TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 353, Number 7, Pages 2941–2969
S 0002-9947(01)02744-1
Article electronically published on January 29, 2001

GALOIS GROUPS OF SOME VECTORIAL POLYNOMIALS

SHREERAM S. ABHYANKAR AND NICHOLAS F. J. INGLIS

Abstract. Previously nice vectorial equations were constructed having various finite classical groups as Galois groups. Here such equations are constructed for the remaining classical groups. The previous equations were genus zero equations. The present equations are strong genus zero.

1. Introduction

Let $q > 1$ be a power of a prime p, let k_q be an overfield of $\mathrm{GF}(q)$, and let $m > 0$ be an integer. In previous papers [Ab4], [Ab5], [Ab6] the Galois groups of the following vectorial q-polynomials

$$E^{\dagger}(Y) = Y^{q^{2m-1}} + X^{q'}Y^{q^m} + XY^{q^{m-1}} + Y,$$
$$E^{\natural}(Y) = Y^{q^{2m}} + T^qY^{q^{m+1}} + XY^{q^m} + TY^{q^{m-1}} + Y,$$
$$E^{-}(Y) = Y^{q^{2m}} + T^{q^2}Y^{q^{m+2}} + X^qY^{q^{m+1}} - XY^{q^{m-1}} - TY^{q^{m-2}} - Y,$$

over the fields $k_q(X)$, $k_q(X,T)$, $k_q(X,T)$ were shown to be the odd dimensional unitary, symplectic, and even dimensional negative (i.e., whose Witt index is one less than half its dimension) orthogonal groups $\mathrm{SU}(2m-1,q')$, $\mathrm{Sp}(2m,q)$, and $\Omega^-(2m,q)$, respectively, where it was assumed that $k_q = \overline{k}_q$ (the algebraic closure of k_q); moreover, it was also assumed that, in the unitary case $m > 1$ and $q = (q')^2$ for some power $q' > 1$ of p, in the symplectic case $m > 2$, and in the orthogonal case $m > 3$ and $p > 2$. For the symplectic case, in [AL1] and [AL2] it was shown that the assumption $k_q = \overline{k}_q$ can be removed and the assumption $m > 2$ can be replaced by the assumption $m > 1$; moreover, in [In2] it was shown that after putting $T = 1$ in $E^{\natural}(Y)$, its Galois group over $k_q(X)$ remains $\mathrm{Sp}(2m,q)$.

Likewise, in [Ab2], [Ab3], [Ab8], [Ab9], it was shown that the Galois groups of the vectorial trinomials

$$E^*(Y) = Y^{q^m} + XY^q + (-1)^mY \quad \text{and} \quad E^{**}(Y) = Y^{q^m} + Y^q + XY$$

over $k_q(X)$ are the special linear and general linear groups $\mathrm{SL}(m,q)$ and $\mathrm{GL}(m,q)$ respectively, where $m > 1$.

Received by the editors March 22, 2000.
2000 *Mathematics Subject Classification.* Primary 12F10, 14H30, 20D06, 20E22.
Abhyankar's work was partly supported by NSF Grant DMS 97-32592 and NSA grant MDA 904-99-1-0019.

In this paper we take care of the remaining classical groups by showing that the Galois groups of the following vectorial q-polynomials

$$E^{\ddagger}(Y) = Y^{q^{2m}} - X^{q'-1}Y^{q^{2m-1}} + X^{q'}Y^{q^m} - Y^q + X^{q'-1}Y,$$
$$E^{\circ}(Y) = Y^{q^{2m+1}} - X^{q-1}Y^{q^{2m-1}} + X^qY^{q^{m+1}} - X^qY^{q^m} + Y^{q^2} - X^{q-1}Y,$$
$$E^{+}(Y) = Y^{q^{2m}} - Y^{q^{2m-1}} - X^{q-1}Y^{q^{2m-2}} + X^{q-1}Y^{q^{2m-3}} + X^qY^{q^m} + Y^{q^3} - Y^{q^2} - X^{q-1}Y^q + X^{q-1}Y,$$

over $k_q(X)$ are the even dimensional unitary, odd dimensional orthogonal, and even dimensional positive (i.e, whose Witt index equals half its dimension) orthogonal groups $\mathrm{U}(2m, q')$, $\mathrm{SO}(2m+1, q)$, and $\mathrm{SO}^+(2m, q)$, where $m > 1$, $m > 2$, and $m > 3$, respectively; in the unitary case we assume $q = (q')^2$ for some power q' of p; in the odd dimensional orthogonal case when q is even we suppose $m > 3$ and note that SO equals O; in the even dimensional orthogonal case when q is even the answer may be $\Omega^+(2m, q)$.

According to the terminology introduced in [Ab7], the symplectic and special linear equations, i.e., the polynomials $Y^{-1}E^{\natural}(Y)$ and $Y^{-1}E^*(Y)$, are genus zero, i.e., they are linear in X, the odd dimensional unitary and even dimensional negative orthogonal equations, i.e., the polynomials $Y^{-1}E^{\dagger}$ and $Y^{-1}E^{-}(Y)$, are almost genus zero, i.e., they have genus zero factors having the same splitting fields as the polynomials themselves, the general linear equation, i.e., the polynomial $Y^{-1}E^{**}(Y)$, is strong genus zero, i.e., it is genus zero and in it only the constant term involves X, and the new polynomials $Y^{-1}E^{\ddagger}(Y)$, $Y^{-1}E^{\circ}(Y)$, and $Y^{-1}E^{+}(Y)$ will be shown to be almost strong genus zero, i.e., they have strong genus zero factors having the same splitting fields as the polynomials themselves. Again as said in [Ab7], this is in concordance with the Guralnick-Saxl List given in Theorem 3.1(B) of their paper [GSa]. Indeed it was this list which prompted the construction of the last three polynomials. We shall explain the link between our approach and that of Guralnick and Saxl in the remarks at the end of the paper.

The establishment of the Galois groups of the first three polynomials $E^{\dagger}$, $E^{\natural}$, E^{-}, was based on the Orbit Size Theorems of Liebeck [Li1], the Rank 3 Theorems of Kantor [Kan], and the Antiflag Transitive Theorems of Cameron-Kantor [CKa], and involved some very intricate polynomial factorizations developed for applying these Recognition Theorems of Group Theory. At the end of [Ab7] these factorizations were codified into a MANTRA. In [AL1], [AL2], and [In2], this mantra helped to convert the subdegree factorizations into factorizations yielding the underlying symplectic forms. Likewise, in this paper we shall use the mantra to construct the relevant quadratic and hermitian forms and hence to factorize the original polynomials.

By writing $(E^{\dagger\dagger}, q, m)$ for $(E^{\ddagger}, q', 2m)$ we get the vectorial q-polynomial

$$E^{\dagger\dagger}(Y) = Y^{q^{2m}} - X^{q-1}Y^{q^{2m-2}} + X^qY^{q^m} - Y^{q^2} + X^{q-1}Y$$

where $m > 2$ (and q need not be a square). This is the incarnation of $E^{\ddagger}$ we shall mostly deal with, and we shall show that in case of odd m the Galois group of $E^{\dagger\dagger}$ over $k_q(X)$ is $\mathrm{SO}^+(2m, q)$ except that when q is even it may be $\Omega^+(2m, q)$. For even m, as indicated, by changing notation we revert to $E^{\ddagger}$ and, as said above, if $\mathrm{GF}(q^2) \subset k_q$, then the Galois group of $E^{\dagger\dagger}$ over $k_q(X)$ is $\mathrm{U}(m, q)$.

In Sections 2–5 we shall discuss some generalities about quadratic and hermitian forms. Then in Section 6, as our main step, by an implicit invocation of the Mantra, we shall factor the three vectorial q-polynomials $E^{\dagger\dagger}$, E°, E^{+}, and show that each one of them gives rise to a quadratic form on its root-space which is left invariant by the corresponding Galois group. Finally, in Section 7 we shall calculate the Galois groups; there we shall also review the definitions of the orthogonal and unitary groups.

Let us start off by recalling that, according to [Ab8], a separable vectorial q-polynomial of q-degree d (with integer $d \geq 0$) over an overfield K of k_q is a polynomial of the form

$$E(Y) = \sum_{0 \leq i \leq d} a_i Y^{q^{d-i}} \quad \text{with } a_i \in K \text{ and } a_0 \neq 0 \neq a_d$$

(where separable refers to $a_d \neq 0$ and monic means $a_0 = 1$) and upon letting

$$V[E] = (\text{the root-space of } E) = \text{the set of all roots of } E \text{ in } \overline{K}$$

where $\overline{K}$ is the algebraic closure of K, we have the following. (Observe that we are using $\leq$ to denote subgroup, although the first author used $<$ in his previous papers.)

Note (1.1). $V[E]$ is a d-dimensional $\mathrm{GF}(q)$-subspace of $\overline{K}$, and in a natural manner $\mathrm{Gal}(E, K) \leq \mathrm{GL}(V[E])$, i.e., the Galois group $\mathrm{Gal}(E, K)$ of E over K is a subgroup of the group $\mathrm{GL}(V[E])$ of all nonsingular $\mathrm{GF}(q)$-linear transformations of $V[E]$, which by choosing a basis of $V[E]$ may be identified with the group $\mathrm{GL}(m, q)$ of all $m \times m$ nonsingular matrices over $\mathrm{GF}(q)$.

For any finite-dimensional $\mathrm{GF}(q)$-subspace V of $\overline{K}$ we put

$$f_V(Y) = \prod_{v \in V} (Y - v)$$

and then, according to the partial converse of (1.1) proved in (3.9) of [Ab9], we see that:

Note (1.2). f_V is a monic separable vectorial q-polynomial over $\overline{K}$ whose q-degree equals $\dim(V)$; moreover $V[f_V] = V$, and if $f_V(Y) \in K[Y]$ then $K(V) =$ the splitting field of f_V over K and $\mathrm{Gal}(f_V, K) \leq \mathrm{GL}(V)$.

It follows that:

Note (1.3). $V \mapsto f_V$ gives a bijection of the set of all finite-dimensional k-subspaces of $\overline{K}$ onto the set of all monic separable vectorial q-polynomials over $\overline{K}$; in this bijection, a d-dimensional V corresponds to a vectorial q-polynomial of q-degree d; in particular, the zero space corresponds to the polynomial Y.

Our assertions about the Galois groups of $E^{\dagger}, \ldots, E^{\ddagger}, \ldots, E^{\dagger\dagger}$ are in the sense of (1.1). For instance, $\mathrm{Gal}(E^{\ddagger}, K) = U(2m, q)$ with $(d, K) = (2m, k_q(X))$ means $\mathrm{Gal}(E^{\ddagger}, K)$ as a subgroup of $\mathrm{GL}(V[E^{\ddagger}])$ coincides with the isometry group of some hermitian form over $V[E^{\ddagger}]$. The polynomials $E^{\dagger}, \ldots, E^{\ddagger}, \ldots, E^{\dagger\dagger}$, like various other explicit polynomials with interesting Galois groups dealt with in [Ab2] to [Ab9], [AL1], [AL2], and [In2], are essentially special cases of the families of polynomials giving unramified coverings of the affine line and once-punctured affine line which were written down in the 1957 paper [Ab1] and which gave rise to the Affine Curve Conjecture formulated in that paper. The said conjecture (sometimes called the

Abhyankar Conjecture) says that for any nonnegative integer t and any nonsingular projective curve C_g of genus g over an algebraically closed ground field of characteristic p we have $\pi_A(C_{g,t}) = Q_{2g+t}(p)$ where the algebraic fundamental group $\pi_A(C_{g,t})$ of $C_{g,t} = C_g$ minus $t+1$ points is defined to be the set of all Galois groups of unramified finite Galois coverings of $C_{g,t}$, and where $Q_t(p)$ is the set of all finite groups G for which $G/p(G)$ is generated by t generators with $p(G)$ being the subgroup of G generated by all of its p-Sylow subgroups. The brilliant proof of this given by Harbater [Har] and Raynaud [Ray] being existential in nature, it is worthwhile to continue with the project of finding explicit equations for the said coverings. Moreover, explicit equations tend to enhance our knowledge of what happens over finite ground fields.

2. Quadratic forms

As common notation for the next four sections, let V be a d-dimensional (d-finite) vector space over a field k, and let $e_1, \dots, e_d$ be a basis of V. Let $\mathrm{Lin}(V)$ be the k-vector-space of all linear functions $\alpha : V \to k$. Note that then

$$\alpha \mapsto h_\alpha(X) = h_\alpha(X_1, \dots, X_d) = \sum \alpha(e_i) X_i$$

gives an isomorphism of $\mathrm{Lin}(V)$ onto the k-vector-space of all homogeneous linear polynomials in $k[X]$, where h_α is characterized by the condition

$$\alpha(\sum x_i e_i) = h_\alpha(x) \text{ for all } x = (x_1, \dots, x_d) \in k^d.$$

Let $\mathrm{Bil}(V)$ be the k-vector-space of all bilinear functions $b : V \times V \to k$. Note that then

$$b \mapsto h_b(X, X') = h_b(X_1, \dots, X_d, X'_1, \dots, X'_d) = \sum b(e_i, e_j) X_i X'_j$$

gives an isomorphism of $\mathrm{Bil}(V)$ onto the k-vector-space of all homogeneous bilinear polynomials in $k[X, X']$, where h_b is characterized by the condition

$$b(\sum x_i e_i, \sum x'_j e_j) = h_b(x, x') \quad \text{for all } x = (x_1, \dots, x_d) \text{ and } x' = (x'_1, \dots, x'_d) \text{ in } k^d.$$

Next we claim "product generation" which says that $\mathrm{Bil}(V)$ is generated by "product elements," i.e., elements of the form $\gamma : V \times V \to k$ where $\gamma(u, v) = \alpha(u)\beta(v)$ for all u, v in V, with α and β in $\mathrm{Lin}(V)$. Note that such a product element, which we may denote by $\alpha\beta$, clearly belongs to $\mathrm{Bil}(V)$. To prove the claim, given any b in $\mathrm{Bil}(V)$, let $b_{ij} = b(e_i, e_j)$. Then $b = \sum b_{ij}\gamma_{ij}$ where γ_{ij} in $\mathrm{Bil}(V)$ is given by $\gamma_{ij}(e_{i'}, e_{j'}) = \delta_{ii'}\delta_{jj'}$ in terms of the Kronecker delta. Let α_i in $\mathrm{Lin}(V)$ be given by $\alpha_i(e_{i'}) = \delta_{ii'}$. Then $\gamma_{ij}(e_{i'}, e_{j'}) = \alpha_i(e_{i'})\alpha_j(e_{j'})$. Therefore γ_{ij} equals the product element $\alpha_i\alpha_j$.

Let $\mathrm{Qua}(V)$ be the k-vector-space of all quadratic functions on V. Recall that these are functions $c : V \to k$ such that $c(\lambda v) = \lambda^2 c(v)$ for all $\lambda \in k$ and $v \in V$ and such that the associated bivariate function $b(u, v) = c(u + v) - c(u) - c(v)$ is bilinear. Note that then

$$c \mapsto \widehat{h}_c(X) = \widehat{h}_c(X_1, \dots, X_d) = \sum_i c(e_i) X_i^2 + \sum_{i<j} b(e_i, e_j) X_i X_j$$

gives an isomorphism of $\mathrm{Qua}(V)$ onto the k-vector-space of all homogeneous quadratic polynomials in $k[X]$, where $\widehat{h}_c$ is characterized by the condition

$$c(\sum_i x_i e_i) = \widehat{h}_c(x) \quad \text{for all } x = (x_1, \ldots, x_d) \in k^d.$$

If

$$\widehat{h}(X) = \sum_i c_i X_i^2 + \sum_{i<j} b_{ij} X_i X_j \quad \text{with } c_i \text{ and } b_{ij} \text{ in } k$$

is a homogeneous quadratic polynomial, then upon letting

$$h(X, Y) = \sum_i c_i X_i Y_i + \sum_{i<j} b_{ij} X_i Y_j$$

and

$$h^*(X, Y) = \sum_i 2c_i X_i Y_i + \sum_{i<j} b_{ij}(X_i Y_j + X_j Y_i)$$

we always have "bilinear generation"

$$\widehat{h}(X) = h(X, X)$$

and for odd characteristic we have "symmetric generation"

$$\widehat{h}(X) = (1/2)h^*(X, X).$$

Note that h^* is symmetric and is independent of the choice of basis whereas h need not be symmetric and is (highly) basis dependent.

By the isometry group of $c \in \mathrm{Qua}(V)$ we mean the subgroup of $\mathrm{GL}(V)$ consisting of all $\tau \in \mathrm{GL}(V)$ such that $c(\tau(v)) = c(v)$ for all $v \in V$. Note that the bilinear form $b(u, v) = c(u + v) - c(u) - c(v)$ associated with $c \in \mathrm{Qua}(V)$ is obviously symmetric. We define the kernel of a symmetric bilinear form b on V to be the subspace $\ker b = \{u \in V : b(u, v) = \text{ for all } v \in V\}$ of V. For any $c \in \mathrm{Qua}(V)$, upon letting b be the symmetric bilinear form on V associated with c, we define the kernel of c to be the subspace $\ker c = \{u \in \ker b : c(u) = 0\}$ of $\ker b$; the quadratic form c is said to be degenerate or singular according to whether $\ker b \neq 0$ or $\ker c \neq 0$.

In older literature, homogeneous linear polynomials (resp., homogeneous bilinear polynomials, homogeneous quadratic polynomials) in $k[X]$ (resp., in $k[X, X']$, $k[X]$) were called linear forms (resp., bilinear forms, quadratic forms); following current convention, their basis free incarnations, i.e., members of $\mathrm{Lin}(V)$ (resp., $\mathrm{Bil}(V)$, $\mathrm{Qua}(V)$) may be called linear forms (resp., bilinear forms, quadratic forms) on V, and the polynomials themselves may be called linear multiforms (resp., bilinear multiforms, quadratic multiforms).

3. Hermitian forms

Given an automorphism σ of k, let k' be the fixed field of σ. For any function $\alpha : V \to k$ let $\sigma\alpha : V \to k$ be the function such that $(\sigma\alpha)(v) = \sigma(\alpha(v))$ for all $v \in V$, and for any polynomial h in one or more variables with coefficients in k let σh be the polynomial in the same variable or variables obtained by applying σ to the coefficients of h. Let $\mathrm{Sem}(V)$ be the k-vector-space of all semilinear (with respect to σ) functions $\alpha : V \to k$, i.e., additive functions $\alpha : V \to k$ such that for

all $\lambda \in k$ and $v \in V$ we have $\alpha(\lambda v) = \sigma(\lambda)(v)$; members of $\mathrm{Sem}(V)$ may be called semilinear forms on V. Note that then

$$\alpha \mapsto h_\alpha(X) = h_\alpha(X_1, \ldots, X_d) = \sum \alpha(e_i) X_i$$

gives an isomorphism of $\mathrm{Sem}(V)$ onto the k-vector-space of all linear multiforms in $k[X]$, where h_α is characterized by the condition

$$\alpha(\sum x_i e_i) = h_\alpha(\sigma(x)) \text{ for all } x = (x_1, \ldots, x_d) \in k^d.$$

Let $\mathrm{Ses}(V)$ be the k-vector-space of all sesquilinear functions $b : V \times V \to k$, i.e., functions which are linear in the first variable and semilinear in the second variable; members of $\mathrm{Ses}(V)$ may be called sesquilinear forms on V. Note that then

$$b \mapsto h_b(X, X') = h_b(X_1, \ldots, X_d, X'_1, \ldots, X'_d) = \sum b(e_i, e_j) X_i X'_j$$

gives an isomorphism of $\mathrm{Ses}(V)$ onto the k-vector-space of all bilinear multiforms in $k[X, X']$, where h_b is characterized by the condition

$$b(\sum x_i e_i, \sum x'_j e_j) = h_b(x, x') \quad \text{for all } x = (x_1, \ldots, x_d) \text{ and } x' = (x'_1, \ldots, x'_d) \text{ in } k^d.$$

Henceforth, assume that σ is of order two. Note that then $\alpha \mapsto \sigma\alpha$ gives a k'-linear isomorphism of $\mathrm{Lin}(V)$ onto $\mathrm{Sem}(V)$ as well as a k'-linear isomorphism of $\mathrm{Sem}(V)$ onto $\mathrm{Lin}(V)$. Also note that, for any $\alpha \in \mathrm{Lin}(V) \cup \mathrm{Sem}(V)$ we have $h_{\sigma\alpha} = \sigma h_\alpha$. Finally, as in the previous section, we get sesquiproduct generation saying that, as a k-vector-space, $\mathrm{Ses}(V)$ is k-generated by sesquiproduct elements $\alpha(\sigma\beta)$ with α, β in $\mathrm{Lin}(V)$. Let $\mathrm{Her}(V)$ be the k'-vector-space of all hermitian functions $b : V \times V \to k$, i.e., left-linear biadditive functions which are hermitian-symmetric with respect to σ, where hermitian-symmetry means that for all u, v in V we have $b(v, u) = \sigma(b(u, v))$; members of $\mathrm{Her}(V)$ may be called hermitian forms on V. Note that $\mathrm{Her}(V)$ is a k'-subspace of $\mathrm{Ses}(V)$, and $b \mapsto h_b$ gives a k'-linear isomorphism of $\mathrm{Her}(V)$ onto the k'-vector-space of all hermitian multiforms over k, i.e., polynomials

$$h(X, X') = \sum b_{ij} X_i X'_j \quad \text{where } b_{ij} \in k \text{ with } b_{ji} = \sigma(b_{ij}).$$

For hermitian functions $b \in \mathrm{Her}(V)$ we have "diagonal determination," i.e., $b(u, v)$ is determined by its diagonal values $b(v, v)$; to see this, it suffices to show $b(v, v) \equiv 0 \Rightarrow b(u, v) \equiv 0$; so assuming $b(v, v) \equiv 0$, for all u, v in V and λ in k we have

$$\begin{aligned} 0 = b(u + \lambda v, u + \lambda v) &= b(u, u) + b(u, \lambda v) + b(\lambda v, u) \\ &\quad + b(v, v) = \sigma(\lambda) b(u, v) + \lambda \sigma(b(u, v)) \end{aligned}$$

and taking $\lambda = 1$ we get

$$\sigma(b(u, v)) = -b(u, v)$$

and hence for any $\lambda \in k$,

$$(\sigma(\lambda) - \lambda) b(u, v) = 0$$

and now taking $\lambda \in k \setminus k'$ we conclude that $b(u, v) = 0$. Actually this only settles the uniqueness part of "diagonal determination." In Note (3.1), we shall discuss the existence part for finite fields.

In the rest of this section assume that $k = \mathrm{GF}(q)$ where q is a square. Then upon letting $q' = q^{1/2}$ we have $k' = \mathrm{GF}(q')$, and for all $\lambda \in k$ we have $\sigma(\lambda) = \lambda^{q'}$. Also, let $k^\times = k \setminus \{0\}$.

Note (3.1). Given any hermitian form b on V, let $c(u) = b(u,u)$ for all $u \in V$. Now b is a bilinear form on V considered as a vector space over k' and so c is a quadratic form on V considered over k'. Moreover,

$$(*) \qquad c(\lambda u) = b(\lambda u, \lambda u) = \lambda^{q'+1} b(u,u) = \lambda^{q'+1} c(u)$$

for all $\lambda \in k$ and $u \in V$. This is precisely the condition for a quadratic form over k' to arise from a hermitian form over k. Indeed, if c is a quadratic form over V considered over k' such that for all $\lambda \in k$ and $u \in V$ we have $c(\lambda u) = \lambda^{q'+1} c(u)$, then b defined by

$$(**) \qquad b(x,y) = -\sum_{\alpha \in k^\times} \alpha^{-1} c(\alpha x + y)$$

is a hermitian form on V with $b(u,u) = c(u)$.

Namely, $(*)$ can be proved by frequent use of the following simple fact about finite fields:

$$(***) \qquad \sum_{\alpha \in k^\times} \alpha^i = \begin{cases} -1 & \text{if } q-1 \text{ divides } i, \\ 0 & \text{otherwise.} \end{cases}$$

To prove $(***)$ note that the elements of $k^\times$ are the roots of $Y^{q-1} - 1$. Since the coefficient of Y^i is 0 for $1 \le i \le q-2$, it follows that the elementary symmetric polynomials of degrees 1 to $q-2$ are all zero and therefore the power sums of degrees 1 to $q-2$ are all zero. The result for $i = 0$ is clear since $q - 1 = -1$ in k. The general result follows since $\alpha^{q-1} = 1$ for all $\alpha \in k^\times$.

To prove the second half of (3.1), let b be defined by $(**)$. Let $b'(x,y) = c(x+y) - c(x) - c(y)$ be the symmetric bilinear form associated with c. Then for $x, y \in V$ we have

$$\begin{aligned} b(x,y) &= -\sum_{\alpha \in k^\times} \alpha^{-1} c(\alpha x + y) = -\sum_{\alpha \in k^\times} \left[\alpha^{-1} c(\alpha x) + \alpha^{-1} b'(\alpha x, y) + \alpha^{-1} c(y)\right] \\ &= -\sum_{\alpha \in k^\times} \left[\alpha^{q'} c(x) + \alpha^{-1} b'(\alpha x, y) + \alpha^{-1} c(y)\right] = -\sum_{\alpha \in k^\times} \alpha^{-1} b'(\alpha x, y). \end{aligned}$$

It follows that b is bilinear over k'. Now for $\beta \in k^\times$ and $x, y \in V$ we have

$$b(\beta x, y) = -\sum_{\alpha \in k^\times} \alpha^{-1} c(\alpha\beta x + y) = -\beta \sum_{\alpha \in k^\times} (\alpha\beta)^{-1} c(\alpha\beta x + y) = \beta b(x,y)$$

and so b is linear (over k) in the first variable. Next, for any $x, y \in V$ we have

$$\begin{aligned} b(y,x) &= -\sum_{\alpha \in k^\times} \alpha^{-1} c(x + \alpha y) = -\sum_{\alpha \in k^\times} \alpha^{q'} c(\alpha^{-1} x + y) \\ &= -\sum_{\beta \in k^\times} (\beta^{-1})^{q'} c(\beta x + y) = b(x,y)^{q'} \end{aligned}$$

so that b is hermitian-symmetric and hence semilinear in the second variable. Finally, for any $x \in V$ we have

$$b(x,x) = -\sum_{\alpha \in k^\times} \alpha^{-1} c((\alpha+1)x) = -\sum_{\alpha \in k^\times} (\alpha^{q'} + \alpha^{q'-1} + 1 + \alpha^{-1}) c(x) = c(x).$$

This completes the proof of (3.1).

Next we note that

$$\alpha \mapsto \widetilde{h}_\alpha(X) = \widetilde{h}_\alpha(X_1, \dots, X_d) = \sum \alpha(e_i) X_i^{q'}$$

gives an isomorphism of $\mathrm{Sem}(V)$ onto the k-vector-space of all protosemilinear multiforms in $k[X]$, where $\widetilde{h}_\alpha$ is characterized by the condition

$$\alpha(\sum x_i e_i) = \widetilde{h}_\alpha(x) \quad \text{for all } x = (x_1, \dots, x_d) \text{ in } k^d$$

and where by a protosemilinear multiform we mean a polynomial

$$h(X) = \sum \alpha_i X_i^{q'} \quad \text{with } \alpha_i \in k.$$

Also

$$b \mapsto \widetilde{h}_b(X,Z) = \widetilde{h}_b(X_1, \dots, X_d, Z_1, \dots, Z_d) = \sum b(e_i, e_j) X_i Z_j^{q'}$$

gives an isomorphism of $\mathrm{Ses}(V)$ onto the k-vector-space of all protosesquilinear multiforms in $k[X,Z]$, where $\widetilde{h}_b$ is characterized by the condition

$$b(\sum x_i e_i, \sum z_j e_j) = \widetilde{h}_b(x,z) \quad \text{for all } x = (x_1, \dots, x_d) \text{ and } z = (z_1, \dots, z_d) \text{ in } k^d$$

and where by a protosesquilinear multiform we mean a polynomial

$$h(X,Z) = \sum b_{ij} X_i Z_j^{q'} \quad \text{with } b_{ij} \in k.$$

Moreover, $b \mapsto \widetilde{h}_b$ gives a k'-linear isomorphism of $\mathrm{Her}(V)$ onto the k'-vector-space of all protohermitian multiforms in $k[X]$, i.e., polynomials

$$h(X,Z) = \sum b_{ij} X_i Z_j^{q'} \quad \text{with } b_{ij} \in k \text{ and } b_{ji} = b_{ij}^{q'}.$$

By the isometry group of $b \in \mathrm{Her}(V)$ we mean the subgroup of $\mathrm{GL}(V)$ consisting of all $\tau \in \mathrm{GL}(V)$ such that $b(\tau(u), \tau(v)) = b(u,v)$ for all u, v in V. Moreover, $b \in \mathrm{Her}(V)$ is degenerate means for some $0 \neq u \in V$ we have $b(u,v) = 0$ for all $v \in V$.

4. Quadratic polynomials

Now assume that $k = \mathrm{GF}(q)$ where q need not be a square, and note that then $k \subset k_q \subset K \subset \overline{K}$. Also assume that $f_V(Y) \in K[Y]$, and $d > 0$. Henceforth, we may use (1.1) to (1.3) tacitly, and we may use q-linear polynomial as a synonym for vectorial q-polynomial.

Given any $0 \neq \alpha \in \mathrm{Lin}(V)$, upon letting $U = \ker \alpha$ we see that U is $(d-1)$-dimensional, and hence by linearity $\alpha(w)/f_U(w)$ is independent of $w \in V \setminus U$, and so we may define $g_\alpha(Y) = [\alpha(w)/f_U(w)] f_U(Y)$; in the case of $\alpha = 0$ let us put $g_\alpha(Y) = 0$. Now clearly

$$\alpha(v) = g_\alpha(v) \quad \text{for all } v \in V$$

and g_α can be characterized as the unique q-linear polynomial in $\overline{K}[Y]$ of q-degree $\leq d-1$ satisfying the above displayed equation. Note that $\alpha \mapsto g_\alpha$ gives a k-linear injection $\mathrm{Lin}(V) \to \overline{K}[Y]$ and it maps $\mathrm{Lin}(V) \setminus \{0\}$ onto the set of all q-linear separable polynomials $g(Y)$ in $K(V)[Y]$ of q-degree $d-1$ such that $g(V) \subset k$, i.e., such that $g(v) \in k$ for all $v \in V$.

In view of product generation, it follows that, given any $b \in \mathrm{Bil}(V)$, there exists a unique $g_b(Y,Z) \in \overline{K}[Y,Z]$ which is q-bilinear of q-bidegree $\leq (d-1, d-1)$ such that

$$b(u,v) = g_b(u,v) \quad \text{for all } u, v \text{ in } V$$

where by q-bilinear we mean g_b is of the form

$$g_b(Y,Z) = \sum b_{ij} Y^{q^i} Z^{q^j} \quad \text{with } b_{ij} \in \overline{K}$$

and by q-bidegree $\leq (d-1, d-1)$ we mean that $b_{ij} = 0$ if $i \geq d$ or $j \geq d$. Note that $b \mapsto g_b$ gives a k-linear injection $\mathrm{Bil}(V) \to \overline{K}[Y,Z]$ and it maps $\mathrm{Bil}(V)$ onto the set of all q-bilinear polynomials $g(Y,Z)$ in $K(V)[Y,Z]$ of q-bidegree $\leq (d-1, d-1)$ such that $g(V,V) \subset k$, i.e., such that $g(u,v) \in k$ for all u, v in V.

Now in view of bilinear generation we see that, given any quadratic function c on V, there exists a unique $\widehat{g}_c(Y) \in \overline{K}[Y]$ which is q-quadratic of q-quadegree $\leq d-1$ such that

$$c(v) = \widehat{g}_c(v) \quad \text{for all } v \in V$$

where by q-quadratic we mean $\widehat{g}_c$ is of the form

$$\widehat{g}_c(Y) = \sum c_{ij} Y^{q^i + q^j} \quad \text{with } c_{ij} \in \overline{K}$$

and by q-quadegree $\leq d-1$ we mean that $c_{ij} = 0$ if $i \geq d$ or $j \geq d$.

Note (4.1). Note that the uniqueness of $\widehat{g}_c$ follows by observing that if $\widehat{g}(Y)$ is any q-quadratic polynomial in $\overline{K}[Y]$ of q-quadegree $\leq d-1$, then the Y-degree of $\widehat{g}(Y)$ is $\leq q^d$ and the coefficient of Y in $\widehat{g}(Y)$ is zero and hence $\widehat{g}(Y) = 0 \Leftrightarrow \widehat{g}(Y)/f_V(Y) \in \overline{K}[Y] \Leftrightarrow \widehat{g}(V) = 0$, i.e., $\Leftrightarrow \widehat{g}(v) = 0$ for all $v \in V$. Also note that $c \mapsto \widehat{g}_c$ gives a k-linear injection $\mathrm{Qua}(V) \to \overline{K}[Y]$ and it maps $\mathrm{Qua}(V)$ onto the set of all q-quadratic polynomials $\widehat{g}(Y)$ in $K(V)[Y]$ of q-quadegree $\leq d-1$ such that $\widehat{g}(V) \subset k$, i.e., such that $\widehat{g}(v) \in k$ for all $v \in V$. Moreover, note that if $\widehat{g}(Y)$ is any q-quadratic polynomial in $K(V)[Y]$ of q-quadegree $\leq d-1$ with $\widehat{g}(V) \subset k$, then $\widehat{g}(Y) \in K[Y] \Leftrightarrow \widehat{g}(\tau(v)) = \widehat{g}(v)$ for all $v \in V$ and $\tau \in \mathrm{Gal}(f_V, K)$; this follows by observing that $\widehat{g}(v) = \tau(\widehat{g}(v)) = \tau(\widehat{g})(\tau(v))$ where $\tau(\widehat{g})$ is obtained by applying τ to the coefficients of $\widehat{g}$. Finally, note that for any $\widehat{g}(Y) \in \overline{K}[Y]$ we have $\widehat{g}(V) \subset k \Leftrightarrow [\widehat{g}^q(Y) - \widehat{g}(Y)]/f_V(Y) \in \overline{K}[Y]$.

5. Hermitian polynomials

Let the situation be as in the previous section, and assume that q is a square. Let $q' = q^{1/2}$, and let σ be the order-two automorphism of k given by $\sigma(\lambda) = \lambda^{q'}$ for all $\lambda \in k$. Note that now the fixed field of σ is $k' = \mathrm{GF}(q')$. From (3.1) and Section 4, we see that given any $b \in \mathrm{Her}(V)$, there exists a unique $\widetilde{g}_b(Y) \in \overline{K}[Y]$ which is q'-quadratic of q'-quadegree $\leq 2d-1$ such that

$$b(v,v) = \widetilde{g}_b(v) \quad \text{for all } v \in V.$$

Since $\widetilde{g}_b(Y)$ is q'-quadratic of q'-quadegree $\leq 2d-1$, we can write

$$\begin{aligned}\widetilde{g}_b(Y) &= \sum a_{ij}Y^{q^i+q^j} + \sum b_{ij}Y^{q^i+q'q^j} + \sum c_{ij}Y^{q'q^i+q'q^j}\\ &= A(Y)+B(Y)+C(Y)\end{aligned}$$

where $A(Y)$, $B(Y)$, $C(Y)$ in $\overline{K}[Y]$ have the exhibited expressions, and $a_{ij}=b_{ij}=c_{ij}=0$ whenever $i\geq d$ or $j\geq d$. We claim that $A(Y)=C(Y)=0$. To establish the claim, by (3.1) we have $\widetilde{g}_b(\lambda u)=\lambda^{q'+1}\widetilde{g}_b(u)$ for all $u\in V$ and $\lambda\in k$, and hence

$$\begin{aligned}0 &= \lambda^{q'+1}\widetilde{g}_b(v)-\widetilde{g}_b(\lambda v)\\ &= \lambda^{q'+1}A(v)+\lambda^{q'+1}B(v)+\lambda^{q'+1}C(v)-\lambda^2A(v)-\lambda^{q'+1}B(v)-\lambda^{2q'}C(v)\\ &= (\lambda^{q'-1}-1)\lambda^2A(v)-\lambda^{q'+1}(\lambda^{q'-1}-1)C(v)\end{aligned}$$

for all $v\in V$ and $\lambda\in k$. Therefore $A(v)=\lambda^{q'-1}C(v)$ for all $v\in V$ and $\lambda\in k\setminus k'$. As λ varies over $k\setminus k'$, $\lambda^{q'-1}$ takes q' different values and hence we see that $A(v)=C(v)=0$ for all $v\in V$. Now, since the Y-degrees of $A(Y)$ and $C(Y)$ are less than q^d, we conclude that $A(Y)=C(Y)=0$. This establishes the claim.

It follows that $\widetilde{g}_b$ is q-hermitian of q-herdegree $\leq d-1$ where by q-hermitian we mean $\widetilde{g}_b$ is of the form

$$\widetilde{g}_b(Y)=\sum b_{ij}Y^{q^i+q'q^j} \quad \text{with } b_{ij}\in\overline{K}$$

and by q-herdegree $\leq d-1$ we mean that $b_{ij}=0$ if either $i\geq d$ or $j\geq d$.

Note (5.1). Note that, in view of diagonal determination, the uniqueness of $\widetilde{g}_b$ also follows by observing that if $\widetilde{g}(Y)$ is any q-hermitian polynomial in $\overline{K}[Y]$ of q-herdegree $\leq d-1$, then the Y degree of $\widetilde{g}(Y)$ is $<q^d$ and hence $\widetilde{g}(Y)=0 \Leftrightarrow \widetilde{g}(Y)/f_V(Y)\in\overline{K}[Y] \Leftrightarrow g(V)=0$, i.e., $\Leftrightarrow \widetilde{g}(v)=0$ for all $v\in V$. Also note that $b\mapsto\widetilde{g}_b$ gives a k'-linear injection $\mathrm{Her}(V)\to\overline{K}[Y]$ and it maps $\mathrm{Her}(V)$ onto the set of all q-hermitian polynomials $\widetilde{g}(Y)$ in $K(V)[Y]$ of q-herdegree $\leq d-1$ such that $\widetilde{g}(V)\subset k'$, i.e., such that $\widetilde{g}(v)\in k'$ for all $v\in V$. Moreover, note that if $\widetilde{g}(Y)$ is any q-hermitian polynomial in $K(V)[Y]$ of q-herdegree $\leq d-1$ with $\widetilde{g}(V)\subset k'$, then $\widetilde{g}(Y)\in K[Y] \Leftrightarrow \widetilde{g}(t(v))=\widetilde{g}(v)$ for all $v\in V$ and $t\in\mathrm{Gal}(f_V,K)$; this follows by observing that $\widetilde{g}(v)=t(\widetilde{g}(v))=(t\widetilde{g})((t(v))$ where $(t\widetilde{g})(Y)\in K(V)[Y]$ is obtained by applying t to the coefficients of $\widetilde{g}(Y)$. Finally, note that for any $\widetilde{g}(Y)\in\overline{K}[Y]$ we have: $\widetilde{g}(V)\subset k' \Leftrightarrow [\widetilde{g}^{q'}(Y)-\widetilde{g}(Y)]/f_V(Y)\in\overline{K}[Y]$.

6. Forms and factorizations

We shall now apply (4.1) to find quadratic forms associated with the three vectorial polynomials $E^{\dagger\dagger}$, E°, E^{+}. So let

$$k=\mathrm{GF}(q)\subset k_q\subset k_q(X)=K\subset\overline{K}$$

and

$$\begin{aligned}A^{\dagger\dagger}(Y) &= Y^{q^{2m-2}}-Y \quad \text{and} \quad I^{\dagger\dagger}(Y)=Y^{q^{m-1}},\\ A^{\circ}(Y) &= Y^{q^{2m-1}}+Y \quad \text{and} \quad I^{\circ}(Y)=Y^{q^m}-Y^{q^{m-1}},\\ A^{+}(Y) &= Y^{q^{2m-2}}-Y^{q^{2m-3}}+Y^q-Y \quad \text{and} \quad I^{+}(Y)=Y^{q^{m-1}}.\end{aligned}$$

Also let

$$C^{\dagger\dagger}(Y) = X^{-1}A^{\dagger\dagger}(Y)^{q+1} + J^{\dagger\dagger}(Y)^q,$$
$$C^{\circ}(Y) = X^{-1}A^{\circ}(Y)^{q+1} + J^{\circ}(Y)^q,$$
$$C^{+}(Y) = X^{-1}A^{+}(Y)^{q+1} + J^{+}(Y)^q$$

where

$$J^{\dagger\dagger}(Y) = \sum_{0\le i\le m-2} Y^{q^{m-1+i}+q^i},$$
$$J^{\circ}(Y) = \sum_{0\le i\le m-1} Y^{q^{m-1+i}+q^i} - \sum_{0\le i\le m-2} Y^{q^{m+i}+q^i},$$
$$J^{+}(Y) = \sum_{0\le i\le m-2} Y^{q^{m-1+i}+q^i} - \sum_{1\le i\le m-2} Y^{q^{m-2+i}+q^i}.$$

Note that each term in the above summations evaluated at any $w \in k$ equals w^2, and the total number of terms in the two summations involved in J° is the odd integer $2m-1$, and hence (1*) if q is even, then $J^{\circ}(w) = w^2$ for all $w \in k$.

Now we have the following Quadratic Form Theorem.

Quadratic Form Theorem (6.1). *Let us put*

$$(E, A, I, J, C) = (E^{\dagger\dagger}, A^{\dagger\dagger}, I^{\dagger\dagger}, J^{\dagger\dagger}, C^{\dagger\dagger})$$

or $(E^{\circ}, A^{\circ}, I^{\circ}, J^{\circ}, C^{\circ})$ *or* $(E^{+}, A^{+}, I^{+}, J^{+}, C^{+})$ *with* $d = 2m \ge 6$ *or* $d = 2m+1 \ge 7$ *or* $d = 2m \ge 8$ *respectively. Then clearly* $A(Y) \in k[Y]$ *is separable monic* q*-linear of* q*-degree* $d-2$ *such that if* d *is odd, then* $A(Y) = Y^{q^{d-2}} + Y$, $I(Y) = Y^{q^{(d-2)/2}}$ *or* $Y^{q^{(d-1)/2}} - Y^{q^{(d-3)/2}}$ *according to whether* d *is even or odd, and* $J(Y) \in k[Y]$ *is* q*-quadratic of* q*-quadegree* $\le d-3$ *and* Y*-order (i.e., the highest power of* Y *dividing it)* $q^{m-1}+1$ *such that if* d *is odd and* q *is even, then* $J(w) = w^2$ *for all* $w \in k$. *Also clearly*

$$C(Y) = X^{-1}A(Y)^{q+1} + J(Y)^q \tag{6.1.1}$$

with

$$A(Y)I(Y) = J(Y)^q - J(Y) \tag{6.1.2}$$

and

$$E(Y) = A(Y)^{q^2} - X^{q-1}A(Y) + X^q I(Y)^q \tag{6.1.3}$$

and hence $C(Y) \in K[Y]$ *is* q*-quadratic of* q*-quadegree* $\le d-1$ *with*

$$X^{-q}A(Y)^q E(Y) = C(Y)^q - C(Y). \tag{6.1.4}$$

Therefore by (4.1) we see that $v \mapsto C(v)$ *gives a* k*-valued quadratic form* c *on* $V[E]$ *whose isometry group contains* $Gal(E, K)$. *Moreover, we claim that:*

(6.1.5) The quadratic form c *is nondegenerate except when* d *is odd and* q *is even, and in that case it is degenerate but nonsingular. More precisely, for the kernel* W *of the symmetric bilinear form* b *associated with* c *we have that if* d *is even or* q *is odd, then* $W = 0$, *whereas if* d *is odd and* q *is even, then* $W = k$ *and* $c(w) = w^2$ *for all* $w \in k$.

To establish the above claim let $B(Y,Z) = C(Y+Z) - C(Y) - C(Z)$. Then $B(Y,Z) \in K[Y,Z]$ is q-bilinear of q-bidegree $\leq (d-1, d-1)$, and for all u, v in V we have $B(u,v) = c(u+v) - c(u) - c(v) = b(u,v)$. Given any $u \in W$, we have $B(u,v) = 0$ for all $v \in V$ and hence $E(Z)$ divides $B(u,Z)$ in $K[Z]$. But $B(u,Z)$ has Z-degree at most q^{d-1}, whereas the Z-degree of $E(Z)$ is q^d. Therefore, $B(u,Z) = 0$. Now $A(Y+Z)^{q+1} - A(Y)^{q+1} - A(Z)^{q+1} = A(Y)^q A(Z) + A(Y)A(Z)^q$ and $A(Y)$ is monic q-linear of q-degree $d-2$; since $J(Y)$ is q-quadratic of q-quadegree $\leq d-3$, we see that there is no term $Z^{q^{d-1}}$ in $J(Y+Z)^q - J(Y) - J(Z)$ or $A(Y)^q A(Z)$; since $C(Y) = X^{-1}A(Y)^{q+1} + J(Y)^q$, we conclude that the coefficient of $Z^{q^{d-1}}$ in $B(u,Z)$ is $X^{-q}A(u)$ and hence $A(u) = 0$. Therefore, since $E(Y) = A(Y)^{q^2} - X^{q-1}A(Y) + X^q I(Y)^q$ and $E(u) = 0$, we get $I(u) = 0$. Hence by the condition on I we see that if d is even, then $u = 0$. Thus if d is even, then c is nondegerate. So assume that d is odd. Then $I(Y) = (Y^q - Y)^{q^{(d-3)/2}}$ and hence $u^q = u$ and therefore $u \in k$. Also, $0 = A(u) = u^{q^{d-2}} + u = u + u$ and thus if q is odd, then $u = 0$, and hence again c is nondegenerate. So also assume that q is even. Then, since $\dim_k(V)$ is odd and $(u,v) \mapsto B(u,v)$ is alternating, we must have $\dim_k(W) > 0$. Therefore, $W = k$ and $\dim_k(W) = 1$. Moreover, for all $w \in k$ we have $C(w) = X^{-1}A(w)^{q+1} + J(w)^q$ with $A(w) = 0$ and $J(w) = w^2$, and hence $c(w) = w^2$.

We shall now prove the following Factorization Theorem where, as notation, for any nonzero $P(Y)$ and $Q(Y)$ in $K[Y]$, by $\mathrm{GCD}(P(Y), Q(Y))$ we denote the monic generator of the ideal generated by $P(Y)$ and $Q(Y)$ in $K[Y]$; note that this is independent of the field K as long as it contains the coefficients of $P(Y)$ and $Q(Y)$; also note that a monic polynomial is a nonzero polynomial in which the highest degree coefficient is 1. As a preparation for the said theorem, we note that $I^\circ(Y) = (Y^q - Y)^{q^{m-1}}$, and by peeling off the initial term in the first summation involved in J° and then suitably pairing the remaining terms in the two summations we get

$$\begin{aligned} J^\circ(Y) &= Y^{q^{2m-2}+q^{m-1}} + \sum_{0 \leq i \leq m-2} (Y^{q^{m-1+i}+q^i} - Y^{q^{m+i}+q^i}) \\ &= Y^{q^{2m-2}+q^{m-1}} - \sum_{0 \leq i \leq m-2} Y^{q^i}(Y^q - Y)^{q^{m-1+i}} \end{aligned}$$

and hence: (2*) $I^\circ(Y) = (Y^q - Y)^{q^{m-1}}$ and $J^\circ(Y) = Y^{q^{2m-2}+q^{m-1}} - Y(Y^q - Y)^{q^{m-1}} - Y^q(Y^q - Y)^{q^m}\overline{J}^\circ(Y)$ where $\overline{J}^\circ(Y) \in k[Y]$ with $\overline{J}^\circ(0) = 1$. By (2*) we get: (3*) $\mathrm{GCD}(I^\circ(Y), J^\circ(Y)) = Y^{q^{m-1}}$. Note that $k^\times$ is the set of all nonzero elements of k, and $k^{\times 2}$ is the set of all squares in $k^\times$; also note that if q is even, then every $w \in k$ has a unique square root in k which we denote by $\sqrt{w}$. Now by expanding the first two terms of $J^\circ(Y)$ in (2*) around a value in k and noting that the remaining terms are divisible by very high powers of $(Y^q - Y)$, we see that: (4*) for any $w \in k^\times \setminus k^{\times 2}$ (i.e., for any nonzero nonsquare w in k) we have $\mathrm{GCD}(I^\circ(Y), J^\circ(Y) - w) = 1$; and (5*) if q is odd, then for any $z \in k^\times$ we have $\mathrm{GCD}(I^\circ(Y), J^\circ(Y) - z^2) = (Y^2 - z^2)^{q^{m-1}}$ and the $(Y \pm z)$-order of $J^\circ(Y) - z^2$ is q^{m-1}; and: (6*) if q is even, then for any $w \in k^\times$ we have $\mathrm{GCD}(I^\circ(Y), J^\circ(Y) - w) = (Y - \sqrt{w})^{q^{m-1}}$ and the $(Y - \sqrt{w})$-order of $J^\circ(Y) - w$ is $q^{m-1} + 1$.

We can alternatively deduce the above by noting that $I^\circ(Y) = (Y^q - Y)^{q^m-1}$ and $A^\circ(Y) = (Y^{q^{2m-1}} - Y) + 2Y$ so that $\mathrm{GCD}(A^\circ(Y), I^\circ(Y))$ is $Y^q - Y$ if q is even and is Y if q is odd. Therefore, for $z \in k$, the $(Y - z)$-order of $J^\circ(Y)^q - J^\circ(Y) = A^\circ(Y)I^\circ(Y)$ is $Y^{q^{m-1}} + 1$ if q is even or $z = 0$, and is $Y^{q^{m-1}}$ if q is odd and $z \neq 0$.

Factorization Theorem (6.2). *In the situation of (6.1), for every $w \in k$ let*

$$E_w(Y) = \prod_{v \in V[E] \text{ with } C(v)=w} (Y - v).$$

Then $E(Y) = \prod_{w\in k} E_w(Y)$ and the $E_w(Y)$ are pairwise coprime monic polynomials in Y over K such that, for every $w \in k$,

$$\begin{cases} E_w(Y) \in K[Y] \text{ is monic of } Y\text{-degree } > 1 \\ \text{and the splitting field of } E_w(y) \text{ over } K \text{ coincides} \\ \text{with the splitting field } K(V[E]) \text{ of } E(Y) \text{ over } K. \end{cases}$$

Then

$$E_w(Y) = GCD(E(Y), XC(Y) - wX)$$

and, noting that $A(Y)^{q+1} \in k[Y]$ is monic of Y-degree $(q+1)q^{d-2}$ which is greater than the Y-degree of $0 \neq (J(Y) - w)^q \in k[Y]$, and letting

$$P_w(Y) = A(Y)^{q+1}/R_w(Y) \quad \text{and} \quad Q_w(Y) = (J(Y) - w)^q/R_w(Y)$$

where

$$R_w(Y) = GCD(A(Y)^{q+1}, (J(Y) - w)^q) \in k[Y] \text{ is monic of } Y\text{-degree } \Delta_w$$

we have

$$XC(Y) - wX = R_w(Y)(P_w(Y) + XQ_w(Y))$$

where

$$\begin{cases} P_w(Y) + XQ_w(Y) \in K[Y] \text{ is monic of } Y\text{-degree } (q+1)q^{d-2} - \Delta_w, \\ \text{and } P_w(Y) \in k[Y] \text{ is monic of } Y\text{-degree } (q+1)q^{d-2} - \Delta_w, \\ \text{and } 0 \neq Q_w(Y) \in k[Y] \text{ is of } Y\text{-degree } < (q+1)q^{d-2} - \Delta_w. \end{cases}$$

Then

$$P_w(Y) + XQ_w(Y) \text{ is irreducible in } K[Y]$$

and finally, we have

$$E_w(Y) = \begin{cases} Y(P_w(Y) + XQ_w(Y)) \text{ if } w = 0, \\ P_w(Y) + XQ_w(Y) \text{ if } w \neq 0 \text{ and } d \text{ is even}, \\ P_w(Y) + XQ_w(Y) \text{ if } w \neq 0 \text{ and } q \text{ is odd}, \\ (Y - \sqrt{w})(P_w(Y) + XQ_w(Y)) \text{ if } d \text{ is odd and } q \text{ is even}. \end{cases}$$

Moreover, upon letting D_w be the Y-degree of $E(Y)$, we have the following:

If $d = 2m$ is even, then $D_0 = 1 + (q^m - 1)(q^{m-1} + 1)$ with $Q_0(Y) = Y^{q^m-1}$, and for all $w \in k^\times$ we have $D_w = q^{m-1}(q^m - 1)$ with $Q_w(Y) = 1 = 1 + P_w(0)$ and if q is odd, then $P_w(Y) = \widehat{P}_w(Y^2)$ with $\widehat{P}_w(Y) \in k[Y]$; whereas, if m is even and we are in the two-dagger case, then $P_w(Y) = \widetilde{P}_w(Y^{q+1})$ with $\widetilde{P}_w(Y) \in k[Y]$. Likewise if $d = 2m + 1$ is odd, then $D_0 = q^{2m}$ with $Q_0(Y) = Y^{q^m-1}$. Similarly, if $d = 2m + 1$ is odd and q is odd, then for all $w \in k^{\times 2}$ we have $D_w = q^m(q^m + 1)$

with $Q_w(Y) = (Y^2 - w)^{q^m}$, *and for all* $w \in k^\times \setminus k^{\times 2}$ *we have* $D_w = q^m(q^m - 1)$ *with* $Q_w(Y) = 1 = 1 + P_w(0)$ *and* $P_w(Y) = \widehat{P}_w(Y^2)$ *with* $\widehat{P}_w(Y) \in k[Y]$. *Finally, if* d *is odd and* q *is even, then for all* $w \in k^\times$ *we have* $D_w = q^{2m}$ *and* $Q_w(Y) = (Y - \sqrt{w})^{q^m - 1}$.

To prove this, for every $w \in k$ let

$$E_w(Y) = \prod_{v \in V[E] \text{ with } C(v) = w} (Y - v). \tag{6.2.1}$$

Then obviously

$$E(Y) = \prod_{w \in k} E_w(Y) \tag{6.2.2}$$

and

(6.2.3) the $E_w(Y)$ are pairwise coprime monic polynomials in Y over $\overline{K}$.

In view of the well-known fact that, in dimension greater than 2, the orthogonal group acts faithfully on each of its orbits on nonzero vectors, we see that, for every $w \in k$,

$$\begin{cases} E_w(Y) \in K[Y] \text{ is monic of } Y\text{-degree } > 1 \\ \text{and the splitting field of } E_w(Y) \text{ over } K \text{ coincides} \\ \text{with the splitting field } K(V[E]) \text{ of } E(Y) \text{ over } K. \end{cases} \tag{6.2.4}$$

By the Remainder Theorem of High School Algebra (which says that for any $F(Y)$ in $K[Y]$ and x, y, z in K with $x \neq 0$ we have $Y - y$ divides $xF(Y) - xz \Leftrightarrow F(y) = z$) we see that

$$E_w(Y) = \mathrm{GCD}(E(Y), XC(Y) - wX). \tag{6.2.5}$$

For every $w \in k$, since $w^q = w$, by (6.1.1) we also see that

$$XC(Y) - wX = A(Y)^{q+1} + (J(Y) - w)^q X$$

where $A(Y) \in k[Y]$ is separable monic q-linear of q-degree $d - 2$ and $J(Y) \in k[Y]$ is q-quadratic of q-quadegree $\leq d - 3$ and Y-order $q^{m-1} + 1$, and hence $A(Y)^{q+1} \in k[Y]$ is monic of Y-degree $(q + 1)q^{d-2}$ which is greater than the Y-degree of $0 \neq (J(Y) - w)^q \in k[Y]$, and therefore upon letting

$$P_w(Y) = A(Y)^{q+1}/R_w(Y) \quad \text{and} \quad Q_w(Y) = (J(Y) - w)^q/R_w(Y) \tag{6.2.6}$$

where

$$R_w(Y) = \mathrm{GCD}(A(Y)^{q+1}, (J(Y) - w)^q) \in k[Y] \text{ is monic of } Y\text{-degree } \Delta_w \tag{6.2.7}$$

we have

$$XC(Y) - wX = R_w(Y)(P_w(Y) + XQ_w(Y)) \tag{6.2.8}$$

where

$$\begin{cases} P_w(Y) + XQ_w(Y) \in K[Y] \text{ is monic of } Y\text{-degree } (q + 1)q^{d-2} - \Delta_w, \\ \text{and } P_w(Y) \in k[Y] \text{ is monic of } Y\text{-degree } (q + 1)q^{d-2} - \Delta_w, \\ \text{and } 0 \neq Q_w(Y) \in k[Y] \text{ is of } Y\text{-degree } < (q + 1)q^{d-2} - \Delta_w, \end{cases} \tag{6.2.9}$$

and by the Gauss Lemma we see that

$$P_w(Y) + XQ_w(Y) \text{ is irreducible in } K[Y]. \tag{6.2.10}$$

Henceforth, let D_w be the Y-degree of $E(Y)$.

For a moment assume that $d = 2m$ is even and $w = 0$. Then $I(Y) = Y^{q^{m-1}}$ and the Y-order of $J(Y)$ is $q^{m-1}+1$, and hence $\mathrm{GCD}(I(Y), J(Y)) = Y^{q^{m-1}}$. Therefore, since the Y-order of $A(Y)^{q+1}$ is $q+1$, by (6.1.2) and (6.2.7) we get $R_w(Y) = J(Y)^q/Y^{q^m-1}$. Clearly, the Y-degree of $J(Y)^q$ is $q^{2m-2}+q^{m-1}$, and hence $\Delta_w = q^{2m-2} - q^m + q^{m-1} + 1$. For any $0 \neq z \in \overline{k}$ with $R_w(z) = 0$ we have $I(z) \neq 0$ and hence by (6.1.3) we see that $Y - z$ does not divide $E(Y)$. Also, the Y-order of $E(Y)$ is 1. Therefore, $\mathrm{GCD}(E(Y), R_w(Y)) = Y$ and hence by (6.2.1) to (6.2.10) we get $E_w(Y) = Y(P_w(Y) + XQ_w(Y))$ with $D_w = 1 + (q^m - 1)(q^{m-1}+1)$ and $Q_w(Y) = Y^{q^m-1}$. Thus,

$$\text{(6.2.11)}\qquad \begin{cases} \text{if } d = 2m \text{ is even and } w = 0, \text{ then} \\ R_w(Y) = J(Y)^q/Y^{q^m-1} \text{ with } \Delta_w = q^{2m-2} - q^m + q^{m-1} + 1 \\ \text{and } E_w(Y) = Y(P_w(Y) + XQ_w(Y)) \\ \text{with } D_w = 1 + (q^m-1)(q^{m-1}+1) \text{ and } Q_w(Y) = Y^{q^m-1}. \end{cases}$$

Next for a moment assume that $d = 2m$ is even and $w \neq 0$. Then $I(Y) = Y^{q^{m-1}}$ and $J(0) = 0$, and hence $\mathrm{GCD}(I(Y), J(Y) - w) = 1$. Therefore, by (6.1.2) and (6.2.7) we get $R_w(Y) = (J(Y) - w)^q$. Clearly, the Y-degree of $(J(Y) - w)^q$ is $q^{2m-2} + q^{m-1}$ and hence $\Delta_w = q^{2m-2} + q^{m-1}$. For any $z \in \overline{k}$ with $R_w(z) = 0$ we have $z \neq 0$ and hence $I(z) \neq 0$ and therefore by (6.1.3) we see that $Y - z$ does not divide $E(Y)$. Consequently, $\mathrm{GCD}(E(Y), R_w(Y)) = 1$ and hence by (6.2.1) to (6.2.10) we get $E_w(Y) = P_w(Y) + XQ_w(Y)$. with $D_w = q^{m-1}(q^m - 1)$ and $Q_w(Y) = 1 = 1 + P_w(0)$. Upon letting $\overline{A}(Y) = A(Y)/Y$ we have $\overline{A}(Y) \in k[Y]$ with $A(Y) = Y\overline{A}(Y)$, and upon letting $\overline{P}_w(Y) = \overline{A}(Y)^{q+1}/(J(Y) - w)^q$ we have $\overline{P}_w(Y) \in k[Y]$ with $P_w(Y) = Y^{q+1}\overline{P}_w(Y)$. If q is odd, then $\overline{A}(Y)$ and $J(Y) - w$ belong to $k[Y^2]$ and hence so does $\overline{P}_w(Y)$ and therefore $P_w(Y) = \widehat{P}_w(Y^2)$ with $\widehat{P}_w(Y) \in k[Y]$. Likewise, if m is even and we are in the two-dagger case, then $\overline{A}(Y)$ and $J(Y) - w$ belong to $k[Y^{q+1}]$ and hence so does $\overline{P}_w(Y)$ and therefore $P_w(Y) = \widetilde{P}_w(Y^{q+1})$ with $\widetilde{P}_w(Y) \in k[Y]$. Thus,

$$\text{(6.2.12)}\qquad \begin{cases} \text{if } d = 2m \text{ is even and } w \neq 0, \text{ then} \\ R_w(Y) = (J(Y) - w)^q \text{ with } \Delta_w = q^{2m-2} + q^{m-1} \\ \text{and } E_w(Y) = P_w(Y) + XQ_w(Y) \\ \text{with } D_w = q^{m-1}(q^m - 1) \text{ and } Q_w(Y) = 1 = 1 + P_w(0), \\ \text{and if } q \text{ is odd, then } P_w(Y) = \widehat{P}_w(Y^2) \text{ with } \widehat{P}_w(Y) \in k[Y], \\ \text{whereas if } m \text{ is even and we are in the two-dagger case,} \\ \text{then } P_w(Y) = \widetilde{P}_w(Y^{q+1}) \text{ with } \widetilde{P}_w(Y) \in k[Y]. \end{cases}$$

Now for a moment assume that $d = 2m+1$ is odd and $w = 0$. Then in view of (3*) we see that $\mathrm{GCD}(I(Y), J(Y)) = Y^{q^{m-1}}$. Therefore, since the Y-order of $A(Y)^{q+1}$ is $q+1$ and the Y-order of $J(Y)^q$ is $q^m + q$, by (6.1.2) and (6.2.7) we get $R_w(Y) = J(Y)^q/Y^{q^m-1}$. Clearly, the Y-degree of $J(Y)^q$ is $q^{2m-1} + q^m$, and hence $\Delta_w = q^{2m-1} + 1$. Again in view of (3*), for any $0 \neq z \in \overline{k}$ with $R_w(z) = 0$ we have $I(z) \neq 0$ and hence by (6.1.3) we see that $Y - z$ does not divide $E(Y)$. Also, the Y-order of $E(Y)$ is 1. Therefore, $\mathrm{GCD}(E(Y), R_w(Y)) = Y$ and hence by (6.2.1) to (6.2.10) we get $E_w(Y) = Y(P_w(Y) + XQ_w(Y))$ with $D_w = q^{2m}$ and $Q_w = Y^{q^m-1}$.

Thus

$$\begin{cases} \text{if } d = 2m+1 \text{ is odd and } w = 0, \text{ then} \\ R_w(Y) = J(Y)^q / Y^{q^m-1} \text{ with } \Delta_w = q^{2m-1}+1 \\ \text{and } E_w(Y) = Y(P_w(Y) + XQ_w(Y)) \\ \text{with } D_w = q^{2m} \text{ and } Q_w = Y^{q^m-1}. \end{cases} \tag{6.2.13}$$

Next, for a moment assume that $d = 2m+1$ is odd and q is odd with $w \in k^{\times 2}$. Then by (5*) we see that $\mathrm{GCD}(I(Y), J(Y)-w) = (Y^2-w)^{q^{m-1}}$. Therefore, by (6.1.2) and (6.2.7) we get $R_w(Y) = (J(Y)-w)^q/(Y^2-w)^{q^m}$. Clearly, the Y-degree of $(J(Y)-w)^q$ is $q^{2m-1}+q^m$, and hence $\Delta_w = q^{2m-1}-q^m$. For any $z \in \overline{k}$ with $R_w(z) = 0$, by (5*) we have $I(z) \neq 0$, and therefore by (6.1.3) we see that $Y - z$ does not divide $E(Y)$. Consequently, $\mathrm{GCD}(E(Y), R_w(Y)) = 1$ and hence by (6.2.1) to (6.2.10) we get $E_w(Y) = P_w(Y) + XQ_w(Y)$ with $D_w = q^m(q^m+1)$ and $Q_w(Y) = (Y^2-w)^{q^m}$. Thus,

$$\begin{cases} \text{if } d = 2m+1 \text{ is odd and } q \text{ is odd with } w \in k^{\times 2}, \text{ then} \\ R_w(Y) = (J(Y)-w)^q/(Y^2-w)^{q^m} \text{ with } \Delta_w = q^{2m-1}-q^m \\ \text{and } E_w(Y) = P_w(Y) + XQ_w(Y) \\ \text{with } D_w = q^m(q^m+1) \text{ and } Q_w(Y) = (Y^2-w)^{q^m}. \end{cases} \tag{6.2.14}$$

Now for a moment assume that $d = 2m+1$ is odd and q is odd with $w \in k^\times \setminus k^{\times 2}$. Then by (4*) we see that $\mathrm{GCD}(I(Y), J(Y)-w) = 1$. Therefore, by (6.1.2) and (6.2.7) we get $R_w(Y) = (J(Y)-w)^q$. Clearly, the Y-degree of $(J(Y)-w)^q$ is $q^{2m-1}+q^m$, and hence $\Delta_w = q^{2m-1}+q^m$. For any $z \in \overline{k}$ with $R_w(z) = 0$, obviously we have $I(z) \neq 0$, and therefore by (6.1.3) we see that $Y - z$ does not divide $E(Y)$. Consequently, $\mathrm{GCD}(E(Y), R_w(Y)) = 1$ and hence by (6.2.1) to (6.2.10) we get $E_w(Y) = P_w(Y) + XQ_w(Y)$ with $D_w = q^m(q^m-1)$ and $Q_w(Y) = 1 = 1 + P_w(0)$. Upon letting $\overline{A}(Y) = A(Y)/Y$ we have $\overline{A}(Y) \in k[Y]$ with $A(Y) = Y\overline{A}(Y)$, and upon letting $\overline{P}_w(Y) = \overline{A}(Y)^{q+1}/(J(Y)-w)^q$ we have $\overline{P}_w(Y) \in k[Y]$ with $P_w(Y) = Y^{q+1}\overline{P}_w(Y)$. Now $\overline{A}(Y)$ and $J(Y)-w$ belong to $k[Y^2]$ and hence so does $\overline{P}_w(Y)$ and therefore $P_w(Y) = \widehat{P}_w(Y^2)$ with $\widehat{P}_w(Y) \in k[Y]$. Thus,

$$\begin{cases} \text{if } d = 2m+1 \text{ is odd and } q \text{ is odd with } w \in k^\times \setminus k^{\times 2}, \text{ then} \\ R_w(Y) = (J(Y)-w)^q \text{ with } \Delta_w = q^{2m-1}+q^m \\ \text{and } E_w(Y) = P_w(Y) + XQ_w(Y) \\ \text{with } D_w = q^m(q^m-1) \text{ and } Q_w(Y) = 1 = 1 + P_w(0) \\ \text{and } P_w(Y) = \widehat{P}_w(Y^2) \text{ with } \widehat{P}_w(Y) \in k[Y]. \end{cases} \tag{6.2.15}$$

Finally, for a moment assume that $d = 2m+1$ is odd and q is even with $w \in k^\times$. Then w has a unique square root in $k^\times$, and hence by (6*) we see that $\mathrm{GCD}(I(Y), J(Y)-w) = (Y-\sqrt{w})^{q^{m-1}}$. Therefore, by (6.1.2) and (6.2.7) we get $R_w(Y) = (J(Y)-w)^q/(Y-\sqrt{w})^{q^m-1}$. Clearly, the Y-degree of $(J(Y)-w)^q$ is $q^{2m-1}+q^m$, and hence $\Delta_w = q^{2m-1}+1$. By (6*) we see that $\mathrm{GCD}(I(Y), R_w(Y)) = (Y-\sqrt{w})^{q+1}$ and therefore by (6.1.3) we see that $\mathrm{GCD}(E(Y), R_w(Y)) = (Y-\sqrt{w})$ and hence by (6.2.1) to (6.2.10) we get $E_w(Y) = (Y-\sqrt{w})(P_w(Y) + XQ_w(Y))$

with $D_w = q^{2m}$ and $Q_w(Y) = (Y - \sqrt{w})^{q^m-1}$. Thus,

$$\text{(6.2.16)} \qquad \begin{cases} \text{if } d = 2m+1 \text{ is odd and } q \text{ is even with } w \in k^\times, \text{ then} \\ R_w(Y) = (J(Y) - w)^q/(Y - \sqrt{w})^{q^m-1} \text{ with } \Delta_w = q^{2m-1} + 1 \\ \text{and } E_w(Y) = (Y - \sqrt{w})(P_w(Y) + XQ_w(Y)) \\ \text{with } D_w = q^{2m} \text{ and } Q_w(Y) = (Y - \sqrt{w})^{q^m-1}. \end{cases}$$

This completes the proof of (6.2).

7. Galois groups

Again let

$$k = \mathrm{GF}(q) \subset k_q \subset K \subset \overline{K}$$

where in a moment we shall assume that $K = k_q(X)$. We shall now calculate the Galois groups of the vectorial polynomials $E^\ddagger$, $E^{\dagger\dagger}$, E°, E^+. To do this our polynomial manipulation material will be Theorems (6.1) and (6.2) of Section 6, and our group theory tools will be Liebeck's Theorem on orbit sizes of classical groups [Li2] and the Guralnick-Saxl Theorem on Strong Genus Zero Polynomials [GSa]. We shall also use Hering's Theorem as given by Liebeck in the Appendix of [Li1], and the criterion for the Galois group of a vectorial polynomial to be contained in SL or Ω given in [In1].

To review the definitions of orthogonal and unitary groups, let V be a vector space over k of finite dimension $d > 0$. Recall that $\mathrm{GL}(V) \lhd \Gamma\mathrm{L}(V) =$ the group of all semilinear transformations of V, and the center of $\mathrm{GL}(V)$ is the group $\mathrm{HL}(V)$ of all homotheties (scalar transformations) of V. Let $\Theta_V : \Gamma\mathrm{L}(V) \to \mathrm{P}\Gamma\mathrm{L}(V)$ be the canonical epimorphism with $\mathrm{P}\Gamma\mathrm{L}(V) = \Gamma\mathrm{L}(V)/\mathrm{HL}(V)$, and let $\mathrm{PGL}(V)$ and $\mathrm{PSL}(V)$ be the respective images of $\mathrm{GL}(V)$ and $\mathrm{SL}(V)$ under Θ_V.

Given a nonsingular quadratic form c on V, by $\mathrm{O}(V,c)$ we denote the isometry group of c, and we put $\mathrm{SO}(V,c) = \mathrm{O}(V,c) \cap \mathrm{SL}(V)$. Recall that if c is nondegenerate, then $\Omega(V,c)$ is a subgroup of index 2 in $\mathrm{SO}(V,c)$, that it is the kernel of the **spinor norm** if q is odd, and it is the kernel of the **Dickson invariant** if q is even; note also that $\Omega(V,c)$ is the commutator subgroup $\mathrm{O}'(V,c)$ of $\mathrm{O}(V,c)$ except when $(d,q) = (4,2)$ and the Witt index of c is 2; finally note that if c is degenerate, then $\Omega(V,c) = \mathrm{O}(V,c)$. (cf. [KLi], [Tay]). Moreover, we put $\Gamma\mathrm{O}(V,c) =$ the subgroup of $\Gamma\mathrm{L}(V)$ consisting of those $g \in \Gamma\mathrm{L}(V)$ for which there exists $\lambda \in k^\times$ and $\alpha \in \mathrm{Aut}(k)$ such that $c(g(v)) = \lambda\alpha(c(v))$ for all $v \in V$, and we put $\mathrm{GO}(V,c) =$ the subgroup of $\mathrm{GL}(V)$ consisting of those $g \in \mathrm{GL}(V)$ for which there exists $\lambda \in k^\times$ such that $c(g(v)) = \lambda c(v)$ for all $v \in V$, and we note that then $\mathrm{GO}(V,c) = \mathrm{GL}(V) \cap \Gamma\mathrm{O}(V,c)$; members of $\mathrm{GO}(V,c)$ are called c-similitudes, and members of $\Gamma\mathrm{O}(V,c)$ are called c-semisimilitudes; also we let $\mathrm{P}\Omega(V,c) \le \mathrm{PSO}(V,c) \le \mathrm{PO}(V,c) \le \mathrm{PGO}(V,c) \le \mathrm{P}\Gamma\mathrm{O}(V,c)$ be the respective images of $\Omega(V,c) \le \mathrm{SO}(V,c) \le \mathrm{O}(V,c) \le \mathrm{GO}(V,c) \le \Gamma\mathrm{O}(V,c)$ under Θ_V. Recall that the Witt index $\mathrm{witt}(c)$ of c is the maximum dimension of a c-singular subspace of V, i.e., a subspace $\overline{V}$ of V such that $c(v) = 0$ for all $v \in \overline{V}$; note that if d is odd, then $\mathrm{witt}(c) = (d/2) - (1/2)$, and if d is even, then $\mathrm{witt}(c) = d/2$ or $(d/2) - 1$. For odd d, up to isomorphism, $\mathrm{O}(V,c)$ is independent of c, and we denote $\Omega(V,c) \le \mathrm{SO}(V,c) \le \mathrm{O}(V,c) \le \mathrm{GO}(V,c) \le \Gamma\mathrm{O}(V,c)$ by $\Omega(d,q) \le \mathrm{SO}(d,q) \le \mathrm{O}(d,q) \le \mathrm{GO}(d,q) \le \Gamma\mathrm{O}(d,q)$ respectively. For even d,

there are two isomorphism classes of $\mathrm{O}(V,c)$ depending on whether $\mathrm{witt}(c) = d/2$ or $(d/2)-1$, and then we denote $\Omega(V,c) \leq \mathrm{SO}(V,c) \leq \mathrm{O}(V,c) \leq \mathrm{GO}(V,c) \leq \Gamma\mathrm{O}(V,c)$ and $\mathrm{P}\Omega(V,c) \leq \mathrm{PSO}(V,c) \leq \mathrm{PO}(V,c) \leq \mathrm{PGO}(V,c) \leq \mathrm{P}\Gamma\mathrm{O}(V,c)$ by $\Omega^+(d,q) \leq \mathrm{SO}^+(d,q) \leq \mathrm{O}^+(d,q) \leq \mathrm{GO}^+(d,q) \leq \Gamma\mathrm{O}^+(d,q)$ and $\mathrm{P}\Omega^+(d,q) \leq \mathrm{PSO}^+(d,q) \leq \mathrm{PO}^+(d,q) \leq \mathrm{PGO}^+(d,q) \leq \mathrm{P}\Gamma\mathrm{O}^+(d,q)$ or $\Omega^-(d,q) \leq \mathrm{SO}^-(d,q) \leq \mathrm{O}^-(d,q) \leq \mathrm{GO}^-(d,q) \leq \Gamma\mathrm{O}^-(d,q)$ and $\mathrm{P}\Omega^-(d,q) \leq \mathrm{PSO}^-(d,q) \leq \mathrm{PO}^-(d,q) \leq \mathrm{PGO}^-(d,q) \leq \mathrm{P}\Gamma\mathrm{O}^-(d,q)$ respectively.

Likewise, if $q = (q')^2$ where q' is a power of p, then, given a nondegenerate hermitian form b on V, by $U(V,b)$ we denote the isometry group of b, and we put $\mathrm{SU}(V,b) = \mathrm{U}(V,b) \cap \mathrm{SL}(V)$. Moreover, we put $\Gamma\mathrm{U}(V,b) =$ the subgroup of $\Gamma\mathrm{L}(V)$ consisting of those $g \in \Gamma\mathrm{L}(V)$ for which there exists $\lambda \in k^\times$ and $\alpha \in \mathrm{Aut}(k)$ such that $b(g(u),g(v)) = \lambda\alpha(b(u,v))$ for all u,v in V, and we put $\mathrm{GU}(V,b) =$ the subgroup of $\mathrm{GL}(V)$ consisting of those $g \in \mathrm{GL}(V)$ for which there exists $\lambda \in k^\times$ such that $b(g(u),g(v)) = \lambda b(u,v)$ for all u,v in V, and we note that then $\mathrm{GU}(V,b) = \mathrm{GL}(V) \cap \Gamma\mathrm{U}(V,b)$; members of $\mathrm{GU}(V,b)$ are called b-similitudes, and members of $\Gamma\mathrm{U}(V,b)$ are called b-semisimilitudes. Now $\mathrm{GU}(V,b) \lhd \Gamma\mathrm{U}(V,b)$ with $\Gamma\mathrm{U}(V,b)/\mathrm{GU}(V,b) = Z_u =$ a cyclic group of order u where $p^u = q$, and hence for every factor δ of u there is a unique $\Gamma\mathrm{U}_\delta(V,b)$ such that $\mathrm{GU}(V,b) \leq \Gamma\mathrm{U}_\delta(V,b) \leq \Gamma\mathrm{U}(V,b)$ and $[\Gamma\mathrm{U}_\delta(V,b) : \mathrm{GU}(V,b)] = \delta$; also we let $\mathrm{PSU}(V,b) \leq \mathrm{PU}(V,b) \leq \mathrm{PGU}(V,b) \leq \mathrm{P}\Gamma\mathrm{U}_\delta(V,b) \leq \mathrm{P}\Gamma\mathrm{U}(V,b)$ be the respective images of $\mathrm{SU}(V,b) \leq \mathrm{U}(V,b) \leq \mathrm{GU}(V,b) \leq \Gamma\mathrm{U}_\delta(V,b) \leq \Gamma\mathrm{U}(V,b)$ under Θ_V. Again, up to isomorphism, $\mathrm{U}(V,b)$ is independent of b, and we denote $\mathrm{SU}(V,b) \leq \mathrm{U}(V,b) \leq \mathrm{GU}(V,b) \leq \Gamma\mathrm{U}_\delta(V,b) \leq \Gamma\mathrm{U}(V,b)$ and $\mathrm{PSU}(V,b) \leq \mathrm{PU}(V,b) \leq \mathrm{PGU}(V,b) \leq \mathrm{P}\Gamma\mathrm{U}_\delta(V,b) \leq \mathrm{P}\Gamma\mathrm{U}(V,b)$ by $\mathrm{SU}(d,q') \leq \mathrm{U}(d,q') \leq \mathrm{GU}(d,q') \leq \Gamma\mathrm{U}_\delta(d,q') \leq \Gamma\mathrm{U}(d,q')$ and $\mathrm{PSU}(d,q') \leq \mathrm{PU}(d,q') \leq \mathrm{PGU}(d,q') \leq \mathrm{P}\Gamma\mathrm{U}_\delta(d,q') \leq \mathrm{P}\Gamma\mathrm{U}(d,q')$ respectively.

Given a vector space $\widetilde{V}$ over $\mathrm{GF}(q^2)$ of finite dimension $m > 0$, in a natural manner $\widetilde{V}$ can be regarded as a d-dimensional vector space V over k with $d = 2m$, and we call this V the **cognate** of $\widetilde{V}$, and we note that if we let $\Phi = \mathrm{HL}(\widetilde{V}) \cup \{0\} \cong \mathrm{GF}(q^2)$, then we have the normalizer and centralizer equations $\Gamma\mathrm{L}(\widetilde{V}) = N_{\Gamma\mathrm{L}(V)}(\Phi) \leq \Gamma\mathrm{L}(V)$ and $\mathrm{GL}(\widetilde{V}) = C_{\mathrm{GL}(V)}(\Phi) \leq \mathrm{GL}(V)$ and $\Gamma\mathrm{L}_2(\widetilde{V}) = N_{\mathrm{GL}(V)}(\Phi) = \Gamma\mathrm{L}(\widetilde{V}) \cap \mathrm{GL}(V) = GL(V)$ where $\Gamma\mathrm{L}_2(\widetilde{V})$ is the unique group such that $\mathrm{GL}(\widetilde{V}) \leq \Gamma\mathrm{L}_2(\widetilde{V}) \leq \Gamma\mathrm{L}(\widetilde{V})$ and $[\Gamma\mathrm{L}_2(\widetilde{V}) : \mathrm{GL}(\widetilde{V})] = 2$. Moreover, given any nondegenerate hermitian form $\widetilde{b}$ on $\widetilde{V}$, there is a unique nonsingular quadratic form c on V such that $c(v) = b(v,v)$ for all $v \in V$, and we call this c the **cognate** of $\widetilde{b}$. Conversely, given any vector space V over k of even finite dimension $d = 2m > 0$, in several ways we may regard V as an m-dimensional vector space $\widetilde{V}$ over $\mathrm{GF}(q^2)$ and we call such a $\widetilde{V}$ an **antecognate** of V, and we note that then V is the cognate of $\widetilde{V}$. Also note that now a nonsingular quadratic form c on V is the cognate of at most one nondegenerate hermitian form $\widetilde{b}$ on $\widetilde{V}$, and when such a $\widetilde{b}$ exists we call it a $\widetilde{V}$-**antecognate** of c. For example, if $E(Y) \in K[Y]$ is a monic separable q-linear polynomial of q-degree $d > 0$, then by (1.1) its root space $V[E]$ is a d-dimensional vector space over k and in a natural manner we have $\mathrm{Gal}(E,K) \leq \mathrm{GL}(V[E])$; moreover, if $d = 2m$ is even and E is q^2-linear with $\mathrm{GF}(q^2) \subset k_q$, then by (1.1) $V[E]$ has a **natural antecognate**, which we denote by $\widehat{V}[E]$, and now by (1.1) in a natural manner we have $\mathrm{Gal}(E,K) \leq \mathrm{GL}(\widehat{V}[E]) \leq \mathrm{GL}(V[E])$.

In his Orbit Size Theorem [Li2], Liebeck discusses subgroups of PGL and the orbit sizes of their action on the projective space, whereas our Theorem (6.2) provides information about subgroups of GL and the orbit sizes of their action on the vector space. Here are the relevant portions of the two versions of the Orbit Size Theorem, first extracts from Liebeck's original projective version and then the vectorial version in the form we need. In converting the projective to the vectorial version we shall use some material in Section 5 of [Ab4] and Section 5 of [Ab6]. Note that cases (a), (b), (c), (d) below are respectively subsumed in cases (a), (b), (b), (d) of Liebeck's Theorem in [Li2].

Extracts From Liebeck's Orbit Size Theorem (7.1). *Given any vector space V over k of finite dimension $d > 0$, and any $G \leq P\Gamma L(V)$, by looking at the sizes of the orbits of G on the associated projective space $\mathcal{P}(V)$ = the set of all 1-spaces in V, we have (7.1.a) to (7.1.d) where the number of orbits is two or three according to whether the listed orbit sizes are two or three.*

(7.1.a) If $d = 2m \geq 4$ is even with $q = (q')^2$ where q' is a power of p, and the orbit sizes are $(q^m - 1)((q')^{2m-1} + 1)/(q - 1)$ and $(q')^{2m-1}(q^m - 1)/(q' + 1)$, then $PSU(V, b) \triangleleft G$ for some nondegenerate hermitian form b on V.

(7.1.b) If $d = 2m \geq 8$ is even with m even, and the orbit sizes are

$$(q^m - 1)(q^{m-1} + 1)/(q - 1) \quad \textit{and} \quad q^{m-1}(q^m - 1)$$

or

$$(q^m - 1)(q^{m-1} + 1)/(q - 1) \quad \textit{and} \quad q^{m-1}(q^m - 1)/2$$

and

$$q^{m-1}(q^m - 1)/2$$

according to whether q is even or odd, then either (i) $P\Omega(V, c) \triangleleft G$ for some nonsingular quadratic form c on V with witt$(c) = m$, or (ii) $\Theta_V(U(\widetilde{V}, \widetilde{b})) \triangleleft G$ for some nondegenerate hermitian form $\widetilde{b}$ on some antecognate $\widetilde{V}$ of V, or (iii) $d = 8$ and G has a normal subgroup isomorphic to $\Omega(7, q)$.

(7.1.c) If $d = 2m \geq 8$ is even with m odd, and the orbit sizes are

$$(q^m - 1)(q^{m-1} + 1)/(q - 1) \quad \textit{and} \quad q^{m-1}(q^m - 1)$$

or

$$(q^m - 1)(q^{m-1} + 1)/(q - 1) \quad \textit{and} \quad q^{m-1}(q^m - 1)/2$$

and

$$q^{m-1}(q^m - 1)/2$$

according to whether q is even or odd, then $P\Omega(V, c) \triangleleft G$ for some nonsingular quadratic form c on V with witt$(c) = m$.

(7.1.d) If $d = 2m + 1 \geq 7$ is odd with q odd, and the orbit sizes are

$$(q^{2m} - 1)/(q - 1) \quad \textit{and} \quad q^m(q^m + 1)/2 \quad \textit{and} \quad q^m(q^m - 1)/2,$$

then either (i) $P\Omega(V, c) \triangleleft G$ for some nonsingular quadratic form c on V, or (ii) $d = 7$ and G has a normal subgroup isomorphic to $G_2(q)$ (which is the finite simple group discovered by Dickson).

Vectorial Orbit Size Theorem (7.2). *Given any monic separable vectorial q-polynomial $E(Y)$ of q-degree $d > 0$ in Y over K, and any nonsingular quadratic form c on $V[E]$ such that $Gal(E,K) \le O(V[E],c)$, when*

$$E_w(Y) = \prod_{v \in V[E] \text{ with } c(v)=w} (Y - v)$$

and D_w = the Y-degree of $E_w(Y)$ for every $w \in k$, assume that the polynomials $Y^{-1}E_0(Y)$ and $E_w(Y)$ for every $w \in k^\times$ are irreducible in $K[Y]$. Then we have (7.2.a)–(7.2.d).

(7.2.a) If $d = 2m \ge 8$ is even with m even, and E is q^2-linear with $GF(q^2) \subset k_q$, and $Gal(E,K) \le U(\widehat{V}[E],\widehat{b})$ for a $\widehat{V}[E]$-antecognate $\widehat{b}$ of c, and $D_0 = 1 + (q^m-1)(q^{m-1}+1)$ with $D_w = q^{m-1}(q^m-1)$ for all $w \in k^\times$, then $SU(\widehat{V},\widehat{b}) \lhd Gal(E,K)$.

(7.2.b) If $d = 2m \ge 8$ is even with m even, and $D_0 = 1+(q^m-1)(q^{m-1}+1)$ with $D_w = q^{m-1}(q^m-1)$ for every $w \in k^\times$, then either (i) $witt(c) = m$ and $\Omega(V[E],c) \lhd Gal(E,K)$, or (ii) $SU(\widetilde{V},\widetilde{b}) \lhd Gal(E,K)$ for some nondegenerate hermitian form $\widetilde{b}$ on some antecognate $\widetilde{V}$ of $V[E]$ and, for each $w \in k^\times$, $Gal(E,K)$ acts imprimitively on $F_w = \{v \in V[E] : c(v) = w\}$ with blocks of size $q+1$, or (iii) $d = 8$ and $\Theta_{V[E]}(Gal(E,K))$ has a normal subgroup isomorphic to $\Omega(7,q)$.

(7.2.c) If $d = 2m \ge 6$ is even with m odd, and $D_0 = 1+(q^m-1)(q^{m-1}+1)$ with $D_w = q^{m-1}(q^m-1)$ for every $w \in k^\times$, then $witt(c) = m$ and $\Omega(V[E],c) \lhd Gal(E,K)$.

(7.2.d) If $d = 2m+1 \ge 7$ is odd with q odd, and $D_0 = 1 + (q^{2m}-1)$ with $D_w = q^m(q^m \pm 1)$ for every $w \in k^\times$ according to whether $w \in k^{\times 2}$ or $w \notin k^{\times 2}$, then either (i) $\Omega(V[E],c) \lhd Gal(E,K)$, or (ii) $d = 7$ and $\Theta_{V[E]}(Gal(E,K))$ has a normal subgroup isomorphic to $G_2(q)$.

For deducing (7.2) from (7.1), we need the following three auxiliary lemmas.

Unitary Lemma (7.3). *Let V be a vector space over k of finite dimension $d > 2$. Assume that $q = (q')^2$ where q' is a power of p, and let b be a nondegenerate hermitian form on V. Then we have the following.*

(7.3.1) For any $H \le GL(V)$ we have

$$SU(V,b) \le H \Leftrightarrow PSU(V,b) \le \Theta_V(H),$$
$$H \le GU(V,b) \Leftrightarrow \Theta_V(H) \le PGU(V,b),$$
$$SU(V,b) \lhd H \Leftrightarrow SU(V,b) \le H \le GU(V,b),$$
$$PSU(V,b) \lhd \Theta_V(H) \Leftrightarrow PSU(V,b) \le \Theta_V(H) \le PGU(V,b).$$

(7.3.2) If $H \le U(V,b)$ is such that $SU(V,b') \le H$ for some nondegenerate hermitian form b' on V, then $U(V,b) = U(V,b')$ and $SU(V,b) = SU(V,b')$.

The four implications of (7.3.1) are proved in (5.1), (5.6), (5.2) and (5.4) of [Ab4] respectively. To prove (7.3.2), let $H \le \mathrm{U}(V,b)$ be such that $\mathrm{SU}(V,b') \le H$ for some nondegenerate hermitian form b' on V. Then $\mathrm{SU}(V,b') \le \mathrm{U}(V,b) \cap \mathrm{U}(V,b')$ and hence by (2.10.3) and (2.10.6) on pages 48-50 of [KLi] we get $\mathrm{U}(V,b) = \mathrm{U}(V,b')$ and $\mathrm{SU}(V,b) = \mathrm{SU}(V,b')$.

Orthogonal Lemma (7.4). *Let V be a vector space over k of finite dimension $d > 3$, and let c be a nondegenerate quadratic form on V. Then we have the following.*

(7.4.1) For any $H \leq GL(V)$ we have

$$\Omega(V,c) \leq H \Leftrightarrow P\Omega(V,c) \leq \Theta_V(H),$$
$$H \leq GO(V,c) \Leftrightarrow \Theta_V(H) \leq PGO(V,c),$$
$$\Omega(V,c) \lhd H \Leftrightarrow \Omega(V,c) \leq H \leq GO(V,c),$$
$$P\Omega(V,c) \lhd \Theta_V(H) \Leftrightarrow P\Omega(V,c) \leq \Theta_V(H) \leq PGO(V,c).$$

(7.4.2) If $H \leq O(V,c)$ is such that $\Omega(V,c') \leq H$ for some nondegenerate quadratic form c' on V, then $O(V,c) = O(V,c')$ and $\Omega(V,c) = \Omega(V,c')$ with witt(c) = witt(c').

The four implications of (7.4.1) are proved in (5.1), (5.6), (5.2) and (5.4) of [Ab6] respectively; although in [Ab6], d was assumed even, the argument given there applies when d is odd. To prove (7.4.2), let $H \leq \mathrm{O}(V,c)$ be such that $\Omega(V,c') \leq H$ for some nondegenerate quadratic form c' on V. Then $\Omega(V,c') \leq \mathrm{O}(V,c) \cap \mathrm{O}(V,c')$ and hence by (2.10.3) and (2.10.6) on pages 48-50 of [KLi] we get $\mathrm{O}(V,c) = \mathrm{O}(V,c')$ and $\Omega(V,c) = \Omega(V,c')$ with $\mathrm{witt}(c) = \mathrm{witt}(c')$.

Supplementary Unitary Lemma (7.5). *Let V be a vector space over k of even finite dimension $d = 2m > 4$, and let $\widetilde{b}$ be a nondegenerate hermitian form on an antecognate $\widetilde{V}$ of V. Then we have the following.*

(7.5.1) For any $H \leq GL(V)$ we have

$$SU(\widetilde{V},\widetilde{b}) \leq H \Leftrightarrow \Theta_V(SU(\widetilde{V},\widetilde{b})) \leq \Theta_V(H),$$
$$H \leq \Gamma U_2(\widetilde{V},\widetilde{b}) \Leftrightarrow \Theta_V(H) \leq \Theta_V(\Gamma U_2(\widetilde{V},\widetilde{b})),$$
$$SU(\widetilde{V},\widetilde{b}) \lhd H \Leftrightarrow SU(\widetilde{V},\widetilde{b}) \leq H \leq \Gamma U_2(\widetilde{V},\widetilde{b}),$$
$$\Theta_V(SU(\widetilde{V},\widetilde{b})) \lhd \Theta_V(H) \Leftrightarrow \Theta_V(SU(\widetilde{V},\widetilde{b})) \leq \Theta_V(H) \leq \Theta_V(\Gamma U_2(\widetilde{V},\widetilde{b})).$$

(7.5.2) If $w \in k^\times$ and $H \leq \Gamma L(\widetilde{V})$ are such that every $h \in H$ maps $\widetilde{F}_w = \{v \in V : \widetilde{b}(v,v) = w\}$ onto itself, then H acts imprimitively on $\widetilde{F}_w$ with blocks of size $q+1$.

(7.5.3) If for some nonsingular quadratic form c on V and some $H \leq O(V,c)$ we have $\Theta_V(SU(\widetilde{V},\widetilde{b})) \lhd \Theta_V(H)$, then, for every $w \in k^\times$, H acts imprimitively on $F_w = \{v \in V : c(v) = w\}$ with blocks of size $q+1$.

The proof of the first implication of (7.5.1) is completely parallel to the proofs of the first implications of (7.3.1) and (7.4.1). They all follow from the following **claim:** Let $\Theta : L \to \overline{L}$ be an epimorphism of finite groups such that $\ker\Theta$ is contained in the center $Z(L)$ of L, and (a given prime) p does not divide its size $|\ker\Theta|$. Also let S be a quasi-p subgroup of L (i.e., S is generated by p-power order elements), and let H be any subgroup of L. Then $S \leq H \Leftrightarrow \Theta(S) \leq \Theta(H)$ and $S \lhd H \Leftrightarrow \Theta(S) \lhd \Theta(H)$.

To apply the claim take Θ_V and $L = \mathrm{GL}(V)$, and in cases (7.3.1), (7.4.1), (7.5.1) take $S = \mathrm{SU}(V,b)$, $\Omega(V,c)$, $\mathrm{SU}(\widetilde{V},\widetilde{b})$ respectively. Also note that the quasi-p-ness of $\mathrm{SU}(V,b)$, and hence of $\mathrm{SU}(\widetilde{V},\widetilde{b})$, is indicated near (5.1) of [Ab4], and the quasi-p-ness of $\Omega(V,c)$ is indicated near (5.1) of [Ab6].

The "$\Rightarrow$" parts of the claim are obvious. Now suppose $\Theta(S) \leq \Theta(H)$. Take any p-power order element π in S. Then $\Theta(\pi)$ is p-power order. Also $\Theta(\pi) \in \Theta(S) \leq \Theta(H)$ and hence $\Theta(\pi) = \Theta(\pi')$ for some $\pi' \in H$. Since $\ker\Theta \leq Z(L)$ and $|\ker\Theta|$

is nondivisible by p, we get $\pi' = \alpha\pi$ for some $\alpha \in Z(L)$ such that the order μ of α is nondivisible by p. Now $\pi'^{\mu} = \pi^{\mu}$ and hence upon letting $\langle x\rangle$ denote subgroup generated by x we get $\pi \in \langle\pi\rangle = \langle\pi^{\mu}\rangle = \langle\pi'^{\mu}\rangle \leq H$. Since S is generated by such elements π, we conclude that $S \leq H$. Now suppose that $\Theta(S) \lhd \Theta(H)$. Then for every π as above, and every $h \in H$ we have that $\Theta(h)\Theta(\pi)\Theta(h^{-1})$ is a p-power order element in S; taking a Θ-preimage π^* of this in S we have $h\pi h^{-1} = \beta\pi^*$ for some $\beta \in \ker\Theta$; Since the order ν of β is prime to p, we get $h\pi^{\nu}h^{-1} = \pi^{*\nu} \in S$ and hence $h\pi h^{-1} \in h\langle\pi\rangle h^{-1} = h\langle\pi^{\nu}\rangle h^{-1} \leq S$. This being so for every such π, we conclude that $S \lhd H$.

The proof of the second implication is also completely parallel to the proofs of the second implications of (7.3.1) and (7.4.1). They all follow from the obvious facts that for any group epimorphism $\Theta : L \to \overline{L}$ and any subgroups H and G of L we have $H \leq G \Rightarrow \Theta(H) \leq \Theta(G)$, and if $\ker\Theta \leq G$, then $\Theta(H) \leq \Theta(G) \Rightarrow H \leq G$.

As in (7.3.1) and (7.4.1), our third implication is equivalent to the equation $N_L(S) = \Gamma\mathrm{U}_2(\widetilde{V}, \widetilde{b})$ for the normalizer $N_L(S)$ of $S = \mathrm{SU}(\widetilde{V}, \widetilde{b})$ in $L = \mathrm{GL}(V)$. To prove this normalizer equation, let $C_L(S)$ be the centralizer of S in L, and let us consider the endomorphism ring R of V over $\mathrm{GF}(q)$; note that R is naturally isomorphic to the ring of $2m$ by $2m$ matrices over $\mathrm{GF}(q)$, and L is the set of all units in R. By (2.10.2) on page 48 of [KLi] we see that $C_L(S)$ is the multiplicative group of all nonzero elements in an overfield Φ of $\Psi = \mathrm{HL}(V) \cup \{0\}$ in R whose field degree δ is a factor of $2m$. Clearly, $\mathrm{HL}(\widetilde{V}) \cup \{0\}$ is a subfield of Φ and its field degree over Ψ is 2, and hence $\delta = 2\epsilon$ for some integer $\epsilon > 0$. Now Φ is isomorphic to $\mathrm{GF}(q^{2\epsilon})$ and V can be regarded as an (m/ϵ)-dimensional vector space $\widetilde{V}_{\epsilon}$ over $\mathrm{GF}(q^{2\epsilon})$ and then we get $S \leq \mathrm{GL}(\widetilde{V}_{\epsilon})$. Therefore, $|S|$ divides $|\mathrm{GL}(\widetilde{V}_{\epsilon})|$. By order formulas, the highest powers of p which divide these orders are $q^{m(m-1)/2}$ and $q^{m((m/\epsilon)-1)}$ respectively, and hence $m(m-1)/2 \leq m((m/\epsilon)-1)$. Consequently, we must have $\epsilon = 1$. Therefore, $\Phi = \mathrm{HL}(\widetilde{V}) \cup \{0\}$ and hence upon letting $\Phi^{\times}$ be the multiplicative group of nonzero elements of Φ we get $C_L(S) = \Phi^{\times} = \mathrm{HL}(\widetilde{V})$.

To continue with the proof of the third implication, we get a homomorphism $\Lambda : N_L(\Phi^{\times}) \to \mathrm{Gal}(\Phi, \Psi)$ which sends every $h \in N_L(\Phi^{\times})$ to the conjugation map $x \mapsto hxh^{-1}$ with x varying in Φ. Clearly, $\ker\Lambda = C_L(\Phi^{\times}) = \mathrm{GL}(\widetilde{V})$. Let $y_1, \ldots, y_m$ be a $\mathrm{GF}(q^2)$-basis of $\widetilde{V}$ which is orthonormal relative to $\widetilde{b}$. Then we get an order two element τ in $\Gamma\mathrm{L}_2(\widetilde{V})$ which sends $a_1y_1 + \cdots + a_my_m$, with $a_1, \ldots, a_m$ varying in $\mathrm{GF}(q^2)$, to $a_1^q y_1 + \cdots + a_m^q y_m$. Clearly, τ generates $\Gamma\mathrm{L}_2(\widetilde{V})$ over the index two normal subgroup $\mathrm{GL}(\widetilde{V})$. Also, clearly $\tau \in N_L(\Phi^{\times})$. Since $|\mathrm{Gal}(\Phi, \Psi)| = 2$, we must have $N_L(\Phi^{\times}) = \Gamma\mathrm{L}_2(\widetilde{V})$. Again, τ generates $\Gamma\mathrm{U}_2(\widetilde{V}, \widetilde{b})$ over the index two normal subgroup $\mathrm{GU}(\widetilde{V}, \widetilde{b})$, and we easily see that $\tau \in N_L(S)$. Now $N_L(S) \leq N_L(C_L(S)) = N_L(\Phi^{\times}) = \Gamma\mathrm{L}_2(\widetilde{V})$ and every $g \in \Gamma\mathrm{L}_2(\widetilde{V})$ can be written as $g = h\tau^i$ with $h \in \mathrm{GL}(\widetilde{V})$ and $i = 0$ or 1. Moreover, $gSg^{-1} = h(\tau^i S\tau^{-i})h^{-1} = hSh^{-1}$, and hence by the third implication of (7.3.1) we see that $g \in N_L(S) \Leftrightarrow h \in \mathrm{GU}(\widetilde{V}, \widetilde{b})$. Thus we conclude that $N_L(S) = \Gamma\mathrm{U}_2(\widetilde{V}, \widetilde{b})$.

The fourth implication follows from the third exactly as in (7.3.1) and (7.4.1). Alternatively, it also follows from the second half of the claim and the first three implications.

To prove (7.5.2), let $w \in k^{\times}$ and $H \leq \Gamma\mathrm{L}(\widetilde{V})$ be such that every $h \in H$ maps $\widetilde{F}_w = \{v \in V : \widetilde{b}(v, v) = w\}$ onto itself. Fix a primitive (q^2-1)-th root ω of 1 in $\mathrm{GF}(q^2)$. Then $\omega^{(q-1)i}$ with $1 \leq i \leq q+1$ are exactly all the distinct elements of

$\mathrm{GF}(q^2)$ whose norm over $\mathrm{GF}(q)$ is 1. Define $u \sim v \Leftrightarrow u = \omega^{(q-1)i}v$ for some i with $1 \le i \le q+1$. This is an equivalence relation on $\widetilde{F}_w$. The equivalence classes under it are blocks of size $q+1$ for the said imprimitive action of H on $\widetilde{F}_w$.

Finally, to prove (7.5.3), let $H \le \mathrm{O}(V,c)$, where c is a nonsingular quadratic form on V, be such that $\Theta_V(\mathrm{SU}(\widetilde{V},\widetilde{b})) \lhd \Theta_V(H)$. Then by (7.5.1) we get $\mathrm{SU}(\widetilde{V},\widetilde{b})) \le H \le \Gamma\mathrm{U}_2(\widetilde{V},\widetilde{b})$. For every $w \in k$ let $F_w = \{v \in V \setminus \{0\} : c(v) = w\}$ and $\widetilde{F}_w = \{v \in V \setminus \{0\} : \widetilde{b}(v,v) = w\}$. By (2.10.5)(ii) on page 49 of [KLi], it follows that $(F_w)_{w\in k}$ and $(\widetilde{F}_{\widetilde{w}})_{\widetilde{w}\in k}$ are the respective orbits of $\mathrm{O}(V,c)$ and $\mathrm{U}(\widetilde{V},\widetilde{b})$ on $V\setminus\{0\}$ and, since $\mathrm{SU}(\widetilde{V},\widetilde{b}) \le H \le \mathrm{O}(V,c)$, we see that $(\widetilde{F}_{\widetilde{w}})_{\widetilde{w}\in k}$ is a subpartition of $(F_w)_{w\in k}$, i.e., each set F_w is the union of a certain number of sets $\widetilde{F}_{\widetilde{w}}$. Therefore, by the possible sizes of F_w and $\widetilde{F}_{\widetilde{w}}$ (which are well-known), we conclude that $F_0 = \widetilde{F}_0$ and $F_w = \widetilde{F}_{\sigma(w)}$ for all $w \in k^\times$ where σ is a permutation of $k^\times$. Now by (7.5.2) we see that, for every $w \in k^\times$, H acts imprimitively on $F_w = \{v \in V \setminus \{0\} : c(v) = w\}$ with blocks of size $q+1$.

This completes the proof of (7.5).

Remarks. (1) Note that in the three cases, i.e., in (7.3.1), (7.4.1), and (7.5.1), the second part of the claim (which we have proved directly) follows from the four implications of each case.

(2) An alternative approach to the first and the fourth implications of (7.5.1) would proceed via the following easy result. Let L be a finite group and M a normal subgroup of L contained in the center $Z(L)$ of L, and let S be an unsolvable subgroup of L with the property that all proper normal subgroups of S are contained in the center $Z(S)$ of S. Then for any subgroup H of L we have $S \le H \Leftrightarrow SM/M \le HM/M$ and $S \lhd H \Leftrightarrow SM/M \lhd HM/M$.

(3) The second part of the proof of the third implication of (7.5.1) which involves some explicit constructions may be replaced by a more conceptual argument. Namely, $N_L(S) \le N_L(C_L(S)) = N_L(\Phi^\times) = \Gamma\mathrm{L}_2(\widetilde{V})$ and hence $N_L(S) = N_{\Gamma\mathrm{L}_2(\widetilde{V})}(S)$. It only remains to show that $N_{\Gamma\mathrm{L}_2(\widetilde{V})}(S) = \Gamma\mathrm{U}_2(\widetilde{V})$ which is straightforward.

Now we turn to deducing (7.2) from (7.1). So let $E(Y) \in K[Y]$, d, c, $E_w(Y)$ and D_w be as in the preamble of (7.2). Also let $V = V[E]$, and for every $w \in k$ let $F_w = \{v \in V \setminus \{0\} : c(v) = w\}$. Then clearly F_w, as w varies in k, gives all the distinct orbits of $\mathrm{Gal}(E,K)$ on $V \setminus \{0\}$. Moreover, $|F_0| = D_0 - 1$, and $|F_w| = D_w$ for every $w \in k^\times$.

To prove (7.2.a), assume that $d = 2m \ge 8$ is even with m even, and E is q^2-linear with $\mathrm{GF}(q^2) \subset k_q$, and $\mathrm{Gal}(E,K) \le \mathrm{U}(\widehat{V},\widehat{b})$ for a $\widehat{V}$-antecognate $\widehat{b}$ of c where $\widehat{V} = \widehat{V}[E]$, and $D_0 = 1 + (q^m-1)(q^{m-1}+1)$ with $D_w = q^{m-1}(q^m-1)$ for every $w \in k^\times$. Let $\widehat{G} = \Theta_{\widehat{V}}(\widehat{H})$ with $\widehat{H} = \mathrm{Gal}(E,K)$. Then all the $\widehat{H}$-orbits F_w with w varying over $k^\times$ fuse into a single $\widehat{G}$-orbit in $\mathcal{P}(\widehat{V})$ and its size is $|\bigcup_{w\in k^\times} F_w|/(q^2-1) = (q-1)q^{m-1}(q^m-1)/(q^2-1) = q^{m-1}(q^m-1)/(q+1)$. The only other $\widehat{H}$-orbit in $\mathcal{P}(\widehat{V})$ is the projection of F_0 and its size is $|F_0|/(q^2-1) = (q^m-1)(q^{m-1}+1)/(q^2-1)$. Now by taking $(q',m,V,G) = (q,m/2,\widehat{V},\widehat{G})$ in (7.1.a) we conclude that $\Theta_{\widehat{V}}(\mathrm{SU}(\widehat{V},\widehat{b}'))\lhd\widehat{G}$ for some nondegenerate form $\widehat{b}'$ on $\widehat{V}$, and then by (7.3) we get $\mathrm{SU}(\widehat{V},\widehat{b}) \lhd \widehat{H}$.

Next, to prove (7.2.b), assume that $d = 2m \ge 8$ is even with m even, and $D_0 = 1 + (q^m-1)(q^{m-1}+1)$ with $D_w = q^{m-1}(q^m-1)$ for every $w \in k^\times$. Let

$G = \Theta_V(H)$ with $H = \mathrm{Gal}(E, K)$. Then, in case of q even, all the H-orbits F_w with w varying over $k^\times$ fuse into a single G-orbit in $\mathcal{P}(V)$ and its size is $|\bigcup_{w\in k^\times} F_w|/(q-1) = (q-1)q^{m-1}(q^m-1)/(q-1) = q^{m-1}(q^m-1)$ whereas, in case of q odd, all the H-orbits F_w with w varying over $k^{\times 2}$ fuse into a single G-orbit in $\mathcal{P}(V)$ and its size is $|\bigcup_{w\in k^{\times 2}} F_w|/(q-1) = (1/2)(q-1)q^{m-1}(q^m-1)/(q-1) = q^{m-1}(q^m-1)/2$, and all the H-orbits F_w with w varying over $k^\times \setminus k^{\times 2}$ also fuse into a single G-orbit in $\mathcal{P}(V)$ and its size is $|\bigcup_{w\in k^\times\setminus k^{\times 2}} F_w|/(q-1) = (1/2)(q-1)q^{m-1}(q^m-1)/(q-1) = q^{m-1}(q^m-1)/2$. The only other H-orbit in $\mathcal{P}(V)$ is the projection of F_0 and its size is $|F_0|/(q-1) = (q^m-1)(q^{m-1}+1)/(q-1)$. Now by (7.1.b) we conclude that either (i) $\mathrm{P}\Omega(V, c') \lhd G$ for some nonsingular quadratic form c' on V with $\mathrm{witt}(c') = m$, or (ii) $\Theta_V(U(\widetilde{V}, \widetilde{b})) \lhd G$ for some nondegenerate hermitian form $\widetilde{b}$ on some antecognate $\widetilde{V}$ of V, or (iii) $d = 8$ and G has a normal subgroup isomorphic to $\Omega(7, q)$. If (i), then by (7.4) we get $\Omega(V, c) \lhd H$ with $\mathrm{witt}(c) = m$. If (ii), then by (7.5.3) we see that, for each $w \in k^\times$, H acts imprimitively on F_w with blocks of size $q+1$. If (iii), then obviously $d = 8$ and $\Theta_V(H)$ has a normal subgroup isomorphic to $\Omega(7, q)$.

Now, to prove (7.2.c), assume that $d = 2m \geq 6$ is even with m odd, and $D_0 = 1+(q^m-1)(q^{m-1}+1)$ with $D_w = q^{m-1}(q^m-1)$ for every $w \in k^\times$. Let $G = \Theta_V(H)$ with $H = \mathrm{Gal}(E, K)$. Then, in case of q even, all the H-orbits F_w with w varying over $k^\times$ fuse into a single G-orbit in $\mathcal{P}(V)$ and its size is $|\bigcup_{w\in k^\times} F_w|/(q-1) = (q-1)q^{m-1}(q^m-1)/(q-1) = q^{m-1}(q^m-1)$ whereas, in case of q odd, all the H-orbits F_w with w varying over $k^{\times 2}$ fuse into a single G-orbit in $\mathcal{P}(V)$ and its size is $|\bigcup_{w\in k^{\times 2}} F_w|/(q-1) = (1/2)(q-1)q^{m-1}(q^m-1)/(q-1) = q^{m-1}(q^m-1)/2$, and all the H-orbits F_w with w varying over $k^\times \setminus k^{\times 2}$ also fuse into a single G-orbit in $\mathcal{P}(V)$ and its size is $|\bigcup_{w\in k^\times\setminus k^{\times 2}} F_w|/(q-1) = (1/2)(q-1)q^{m-1}(q^m-1)/(q-1) = q^{m-1}(q^m-1)/2$. The only other H-orbit in $\mathcal{P}(V)$ is the projection of F_0 and its size is $|F_0|/(q-1) = (q^m-1)(q^{m-1}+1)/(q-1)$. Now by (7.1.c) we conclude that $\mathrm{P}\Omega(V, c') \lhd G$ for some nonsingular quadratic form c' on V with $\mathrm{witt}(c') = m$, and then by (7.4) we get $\Omega(V, c) \lhd H$ with $\mathrm{witt}(c) = m$.

Finally, to prove (7.2.d), assume that $d = 2m+1 \geq 7$ is odd with q odd, and $D_0 = 1 + (q^{2m}-1)$ with $D_w = q^m(q^m \pm 1)$ for every $w \in k^\times$ according to whether $w \in k^{\times 2}$ or $w \notin k^{\times 2}$. Let $G = \Theta_V(H)$ with $H = \mathrm{Gal}(E, K)$. Then, all the H-orbits F_w with w varying over $k^{\times 2}$ fuse into a single G-orbit in $\mathcal{P}(V)$ and its size is $|\bigcup_{w\in k^{\times 2}} F_w|/(q-1) = (1/2)(q-1)q^m(q^m+1)/(q-1) = q^m(q^m+1)/2$, and all the H-orbits F_w with w varying over $k^\times \setminus k^{\times 2}$ also fuse into a single G-orbit in $\mathcal{P}(V)$ and its size is $|\bigcup_{w\in k^\times\setminus k^{\times 2}} F_w|/(q-1) = (1/2)(q-1)q^m(q^m-1)/(q-1) = q^m(q^m-1)/2$. The only other H-orbit in $\mathcal{P}(V)$ is the projection of F_0 and its size is $|F_0|/(q-1) = (q^{2m}-1)/(q-1)$. Now by (7.1.d) we conclude that either (i) $\mathrm{P}\Omega(V, c') \lhd G$ for some nonsingular quadratic form c' on V with $\mathrm{witt}(c') = m$, or (ii) $d = 7$ and G has a normal subgroup isomorphic to $G_2(q)$. If (i), then by (7.4) we get $\Omega(V, c) \lhd H$ with $\mathrm{witt}(c) = m$. If (ii), then obviously $d = 7$ and $\Theta_V(H)$ has a normal subgroup isomorphic to $G_2(q)$.

As said in the beginning of this section, we shall use the following SL and Ω criterion given in Corollaries 4.3 and 4.4 of [In1].

Criterion (7.6). *For any monic separable vectorial q-polynomial $E(Y)$ of q-degree $d > 0$ in Y over K we have the following.*

(7.6.1) Upon letting a be the coefficient of Y in $E(Y)$, the image of $Gal(E, K)$ under the determinant map $GL(V[E]) \to k^\times$ has order $(q-1)/l$ where l is the

largest divisor of $q-1$ for which $(-1)^d a$ is an l-th power in K. In particular, $Gal(E,K) \le SL(V[E]) \Leftrightarrow (-1)^d a$ is a $(q-1)$-th power in K.

(7.6.2) If q is odd and c is a nonsingular quadratic form on $V[E]$ such that $Gal(E,K) \le O(V[E],c)$, then by letting $E_w(Y) = \prod_{v\in V[E] \text{ with } c(v)=w}(Y-v)$ and $D_w =$ the Y-degree of $E_w(Y)$ for every $w \in k^\times$, we have $Gal(E,K) \le \Omega(V[E],c) \Leftrightarrow (-1)^{D_w/2}E_w(0) \in k^{\times 2}$ for all $w \in k^\times$.

Remark. We take this opportunity to point out that a statement in [In1] is incorrect: "G is a subgroup of the kernel of the spinor norm if and only if c_ϵ is a nonsquare in $\mathbb{F}_q$" should read "G is a subgroup of the kernel of the spinor norm if and only if c_ϵ is a *square* in $\mathbb{F}_q$" and the index $d/2$ in the definition of c_α appears as d.

We shall now prove the following corollary of (7.6.1), (7.6.2), (6.2.12), and (5.1).

Corollary (7.7). *In the situation of (6.1) with $K = k_q(X)$, upon letting c be the nonsingular quadratic form on $V[E]$ given by $v \mapsto C(v)$, we have the following.*

(7.7.1) $Gal(E,K) \le SL(V[E])$.

(7.7.2) If q is odd, then $Gal(E,K) \not\subset \Omega(V[E],c)$.

(7.7.3) If $d = 2m \ge 6$ is even and m is even with $E = E^+$, then the action of $Gal(E,K)$ on $F_1 = \{v \in V[E] : c(v) = 1\}$ cannot be imprimitive with blocks of size $q+1$.

(7.7.4) If $d = 2m \ge 8$ is even and m is even with $E = E^{\dagger\dagger}$ and $GF(q^2) \subset k_q$, then E is q^2-linear and there is a unique nondegenerate hermitian form $\widehat{b}$ on $\widehat{V}[E]$ such that $\widehat{b}(v) = c(v)$ for all $v \in \widehat{V}[E]$; (note that according to the terminology introduced at the beginning of this section, $\widehat{V}[E]$ is a natural antecognate of $V[E]$, and $\widehat{b}$ is a $\widehat{V}[E]$-antecognate of c). Moreover, $Gal(E,K) \le U(\widehat{V}[E],\widehat{b})$ and

$$[Gal(E,K) : Gal(E,K) \cap SU(\widehat{V}[E],\widehat{b})] = q+1 = [U(\widehat{V}[E],\widehat{b}) : SU(\widehat{V}[E],\widehat{b})].$$

Namely, (7.7.1) follows from (7.6.1) by noting that, by letting a be the coefficient of Y in $E(Y)$, we have $(-1)^d a = X^{q-1} =$ a $(q-1)$-th power in K.

Likewise, if q is odd, then (7.7.2) follows from (7.6.2) by noting that, if d is even, then, in view of (6.2.12), for every $w \in k^\times$ we have $(-1)^{D_w/2}E_w(0) = \pm X \notin k^{\times 2}$, and if d is odd, then, in view of (6.2.15), for every $w \in k^\times \setminus k^{\times 2}$ we have $(-1)^{D_w/2}E_w(0) = \pm X \notin k^{\times 2}$.

To prove (7.7.3) assume that $d = 2m \ge 6$ is even and m is even with $E = E^+$, and suppose if possible that the action of $\mathrm{Gal}(E,K)$ on $F_1 = \{v \in V[E] : c(v) = 1\}$ is imprimitive with blocks of size $q+1$. By (6.2.4), (6.2.6), (6.2.7), (6.2.12), the action of $\mathrm{Gal}(E,K)$ is faithful on the roots F_1 of $E_1(Y) = P_1(Y) + X$ where $P_1(Y) = A(Y)^{q+1}/(J(Y)-1)^q \in k[Y]$ is monic of degree $D_1 = q^{m-1}(q^m-1)$ with $A(Y) = Y^{q^{2m-2}} - Y^{q^{2m-3}} + Y^q - Y$ and $J(Y) = \sum_{0\le i\le m-2} Y^{q^{m-1+i}+q^i} - \sum_{1\le i\le m-2} Y^{q^{m-2+i}+q^i}$. In view of Lüroth's Theorem, the imprimitivity assumption says that $P_1(Y) = R(S(Y))$ where $S(Y) \in k[Y]$ and $R(Y) \in k[Y]$ are monic of degrees $q+1$ and $D_1/(q+1)$ respectively. Let prime denote Y-derivative. Then clearly

$$(\bullet) \qquad A'(Y) = -1 \text{ and } P_1(Y) = A(Y)[A(Y)/(J(Y)-1)]^q.$$

Therefore, $P_1'(Y) = A'(Y)[A(Y)/(J(Y)-1)]^q = -[A(Y)/(J(Y)-1)]^q$, and hence $P_1(Y) \in P_1'(Y)k[Y]$; since $P_1(Y) = R(S(Y))$, we also get $P_1'(Y) = R'(S(Y))S'(Y)$. Therefore, every root α of $S'(Y)$ (in the algebraic closure $\overline{k}$ of k) is a multiple root of $P_1(Y)$. Because of $(\bullet)$, the multiplicity of a root of $P_1(Y)$ is either 1 or

$q+1$. Therefore, any root α of $S'(Y)$ is a root of $P_1(Y)$ of multiplicity $q+1$. Let $\beta = S(\alpha)$. Then α is a multiple root of $S(Y)-\beta$, say of multiplicity $\mu > 1$, and β is a root of $R(Y)$ of multiplicity ν with $\mu\nu = q+1$. If $\nu > 1$, then any other root γ of $S(Y)-\beta$ must have multiplicity $q+1$ as a root of $P_1(Y)$ and multiplicity μ as a root of $S(Y)-\beta$, and hence $S(Y)-\beta$ would have ν roots $\alpha_1, \dots, \alpha_\nu$ of multiplicity μ and each would have multiplicity $\mu-1$ as a root of $S'(Y)$ (we know that μ is prime to q because μ divides $q+1$); this gives $(\mu-1)\nu$ roots of $S'(Y)$, which is more than half, but not all the roots; this leads to a contradiction. Therefore, $\nu = 1$ and hence $\mu = q+1$. Thus

$$(\bullet\bullet) \qquad S(Y) - \beta = (Y-\alpha)^{q+1}.$$

By $(\bullet)$ we see that $P_1(Y) = (J(Y)-1)[A(Y)/(J(Y)-1)]^{q+1}$ where the polynomial $J(Y)-1$ has no multiple roots and has no common root with $[A(Y)/(J(Y)-1)]^{q+1}$; since $P_1(Y) = R(S(Y))$, we can uniquely write $R(Y) = \widehat{R}(Y)\widehat{R}^*(Y)$ where $\widehat{R}(Y) \in \overline{k}[Y]$ with $\widehat{R}(\beta) \neq 0$ is monic having only simple roots (in $\overline{k}$), $\widehat{R}^*(Y) \in \overline{k}[Y]$ with $\widehat{R}^*(\beta) = 0$ has no simple root other than β, and the polynomials $\widehat{R}(Y)$ and $\widehat{R}^*(Y)$ have no common roots; by substituing $S(Y)$ for Y we get $P_1(Y) = \widehat{R}(S(Y))\widehat{R}^*(S(Y))$ and in view of $(\bullet\bullet)$ we see that $\widehat{R}(S(Y))$ has only simple roots and it has no common roots with $\widehat{R}^*(S(Y))$ which has only multiple roots; consequently, by uniqueness we must have

$$J(Y)-1 = \widehat{R}(S(Y)) \quad \text{and} \quad [A(Y)/(J(Y)-1)]^{q+1} = \widehat{R}^*(S(Y)).$$

Therefore, by $(\bullet\bullet)$ we see that

$$(\bullet\bullet\bullet) \qquad \begin{cases} J(Y+\alpha) = \widetilde{R}(Y^{q+1}) \text{ with} \\ \widetilde{R}(Y) \in \overline{k}[Y] \text{ monic of degree } (q^{2m-3}+q^{m-2})/(q+1). \end{cases}$$

Now $J(Y) = Y^{q^{2m-3}+q^{m-2}} - Y^{q^{2m-4}+q^{m-2}} + (\text{terms of degree} < q^{2m-4}+q^{m-2})$, and hence $J(Y+\alpha) = Y^{q^{2m-3}+q^{m-2}} + \alpha^{q^{m-2}}Y^{q^{2m-3}} - Y^{q^{2m-4}+q^{m-2}} + (\text{terms of degree} < q^{2m-4}+q^{m-2})$ where the three exhibited exponents of Y are all distinct, and out of them the first and the third (which have nonzero coefficients) cannot be simultaneously divisible by $q+1$; this contradicts $(\bullet\bullet\bullet)$.

To prove (7.7.4) assume that $d = 2m \geq 8$ is even and m is even with $E = E^{\dagger\dagger}$ and $\mathrm{GF}(q^2) \subset k_q$. Then $E(Y) \in K[Y]$ is q^2-linear of q^2-degree m and hence $V[E]$ has the structure of an m-dimensional vector space $\widehat{V}[E]$ over $\mathrm{GF}(q^2)$, and $C(Y)$ is easily seen to be q^2-hermitian of q^2-herdegree $\leq m-1$. Therefore, by (5.1) there is a unique hermitian form $\widehat{b}$ on $\widehat{V}[E]$ such that $\widehat{b}(v) = c(v)$ for all $v \in \widehat{V}[E]$. Since c is nondegerate, so is $\widehat{b}$. By (5.1) and (6.1) we also see that $\mathrm{Gal}(E,K) \leq U(\widehat{V}[E], \widehat{b})$. Since $(-1)^m a = X^{q-1}$, the largest divisor l of q^2-1 for which this is an l-th power in K is $q-1$. Consequently, by (7.6.1) we see that the image of $\mathrm{Gal}(E,K)$ under the determinant map of $\mathrm{GL}(\widehat{V}[E])$ onto the nonzero elements of $\mathrm{GF}(q^2)$ has order $q+1$. Therefore,

$$[\mathrm{Gal}(E,K) : \mathrm{Gal}(E,K) \cap \mathrm{SU}(\widehat{V}[E], \widehat{b})] = q+1 = [\mathrm{U}(\widehat{V}[E], \widehat{b}) : \mathrm{SU}(\widehat{V}[E], \widehat{b})]$$

where the last equality is well-known.

Finally, we are ready to prove our Main Theorem.

Main Theorem (7.8). *In the situation of (6.1) with $K = k_q(X)$, by letting c be the nonsingular quadratic form on $V[E]$ given by $v \mapsto C(v)$, we have the following.*

(7.8.1) If $d = 2m + 1 \geq 7$ is odd and q is odd with $E = E^{\circ}$, then E is almost strong genus zero and we have $Gal(E, K) = SO(V[E], c) = SO(2m + 1, q)$.

(7.8.2) If $d = 2m + 1 \geq 9$ is odd and q is even with $E = E^{\circ}$, then we have $Gal(E, K) = SO(V[E], c) = O(V[E], c) = O(2m + 1, q) = SO(2m + 1, q)$.

(7.8.3) If $d = 2m$ is even, with either $E = E^{\dagger\dagger}$ and $m > 2$ or $E = E^{+}$ and $m > 3$, then E is almost strong genus zero.

(7.8.4) If $d = 2m$ is even and m is odd, with either $E = E^{\dagger\dagger}$ and $m > 2$ or $E = E^{+}$ and $m > 3$, then $witt(c) = m$ and we have $Gal(E, K) = SO(V[E], c) = SO^{+}(2m, q)$, except that if q is even, then we may have $Gal(E, K) = \Omega(V[E], c) = \Omega^{+}(2m, q)$.

(7.8.5) If $d = 2m \geq 8$ is even and m is even with $E = E^{+}$, then $witt(c) = m$ and we have $Gal(E, K) = SO(V[E], c) = SO^{+}(2m, q)$, except that if q is even, then we may have $Gal(E, K) = \Omega(V[E], c) = \Omega^{+}(2m, q)$.

(7.8.6) If $d = 2m \geq 8$ is even and m is even with $E = E^{\dagger\dagger}$ and $GF(q^2) \subset k_q$, then E is q^2-linear and with $\widehat{V}[E]$ and $\widehat{b}$ as in (7.7.4) we have $Gal(E, K) = U(\widehat{V}, \widehat{b}) = U(m, q)$.

(7.8.7) If $d = 2m \geq 4$ is even with $E = E^{\ddagger}$ and $q = (q')^2$ where q' is a power of p as in Section 1, then E is almost strong genus zero and we have $Gal(E, K) = U(2m, q')$.

Briefly, in view of (6.1), (6.2) and (7.7), this follows by invoking the Vectorial (Version of Liebeck's) Orbit Size Theorem (7.2), the Guralnick-Saxl list of possible strong genus zero coverings [GSa], and Hering's Theorem as given in the Appendix of Liebeck [Li1]. In greater detail, tacitly using (6.1) and (6.2), we have the following.

Item (7.8.1) follows from (7.7.1)–(7.7.2) and case (7.2.d) of the Vectorial Orbit Size Theorem, with the clarification that because E is almost strong genus zero by (6.2.4) and (6.2.15), $G_2(q)$ is eliminated by Guralnick-Saxl [GSa]; see the remark below.

In the situation of (7.8.2), orbit sizes do not work, but $\mathrm{Gal}(E, K)$ acts transitively on the nonzero vectors in the quotient space $V[E]/W$ where $W = k$ as in (6.1), and so we may use Hering's Theorem (cf. Appendix of [Li1]), with the understanding that $G_2(q)$ is excluded by the assumption of $d \neq 7$.

Item (7.8.3) follows from (6.2.4) and (6.2.12).

Item (7.8.4) follows from (7.7.1)–(7.7.2) and case (7.2.c) of the Vectorial Orbit Size Theorem.

To prove (7.8.5) assume that $d = 2m \geq 8$ is even and m is even with $E = E^{+}$. Then by case (7.2.b) of the Vectorial Orbit Size Theorem we have either (i) $\mathrm{witt}(c) = m$ and $\Omega(V[E], c) \triangleleft \mathrm{Gal}(E, K)$, or (ii) $\mathrm{Gal}(E, K)$ acts imprimitively on $F_1 = \{v \in V[E] : c(v) = 1\}$ with blocks of size $q + 1$, or (iii) $d = 8$ and $\Theta_{V[E]}(\mathrm{Gal}(E, K))$ has a normal subgroup isomorphic to $\Omega(7, q)$. In view of (7.8.3), by the Guralnick-Saxl list [GSa] we see that (iii) cannot occur; see the remark below. Likewise, by (7.7.3) we see that (ii) cannot occur. Therefore, we must have (i). Now by (7.7.1) and (7.7.2) we see that $\mathrm{Gal}(E, K) = \mathrm{SO}(V[E], c) = \mathrm{SO}^{+}(2m, q)$, except that if q is even, then we may have $\mathrm{Gal}(E, K) = \Omega(V[E], c) = \Omega^{+}(2m, q)$.

To prove (7.8.6) assume that $d = 2m \geq 8$ is even and m is even with $E = E^{\dagger\dagger}$ and $\mathrm{GF}(q^2) \subset k_q$. Then clearly E is q^2-linear and by (7.7.4) we know that c has a $\widehat{V}[E]$-antecognate $\widehat{b}$ and for it we have $\mathrm{Gal}(E, K) \leq U(\widehat{V}[E], \widehat{b})$ and

$$[\mathrm{Gal}(E, K) : \mathrm{Gal}(E, K) \cap \mathrm{SU}(\widehat{V}[E], \widehat{b})] = q + 1 = [\mathrm{U}(\widehat{V}[E], \widehat{b}) : \mathrm{SU}(\widehat{V}[E], \widehat{b})].$$

Now by case (7.2.a) of the Vectorial Orbit Size Theorem we get $\mathrm{SU}(\widehat{V}[E], \widehat{b}) \triangleleft \mathrm{Gal}(E, K)$, and therefore we must have $\mathrm{Gal}(E, K) = U(\widehat{V}[E], \widehat{b})$.

Finally, as indicated in the Introduction, (7.8.7) follows from (7.8.3) and (7.8.6) simply by changing notation.

Remark. Guralnick and Saxl ([GSa]) consider Galois extensions $k(Y)$ over $k(X)$ where $f(Y) \in k[Y]$ is an indecomposable polynomial over a field k of characteristic p and $X = f(Y)$. They give permutation group theoretic conditions that the Galois group of $k(Y)$ over $k(X)$ must satisfy and then classify all finite primitive permutation groups satisfying these conditions. The list of possible groups includes precisely the unitary and orthogonal groups that are the focus of this paper ([GSa], Theorem 3.1 case (B)(i)). In our terminology the polynomial $f(Y) - X$ is strong genus zero.

To apply the Guralnick-Saxl Theorem we find it convenient to use the following: Let G be the Galois group of a strong genus zero polynomial $f(Y) - X$ of degree n over the field $k(X)$ where k is a field of characteristic p, and suppose that S is a non-abelian composition factor of G. Then there is an indecomposable polynomial $g(Y) \in k[Y]$ of degree dividing n such that S is a composition factor of the Galois group of the strong genus zero polynomial $g(Y) - X$ over $k(X)$.

In the case of $G_2(q)$ we note that no exceptional groups of Lie type occur in the Guralnick-Saxl list.

In the case of $O(7, q)$ we have a strong genus zero polynomial of degree $q^3(q^4 - 1)$. Now this group only occurs on the Guralnick-Saxl list in an action of degree $q^3(q^3 - 1)$ except when $q = 3$, when there is an additional action of degree 3159. Since $q^3(q^3 - 1)$ does not divide $q^3(q^4 - 1)$ and 3159 does not divide $3^3(3^4 - 1)$, we conclude that this case cannot occur.

References

[Ab1] S. S. Abhyankar, *Coverings of algebraic curves*, American Journal of Mathematics **79** (1957), 825-856. MR **20:**872

[Ab2] S. S. Abhyankar, *Galois theory on the line in nonzero characteristic*, Bulletin of the American Mathematical Society **27** (1992), 68-133. MR **94a:**12004

[Ab3] S. S. Abhyankar, *Nice equations for nice groups*, Israel Journal of Mathematics **88** (1994), 1-23. MR **96f:**12003

[Ab4] S. S. Abhyankar, *Again nice equations for nice groups*, Proceedings of the American Mathematical Society **124** (1996), 2967-2976. MR **96m:**12004

[Ab5] S. S. Abhyankar, *More nice equations for nice groups*, Proceedings of the American Mathematical Society **124** (1996), 2977-2991. MR **96m:**12005

[Ab6] S. S. Abhyankar, *Further nice equations for nice groups*, Transactions of the American Mathematical Society **348** (1996), 1555-1577. MR **96m:**14021

[Ab7] S. S. Abhyankar, *Factorizations over finite fields*, Finite Fields and Applications, London Mathematical Society Lecture Notes Series **233** (1996), 1-21. MR **98c:**11130

[Ab8] S. S. Abhyankar, *Projective polynomials*, Proceedings of the American Mathematical Society **125** (1997), 1643-1650. MR **98a:**12001

[Ab9] S. S. Abhyankar, *Galois theory of semilinear transformations*, Aspects of Galois Theory, London Mathematical Society Lecture Notes Series **256** (1999), 1-37. MR **2000j:**12008

[AL1] S. S. Abhyankar and P. A. Loomis, *Once more nice equation for nice groups*, Proceedings of the American Mathematical Society **126** (1998), 1885-1896. MR **98k:**12003

[AL2] S. S. Abhyankar and P. A. Loomis, *Twice more nice equations for nice groups*, Contemp. Math., 256, Amer. Math. Soc., 1999, 63–76. CMP 2000:09

[CKa] P. J. Cameron and W. M. Kantor, *2-Transitive and antiflag transitive collineation groups of finite projective spaces*, Journal of Algebra **60** (1979), 384-422. MR **81c:**20032

[GSa] R. M. Guralnick and J. Saxl, *Monodromy groups of polynomials*, Groups of Lie Type and Their Geometries (W. M. Kantor and L. Di Martino, eds.), Cambridge University Press (1995), 125-150. MR **96b:**20003

[Har] D. Harbater, *Abhyankar's conjecture on Galois groups over curves*, Inventiones Mathematicae **117** (1994), 1-25. MR **95i:**14029

[In1] N. F. J. Inglis, *Linear characters of finite linear groups*, Journal of Algebra **214** (1999), 545-552. MR **2000c:**20065

[In2] N. F. J. Inglis, *Symplectic groups as Galois groups*, Journal of Algebra, **227** (2000), 499–503. CMP 2000:13

[Kan] W. M. Kantor, *Rank 3 characterizations of classical geometries*, Journal of Algebra **36** (1975), 309-313. MR **52:**8229

[KLi] P. B. Kleidman and M. W. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, Cambridge University Press, 1990. MR **91g:**20001

[Li1] M. W. Liebeck, *The affine permutation groups of rank three*, Proceedings of the London Mathematical Society **54** (1987), 477-516. MR **88m:**20004

[Li2] M. W. Liebeck, *Characterization of classical groups by orbit sizes on the natural module*, Proceedings of the American Mathematical Society **124** (1996), 2961-2966. MR **97e:**20068

[Ray] M. Raynaud, *Revêtment de la droit affine en charactéristic $p > 0$ et conjecture d'Abhyankar*, Inventiones Mathematicae **116** (1994), 425-462. MR **94m:**14034

[Tay] D. E. Taylor, *The Geometry of the Classical Groups*, Heldermann Verlag, Berlin, 1992. MR **94d:**20028

Department of Mathematics, Purdue University, West Lafayette, Indiana 47907
E-mail address: ram@cs.purdue.edu

Department of Mathematics and Statistics, Sultan Qaboos University, P.O. Box 36, Al-Khod, Postal Code 123, Sultanate of Oman
E-mail address: ninglis@squ.edu.om