DE GRUYTER
OPEN

DEMONSTRATIO MATHEMATICA
Vol. 49 No 2 2016

Sara Arias-de-Reyna, Luis Dieulefait, Gabor Wiese

CLASSIFICATION OF SUBGROUPS OF SYMPLECTIC GROUPS OVER FINITE FIELDS CONTAINING A TRANSVECTION

Communicated by J. Smith

Abstract. In this note, we give a self-contained proof of the following classification (up to conjugation) of finite subgroups of $\mathrm{GSp}_n(\overline{\mathbb{F}}_\ell)$ containing a nontrivial transvection for $\ell \geq 5$, which can be derived from work of Kantor: G is either reducible, symplectically imprimitive or it contains $\mathrm{Sp}_n(\mathbb{F}_\ell)$. This result is for instance useful for proving 'big image' results for symplectic Galois representations.

1. Introduction

In this paper, we provide a self-contained proof of a classification result of subgroups of the general symplectic group over a finite field of characteristic $\ell \geq 5$ that contain a nontrivial transvection (cf. Theorem 1.1 below).

The motivation for this work came originally from Galois representations attached to automorphic forms and the applications to the inverse Galois problem. In a series of papers, we prove that for any even positive integer n and any positive integer d, $\mathrm{PSp}_n(\mathbb{F}_{\ell^d})$ or $\mathrm{PGSp}_n(\mathbb{F}_{\ell^d})$ occurs as a Galois group over the rational numbers for a positive density set of primes ℓ (cf. [2], [3], [1]). A key ingredient in our proof is Theorem 1.1. When we were working on this project, we were not aware that this result could be obtained as a particular case of some results of Kantor [6], hence we worked out a complete proof, inspired by the work of Mitchell on the classification of subgroups of classical groups. More precisely, in an attempt to generalise Theorem 1 of [9] to arbitrary dimension, one of us (S. A.-d.-R.) came up with a precise strategy for Theorem 1.1. Several ideas and some notation are borrowed from [7].

2010 *Mathematics Subject Classification*: 20G14.
Key words and phrases: sympletic group over a finite field, transvection, classification of subgroups of linear groups.

DOI: 10.1515/dema-2016-0012
© Copyright by Faculty of Mathematics and Information Science, Warsaw University of Technology
Brought to you by | Biblioteca de la Universidad de Sevilla
Authenticated
Download Date | 10/13/16 7:54 AM

We believe that our proof of Theorem 1.1 can be of independent interest, since it is self-contained and does not require any previous knowledge on linear algebraic groups beyond the basics.

In order to fix terminology, we recall some standard definitions. Let K be a field. An n-dimensional K-vector space V equipped with a symplectic form (i.e. nonsingular and alternating), denoted by $\langle v, w\rangle = v \bullet w$ for $v, w \in V$, is called a *symplectic K-space*. A K-subspace $W \subseteq V$ is called a *symplectic K-subspace* if the restriction of $\langle v, w\rangle$ to $W \times W$ is nonsingular (hence, symplectic). The *general symplectic group* $\mathrm{GSp}(V, \langle\cdot,\cdot\rangle) =: \mathrm{GSp}(V)$ consists of those $A \in \mathrm{GL}(V)$ for which, there is $\alpha \in K^\times$, the *multiplier* (or *similitude factor*) of A, such that $(Av) \bullet (Aw) = \alpha(v \bullet w)$ for all $v, w \in V$. The multiplier of A is denoted by $m(A)$. The *symplectic group* $\mathrm{Sp}(V, \langle\cdot,\cdot\rangle) =: \mathrm{Sp}(V)$ is the subgroup of $\mathrm{GSp}(V)$ of elements with multiplier 1. An element $\tau \in \mathrm{GL}(V)$ is a *transvection* if $\tau - \mathrm{id}_V$ has rank 1, i.e. if τ fixes a hyperplane pointwisely, and there is a line U such that $\tau(v) - v \in U$ for all $v \in V$. The fixed hyperplane is called the *axis* of τ and the line U is the *centre* (or the *direction*). We will consider the identity as a "trivial transvection". Any transvection has determinant 1. A *symplectic transvection* is a transvection in $\mathrm{Sp}(V)$. Any symplectic transvection has the form

$$T_v[\lambda] \in \mathrm{Sp}(V) : u \mapsto u + \lambda\langle u, v\rangle v$$

with *direction vector* $v \in V$ and *parameter* $\lambda \in K$ (see e.g. [4], pp. 137–138).

The main classification result of this note follows. A short proof, deriving it from [6], is contained in [3].

Theorem 1.1. *Let K be a finite field of characteristic at least 5 and V a symplectic K-vector space of dimension n. Then any subgroup G of $\mathrm{GSp}(V)$ which contains a nontrivial symplectic transvection satisfies one of the following assertions:*

1. *There is a proper K-subspace $S \subset V$ such that $G(S) = S$.*
2. *There are nonsingular symplectic K-subspaces $S_i \subset V$ with $i = 1, \dots, h$ of dimension m for some $m < n$ such that $V = \bigoplus_{i=1}^h S_i$ and for all $g \in G$ there is a permutation $\sigma_g \in \mathrm{Sym}_h$ (the symmetric group on $\{1, \dots, h\}$) with $g(S_i) = S_{\sigma_g(i)}$. Moreover, the action of G on the set $\{S_1, \dots, S_h\}$ thus defined is transitive.*
3. *There is a subfield L of K such that the subgroup generated by the symplectic transvections of G is conjugated (in $\mathrm{GSp}(V)$) to $\mathrm{Sp}_n(L)$.*

2. Symplectic transvections in subgroups

Recall that the full symplectic group is generated by all its transvections. The main idea in this part is to identify the subgroups of the general symplectic

Brought to you by | Biblioteca de la Universidad de Sevilla
Authenticated
Download Date | 10/13/16 7:54 AM

group containing a transvection by the centres of the transvections in the subgroup.

Let K be a finite field of characteristic ℓ and let V be a symplectic K-vector space of dimension n. Let G be a subgroup of $\mathrm{GSp}(V)$. The main difficulty in this part stems from the fact that K need not be a prime field, whence the set of direction vectors of the transvections contained in G need not be a K-vector space. Suppose, for example, that we want to deal with the subgroup $G = \mathrm{Sp}_n(L)$ of $\mathrm{Sp}_n(K)$ with L a subfield of K. Then the directions of the transvections of G form the L-vector space L^n contained in K^n. This is what we have in mind when we introduce the term (L, G)-rational subspace below. In order to do so, we set up some more notation.

Write $\mathcal{L}(G)$ for the set of $0 \neq v \in V$ such that $T_v[\lambda] \in G$ for some $\lambda \in K$. More naturally, this set should be considered as a subset of $\mathbb{P}(V)$, the projective space consisting of the lines in V. We call it the *set of centres (or directions) of the symplectic transvections in* G. For a given nonzero vector $v \in V$, define the *parameter group of direction* v *in* G as

$$\mathcal{P}_v(G) := \{\lambda \in K \mid T_v[\lambda] \in G\}.$$

The fact that $T_v[\mu] \circ T_v[\lambda] = T_v[\mu + \lambda]$ shows that $\mathcal{P}_v(G)$ is a subgroup of the additive group of K. If K is a finite field of characteristic ℓ, then $\mathcal{P}_v(G)$ is a finite direct product of copies of $\mathbb{Z}/\ell\mathbb{Z}$. Denote the number of factors by $\mathrm{rk}_v(G)$. Because $\mathcal{P}_{\lambda v}(G) = \frac{1}{\lambda^2}\mathcal{P}_v(G)$ for $\lambda \in K^\times$, it only depends on the centre $U := \langle v \rangle_K \in \mathcal{L}(G) \subseteq \mathbb{P}(V)$, and we call it the *rank of* U *in* G, although we will not make use of this in our argument.

We find it useful to consider the surjective map

$$\Phi : V \times K \xrightarrow{(v,\lambda)\mapsto T_v[\lambda]} \{\text{symplectic transvections in } \mathrm{Sp}(V)\}.$$

The multiplicative group $K^\times$ acts on $V \times K$ via $x(v, \lambda) := (xv, x^{-2}\lambda)$. Passing to the quotient modulo this action yields a bijection

$$(V\backslash\{0\} \times K)/K^\times \xrightarrow{(v,\lambda)\mapsto T_v[\lambda]} \{\text{nontrivial symplectic transvections in } \mathrm{Sp}(V)\}.$$

When we consider the first projection $\pi_V : V \times K \twoheadrightarrow V$ modulo the action of $K^\times$ we obtain

$$\pi_V : (V\backslash\{0\} \times K)/K^\times \twoheadrightarrow \mathbb{P}(V),$$

which corresponds to sending a nontrivial transvection to its centre. Let W be a K-subspace of V. Then Φ gives a bijection

$$(W\backslash\{0\} \times K)/K^\times \xrightarrow{(v,\lambda)\mapsto T_v[\lambda]} \{\text{nontrivial symplectic transvections in } \mathrm{Sp}(V) \text{ with centre in } W\}.$$

Let L be a subfield of K. For a subset $S \subseteq V$, we denote by $\langle S \rangle_L$ the L-span

Brought to you by | Biblioteca de la Universidad de Sevilla
Authenticated
Download Date | 10/13/16 7:54 AM

of the elements of S inside V. We call an L-vector space $W_L \subseteq V$ *L-rational* if $\dim_K W_K = \dim_L W_L$ with $W_K := \langle W_L \rangle_K$ and $\langle \cdot, \cdot \rangle$ restricted to $W_L \times W_L$ takes values in L. An L-vector space $W_L \subseteq V$ is called *(L,G)-rational* if W_L is L-rational and Φ induces a bijection

$$(W_L \backslash \{0\} \times L)/L^\times \xrightarrow{(v,\lambda)\mapsto T_v[\lambda]} G \cap \{\text{nontrivial sympl. transvections in } \mathrm{Sp}(V) \text{ with centre in } W_K\}.$$

Note that $(W_L \backslash \{0\} \times L)/L^\times$ is naturally a subset of $(W_K \backslash \{0\} \times K)/K^\times$.

A typical example of $(L, \mathrm{Sp}_n(L))$-rational subspace can be constructed as follows: let V_L be a symplectic L-vector space of dimension n, and consider the symplectic K-vector space $V = V_L \otimes_L K$ (where the symplectic form on V_L is extended K-linearly to V). Then any L-subvector space W_L of V_L is $(L, \mathrm{Sp}(V_L))$-rational.

A K-subspace $W \subseteq V$ is called *(L,G)-rationalisable* if there exists an (L,G)-rational W_L with $W_K = W$. We speak of an (L,G)-rational symplectic subspace W_L if it is (L,G)-rational and symplectic in the sense that the restricted pairing is non-degenerate on W_L. Let H_L and I_L be two (L,G)-rational symplectic subspaces of V. We say that *H_L and I_L are (L,G)-linked* if there is $0 \neq h \in H_L$ and $0 \neq w \in I_L$ such that $h + w \in \mathcal{L}(G)$.

3. Strategy

Now that we have set up all notation, we will describe the strategy behind the proof of Theorem 1.1, as a service for the reader.

If one is not in case 1, then there are 'many' transvections in G, as otherwise the K-span of $\mathcal{L}(G)$ would be a proper subspace of V stabilised by G. The presence of 'many' transvection is used first in order to show the existence of a subfield $L \subseteq K$ and an (L,G)-rational symplectic plane $H_L \subseteq V$. For this it is necessary to replace G by one of its conjugates inside $\mathrm{GSp}(V)$. The main ingredient for the existence of (L,G)-rational symplectic planes, which is treated in Section 5, is Dickson's classification of the finite subgroups of $\mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$.

The next main step is to show that two (L,G)-linked symplectic spaces in V can be merged into a single one. This is the main result of Section 6. The main input is a result of Wagner for transvections in three dimensional vector spaces, proved in Appendix A.

The merging results are applied to extend the (L,G)-rational symplectic plane further, using again the existence of 'many' transvections. We obtain a maximal (L,G)-rational symplectic space $I_L \subseteq V$ in the sense that $\mathcal{L}(G) \subset I_K \cup I_K^\perp$, which is proved in Section 7. The proof of Theorem 1.1 can be deduced from this (see Section 8) because either I_K equals V, that is the

Brought to you by | Biblioteca de la Universidad de Sevilla
Authenticated
Download Date | 10/13/16 7:54 AM

huge image case, or translating I_K by elements of G gives the decomposition in case 2.

4. Simple properties

We use the notation from the Introduction. In this subsection we list some simple lemmas illustrating and characterising the definitions made above.

Lemma 4.1. *Let $v \in \mathcal{L}(G)$. Then $\langle v\rangle_L$ is an (L,G)-rational line if and only if $\mathcal{P}_v(G) = L$.*

Proof. This follows immediately from that fact that all transvections with centre $\langle v\rangle_K$ can be written uniquely as $T_v[\lambda]$ for some $\lambda \in K$. ∎

Lemma 4.2. *Let $W_L \subseteq V$ be an (L,G)-rational space and U_L an L-vector subspace of W_L. Then U_L is also (L,G)-rational.*

Proof. We first give two general statements about L-rational subspaces. Let $u_1, \ldots, u_d$ be an L-basis of U_L and extend it by $w_1, \ldots, w_e$ to an L-basis of W_L. As W_L is L-rational, the chosen vectors remain linearly independent over K, and, hence, U_L is L-rational. Moreover, we see, e.g. by writing down elements in the chosen basis, that $W_L \cap U_K = U_L$.

It is clear that Φ sends elements in $(U_L \times L)/L^\times$ to symplectic transvections in G with centres in U_K. Conversely, let $T_v[\lambda]$ be such a transvection. As W_L is (L,G)-rational, $T_v[\lambda] = T_u[\mu]$ with some $u \in W_L$ and $\mu \in L$. Due to $W_L \cap U_K = U_L$, we have $u \in U_L$ and the tuple (u,μ) lies in $U_L \times L$. ∎

Lemma 4.3. *Let $W_L \subseteq V$ be an L-rational subspace of V. Then the following assertions are equivalent:*

(i) *W_L is (L,G)-rational.*
(ii) (a) *$T_{W_L}[L] := \{T_v[\lambda] \mid \lambda \in L,\ v \in W_L\} \subseteq G$ and*
  (b) *for each $U \in \mathcal{L}(G) \subseteq \mathbb{P}(V)$ with $U \subseteq W_K$ there is a $u \in U \cap W_L$ such that $\mathcal{P}_u(G) = L$ (i.e. $\langle u\rangle_L$ is an (L,G)-rational line contained in U by Lemma 4.1).*

Proof. (i)⇒(ii). Note that (iia) is clear. For (iib), let $U \in \mathcal{L}(G)$ with $U \subseteq W_K$. Hence, there is $u \in U$ and $\lambda \in K^\times$ with $T_u[\lambda] \in G$. As W_L is (L,G)-rational, we may assume that $u \in W_L$ and $\lambda \in L$. Lemma 4.2 implies that $\langle u\rangle_L$ is an (L,G)-rational line.

(ii)⇒(i). Denote by ι the injection $(W_L \backslash \{0\} \times L)/L^\times \hookrightarrow (W_K \backslash \{0\} \times K)/K^\times$. By (iia), the image of $\Phi \circ \iota$ lies in G. It remains to prove the surjectivity of this map onto the symplectic transvections of G with centres in W_K. Let $T_v[\lambda]$ be one such. Take $U = \langle v\rangle_K$. By (iib), there is $v_0 \in U$ such that $U_L = \langle v_0\rangle_L \subseteq W_L$ is an (L,G)-rational line. In particular, $T_v[\lambda] = T_{v_0}[\mu]$ with some $\mu \in L$, finishing the proof. ∎

Brought to you by | Biblioteca de la Universidad de Sevilla
Authenticated
Download Date | 10/13/16 7:54 AM

Lemma 4.4. *Let $A \in \mathrm{GSp}(V)$ with multiplier $\alpha \in K^\times$. Then $AT_v[\lambda]A^{-1} = T_{Av}[\frac{\lambda}{\alpha}]$. In particular, the notion of (L,G)-rationality is not stable under conjugation.*

Proof. For all $w \in V$, $AT_v[\lambda]A^{-1}(w) = A(A^{-1}w + \lambda(A^{-1}w \bullet v)v) = w + \lambda(A^{-1}w \bullet v)Av$. Since A has multiplier α, $w \bullet Av = \alpha(A^{-1}w \bullet v)$, hence $AT_v[\lambda]A^{-1}(w) = w + \frac{\lambda}{\alpha}(w \bullet Av)Av = T_{Av}[\frac{\lambda}{\alpha}](w)$. ∎

Lemma 4.5. *The group G maps $\mathcal{L}(G)$ into itself.*

Proof. Let $g \in G$ and $w \in \mathcal{L}(G)$, say $T_w[\lambda] \in G$. Then by Lemma 4.4 we have $gT_w[\lambda]g^{-1} = T_{gw}[\frac{\lambda}{\alpha}]$, where α is the multiplier of g. Hence, $g(w) \in \mathcal{L}(G)$. ∎

The following lemma shows that the natural projection yields a bijection between transvections in the symplectic group and their images in the projective symplectic group.

Lemma 4.6. *Let V be a symplectic K-vector space, $0 \neq u_1, u_2 \in V$. If $T_{u_1}[\lambda_1]^{-1}T_{u_2}[\lambda_2] \in \{a \cdot \mathrm{Id} : a \in K^\times\}$, then $T_{u_1}[\lambda_1] = T_{u_2}[\lambda_2]$.*

Proof. Assume that $T_{u_1}[\lambda_1]^{-1}T_{u_2}[\lambda_2] = a\mathrm{Id}$. Then for all $v \in V$,

$$T_{u_2}[\lambda_2](v) - T_{u_1}[\lambda_1](av) = 0.$$

In particular, taking $v = u_1$,

$$T_{u_2}[\lambda_2](u_1) - T_{u_1}[\lambda_1](au_1) = u_1 + \lambda_2(u_1 \bullet u_2)u_2 - au_1 = 0,$$

hence either u_1 and u_2 are linearly dependent or $a = 1$ (thus both transvections coincide). Assume then that $u_2 = bu_1$ for some $b \in K^\times$. Then for all $v \in V$ we have

$$\begin{aligned} T_{bu_1}[\lambda_2](v) - T_{u_1}[\lambda_1](av) &= v + \lambda_2 b^2(v \bullet u_1)u_1 - av - \lambda_1 a(v \bullet u_1)u_1 \\ &= (a-1)v + (\lambda_2 b^2 - a\lambda_1)(v \bullet u_1)u_1 = 0. \end{aligned}$$

Choosing v linearly independent from u_1, we obtain $a = 1$, as we wished to prove. ∎

5. Existence of (L,G)-rational symplectic planes

Let, as before, K be a finite field of characteristic ℓ, let V be a n-dimensional symplectic K-vector space and let $G \subseteq \mathrm{GSp}(V)$ be a subgroup. We will now prove the existence of (L,G)-rational symplectic planes if there are two transvections in G with nonorthogonal directions.

Note that any additive subgroup $H \subseteq K$ can appear as a parameter group of a direction. Just take G to be the subgroup of $\mathrm{GSp}(V)$ generated by the transvections in one fixed direction with parameters in H. It might seem surprising that the existence of two nonorthogonal centres forces the parameter group to be the additive group of a subfield L of K (up to multiplication by a fixed scalar). This is the contents of Proposition 5.5,

Brought to you by | Biblioteca de la Universidad de Sevilla
Authenticated
Download Date | 10/13/16 7:54 AM

which is one of the main ingredients for this article. This proposition, in turn, is based on Proposition 5.1, going back to Mitchell (cf. [8]). To make this exposition self-contained we also include a proof of it, which essentially relies on Dickson's classification of the finite subgroups of $\mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$. Recall that an *elation* is the image in $\mathrm{PGL}(V)$ of a transvection in $\mathrm{GL}(V)$.

Proposition 5.1. *Let V be a 2-dimensional K-vector space with basis $\{e_1, e_2\}$ and $\Gamma \subseteq \mathrm{PGL}(V)$ a subgroup that contains two nontrivial elations whose centers U_1 and U_2 are different. Let ℓ^m be the order of an ℓ-Sylow subgroup of Γ.*

Then K contains a subfield L with ℓ^m elements. Moreover, there exists $A \in \mathrm{PGL}_2(K)$ such that $AU_1 = \langle e_1 \rangle_K$, $AU_2 = \langle e_2 \rangle_K$, and $A\Gamma A^{-1}$ is either $\mathrm{PGL}(V_L)$ or $\mathrm{PSL}(V_L)$, where $V_L = \langle e_1, e_2 \rangle_L$.

Proof. Since there are two elations τ_1 and τ_2 with independent directions U_1 and U_2, Dickson's classification of subgroups of $\mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$ (Section 260 of [5]) implies that there is $B \in \mathrm{PGL}_2(K)$ such that $B\Gamma B^{-1}$ is either $\mathrm{PGL}(V_L)$ or $\mathrm{PSL}(V_L)$, where L is a subfield of K. Note that the order of an ℓ-Sylow of $\Gamma \simeq \mathrm{PGL}_2(V_L)$ (resp. $\Gamma \simeq \mathrm{PSL}_2(V_L)$) coincides with the cardinality of L; this implies that L has exactly ℓ^m elements. By Lemma 4.4, the direction of $B\tau_i B^{-1}$ is BU_i for $i = 1, 2$ and the lines BU_i are of the form $\langle d_i \rangle_K$ with $d_i \in V_L$ for $i = 1, 2$. As $\mathrm{PSL}(V_L)$ acts transitively on V_L, there is $C \in \mathrm{PSL}(V_L)$ such that $CU_1 = \langle e_1 \rangle_K$ and $CU_2 = \langle e_2 \rangle_K$. Setting $A := CB$ yields the proposition. ∎

Although the preceding proposition is quite simple, the very important consequence it has is that the conjugated elations $A\tau_i A^{-1}$ both have direction vectors that can be defined over the same L-rational plane.

Lemma 5.2. *Let V be a 2-dimensional K-vector space, $G \subseteq \mathrm{GL}(V)$ containing two transvections with linearly independent directions U_1 and U_2. Let ℓ^m be the order of any ℓ-Sylow subgroup of G.*

Then K contains a subfield L with ℓ^m elements and there are $A \in \mathrm{GL}(V)$ and an (L, AGA^{-1})-rational plane $V_L \subseteq V$. Moreover, A can be chosen such that $AU_i = U_i$ for $i = 1, 2$. Furthermore, if $u_1 \in U_1$ and $u_2 \in U_2$ are such that $u_1 \bullet u_2 \in L^\times$, then V_L can be chosen to be $\langle u_1, u_2 \rangle_L$.

Proof. We apply Proposition 5.1 with $e_1 = u_1$, $e_2 = u_2$, and Γ the image of G in $\mathrm{PGL}(V)$, and obtain $A \in \mathrm{GL}(V)$ (any lift of the matrix provided by the proposition) such that $A\Gamma A^{-1}$ equals $\mathrm{PSL}(V_L)$ or $\mathrm{PGL}(V_L)$ for the L-rational plane $V_L = \langle u_1, u_2 \rangle_L \subseteq V$, and $AU_i = U_i$ for $i = 1, 2$. For $\mathrm{PSL}(V_L)$ and $\mathrm{PGL}(V_L)$ it is true that the elations contained in them are precisely the images of $T_v[\lambda]$ for $v \in V_L$ and $\lambda \in L$.

Brought to you by | Biblioteca de la Universidad de Sevilla
Authenticated
Download Date | 10/13/16 7:54 AM

First, we know that all such $T_v[\lambda]$ are contained in $\mathrm{SL}(V_L)$ and, thus, in AGA^{-1} (since $A\Gamma A^{-1}$ is $\mathrm{PSL}(V_L)$ or $\mathrm{PGL}(V_L)$). Second, by Lemma 4.6 the image of $T_v[\lambda]$ in $A\Gamma A^{-1}$ has a unique lift to a transvection in $\mathrm{SL}(V_L) \subseteq AGA^{-1}$, namely $T_v[\lambda]$. This proves that the transvections of AGA^{-1} are precisely the $T_v[\lambda]$ for $v \in V_L$ and $\lambda \in L$. Hence, V_L is an (L, AGA^{-1})-rational plane. ∎

Lemma 5.3. *Let $U_1, U_2 \in \mathcal{L}(G)$ be such that $H = U_1 \oplus U_2$ is a symplectic plane in V. By G_0 we denote the subgroup $\{g \in G \mid g(H) \subseteq H\}$ and by $G|_H$ the restrictions of the elements of G_0 to H. Then $\mathcal{L}(G|_H) \subseteq \mathcal{L}(G)$ (under the inclusion $\mathbb{P}(H) \subseteq \mathbb{P}(V)$).*

Proof. Let $\tau_i \in G$ be transvections with directions U_i for $i = 1, 2$. Clearly, $\tau_1, \tau_2 \in G_0$ and their restrictions to H are symplectic transvections with the same directions. Consequently, Lemma 5.2 provides us with $A \in \mathrm{GL}(H)$ and an (L, AGA^{-1})-rational plane $H_L \subseteq H$.

Let $U \in \mathcal{L}(G|_H)$. This means that there is $g \in G_0$ such that $g|_H$ is a transvection with direction U, so that $Ag|_H A^{-1}$ is a transvection in $AG|_H A^{-1}$ with direction AU by Lemma 4.4. As H_L is $(L, AG|_H A^{-1})$-rational, all transvections $T_v[\lambda]$ for $v \in H_L$ and $\lambda \in L$ lie in $AG|_H A^{-1}$, whence $AG|_H A^{-1}$ contains $\mathrm{SL}(H_L)$. Consequently, there is $h \in AG|_H A^{-1}$ such that $hAU = AU_1$. But $A^{-1}hA \in G|_H$, whence there is $\gamma \in G_0$ with restriction to H equal to $A^{-1}hA$. As $\gamma H \subseteq H$, it follows that $\gamma U = \gamma|_H U = A^{-1}hAU = U_1$. Now, $\gamma^{-1}\tau_1\gamma$ is a transvection in G with centre $\gamma^{-1}U_1 = U$, showing $U \in \mathcal{L}(G)$. ∎

Corollary 5.4. *Let $U_1, U_2 \in \mathcal{L}(G)$ be such that $H = U_1 \oplus U_2$ is a symplectic plane in V. By G_0 we denote the subgroup $\{g \in G \mid g(H) \subseteq H\}$ and by $G|_H$ the restrictions of the elements of G_0 to H. Then the transvections of $G|_H$ are the restrictions to H of the transvections of G with centre in H.*

Proof. Let T be the subgroup of G generated by the transvections of G with centre in H. We can naturally identify T with $T|_H$. Let U be the subgroup of $G|_H$ generated by the transvections of $G|_H$. We have that $T|_H \subset U$.

Apply Lemma 5.2 to the K-vector space H and the subgroup $U \subset \mathrm{GL}(H)$. There exists a subfield $L \subset K$, and an L-rational plane H_L such that U is conjugate to $\mathrm{SL}(H_L)$, hence $U \simeq \mathrm{SL}_2(L)$. Applying Lemma 5.2 to the K-vector space H and the subgroup $T|_H$, we obtain a subfield $L' \subset K$, and an L'-rational plane $H_{L'}$ such that $T|_H$ is conjugate to $\mathrm{SL}(H_{L'})$, hence $H \simeq \mathrm{SL}_2(L')$. But $\mathcal{L}(T|_H) = \mathcal{L}(G) \cap H = \mathcal{L}(G|_H) = \mathcal{L}(U)$ by Lemma 5.3, whence $L = L'$ and the cardinalities of U and $T|_H$ coincide. Therefore they are equal. ∎

Proposition 5.5. *Let $U_1, U_2 \in \mathcal{L}(G) \subseteq \mathbb{P}(V)$ which are not orthogonal. Then there exist a subfield $L \leq K$, $A \in \mathrm{GSp}(V)$, and an L-rational symplectic*

Brought to you by | Biblioteca de la Universidad de Sevilla
Authenticated
Download Date | 10/13/16 7:54 AM

plane H_L such that $AU_1 \subseteq H_K$, $AU_2 \subseteq H_K$ and such that H_L is (L, AGA^{-1})-rational. Moreover, if we fix $u_1 \in U_1$, $u_2 \in U_2$ such that $u_1 \bullet u_2 \in L^\times$, we can choose $H_L = \langle u_1, u_2\rangle_L$ and A satisfying $AU_1 = U_1$, $AU_2 = U_2$.

Proof. Let $H = U_1 \oplus U_2$ and note that this is a symplectic plane. Define G_0 and $G|_H$ as in Lemma 5.3. Lemma 5.2 provides us with $B \in \mathrm{GL}(H)$ such that $BU_i = U_i$ for $i = 1, 2$ and such that $H_L = \langle u_1, u_2\rangle_L$ is an $(L, BG|_H B^{-1})$-rational plane. We choose $A \in \mathrm{GSp}(V)$ such that $AH \subseteq H$ and $A|_H = B$ (this is possible as any symplectic basis of H can be extended to a symplectic basis of V). We want to prove that H_L is an (L, AGA^{-1})-rational symplectic plane in V.

And, indeed, by Corollary 5.4, the nontrivial transvections of AGA^{-1} with direction in H coincide with the nontrivial transvections of $BG|_H B^{-1}$, which in turn correspond bijectively to $(H_L\backslash\{0\} \times L)/L$. ∎

Note that Theorem 1.1 is independent of conjugating G inside $\mathrm{Sp}(V)$. Hence, we will henceforth work with (L, G)-rational symplectic spaces (instead of (L, AGA^{-1})-rational ones).

Corollary 5.6.

(a) *Let H_L be an L-rational plane which contains an (L, G)-rational line $U_{1,L}$ as well as an L-rational line $U_{2,L}$ not orthogonal to $U_{1,L}$ with $U_{2,K} \in \mathcal{L}(G)$. Then H_L is an (L, G)-rational symplectic plane.*

(b) *Let $U_{1,L} = \langle u_1\rangle_L$ be an (L, G)-rational line and $U_2 = \langle u_2\rangle_K \in \mathcal{L}(G)$ such that $u_1 \bullet u_2 \in L^\times$. Then $\langle u_1, u_2\rangle_L$ is an (L, G)-rational symplectic plane.*

Proof. (a) Fix $u_1 \in U_{1,L}$ and $u_2 \in U_{2,L}$ such that $u_1 \bullet u_2 = 1$, and call $W_L = \langle u_1, u_2\rangle_L$. Apply Proposition 5.5: we get $L \subseteq K$ and $A \in \mathrm{GSp}(V)$ such that $\langle AU_{1,L}\rangle_K = \langle u_1\rangle_K$, $AU_2 = \langle u_2\rangle_K$ and W_L is (L, AGA^{-1})-rational. Let $a_1, a_2 \in K^\times$ be such that $Au_1 = a_1u_1$ and $Au_2 = a_2u_2$. The proof will follow three steps: we will first see that $\mathcal{P}_{u_2}(G) = L$, then we will see that H_L satisfies Lemma 4.3(iia) and finally we will see that H_L satisfies Lemma 4.3(iib).

Let α be the multiplier of A. First note the following equality between α, a_1 and a_2:

$$1 = u_1 \bullet u_2 = \frac{1}{\alpha}(Au_1 \bullet Au_2) = \frac{1}{\alpha}(a_1u_1 \bullet a_2u_2) = \frac{a_1a_2}{\alpha}.$$

Recall that $\mathcal{P}_{av}(G) = \frac{1}{a^2}\mathcal{P}_v(G)$. From Lemma 4.4 we have $\mathcal{P}_{Av}(AGA^{-1}) = \frac{1}{\alpha}\mathcal{P}_v(G)$.

On the one hand, since $U_{1,L}$ is (L, G)-rational and $u_1 \in U_{1,L}$, we know that $\mathcal{P}_{u_1}(G) = L$ by Lemma 4.1. On the other hand, since $\langle u_1\rangle_L$ is (L, AGA^{-1})-rational, $\mathcal{P}_{u_1}(AGA^{-1}) = L$, hence $\mathcal{P}_{u_1}(G) = \frac{\alpha}{a_1^2}L$. We thus have $\frac{\alpha}{a_1^2} \in L$.

Brought to you by | Biblioteca de la Universidad de Sevilla
Authenticated
Download Date | 10/13/16 7:54 AM

Moreover, since $\langle u_2\rangle_L$ is (L, AGA^{-1})-rational (e.g. using Lemma 4.2), we have that $\mathcal{P}_{u_2}(AGA^{-1}) = L$, hence $\mathcal{P}_{u_2}(G) = \frac{\alpha}{a_2^2}L = \frac{a_1^2\alpha}{\alpha^2}L = \frac{a_1^2}{\alpha}L = L$. This proves that $\langle u_2\rangle_L$ is (L, G)-rational by Lemma 4.1.

Next, we will see that $T_{H_L}[L] \subseteq G$. Let $b_1, b_2 \in L$ with $b_1 \neq 0$ and $\lambda \in L^\times$. Consider the transvection $T_{b_1u_1+b_2u_2}[\lambda]$. We want to prove that it belongs to G. We compute

$$\begin{aligned} AT_{b_1u_1+b_2u_2}[\lambda]A^{-1} &= T_{A(b_1u_1+b_2u_2)}\left[\frac{\lambda}{\alpha}\right] \\ &= T_{b_1a_1u_1+b_2a_2u_2}\left[\frac{\lambda}{\alpha}\right] = T_{u_1+\frac{b_2a_2}{b_1a_1}u_2}\left[\frac{b_1^2a_1^2\lambda}{\alpha}\right]. \end{aligned}$$

Note that since $\frac{a_1}{a_2} = \frac{a_1^2}{\alpha} \in L$ and since $W_L = \langle u_1, u_2\rangle_L$ is (L, AGA^{-1})-rational, it follows that $AT_{b_1u_1+b_2u_2}[\lambda]A^{-1} \in AGA^{-1}$, and therefore $T_{b_1u_1+b_2u_2}[\lambda] \in G$. Note that the same conclusion is valid for $b_1 = 0$ as $\langle u_2\rangle_L$ is (L, G)-rational.

Finally, it remains to see that if $U \in \mathcal{L}(G) \cap \langle H_L\rangle_K$, then there is $u \in U \cap H_L$ with $\mathcal{P}_u(G) = L$. Assume that $U \in \mathcal{L}(G) \cap \langle H_L\rangle_K$. Since we have seen that $\langle u_2\rangle_L$ is (L, G)-rational, we can assume that $U \neq \langle u_2\rangle_K$. Therefore, we can choose an element $v \in U$ with $v = u_1 + bu_2$, for some $b \in K$. It suffices to show that $b \in L$. Let $T_v[\lambda] \in G$ be a transvection with direction U. Then computing $AT_v[\lambda]A^{-1}$ as above, we get that $AT_v[\lambda]A^{-1} = T_{u_1+\frac{ba_2}{a_1}u_2}[\frac{a_1^2\lambda}{\alpha}]$ is a transvection with direction in $\mathcal{L}(AGA^{-1}) \cap W_L$, hence the (L, AGA^{-1})-rationality of W_L implies that $b \in L$.

(b) follows from (a) by observing that the condition $u_1 \bullet u_2 \in L^\times$ ensures that $\langle u_1, u_2\rangle_L$ is an L-rational symplectic plane. ∎

The next corollary says that the translate of each vector in an (L, G)-rational symplectic space by some orthogonal vector w is the centre of a transvection if this is the case for one of them.

Corollary 5.7. *Let $H_L \subseteq V$ be an (L, G)-rational symplectic space. Let $w \in H_K^\perp$ and $0 \neq h \in H_L$ such that $\langle h + w\rangle_K \in \mathcal{L}(G)$. Then $\langle h_1 + w\rangle_L$ is an (L, G)-rational line for all $0 \neq h_1 \in H_L$.*

Proof. Assume first that H_L is a plane. Let $\hat{h} \in H_L$ with $\hat{h} \bullet h = 1$ (hence $H_L = \langle h, \hat{h}\rangle_L$). As $\langle \hat{h}\rangle_L$ is an (L, G)-rational line and $\hat{h}\bullet(h+w) = 1$, it follows that $\langle \hat{h}, h + w\rangle_L$ is an (L, G)-rational plane by Corollary 5.6. Consequently, for all $\mu \in L$ we have that $\langle \mu\hat{h} + h + w\rangle_L$ is an (L, G)-rational line. Let now $\mu \in L^\times$. Then $(\mu\hat{h} + h + w) \bullet h = \mu \neq 0$, whence again by Corollary 5.6 $\langle \mu\hat{h} + h + w, h\rangle_L$ is an (L, G)-rational plane. Thus, for all $\nu \in L$ it follows that $\langle \mu\hat{h} + (\nu + 1)h + w\rangle_L$ is an (L, G)-rational line. In order to get rid of

Brought to you by | Biblioteca de la Universidad de Sevilla
Authenticated
Download Date | 10/13/16 7:54 AM

the condition $\mu \neq 0$, we exchange the roles of h and $\hat{h}$, yielding the statement for planes.

To extend it to any symplectic space H_L, note that, if $h_1, h_2 \in H_L$ are nonzero elements, there exists an element $\hat{h} \in H_L$ such that $h_1 \bullet \hat{h} \neq 0$, $h_2 \bullet \hat{h} \neq 0$. Namely, let $\hat{h}_1, \hat{h}_2$ be such that $h_1 \bullet \hat{h}_1 \neq 0$, $h_2 \bullet \hat{h}_2 \neq 0$ (they exist because on H_L the symplectic pairing is nondegenerate). If $h_2 \bullet \hat{h}_1 \neq 0$ or $h_1 \bullet \hat{h}_2 \neq 0$, we are done. Otherwise $\hat{h} = \hat{h}_1 + \hat{h}_2$ satisfies the required condition.

Returning to the proof, if $h_1 \in H_L$ is nonzero, take $\hat{h} \in H_L$ such that $h \bullet \hat{h} \neq 0$ and $h_1 \bullet \hat{h} \neq 0$. First apply the corollary to the plane $\langle h, \hat{h}\rangle_L$, yielding that $\hat{h} + w$ is an (L, G)-rational line, and then apply it to the plane $\langle \hat{h}, h_1\rangle_L$, showing that $h_1 + w$ is an (L, G)-rational line, as required. ∎

In the next lemma, it is important that the characteristic of K is greater than 2.

Lemma 5.8. *Let H_L be an (L, G)-rational symplectic space. Let $h, \tilde{h} \in H_L$ different from zero and let $w, \tilde{w} \in H_K^\perp$ such that $w \bullet \tilde{w} \in L^\times$ and $h + w, \tilde{h} + \tilde{w} \in \mathcal{L}(G)$. Then $\langle w, \tilde{w}\rangle_L$ is an (L, G)-rational symplectic plane.*

Proof. By Corollary 5.7 we have that $\langle h + \tilde{w}\rangle_L$ is an (L, G)-rational line. As $(h + w) \bullet (h + \tilde{w}) = w \bullet \tilde{w} \in L^\times$, by Corollary 5.6 it follows that $\langle w - \tilde{w}\rangle_L$ is an (L, G)-rational line. Since $\langle -h - w\rangle_K \in \mathcal{L}(G)$, by Corollary 5.7 we have that $\langle -h + w\rangle_L$ is (L, G)-rational, and from $(-h + w) \bullet (h + \tilde{w}) = w \bullet \tilde{w} \in L^\times$ we conclude that $\langle w + \tilde{w}\rangle_L$ is an (L, G)-rational line. As $(w - \tilde{w}) \bullet (w + \tilde{w}) = 2w \bullet \tilde{w} \in L^\times$, we obtain that $\langle w + \tilde{w}, w - \tilde{w}\rangle_L = \langle w, \tilde{w}\rangle_L$ is an (L, G)-rational symplectic plane, as claimed. ∎

We now deduce that linking is an equivalence relation between mutually orthogonal spaces. Note that reflexivity and symmetry are clear and only transitivity need be shown.

Lemma 5.9. *Let H_L, I_L and J_L be mutually orthogonal (L, G)-rational symplectic subspaces of V. If H_L and I_L are (L, G)-linked and also I_L and J_L are (L, G)-linked, then so are H_L and J_L.*

Proof. By definition there exist nonzero $h_0 \in H_L$, $i_0, i_1 \in I_L$ and $j_0 \in J_L$ such that $h_0 + i_0 \in \mathcal{L}(G)$ and $i_1 + j_0 \in \mathcal{L}(G)$. There are $\hat{h}_0 \in H_L$ and $\hat{i}_0 \in I_L$ such that $\hat{h}_0 \bullet h_0 = 1$ and $\hat{i}_0 \bullet i_0 = 1$.

By Corollary 5.7 we have, in particular, that $\langle h_0 + i_0\rangle_L$, $\langle \hat{i}_0 + j_0\rangle_L$ and $\langle \hat{h}_0 + (i_0 + \hat{i}_0)\rangle_L$ are (L, G)-rational lines. As $(h_0 + \hat{i}_0) \bullet (i_0 + j_0) = 1$, by Corollary 5.6 also $\langle h_0 + (i_0 + \hat{i}_0) + j_0\rangle_L$ is (L, G)-rational. Furthermore, due to $(\hat{h}_0 + (i_0 + \hat{i}_0)) \bullet (h_0 + (i_0 + \hat{i}_0) + j_0) = 1$, it follows that $\langle (h_0 - \hat{h}_0) + j_0\rangle_L$ is (L, G)-rational, whence H_L and J_L are (L, G)-linked. ∎

Brought to you by | Biblioteca de la Universidad de Sevilla
Authenticated
Download Date | 10/13/16 7:54 AM

6. Merging linked orthogonal (L, G)-rational symplectic subspaces

We continue using our assumptions: K is a finite field of characteristic at least 5, $L \subseteq K$ a subfield, V an n-dimensional symplectic K-vector space, $G \subseteq \mathrm{GSp}(V)$ a subgroup. In the previous section, we established the existence of (L, G)-rational symplectic planes in many cases (after allowing a conjugation of G inside $\mathrm{GSp}(V)$). In this section, we aim at merging (L, G)-linked (L, G)-rational symplectic planes into (L, G)-rational symplectic subspaces.

It is important to remark that no new conjugation of G is required. The only conjugation that is needed is the one from the previous section in order to have an (L, G)-rational plane to start from.

Lemma 6.1. *Let H_L and I_L be two (L, G)-rational symplectic subspaces of V which are (L, G)-linked. Suppose that H_L and I_L are orthogonal to each other. Then all lines in $H_L \oplus I_L$ are (L, G)-rational.*

Proof. The (L, G)-linkage implies the existence of $h_1 \in H_L$ and $w_1 \in I_L$ such that $\langle h_1 + w_1 \rangle_K \in \mathcal{L}(G)$. By Corollary 5.7 $\langle h + w_1 \rangle_L$ is an (L, G)-rational line for all $h \in H_L$. The same reasoning now gives that $\langle h + w \rangle_L$ is an (L, G)-rational line for all $h \in H_L$ and all $w \in I_L$. ∎

In view of Lemma 4.3 the above is (iia). In order to obtain (iib), we need to invoke a result of Wagner (see Proposition A.1 in Appendix A).

Proposition 6.2. *Let $U_1, U_2, U_3 \in \mathcal{L}(G)$ and $W = U_1 + U_2 + U_3$. Assume that $\dim W = 3$, U_1 and U_2 not orthogonal and let U be a line in $W \cap W^\perp$ which is linearly independent from U_3 and is not contained in $U_1 \oplus U_2$. Then $(U_1 \oplus U_2) \cap (U \oplus U_3)$ is a line in $\mathcal{L}(G)$.*

Proof. Fix transvections $T_i \in G$ with centre U_i, $i = 1, 2, 3$. These transvections fix W; let $H \subseteq \mathrm{SL}(W)$ be the group generated by the restrictions of the T_i to W. The condition $U \subseteq W^\perp$ guarantees that the T_i fix U pointwise. Note that furthermore $U \neq U_3$ and $U \nsubseteq U_1 \oplus U_2$. We can apply Proposition A.1, and conclude that $(U_1 \oplus U_2) \cap (U \oplus U_3)$ is the centre of a transvection T of H. This transvection fixes the symplectic plane $U_1 \oplus U_2$. Call T_0 the restriction of T to this plane. It is a nontrivial transvection (since no line of $U_1 \oplus U_2$ can be orthogonal to all $U_1 \oplus U_2$). Hence by Lemma 5.3 the line $(U_1 \oplus U_2) \cap (U \oplus U_3)$ belongs to $\mathcal{L}(G)$. ∎

We now deduce rationality statements from it.

Corollary 6.3. *Let H_L be an (L, G)-rational symplectic plane and let U_3 and U_4 be linearly independent lines not contained in H_K. Assume that $U_4 \subseteq H_K \oplus U_3$ is orthogonal to H_K and to U_3 and assume that $U_3 \in \mathcal{L}(G)$. Then the intersection $H_K \cap (U_3 \oplus U_4) = I_K$ for some line $I_L \subseteq H_L$.*

Brought to you by | Biblioteca de la Universidad de Sevilla
Authenticated
Download Date | 10/13/16 7:54 AM

Proof. Choose two (L,G)-rational lines $U_{1,L}$ and $U_{2,L}$ such that $H_L = U_{1,L} \oplus U_{2,L}$. With $U = U_4$ we can apply Proposition 6.2 in order to obtain that $I := H_K \cap (U_3 \oplus U_4)$ is a line in $\mathcal{L}(G)$ contained in H_K. As H_L is (L,G)-rational, it follows that I is (L,G)-rationalisable. ∎

Corollary 6.4. *Let $H_L \subseteq V$ be an (L,G)-rational symplectic space. Let $h + w \in \mathcal{L}(G)$ with $0 \neq h \in H_K$ and $w \in H_K^{\perp}$. Then $h \in \mathcal{L}(G)$. In particular, $\langle h \rangle_K$ is an (L,G)-rationalisable line, i.e. there is $\mu \in K^{\times}$ such that $\mu h \in H_L$.*

Proof. Replacing, if necessary H_L by any (L,G)-rational plane contained in H_L, we may without loss of generality assume that H_L is an (L,G)-rational plane. Let $y := h + w$. If $w = 0$, the claim follows from the (L,G)-rationality of H_L. Hence, we suppose that $w \neq 0$. Then $U_3 := \langle y \rangle_K$ is not contained in H_K. Note that w is perpendicular to U_3 and to H_K, and $w \in H_k \oplus \langle y \rangle_K$. Hence, Corollary 6.3 gives that the intersection $H_K \cap (U_3 \oplus \langle w \rangle_K) = \langle h \rangle_K$ is in $\mathcal{L}(G)$. ∎

Corollary 6.4 gives the rationalisability of a line. In order to actually find a direction vector for a parameter in L, we need something extra to rigidify the situation. For this, we now take a second link which is sufficiently different from the first link.

Corollary 6.5. *Let $H_L \subseteq V$ be an (L,G)-rational symplectic space. Let $0 \neq \tilde{h} \in H_K$ and $\tilde{w} \in H_K^{\perp}$ such that $\tilde{h} + \tilde{w} \in \mathcal{L}(G)$. Suppose that there are nonzero $h \in H_L$ and $w \in H_K^{\perp}$ such that $h + w \in \mathcal{L}(G)$ and $w \bullet \tilde{w} \in L^{\times}$. Then $\tilde{h} \in H_L$.*

Proof. By Corollary 6.4 there is some $\beta \in K^{\times}$ such that $\beta \tilde{h} \in H_L$. We want to show that $\beta \in L$. By Corollary 5.7 we may assume that $h \bullet \tilde{h} \neq 0$, more precisely, $h \bullet (\beta \tilde{h}) = 1$; and we have furthermore that $\langle h + w \rangle_L$ is an (L,G)-rational line. By Corollary 5.6 (b), $\langle h, \beta \tilde{h} \rangle_L$ is an (L,G)-rational symplectic plane contained in H_L. Let $c := w \bullet \tilde{w} \in L^{\times}$. We have

$$(h + w) \bullet (\tilde{h} + \tilde{w}) = h \bullet \tilde{h} + w \bullet \tilde{w} = \frac{1}{\beta} + c =: \mu.$$

If $\mu = 0$, then $\beta \in L$ and we are done. Assume that $\mu \neq 0$. By Corollary 5.6 (b) it follows that $\langle h + w, \mu^{-1}(\tilde{h} + \tilde{w}) \rangle_L$ is an (L,G)-rational symplectic plane. Thus, $\langle h + w + \mu^{-1}(\tilde{h} + \tilde{w}) \rangle_L$ is an (L,G)-rational line. By Corollary 6.4 there is some $\nu \in K^{\times}$ such that $\nu(h + \mu^{-1}\tilde{h}) \in H_L$. Consequently, $\nu \in L^{\times}$, whence $\mu \in L$, so that $\beta \in L$. ∎

The main result of this section is the following merging result.

Proposition 6.6. *Let H_L and I_L be orthogonal (L,G)-rational symplectic subspaces of V that are (L,G)-linked. Then $H_L \oplus I_L$ is an (L,G)-rational symplectic subspace of V.*

Brought to you by | Biblioteca de la Universidad de Sevilla
Authenticated
Download Date | 10/13/16 7:54 AM

Proof. We use Lemma 4.3. Part (iia) follows directly from Lemma 6.1. We now show (iib). Let $h+w \in \mathcal{L}(G)$ with nonzero $h \in H_K$ and $w \in I_K$ be given. Corollary 6.4 yields $\mu, \nu \in K^\times$ such that $\mu h \in H_L$ and $\nu w \in I_L$. Let $\hat{h} \in H_L$ with $(\mu h) \bullet \hat{h} = 1$, as well as $\hat{w} \in I_L$ with $(\nu w) \bullet \hat{w} = 1$. Lemma 6.1 tells us that $\hat{h} + \hat{w} \in \mathcal{L}(G)$. Together with $(\nu h) + (\nu w) \in \mathcal{L}(G)$, Corollary 6.5 yields $\nu h \in H_L$, whence $\nu h + \nu w \in H_L \oplus I_L$. ∎

7. Extending (L, G)-rational spaces

We continue using the same notation as in the previous sections. Here, we will use the merging results in order to extend (L, G)-rational symplectic spaces.

Proposition 7.1. *Let H_L be a nonzero (L, G)-rational symplectic subspace of V. Let nonzero $h, \tilde{h} \in H_K$, $w, \tilde{w} \in H_K^\perp$ be such that $h + w, \tilde{h} + \tilde{w} \in \mathcal{L}(G)$ and $w \bullet \tilde{w} \neq 0$. Then there exist $\alpha, \beta \in K^\times$ such that $\langle \alpha w, \beta \tilde{w} \rangle_L$ is an (L, G)-rational symplectic plane which is (L, G)-linked with H_L.*

Proof. By Corollary 6.4 we may and do assume by scaling $h+w$ that $h \in H_L$. Furthermore, we assume by scaling $\tilde{h} + \tilde{w}$ that $w \bullet \tilde{w} = 1$. Then Corollary 6.5 yields that $\tilde{h} \in H_L$. We may appeal to Lemma 5.8 yielding that $\langle w, \tilde{w} \rangle_L$ is an (L, G)-rational plane. The (L, G)-link is just given by $h + w$. ∎

Corollary 7.2. *Let H_L be a non-zero (L, G)-rational symplectic subspace of V. Let nonzero $h, \tilde{h} \in H_K$, $w, \tilde{w} \in H_K^\perp$ be such that $h + w, \tilde{h} + \tilde{w} \in \mathcal{L}(G)$ and $w \bullet \tilde{w} \neq 0$. Then there is an (L, G)-rational symplectic subspace I_L of V containing H_L and such that $I_K = \langle H_K, w, \tilde{w} \rangle_K$.*

Proof. This follows directly from Propositions 7.1 and 6.6. ∎

Proposition 7.3. *Assume that $\langle \mathcal{L}(G) \rangle_K = V$. Let H_L be a nonzero (L, G)-rational symplectic space. Let $0 \neq v \in \mathcal{L}(G) \backslash (H_K \cup H_K^\perp)$. Then there is an (L, G)-rational symplectic space I_L containing H_L such that $v \in I_K$.*

Proof. We write $v = h + w$ with $h \in H_K$ and $w \in H_K^\perp$. Note that both h and w are nonzero by assumption. As $\langle \mathcal{L}(G) \rangle_K = V$, we may choose $\tilde{v} \in \mathcal{L}(G)$ such that $\tilde{v} \bullet w \neq 0$. We again write $\tilde{v} = \tilde{h} + \tilde{w}$ with $\tilde{h} \in H_K$ and $\tilde{w} \in H_K^\perp$.

We, moreover, want to ensure that $\tilde{h} \neq 0$. If $\tilde{h} = 0$, then we proceed as follows. Corollary 6.4 implies the existence of $\mu \in K^\times$ such that $\mu h \in H_L$. Now replace h by μh and w be μw. Then Corollary 5.7 ensures that $\langle h + w \rangle_L$ is an (L, G)-rational line. Furthermore, scale $\tilde{w}$ so that $(h + w) \bullet \tilde{w} \in L^\times$, whence by Corollary 5.6 $h + w + \tilde{w} \in \mathcal{L}(G)$. We use this element as $\tilde{v}$ instead. Note that it still satisfies $\tilde{v} \bullet w \neq 0$, but now $\tilde{h} \neq 0$.

Now we are done by Corollary 7.2. ∎

Brought to you by | Biblioteca de la Universidad de Sevilla
Authenticated
Download Date | 10/13/16 7:54 AM

Corollary 7.4. *Assume that $\langle \mathcal{L}(G) \rangle_K = V$, and let H_L be an (L,G)-rational symplectic space. Then there is an (L,G)-rational symplectic space I_L containing H_L such that $\mathcal{L}(G) \subseteq I_K \cup I_K^\perp$.*

Proof. Iterate Proposition 7.3. ∎

8. Proof of Theorem 1.1

In this section we will finish the proof of Theorem 1.1.

Lemma 8.1. *Let $V = S_1 \oplus \cdots \oplus S_h$ be a decomposition of V into linearly independent, mutually orthogonal subspaces such that $\mathcal{L}(G) \subseteq S_1 \cup \cdots \cup S_h$.*

(a) *If $v_1, v_2 \in \mathcal{L}(G) \cap S_1$ are such that $v_1 + v_2 \in \mathcal{L}(G)$, then for all $g \in G$ there exists an index $i \in \{1, \ldots, h\}$ such that $g(v_1)$ and $g(v_2)$ belong to the same S_i.*
(b) *If S_1 is (L,G)-rationalisable, then for all $g \in G$ there exists an index $i \in \{1, \ldots, h\}$ such that $gS_1 \subseteq S_i$.*

Proof. (a) Assume that $g(v_1) \in S_i$ and $g(v_2) \in S_j$ with $i \neq j$. Then $g(v_1) + g(v_2) = g(v_1 + v_2) \in \mathcal{L}(G)$ satisfies $g(v_1 + v_2) \in S_i \oplus S_j$, but it neither belongs to S_i nor to S_j. This contradicts the assumption that $\mathcal{L}(G) \subseteq S_1 \cup \cdots \cup S_h$.

(b) If $S_1 = S_{1,L}$ with $S_{1,L}$ an (L,G)-rational space, we can apply (a) to an L-basis of $S_{1,L}$. ∎

Corollary 8.2. *Let $I_L \subseteq V$ be an (L,G)-rational symplectic subspace such that $\mathcal{L}(G) \subseteq I_K \cup I_K^\perp$ and let $g \in G$. Then either $g(I_K) = I_K$ or $g(I_K) \subseteq I_K^\perp$; in the latter case $I_K \cap g(I_K) = 0$.*

Proof. This follows from Lemma 8.1 with $S_1 = I_K$ and $S_2 = I_K^\perp$. ∎

We are now ready to prove Theorem 1.1.

Proof of Theorem 1.1. As we assume that G contains some transvection, it follows that $\mathcal{L}(G)$ is nonempty and consequently $\langle \mathcal{L}(G) \rangle_K$ is a nonzero K-vector space stabilised by G due to Lemma 4.5. Hence, either we are in case 1 of Theorem 1.1 or $\langle \mathcal{L}(G) \rangle_K = V$, which we assume now.

From Proposition 5.5, we obtain that there is some $A \in \mathrm{GSp}(V)$, a subfield $L \leq K$ such that there is an (L, AGA^{-1})-rational symplectic plane H_L. Since the statements of Theorem 1.1 are not affected by this conjugation, we may now assume that H_L is (L,G)-rational.

From Corollary 7.4, we obtain an (L,G)-rational symplectic space $I_{1,L}$ such that $\mathcal{L}(G) \subseteq I_{1,K} \cup I_{1,K}^\perp$. If $I_{1,K} = V$, then it follows that $I_{1,L} \cong L^n$, thus G contains a transvection whose direction is any vector of $I_{1,L}$. As the transvections generate the symplectic group, it follows that G contains

Brought to you by | Biblioteca de la Universidad de Sevilla
Authenticated
Download Date | 10/13/16 7:54 AM

$\mathrm{Sp}(I_{1,L}) \cong \mathrm{Sp}_n(L)$ and we are in Case 3 of Theorem 1.1. Hence, suppose now that $I_{1,K} \neq V$.

Either every $g \in G$ stabilises $I_{1,K}$, and we are in Case 1 and done, or there is $g \in G$ and $v \in I_{1,L}$ with $g(v) \notin I_{1,K}$. Set $I_{2,L} := gI_{1,L}$. Note that $I_{2,L} \subseteq \mathcal{L}(G)$ because of Lemma 4.4. Now we apply Corollary 8.2 to the decomposition $V = I_{1,K} \oplus I_{1,K}^{\perp}$ and obtain that $g(I_{1,K}) \subseteq I_{1,K}^{\perp}$. Moreover

$$\mathcal{L}(G) = \mathcal{L}(gGg^{-1}) \subseteq gI_{1,K} \cup gI_{1,K}^{\perp} = I_{2,K} \cup I_{2,K}^{\perp}.$$

We now have $\mathcal{L}(G) \subseteq I_{1,K} \cup I_{2,K} \cup (I_{1,K} \oplus I_{2,K})^{\perp}$. Either $I_{1,K} \oplus I_{2,K} = V$ and $(I_{1,K} \oplus I_{2,K})^{\perp} = 0$, or there are two possibilities:

- For all $g \in G$, $gI_{1,L} \subseteq I_{1,K} \cup I_{2,K}$. If this is the case, then G fixes the space $I_{1,K} \oplus I_{2,K}$, and we are in Case 1, and done.
- There exists $g \in G$, $v \in I_{1,L}$ such that $g(v) \notin I_{1,K} \cup I_{2,K}$. Set $I_{3,L} = gI_{1,L}$. Due to $\mathcal{L}(G) \subseteq I_{3,K} \cup I_{3,K}^{\perp}$, we then have

$$\mathcal{L}(G) \subseteq I_{1,K} \cup I_{2,K} \cup I_{3,K} \cup (I_{1,K} \oplus I_{2,K} \oplus I_{3,K})^{\perp}.$$

Hence, iterating this procedure, we see that either we are in Case 1, or we obtain a decomposition $V = I_{1,K} \oplus \cdots \oplus I_{h,K}$ with mutually orthogonal symplectic spaces such that $\mathcal{L}(G) \subseteq I_{1,K} \cup \cdots \cup I_{h,K}$.

Note that Lemma 8.1 implies that G respects this decomposition in the sense that for all $i \in \{1, \ldots, h\}$ there is $j \in \{1, \ldots, h\}$ such that $g(I_{i,K}) = I_{j,K}$. If the resulting action of G on the index set $\{1, \ldots, h\}$ is not transitive, then we are again in case 1, otherwise in case 2. ∎

A. A result on transvections in a 3-dimensional vector space

In this appendix, we provide a proof of the following result concerning subgroups in a 3-dimensional vector space that was used in Section 6:

Proposition A.1. *Let V be a 3-dimensional vector space over a finite field K of characteristic $\ell \geq 5$, and let $G \subseteq \mathrm{SL}(V)$ be a subgroup satisfying:*

1. *There exists a 1-dimensional K-vector space U such that $G|_U = \{\mathrm{id}_U\}$.*
2. *There exist U_1, U_2, U_3 three distinct centres of transvections in G such that $U \nsubseteq U_1 \oplus U_2$ and $U \neq U_3$.*

Then $(U_1 \oplus U_2) \cap (U \oplus U_3)$ is the centre of a transvection of G.

This result is Theorem 3.1(a) of [10]. Below, we have written the proof in detail. We will essentially follow the original proof of Wagner [10], reformulating it with the terminology developed in this paper. We follow [8] when Wagner refers to the results proven there. We also used [9] to ‘get a feeling’ of the ideas used in [10].

Brought to you by | Biblioteca de la Universidad de Sevilla
Authenticated
Download Date | 10/13/16 7:54 AM

The setting differs from that of the rest of the paper, since there is no symplectic structure. One consequence of this is that the axis of a transvection τ in $\mathrm{SL}(V)$ is not determined by its centre. Given any plane $W \subset V$ and any line $U \subset V$, there exist transvections with axis W and centre U; namely, fixing an element $\varphi \in \mathrm{Hom}(V, K) = V^*$ of the dual vector space of V such that $W = \ker(\varphi)$, and fixing a nonzero vector $u \in U$, then all transvections in $\mathrm{SL}(V)$ with axis W and centre U are given by $\tau(v) := v + \lambda\varphi(v)u$ for some $\lambda \in K$ (cf. [4], p. 160).

A key input in the proof is Lemma 5.2. In order to apply it to a subplane $W \subset V$, we need to endow it with some symplectic structure. We do so by choosing any two linearly independent vectors e_1, e_2 and considering the symplectic structure defined by declaring $\{e_1, e_2\}$ to be a symplectic basis.

Proof of Proposition A.1. Without loss of generality, we may assume that G is generated by transvections. In particular, we may assume that $G \subseteq \mathrm{SL}(V)$.

The hypotheses imply that the inclusion $U_3 \subseteq (U_1 \oplus U) \cap (U_2 \oplus U)$ does not hold. Indeed, assume that $U_3 \subseteq (U_1 \oplus U) \cap (U_2 \oplus U)$. We know that $V = U_1 \oplus U_2 \oplus U$, hence $U_1 \oplus U \neq U_2 \oplus U$, so that $(U_1 \oplus U) \cap (U_2 \oplus U)$ has dimension 1. Therefore $U_3 = (U_1 \oplus U) \cap (U_2 \oplus U) = U$, but by hypothesis $U_3 \neq U$. Interchanging U_1 and U_2 if necessary we can assume that $U_3 \nsubseteq U_1 \oplus U$.

For $i = 2, 3$, let $W_{1,i} = U_1 \oplus U_i$ and $G_{1,i}$ be the subgroup of $\mathrm{GL}(W_{1,i})$ generated by the transvections in G that preserve the plane $W_{1,i}$. We want to endow $W_{1,i}$ with a suitable $(L, G_{1,i})$-rational structure. In particular, we want that these structures be compatible.

For each $i = 1, 2, 3$, fix a transvection $T_i \in G$ with centre U_i. Note that, since $G|_U$ is the identity and $U \neq U_i$, the axis of T_i (that is, the plane pointwise fixed by it) must be $U_i \oplus U$.

The transvections T_1 and T_2 preserve the plane $U_1 \oplus U_2$, and since this plane does not coincide with the axis of T_1 or T_2, they both act as nontrivial transvections on $U_1 \oplus U_2$. We apply Lemma 5.2 to the 2-dimensional K-vector space $W_{1,2}$ (which we endow with a symplectic structure with symplectic basis $\{u_1, u_2\}$ such that $u_1 \in U_1$ and $u_2 \in U_2$) and the group $G_{1,2}$ and obtain a matrix $A \in \mathrm{GL}_2(K)$ such that $AU_1 = U_1$, $AU_2 = U_2$ and a subfield L of K such that $(W_{1,2})_L$ is an $(L, AG_{1,2}A^{-1})$-rational plane. Since U is linearly independent from $U_1 \oplus U_2$, we can extend A to an element of $\mathrm{GL}(V)$ such that $AU = U$. Without loss of generality, we can replace G by AGA^{-1} and U_3 by AU_3. Thus $(W_{1,2})_L = \langle u_1, u_2 \rangle_L$ is an $(L, G_{1,2})$-rational plane.

Since $V = U_1 \oplus U_2 \oplus U$, we find $a_1, a_2 \in K$ such that $0 \neq u + a_1u_1 + a_2u_2 \in U_3$ with some $u \in U$. By hypothesis $a_2 \neq 0$. Hence by normalising, we can

Brought to you by | Biblioteca de la Universidad de Sevilla
Authenticated
Download Date | 10/13/16 7:54 AM

assume $0 \neq u_3 := -u + a_1u_1 + u_2 \in U_3$, so that we have the relation

$$u = a_1u_1 + u_2 + u_3. \tag{1.1}$$

The set $\mathcal{B} = \{u_1, u_2, u\}$ is a K-basis of V. The proof will be finished if we show that G contains a transvection of direction $u_3 - u = -a_1u_1 - u_2 \in (U \oplus U_3) \cap (U_1 \oplus U_2)$.

Now we consider the plane $W_{1,3}$, and endow it with a symplectic structure with symplectic basis $\{u_1, u_3\}$. We claim that $\langle u_1, u_3\rangle_L$ is an $(L, G_{1,3})$-rational plane. Indeed, if we show that $\langle u_1\rangle_L$ is an $(L, G_{1,3})$-rational line, then Corollary 5.6(b) applied to $U_{1,L} = \langle u_1\rangle_L$ and U_3 (which lies in $\mathcal{L}(G_{1,3})$ because by hypothesis G contains a transvection with centre U_3) yields the result. Consider the set of transvections of G with centre U_1. As discussed above, their axis is $U \oplus U_1 = \{v \in V : p_2(v) = 0\}$, where p_2 denotes the projection in the second coordinate with respect to the basis $\mathcal{B}$. Thus any transvection of G with direction U_1 can be written as $T_1(v) = v + \lambda p_2(v)u_1$ for some $\lambda \in K$. Restricting T_1 to $W_{1,2}$, and taking into account that $p_2(v) = -v \bullet u_1$ with $v \in W_{1,2}$ for the symplectic structure on $W_{1,2}$ with symplectic basis $\{u_1, u_2\}$, it follows from the $(L, G_{1,2})$-rationality of $\langle u_1, u_2\rangle_L$ that $\lambda \in L$. Now we restrict to $W_{1,3}$. Note that $p_2(v) = v \bullet u_1$ for $v \in W_{1,3}$, where $\bullet$ denotes the symplectic structure on $W_{1,3}$ defined by the symplectic basis $\{u_1, u_3\}$. Thus the restriction of T_1 to $W_{1,3}$ is $T_1(v) = v + \lambda(v \bullet u_1)u_1$. This proves the $(L, G_{1,3})$-rationality of $\langle u_1\rangle_L$.

The discussion above shows that, if we fix the basis $\{u_1, u_i\}$ of $W_{1,i}$, then $G_{1,i}$ contains $\mathrm{SL}_2(L)$; in particular it contains the reflection given by $(u_1 \mapsto -u_1, u_i \mapsto -u_i)$. Since G acts as the identity on U, we obtain that G contains the element $\delta_{1,i}$ given by $(u_1 \mapsto -u_1, u_i \mapsto -u_i, u \mapsto u)$. With respect to the basis $\mathcal{B}$, these elements have the shape

$$\delta_{1,2} = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \delta_{1,3} = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 2 & 1 \end{pmatrix}.$$

Thus

$$T := \delta_{1,2}\delta_{1,3} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 2 & 1 \end{pmatrix}$$

is a transvection of centre U and axis $U \oplus U_1$. Since 2 is invertible in $\mathbb{F}_\ell$, we

Brought to you by | Biblioteca de la Universidad de Sevilla
Authenticated
Download Date | 10/13/16 7:54 AM

can find $k \in \mathbb{Z}$ such that

$$T^k = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

The transvection $T^k \circ T_3 \circ T^{-k} \in G$ has direction $T^k(u_3) = u_3 - u$; this is the transvection we were seeking. ∎

Acknowledgements. S. A.-d.-R. worked on this article as a fellow of the Alexander-von-Humboldt foundation. She thanks the Université du Luxembourg for its hospitality during a long term visit in 2011. She was also partially supported by the project MTM2012-33830 of the Ministerio de Economía y Competitividad of Spain. L. V. D. was supported by the project MTM2012-33830 of the Ministerio de Economía y Competitividad of Spain and by an ICREA Academia Research Prize. G. W. was partially supported by the DFG collaborative research centre TRR 45, the DFG priority program 1489 and the Fonds National de la Recherche Luxembourg INTER/DFG/12/10COMFGREP. S. A.-d.-R. and G. W. thank the Centre de Recerca Matemàtica for its support and hospitality during a long term visit in 2010.

The authors thank the anonymous referee of [3] and Gunter Malle for suggesting the alternative proof of Theorem 1.1 based on Kantor's paper [6], which is given in [3].

References

[1] S. Arias-de-Reyna, L. Dieulefait, S. W. Shin, G. Wiese, *Compatible systems of symplectic Galois representations and the inverse Galois problem III. Automorphic construction of compatible systems with suitable local properties*, Math. Ann. 361(3) (2015), 909–925.

[2] S. Arias-de-Reyna, L. Dieulefait, G. Wiese, *Compatible systems of symplectic Galois representations and the inverse Galois problem I. Images of projective representations*, Trans. Amer. Math. Soc., in press, 2016.

[3] S. Arias-de-Reyna, L. Dieulefait, G. Wiese, *Compatible systems of symplectic Galois representations and the inverse Galois problem II. Transvections and huge image*, Pacific J. Math. 281(1) (2016), 1–16.

[4] E. Artin, *Geometric Algebra*, Interscience Publishers, Inc., New York-London, 1957.

[5] L. E. Dickson, *Linear Groups: With an Exposition of the Galois Field Theory*, with an introduction by W. Magnus, Dover Publications Inc., New York, 1958.

[6] W. M. Kantor, *Subgroups of classical groups generated by long root elements*, Trans. Amer. Math. Soc. 248 (1979), 347–379.

[7] S. Z. Li, J. G. Zha, *On certain classes of maximal subgroups in* $\mathrm{PSp}(2n, F)$, Sci. Sinica Ser. A 25 (1982), 1250–1257.

Brought to you by | Biblioteca de la Universidad de Sevilla
Authenticated
Download Date | 10/13/16 7:54 AM

[8] H. H. Mitchell, *Determination of the ordinary and modular ternary linear groups*, Trans. Amer. Math. Soc. 12 (1911), 207–242.
[9] H. H. Mitchell, *The subgroups of the quaternary Abelian linear group*, Trans. Amer. Math. Soc. 15 (1914), 379–396.
[10] A. Wagner, *Groups generated by elations*, Abh. Math. Sem. Univ. Hamburg 41 (1974), 190–205.

S. Arias-de-Reyna
UNIVERSITÉ DU LUXEMBOURG
FACULTÉ DES SCIENCES, DE LA TECHNOLOGIE ET DE LA COMMUNICATION
6, RUE RICHARD COUDENHOVE-KALERGI
L-1359 LUXEMBOURG, LUXEMBOURG
E-mail: sara.ariasdereyna@uni.lu

L. Dieulefait
DEPARTAMENT D'ÀLGEBRA I GEOMETRIA
FACULTAT DE MATEMÀTIQUES
UNIVERSITAT DE BARCELONA
GRAN VIA DE LES CORTS CATALANES, 585
08007 BARCELONA, SPAIN
E-mail: ldieulefait@ub.edu

G. Wiese
UNIVERSITÉ DU LUXEMBOURG
FACULTÉ DES SCIENCES, DE LA TECHNOLOGIE ET DE LA COMMUNICATION
6, RUE RICHARD COUDENHOVE-KALERGI
L-1359 LUXEMBOURG, LUXEMBOURG
E-mail: gabor.wiese@uni.lu

Received June 9, 2014; revised version December 12, 2014.

Brought to you by | Biblioteca de la Universidad de Sevilla
Authenticated
Download Date | 10/13/16 7:54 AM