S be the matrix for the basis change from B to B_1, so that T has matrix

$$S^{-1} M S^{\sigma} = \begin{bmatrix} C & D_1 \\ 0 & D_2 \end{bmatrix}, \text{ where } C = \begin{bmatrix} & & & a_1 \\ 1 & & & a_2 \\ & \ddots & & \vdots \\ & & 1 & a_m \end{bmatrix}.$$

Transposing yields

$$\begin{bmatrix} C^t & 0 \\ {D_1}^t & {D_2}^t \end{bmatrix} = (S^t)^{\sigma} M^t S^{-t} = R^{-1} M^t R^{\sigma^{-1}},$$

where $S^{-t} = (S^t)^{-1}$ and $R = (S^{-t})^{\sigma}$. Thus R defines a basis change from B to $B_2 = \{u_1, \dots, u_n\}$ such that T' leaves the space spanned by $\{u_{m+1}, \dots, u_n\}$ invariant. Call this space W. This means that T' acts on the space V/W, with matrix C^t with respect to the basis $\{\bar{u}_1, \dots, \bar{u}_m\}$, where $\bar{u}_i = u_i + W$ for $1 \leq i \leq m$. By the form of C^t, $(T')^k(\bar{u}_m) = b_0 \bar{u}_m + \dots + b_k \bar{u}_{m-k}$ for $k < m$, with $b_k \neq 0$. Thus $[\bar{u}_m]' = V/W$, where $[\bar{u}_m]'$ is the T'-cyclic subspace of V/W spanned by $\{\bar{u}_m, T'(\bar{u}_m), (T')^2(\bar{u}_m), \dots\}$. This proves (1), since the dual statement follows just by interchanging T and T'.

As a consequence of (1), we have the following result.

(2) *If m is the maximal dimension of T-cyclic subspaces of V, and m' is the maximal dimension of T'-cyclic subspaces of V, then $m = m'$.*

In the notation of (1), we have

$$m = \dim[\bar{u}_m]' \leq \dim[u_m]' \leq m',$$

and so the dual statement implies that $m = m'$.

Theorem 1 follows by induction from the next claim.

(3) *If m is the maximal dimension of a T-cyclic subspace of V, and $w \in V$ satisfies* $\dim[w] = m$, *then* $[w]$ *has a T-invariant complement.*

To prove (3), let $w \in V$ with $\dim[w] = m$. Let $B_1 = \{w_1, \dots, w_m, w_{m+1}, \dots, w_n\}$ be a basis of V chosen so that $w = w_1$, $T(w_i) = w_{i+1}$ for $1 \leq i < m$, and

$$T(w_m) = \sum_{i=1}^{m} a_i w_i.$$

Then the matrix M of T with respect to B_1 has the form

$$M = \begin{bmatrix} C & D_1 \\ 0 & D_2 \end{bmatrix}, \text{ where } C = \begin{bmatrix} & & & a_1 \\ 1 & & & a_2 \\ & \ddots & & \vdots \\ & & 1 & a_m \end{bmatrix}.$$

https://doi.org/10.1017/S0017089500020164 Published online by Cambridge University Press

Let T' be the σ^{-1}-semilinear map having matrix M^t with respect to B_1. As in (1), the span of $\{w_{m+1}, \ldots, w_n\}$ is a T'-invariant space W, and $[\bar{w}_m]' = V/W$. Thus $m = \dim[\bar{w}_m]' \leq \dim[w_m]' \leq m'$ and so, by (2), it follows that $\dim[w_m]' = m$. Since $(T')^k(w_m) = \sum_{j=0}^{k} c_j w_{m-j}$ with $c_k \neq 0$, for all $k < m$, we see that $[w_m]' = [w_1] = [w]$. Let $B_2 = \{u_1, \ldots, u_m, w_{m+1}, \ldots, w_n\}$ be a basis of V chosen so that $u_1 = w_m$, $T'(u_i) = u_{i+1}$ for $1 \leq i < m$, and

$$T'(u_m) = \sum_{i=1}^{m} b_i u_i.$$

If R denotes the matrix for the basis change from B_1 to B_2, then

$$R^{-1} M^t R^{\sigma^{-1}} = \begin{bmatrix} C' & 0 \\ 0 & {D_2}^t \end{bmatrix}, \text{ where } C' = \begin{bmatrix} & & & b_1 \\ 1 & & & b_2 \\ & \ddots & & \vdots \\ & & 1 & b_m \end{bmatrix}.$$

Thus the matrix of T with respect to B_2 is

$$\begin{bmatrix} (C')^t & 0 \\ 0 & D_2 \end{bmatrix} = S^{-1} M S^{\sigma},$$

where $S = (R^{-t})^{\sigma^{-1}}$. Thus V decomposes into the direct sum of T invariant subspaces $[u_m]$ and W with $\dim[u_m] = m$. As previously, we can see that $[u_m] = [w_m]' = [w]$, which proves (3). Theorem 1 follows by induction on dim V. □

Theorem 1 implies immediately that the matrix for any semilinear transformation has a normal form: choose the basis of V to be the union of the appropriate bases of the T-cyclic subspaces $[u_1], \ldots, [u_r]$.

THEOREM. (Normal form of a semilinear transformation.) *By a change of basis the matrix M of any σ-semilinear transformation can be given in the form*

$$M = \begin{bmatrix} M_1 & & \\ & \ddots & \\ & & M_r \end{bmatrix},$$

where

$$M_k = \begin{bmatrix} 0 & \ldots & \ldots & 0 & a_{k,1} \\ 1 & \ddots & & \vdots & a_{k,2} \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \ldots & 0 & 1 & a_{k,m_k} \end{bmatrix}.$$

§**3. Proof of the main theorem.** We now suppose that T is a q-semilinear map on $V = V(n, K)$, where K is the algebraic closure of the finite field $GF(q)$. Our main theorem will follow by showing that there are exactly q^n solutions in V to the equation

https://doi.org/10.1017/S0017089500020164 Published online by Cambridge University Press

$T(v) = v$. The fact that the field automorphism associated with T is in the form of a power map is essential, since T need not have any non-zero fixed vectors when σ is not a power map. For example, the semilinear transformation on $\mathbb{C}^2$ given by $(z_1, z_2) \mapsto (-\bar{z}_2, \bar{z}_1)$, with $\bar{z}$ the complex conjugate of z, has no non-zero fixed vectors in $\mathbb{C}^2$ (even though $\mathbb{C}$ is algebraically closed).

Note that whenever we can solve the equation $T(v) = \lambda v$ for some non-zero $\lambda \in K$, then $T(\lambda^{\overline{\frac{-1}{q-1}}} v) = \lambda^{\overline{\frac{-q}{q-1}}}(\lambda v) = \lambda^{\overline{\frac{-1}{q-1}}} v$, so that some K-multiple of v is a fixed vector for T.

Proof of the main theorem. By Theorem 1, we can assume that $V = [v]$ is a T-cyclic subspace, and the matrix of T with respect to the basis $B = \{v_1 = v, v_2 = T(v), \ldots, v_n = T^{n-1}(v)\}$ is the companion matrix. Since T is invertible, we must have $a_1 \neq 0$. Solving $T(\sum_{i=1}^{n} x_i v_i) = \sum x_i v_i$ for $x_i \in K$ leads to the system of equations

$$\begin{aligned} a_1 x_n{}^q &= x_1, \\ x_1{}^q + a_2 x_n{}^q &= x_2, \\ \vdots \quad & \quad \vdots \\ x_{n-1}{}^q + a_n x_n{}^q &= x_n. \end{aligned}$$

Eliminating $x_1, \ldots, x_{n-1}$, we obtain the equation

$$a_1{}^{q^{n-1}} x_n{}^{q^n} + a_2{}^{q^{n-2}} x_n{}^{q^{n-1}} + \ldots + a_n x_n{}^q - x_n = 0.$$

This equation has q^n distinct solutions for x_n in K by the derivative test. Each solution determines a unique fixed vector, and the set of fixed vectors constitutes a subspace over the field $GF(q)$. It remains to show that there are n fixed vectors that are linearly independent over K. If $\{v_1, \ldots, v_m\}$ is a set of m fixed vectors that is linearly independent over K, then $\sum_{i=1}^{m} a_i v_i$ is a fixed vector for T if and only if all $a_i \in GF(q)$. Thus the K-span of these vectors contains precisely q^m fixed vectors. Since there are exactly q^n fixed vectors for T, we can conclude that any T-cyclic space V has a basis consisting of fixed vectors for T.

The main theorem now follows from Theorem 1.

§**4. Extending Lang's theorem.** The theorem of Lang mentioned above has been substantially generalized; it applies to connected algebraic groups. (See [**6**, 10.1].) Our result can be applied to the case of classical groups over finite fields. As an example, we show how to do this in the case of the special orthogonal groups. (A similar argument applies to symplectic or special linear groups.)

Let K be the algebraic closure of $GF(q)$, and let V be an n-dimensional vector space with non-degenerate quadratic form Q. If char $K \neq 2$, then V has an orthonormal basis $B = \{v_1, \ldots, v_n\}$, with $Q(\sum a_i v_i) = 2^{-1} \sum a_i{}^2$. If char $K = 2$, then either $n = 2m$ and B has a symplectic basis $\{v_1, w_1, \ldots, v_m, w_m\}$ with $Q(\sum(a_i v_i + b_i w_i)) = \sum a_i b_i$, or $n = 2m + 1$ and V has a basis $B = \{v_1, w_1, \ldots, v_m, w_m, u\}$ such that $Q(\sum(a_i v_i + b_i w_i) + cu) = \sum a_i b_i + c^2$ [**2**, p. 34]. Let $G = O(V)$ be the group of isometries of V with respect to Q, and identify G with the matrices over K with respect to the basis B. The Frobenius map $A \mapsto A^{(q)}$ induces an automorphism of G, which

https://doi.org/10.1017/S0017089500020164 Published online by Cambridge University Press

leaves invariant the special orthogonal group $SO(V)$ defined by $\{A \in G : \det A = 1\}$ when char $K \neq 2$, and $\{A \in G : D(A) = 0\}$ when char $K \neq 2$. (Here D denotes the Dickson invariant [**2**, p. 65].)

THEOREM. *Let $M \in SO(n, K)$. Then there exists a matrix $P \in SO(n, K)$ such that $M = PP^{-(q)}$.*

Proof. Let T be the q-semilinear map on V that has matrix M with respect to the aforementioned basis B. Then T is a q-isometry with respect to Q; i.e. for all $v, w \in V$, $Q(T(v)) = Q(v)^q$. Our main theorem implies that there is a basis B' of fixed vectors for T. Let W be the $GF(q)$-span of the vectors B'. Then, for all $w \in W$, $Q(w) \in GF(q)$. Thus Q is a non-degenerate quadratic form on the n-dimensional $GF(q)$-space W. If we can choose a basis B_1 of W that is orthonormal (or symplectic if char $K = 2$), then the change of basis matrix X from B to B_1 coefficients is orthogonal, and satisfies $X^{-1}MX^{(q)} = I$. If $X \notin SO(n, K)$, then we can find a matrix $Y \in G$ such that $Y^{(q)} = Y$ and $XY \in SO(n, K)$; in fact

$$Y = \begin{bmatrix} 0 & 1 & \\ 1 & 0 & \\ & & I_{n-2} \end{bmatrix}$$

will suffice for any characteristic. Letting $P = XY$, we obtain $P^{-1}MP^{(q)} = I$ with $P \in SO(n, K)$, as required.

Since W is a vector space over $GF(q)$ rather than K, it is not obvious that one can always find an orthonormal or symplectic basis of W. Indeed, suppose that W does not have a suitable basis.

If char $K \neq 2$, then W would have a basis $B_1 = \{u_1, \dots, u_n\}$ such that $Q(\sum b_i u_i) = 2^{-1} \sum b_i{}^2 + 2^{-1} d b_n{}^2$, where d is a non-square in $GF(q)$ [**2**, p. 16]. Choose $\delta \in GF(q^2)$ such that $\delta^2 = d$, and let $\tilde{u}_n = \delta^{-1} u_n$. Then $B_1 = \{u_1, \dots, u_{n-1}, \tilde{u}_n\}$ would be an orthonormal basis of V and the matrix of T with respect to B_1 would be

$$N = \begin{bmatrix} I_{n-1} & \\ & \delta^{-q+1} \end{bmatrix}.$$

Thus there would exist an $X \in G$ such that $X^{-1}MX^{(q)} = N$. Since $\det X = \pm 1$ when $X \in G$, taking the determinant on both sides results in a contradiction.

If char $K = 2$ and W did not have a suitable basis, then dim W would have to be even [**2**, p. 34]; so let $n = 2m$. W would have basis $B_1 = \{v_1', w_1', \dots, v_m', w_m'\}$ such that

$$Q(\sum (a_i v_i' + b_i w_i')) = \sum_{i=1}^{m-1} a_i b_i + \alpha a_m^2 + a_m b_m + \alpha b_m^2,$$

with $f(X) = \alpha X^2 + X + \alpha$ irreducible over $GF(q)$ [**2**, p. 34]. Let $\delta \in GF(q^2)$ be a root of f, and set $\tilde{v}_m{}' = \delta v_m' + w_m'$, $\tilde{w}_m{}' = \delta^q v_m' + w_m'$. $B_2 = \{v_1', w_1', \dots, v_{m-1}', w_{m-1}', \tilde{v}_m{}', \tilde{w}_m{}'\}$ would be a symplectic basis of V, and the matrix of T with respect to B_2 would be

$$N = \begin{bmatrix} I_{n-2} & & \\ & 0 & 1 \\ & 1 & 0 \end{bmatrix}.$$

https://doi.org/10.1017/S0017089500020164 Published online by Cambridge University Press

Thus $D(N) = 1$. However, if X were the change of basis matrix from B to B_2 coefficients, then $X \in G$ and $X^{-1}MX^{(q)} = N$. Since $D(X) = D(X^{-1}) = D(X^{(q)})$, the Dickson invariant of the left side would be $2D(X) = 0$, a contradiction. Thus W always has a basis for which the matrix for T is the identity, as required. □

§**5. Consequences in projective geometry.** We conclude with three immediate consequences of the main theorem in projective geometry. Recall that every collineation of n-dimensional projective space is induced by a semilinear transformation. A *projectivity* is a collineation that preserves cross ratios; it is induced by a linear transformation.

COROLLARY 1. *Every projectivity of $PG(n, q^h)$ can be written as the product $\phi_2\phi_1$ of two Frobenius maps; ϕ_1 can be chosen arbitrarily and ϕ_2 acts on $PG(n, q^{h'})$ with $h' \geq h$.*

Proof. If T is the projectivity, then $T{\phi_1}^{-1}$ is a semilinear transformation. □

COROLLARY 2. (cf. [**3**, p. 46].) *Given a projectivity T of period h on $\Pi = PG(n, q)$, there exists a copy of Π in $PG(n, q^h)$ on which the restriction of the Frobenius map is projectively equivalent to T (restricted to Π).*

Proof. Restricted to the fixed points of ϕ_2, $T{\phi_1}^{-1}$ is the identity. This implies the desired result, because ϕ_1 has period h and commutes with T. □

By restricting Corollary 2 to a single orbit of T, we see that every projective orbit of $PG(n, q)$ is mimicked by a Frobenius map; more precisely, we have the following result.

COROLLARY 3. (cf. [**3**, p. 47].) *If an orbit S in $PG(n, q)$ of the cyclic group generated by some projectivity consists of h points, then there exists a point Q in $PG(n, q^h)$ whose orbit under successive applications of the Frobenius map is projectively equivalent to S.*

REFERENCES

1. U. Dempwolff, Normal forms and fixed subspaces of semilinear maps, *Boll. Un. Math. Ital. A, (7)* **4** (1990), No. 2, 209–218.
2. J. Dieudonné, *La geometrie des groupes classiques* (Springer-Verlag, 1955).
3. J. C. Fisher, Frobenius orbits, *Rend. Circ. Mat. Palermo (2) Suppl.* No. 53 (1998), 45–54.
4. N. Jacobson, Pseudo-linear transformations, *Ann. of Math.* **38** (1937), No. 2, 484–507.
5. S. Lang, Algebraic groups over finite fields, *Amer. J. Math.* **78** (1956), 555–563.
6. R. Steinberg, *Endomorphisms of linear algebraic groups*. Memoirs of the American Mathematical Society, No. 80 (A.M.S., Providence, R. I., 1968).