ISRAEL JOURNAL OF MATHEMATICS 106 (1998), 13–28

FINITE QUOTIENTS OF THE PURE SYMPLECTIC BRAID GROUP

BY

KAY MAGAARD

Department of Mathematics, Wayne State University
Detroit, MI 48202, USA
e-mail: kaym@math.wayne.edu

AND

KARL STRAMBACH

Mathematische Institut, Universität Erlangen
Bismarckstrasse $1\frac{1}{2}$, 91054 Erlangen, Germany
e-mail: stramba@mi.uni-erlangen.de

AND

HELMUT VÖLKLEIN*

Department of Mathematics, University of Florida
Gainesville, FL 32611, USA
e-mail: helmut@math.ufl.edu

ABSTRACT

We show how the finite symplectic groups arise as quotients of the pure symplectic braid group. Via [SV] certain of these groups — in particular, all groups $\mathrm{Sp}_n(2)$ — occur as Galois groups over $\mathbb{Q}$.

Introduction

Let $\mathcal{B}_r$ be the Artin braid group on r strings, and $\mathcal{B}^{(r)} \subset \mathcal{B}_r$ the pure braid group. For each vector of parameters $\zeta = (\zeta_1, \ldots, \zeta_r)$ from a finite field $\mathbf{F}_q$ (satisfying certain conditions), a certain group $\mathcal{B}_r(\zeta)$ between $\mathcal{B}^{(r)}$ and $\mathcal{B}_r$ was defined in [V1], [V2], and a homomorphism $\Phi_\zeta : \mathcal{B}_r(\zeta) \to \mathrm{GL}_n(q)$, where $n = r - 2$. This

* Supported by NSF grant DMS-9306479.
Received September 9, 1996

is essentially the classical Gassner representation of $\mathcal{B}^{(r)}$ (a generalization of the Burau representation of $\mathcal{B}_r$) with coefficients in $\mathbf{F}_q$. The image of Φ_ζ, a certain subgroup Δ_ζ of $\mathrm{GL}_n(q)$, occurs naturally as a Galois group over various function fields. In [V1] and [V3] this led to Galois realizations (including GAL-realizations) over $\mathbb{Q}$ of certain groups $\mathrm{PGL}_n(q)$ and $\mathrm{PU}_n(q)$.

In [SV] a certain subgroup $\mathcal{L}_r$ of $\mathcal{B}_r$ for even $r = 2\ell$ was introduced in a geometric context. It has generators satisfying the braid relations of type C_ℓ (in the sense of Brieskorn [Br]), and we call it the symplectic braid group. It is shown in [SV] that the image Λ_ζ of $\mathcal{L}_r \cap \mathcal{B}_r(\zeta)$ under Φ_ζ also occurs naturally as a Galois group. The groups Λ_ζ are determined for certain values of ζ in the present paper, and this leads to Galois realizations over $\mathbb{Q}$ of certain of the simple groups $\mathrm{Sp}_n(2^s)$.

In §1 we define the Artin and symplectic braid groups and give some of their basic properties. In §2 we study the representations $\tilde{\Phi}_\zeta$ and Φ_ζ. The classification of the groups Λ_ζ in the most interesting case $\zeta^* = \zeta^{-1}$ is given in §3: We get $\Lambda_\zeta = \mathrm{Sp}_n(q)$ or $= \mathrm{Sp}_n(\sqrt{q})$. This is based on a deep theorem of Kantor [Ka] classifying primitive linear groups generated by transvections. An important step is to show that the orthogonal groups in characteristic 2 (one of the possibilities in Kantor's theorem) do not occur in our situation. It is just the most difficult part of this theorem (in characteristic 2) that yields our final Galois-theoretic application in §4. Finally, in the Appendix we indicate what happens in the other cases (where Λ_ζ is between a special and general linear (resp., unitary) group).

We obtain Galois realizations over $\mathbb{Q}$ (even GAL-realizations) for the symplectic groups $\mathrm{Sp}_n(2^f)$, essentially for $n > 2^{f+1}$, $n \neq 4$. In particular, all groups $\mathrm{Sp}_n(2)$ are included. This improves a result of Häfner [H] who realized those groups $\mathrm{Sp}_n(2)$ for which $n+1$ is a prime having 2 as a primitive residue mod $n+1$. See [MM] and [V4] for the notion of GAL- and GAR-realization, and further results on Galois realizations.

§1. The Artin and symplectic braid groups

1.1. THE ARTIN BRAID GROUP $\mathcal{B}_r$. Let G be a finite group, and $r \geq 2$ an integer. The free group F_{r-1} on generators $Q_1, \ldots, Q_{r-1}$ acts on r-tupels of group elements by the following rule: The element Q_i $(1 \leq i \leq r-1)$ sends $(g_1, \ldots, g_r) \in G^r$ to

$$(g_1, \ldots, g_{i+1}, g_{i+1}^{-1} g_i g_{i+1}, \ldots, g_r). \tag{1}$$

Here g_{i+1} is in the i-th place, and $g_{i+1}^{-1} g_i g_{i+1}$ in the $(i+1)$-th. All other entries are unchanged. We let F_{r-1} act from the right, so $Q_i Q_j$ acts by first applying Q_i,

then Q_j. One checks easily that the elements $Q_iQ_{i+1}Q_i$ and $Q_{i+1}Q_iQ_{i+1}$ induce the same transformation via (1) (for $i = 1, \dots, r-2$); same for the elements Q_iQ_j and Q_jQ_i with $|i-j| \geq 2$. Hence the above action of F_{r-1} induces an action of the **Artin braid group** $\mathcal{B}_r$, where $\mathcal{B}_r$ is the quotient of F_{r-1} by the above relations. From now on we work only in $\mathcal{B}_r$, and let the Q_i's denote the corresponding generators of $\mathcal{B}_r$.

Clearly there is a (unique) involutory automorphism ρ of $\mathcal{B}_r$ with

$$\rho(Q_i) = Q_{r-i} \quad \text{for } i = 1, \dots, r-1.$$

This automorphism is inner: $\rho(Q) = Q^R$ $(= R^{-1}QR)$ for each $Q \in \mathcal{B}_r$, where

$$R = Q_{r-1}(Q_{r-2}Q_{r-1}) \cdots (Q_1 \cdots Q_{r-1}).$$

1.2. THE MAP $\kappa : \mathcal{B}_r \to S_r$. From the defining relations of $\mathcal{B}_r$ it is clear that there is a (surjective) homomorphism $\kappa : \mathcal{B}_r \to S_r$ sending Q_i to the transposition $(i, i+1)$. The kernel of κ is called the **pure braid group**, and denoted by $\mathcal{B}^{(r)}$. We compute that $\kappa(R)$ is the permutation in S_r interchanging i and $r+1-i$ $(i = 1, \dots, r-1)$.

Let $\mathcal{C} = (C_1, \dots, C_r)$ be an r-tuple of conjugacy classes of G. For $\pi \in S_r$ let $\mathcal{C}^\pi = (C_{\pi(1)}, \dots, C_{\pi(r)})$. We let $E(\mathcal{C})$ be the set of all $(g_1, \dots, g_r) \in G^r$ with $g_i \in C_i$ for all i. Then each $Q \in \mathcal{B}_r$ maps the set $E(\mathcal{C})$ to $E(\mathcal{C}^{\kappa(Q)})$.

1.3. THE SYMPLECTIC BRAID GROUP. Now assume that $r = 2\ell$ is even. Let $\mathcal{L}_r$ be the subgroup of $\mathcal{B}_r$ generated by $P_1, \dots, P_\ell$, where

$$P_i = Q_iQ_{r-i} \quad \text{for } i = 1, \dots, \ell-1$$

and

$$P_\ell = Q_\ell.$$

These elements satisfy the braid relations of type C_ℓ; actually, this yields a presentation for $\mathcal{L}_r$, thus $\mathcal{L}_r$ is isomorphic to the braid group of type C_ℓ in the sense of [Br]. But this is not needed here and will appear elsewhere. We call $\mathcal{L}_r$ the **symplectic braid group**. For the geometric interpretation of the embedding of $\mathcal{L}_r$ into $\mathcal{B}_r$ see [SV].

Note that ρ centralizes $\mathcal{L}_r$. The map κ maps $\mathcal{L}_r$ onto $W \stackrel{\text{def}}{=} \kappa(\mathcal{L}_r) \leq S_r$, the Coxeter group of type C_ℓ. The **pure symplectic braid group** $\mathcal{L}^{(r)} = \mathcal{B}^{(r)} \cap \mathcal{L}_r$ is the kernel of this map $\mathcal{L}_r \to W$.

Remark 1: If $r = 2\ell + 1$ is odd then the elements $\bar{P}_i = Q_i Q_{r-i}$, $i < \ell$, and $\bar{P}_\ell = Q_\ell Q_{\ell+1} Q_\ell$ also satisfy the braid relations of type C_ℓ. Also they are centralized by ρ. The group generated by $\bar{P}_1, \ldots, \bar{P}_\ell$ has a similar geometric interpretation as $\mathcal{L}_r$, but this does not lead to new Galois realizations.

§2. Braid group action through the matrices $\tilde{\Phi}(Q, \zeta)$

2.1. Let q be a power of the prime p, and let $\mathbf{F}_q$ be the finite field with q elements. Let $r \geq 2$ be an integer. Let $Z = \langle \zeta_1, \ldots, \zeta_r \rangle$ be a subgroup of the multiplicative group $\mathbf{F}_q^*$, where $\zeta_i \neq 1$ for all i. Assume further $\mathbf{F}_q = \mathbf{F}_p(\zeta_1, \ldots, \zeta_r)$. Set $\zeta = (\zeta_1, \ldots, \zeta_r)$. We write $\zeta^\pi = (\zeta_{\pi(1)}, \ldots, \zeta_{\pi(r)})$ for $\pi \in S_r$. Let $\mathcal{B}_r(\zeta)$ (resp., $\mathcal{L}_r(\zeta)$) be the group of all $Q \in \mathcal{B}_r$ (resp., $Q \in \mathcal{L}_r$) with $\zeta^{\kappa(Q)} = \zeta$.

Let $\mathbf{G} \stackrel{\text{def}}{=} \mathbf{F}_q \times^s Z$ be the semi-direct product of Z and the additive group $\mathbf{F}_q$ (where Z acts on $\mathbf{F}_q$ via multiplication). We write the elements of $\mathbf{G}$ as pairs $[u, z]$ with $u \in \mathbf{F}_q, z \in Z$. For $i = 1, \ldots, r$ let $C(\zeta_i)$ be the conjugacy class of $\mathbf{G}$ consisting of all $[u, \zeta_i]$, $u \in \mathbf{F}_q$. Set $\mathcal{C} \stackrel{\text{def}}{=} (C(\zeta_1), \ldots, C(\zeta_r))$, and $E(\zeta) \stackrel{\text{def}}{=} E(\mathcal{C})$.

2.2. THE REPRESENTATION $\tilde{\Phi}_\zeta$. Write the elements of $E(\zeta)$ in the form

$$\Omega(u, \zeta) = ([u_1, \zeta_1], [u_2, \zeta_2], \ldots, [u_r, \zeta_r])$$

with $u = (u_1, \ldots, u_r)$ in the space $\tilde{U}$ of row vectors of length r over $\mathbf{F}_q$. One checks easily that

$$\Omega(u, \zeta)^{Q_i} = \Omega(u \cdot \tilde{\Phi}_i(\zeta), \zeta^{(i,i+1)})$$

for $i = 1, \ldots, r-1$, where $\tilde{\Phi}_i(\zeta) \in \mathrm{GL}_r(q)$ is the following matrix:

The matrix $\tilde{\Phi}_i(\zeta)$ has j-th column e_j for $j \notin \{i, i+1\}$, has i-th column e_{i+1} and $(i+1)$-th column $\zeta_{i+1}^{-1} e_i + \zeta_{i+1}^{-1}(\zeta_i - 1) e_{i+1}$. Here $e_1 = (1, 0, \ldots, 0)^t, \ldots, e_r = (0, \ldots, 0, 1)^t$ are the unit column vectors of length r.

Since the Q_i's generate $\mathcal{B}_r$, it follows that for each $Q \in \mathcal{B}_r$ there is unique $\tilde{\Phi}(Q, \zeta) \in \mathrm{GL}_r(q)$ such that

$$\Omega(u, \zeta)^Q = \Omega(u \cdot \tilde{\Phi}(Q, \zeta), \zeta^{\kappa(Q)}) \tag{2}$$

for all $u \in \tilde{U}$. Here $\kappa : \mathcal{B}_r \to S_r$ is the natural surjection from §1.2. For $Q, Q' \in \mathcal{B}_r$ we have

$$\tilde{\Phi}(QQ', \zeta) = \tilde{\Phi}(Q, \zeta) \tilde{\Phi}(Q', \zeta^{\kappa(Q)}), \tag{3}$$

and if $Q' \in \mathcal{B}_r(\zeta^{\kappa(Q)})$ then

$$\tilde{\Phi}(QQ'Q^{-1}, \zeta) = \tilde{\Phi}(Q, \zeta) \tilde{\Phi}(Q', \zeta^{\kappa(Q)}) \tilde{\Phi}(Q, \zeta)^{-1}. \tag{4}$$

The group $\mathcal{B}_r(\zeta)$ is the stabilizer in $\mathcal{B}_r$ of the set $E(\zeta)$, and it contains the pure braid group $\mathcal{B}^{(r)} = \ker(\kappa)$. The map $\tilde{\Phi}_\zeta : \mathcal{B}_r(\zeta) \to \mathrm{GL}_r(q)$ sending Q to $\tilde{\Phi}(Q,\zeta)$ is a homomorphism by (3). The image of this homomorphism is a subgroup of $\mathrm{GL}_r(q)$ that we denote by $\tilde{\Delta}_\zeta$. For even r we let $\tilde{\Lambda}_\zeta$ be the $\tilde{\Phi}_\zeta$-image of $\mathcal{L}_r(\zeta)$. Thus

$$\tilde{\Lambda}_\zeta \leq \tilde{\Delta}_\zeta \leq \mathrm{GL}_r(q).$$

Set $\zeta^* = \zeta^{\kappa(R)} = (\zeta_r, \ldots, \zeta_1)$. Then from (4) and §1.1 we get

$$\tilde{\Phi}_\zeta(\rho(Q)) = \tilde{\Phi}_\zeta(R^{-1}QR) = T\tilde{\Phi}_{\zeta^*}(Q)T^{-1}$$

for $Q \in \mathcal{B}_r(\zeta^*)$, where $T = \tilde{\Phi}(R^{-1}, \zeta) \in \mathrm{GL}_r(q)$. Note $\mathcal{B}_r(\zeta^*) = \rho(\mathcal{B}_r(\zeta))$, hence $\mathcal{L}_r(\zeta^*) = \mathcal{L}_r(\zeta)$. Thus we get

$$\tilde{\Phi}_\zeta(Q) = T\tilde{\Phi}_{\zeta^*}(Q)T^{-1} \tag{5}$$

for all $Q \in \mathcal{L}_r(\zeta)$ (if the latter is defined, i.e., if r is even).

2.3. THE INVARIANT HYPERPLANE H_ζ. In the following, we view $\mathrm{GL}_r(q)$ as acting on $\tilde{U}$ (the row vectors of length r) by right multiplication, and on the dual space $\tilde{V}$ of column vectors of length r by left multiplication.

The product of the entries of $\Omega(u,\zeta)$ is invariant under the braiding action. This product equals $[u \cdot v(\zeta), \zeta_1 \ldots \zeta_r]$, where

$$v(\zeta) = (1, \zeta_1, \zeta_1\zeta_2, \ldots, \zeta_1 \ldots \zeta_{r-1})^t \in \tilde{V}.$$

Thus $u \cdot v(\zeta) = u\tilde{\Phi}(Q,\zeta) \cdot v(\zeta^{\kappa(Q)})$, hence

$$\tilde{\Phi}(Q,\zeta)^{-1}v(\zeta) = v(\zeta^{\kappa(Q)}). \tag{6}$$

Thus $\tilde{\Delta}_\zeta$ fixes $v(\zeta) \in \tilde{V}$, and the corresponding hyperplane H_ζ of $\tilde{U}$ consisting of all $u \in \tilde{U}$ with $u \cdot v(\zeta) = 0$. For $u \in \tilde{U}$, the product of the entries of $\Omega(u,\zeta)$ equals $[0, \zeta_1 \ldots \zeta_r]$ if and only if $u \in H_\zeta$.

2.4. THE INVARIANT 1-SPACE E_ζ. Let the group $\mathrm{Aut}(G)$ act component-wise on G^r, i.e., $A \in \mathrm{Aut}(G)$ sends $(g_1, \ldots, g_r)$ to $(A(g_1), \ldots, A(g_r))$. If A is the inner automorphism of $\mathbf{G}$ induced by $[t,1]$ we obtain: A sends $\Omega(u,\zeta)$ to $\Omega(u+tu(\zeta),\zeta)$, where

$$u(\zeta) = (1-\zeta_1, 1-\zeta_2, \ldots, 1-\zeta_r) \in \tilde{U}.$$

Clearly, the action of $\mathrm{Aut}(G)$ centralizes the braid group action on G^r. Thus A maps $\Omega(u,\zeta)^Q$ to $\Omega(u+tu(\zeta),\zeta)^Q$. Hence $\Omega(u\tilde{\Phi}(Q,\zeta) + tu(\zeta^{\kappa(Q)}), \zeta^{\kappa(Q)}) = \Omega(u+tu(\zeta),\zeta)^Q$. Hence

$$u(\zeta) \cdot \tilde{\Phi}(Q,\zeta) = u(\zeta^{\kappa(Q)}). \tag{7}$$

Thus $\tilde{\Delta}_\zeta$ fixes $u(\zeta)$, and the 1-dimensional subspace E_ζ of $\tilde{U}$ spanned by this vector. One checks that H_ζ contains E_ζ (i.e., $u(\zeta) \cdot v(\zeta) = 0$) if and only if $\zeta_1 \cdots \zeta_r = 1$.

2.5. ALL INVARIANT SUBSPACES. For $i = 1, \ldots, r-1$ we have $Q_i^2 \in \mathcal{B}^{(r)} \subset \mathcal{B}_r(\zeta)$. Hence the matrix $\tilde{B}_i \stackrel{\text{def}}{=} \tilde{\Phi}_\zeta(Q_i^2)$ lies in $\tilde{\Delta}_\zeta$. One computes that $\tilde{B}_i$ has j-th column e_j for $j \notin \{i, i+1\}$, has i-th column

$$\zeta_{i+1}^{-1} e_i + \zeta_{i+1}^{-1}(\zeta_i - 1) e_{i+1}$$

and has $(i+1)$-st column

$$\zeta_i^{-1}(1 - \zeta_{i+1}^{-1}) e_i + (1 - \zeta_{i+1}^{-1} + \zeta_{i+1}^{-1}\zeta_i^{-1}) e_{i+1}.$$

PROPOSITION 1: *Suppose $r \geq 4$. Then the non-trivial, proper subspaces of $\tilde{U}$ invariant under $\tilde{\Delta}_\zeta$ are exactly E_ζ and H_ζ. In particular, $\tilde{\Delta}_\zeta$ acts irreducibly in H_ζ/E_ζ (resp., in H_ζ) if $\zeta_1 \cdots \zeta_r = 1$ (resp., if $\zeta_1 \cdots \zeta_r \neq 1$). The same holds for the group $\langle \tilde{B}_1, \ldots, \tilde{B}_{r-1} \rangle$ in place of $\tilde{\Delta}_\zeta$. If $r > 4$ then $\tilde{\Delta}_\zeta$ acts primitively in H_ζ/E_ζ (resp., in H_ζ).*

Proof: Once we have shown that $\tilde{\Delta}_\zeta$ acts irreducibly in H_ζ/E_ζ (resp., in H_ζ) then it follows by the argument in [V2, Cor. 2] that it even acts primitively if $r > 4$. Since E_ζ and H_ζ are invariant under $\tilde{\Delta}_\zeta$, it suffices to prove the claim for the group $\Gamma := \langle \tilde{B}_1, \ldots, \tilde{B}_{r-1} \rangle$.

STEP 1: Each Γ-invariant subspace W of $\tilde{U}$ has dimension ≤ 1 or $\geq r-1$.

Proof: Let $d = \dim W$.

CASE 1: *Γ fixes all vectors in W.* Then the annihilator W' of W in $\tilde{V}$ is a subspace of codimension d such that the $\tilde{B}_i$ act trivially in $\tilde{V}/W'$. Hence W' contains all vectors

$$\tilde{B}_i \cdot e_i - e_i = (\zeta_{i+1}^{-1} - 1) e_i + \zeta_{i+1}^{-1}(\zeta_i - 1) e_{i+1}$$

which clearly span a hyperplane of $\tilde{V}$. Thus $d \leq 1$.

CASE 2: *We have $w \cdot \tilde{B}_i - w \neq 0$ for some i and some $w \in W$.* The space of all $u \cdot \tilde{B}_i - u$, $u \in \tilde{U}$ is 1-dimensional, spanned by the vector

$$(0, \ldots, 0, \zeta_i, -1, 0, \ldots, 0)$$

(where ζ_i is in the i-th coordinate). Hence W contains this vector (by the hypothesis of Case 2). However, it is clear that the images of this vector under all $\tilde{B}_j$ span a hyperplane of $\tilde{U}$. Thus $d \geq r-1$. This completes Step 1.

STEP 2: It follows from Step 1 that E_ζ is the only Γ-invariant 1-space in $\tilde{U}$ (if there was another one, their sum would be a Γ-invariant 2-space). Similarly, H_ζ is the only Γ-invariant hyperplane in $\tilde{U}$. This proves the Proposition.

COROLLARY 1: *Suppose $r > 4$ and not all $\zeta_i = -1$. Let $n = r-2$ (resp., $n = r-1$) if $\zeta_1 \cdots \zeta_r = 1$ (resp., if $\zeta_1 \cdots \zeta_r \neq 1$). Let $\bar{\Delta}$ be the subgroup of $\mathrm{PGL}(H_\zeta/E_\zeta)$ (resp., $\mathrm{PGL}(H_\zeta)$) induced by $\tilde{\Delta}_\zeta$. Then $\bar{\Delta}$ contains a subgroup isomorphic to $\mathrm{PSL}_n(q)$ or $\mathrm{PSU}_n(q)$, unless q is odd and either $n = 3$, $\bar{\Delta} = \mathrm{PU}_3(4)$, or $n = 4$, $\bar{\Delta} = \mathrm{PSU}_4(4)$.*

Proof: As in [V2, proof of Prop. 3] we see that $\bar{\Delta}$ contains a non-involutory homology (since not all $\zeta_i = -1$). As in [V2, Cor. 6] we see that $\bar{\Delta}$, in its action on the projective space associated with H_ζ/E_ζ, resp., H_ζ, does not leave a proper projective subspace of the same dimension (defined over a subfield of $\mathbf{F}_q$) invariant. Since $\bar{\Delta}$ acts primitively, the claim follows from Wagner's theorem [Wa2]. ∎

Actually, for $\zeta_1 \cdots \zeta_r = 1$ the groups $\bar{\Delta}$ have been completely classified in [V2, Theorem 1]. If q is a square, we let $\mathrm{SU}_n(q)$ denote the special unitary group in $\mathrm{GL}_n(q)$, **not** that in $\mathrm{GL}_n(q^2)$. (This departs from current group-theoretic notation, but is more convenient for our purpose.)

2.6. THE NORMALIZED REPRESENTATION Φ_ζ AND THE INVARIANT BILINEAR FORM. From now on we assume $\zeta_1 \cdots \zeta_r = 1$. Let U (resp., V) be the space of row (resp., column) vectors of length $n := r-2$ over $\mathbf{F}_q$. Let $\lambda : \tilde{U} \to U$, $(x_1, \ldots, x_r) \mapsto (x_2, \ldots, x_{r-1})$. Each coset in H_ζ/E_ζ contains exactly one $u \in H_\zeta$ with first coordinate zero. Mapping this coset to $\lambda(u)$ we obtain an isomorphism $\lambda_\zeta : H_\zeta/E_\zeta \to U$.

The group $\tilde{\Delta}_\zeta$ acts naturally (from the right) on H_ζ/E_ζ. Via the isomorphism λ_ζ, this yields a right action of $\tilde{\Delta}_\zeta$ on U. Let $\Phi_\zeta : \mathcal{B}_r(\zeta) \to \mathrm{GL}_n(q)$ be the homomorphism such that this action of $\tilde{\Phi}_\zeta(Q)$ on U is given by right multiplication with the matrix $\Phi_\zeta(Q)$:

$$u_0 \cdot \Phi_\zeta(Q) = \lambda_\zeta(\lambda_\zeta^{-1}(u_0) \cdot \tilde{\Phi}_\zeta(Q)), \quad u_0 \in U.$$

The homomorphism Φ_ζ is the same occurring in Theorem 1 of [V2]. The image Δ_ζ of Φ_ζ — a subgroup of $\mathrm{GL}_n(q)$ — has been determined in [loc. cit.].

Set $\mathcal{L}_r(\zeta) = \mathcal{B}_r(\zeta) \cap \mathcal{L}_r$. Let Λ_ζ be the image of $\mathcal{L}_r(\zeta)$ under Φ_ζ. Thus

$$\Lambda_\zeta \leq \Delta_\zeta \leq \mathrm{GL}_n(q).$$

Let $\zeta^{-1} = (\zeta_1^{-1}, \ldots, \zeta_r^{-1})$, and note $\mathcal{B}_r(\zeta^{-1}) = \mathcal{B}_r(\zeta)$. The representation Φ_ζ of $\mathcal{B}_r(\zeta)$ is dual to $\Phi_{\zeta^{-1}}$ by [V2, Prop.2]. Hence if $\zeta^* = \zeta^{-1}$ then it follows from (5) that the restriction of Φ_ζ to $\mathcal{L}_r(\zeta)$ is self-dual. This proves the first part of

PROPOSITION 2:

(a) *If $\zeta^* = \zeta^{-1}$ then Λ_ζ leaves a non-degenerate bilinear form on U invariant.*

(b) *If q is a square and $\zeta^* = \bar{\zeta}$, where $\bar{\zeta} = (\zeta_1^{\sqrt{q}}, \ldots, \zeta_r^{\sqrt{q}})$, then Λ_ζ is conjugate to a subgroup of $\mathrm{GL}_n(\sqrt{q})$ by an element of $\mathrm{GL}_n(K)$, K an algebraic closure of $\mathbf{F}_q$.*

Proof: It remains to prove (b). For $t \in K$ write $\bar{t} = t^{\sqrt{q}}$, and for $A \in \mathrm{GL}_r(K)$ let $\bar{A}$ be the matrix obtained by applying the automorphism $t \mapsto \bar{t}$ to each coefficient. From (5) there is $S \in \mathrm{GL}_n(q)$ such that $\Phi_\zeta(P) = S\Phi_{\zeta^*}(P)S^{-1} = S\Phi_{\bar{\zeta}}(P)S^{-1} = S\overline{\Phi_\zeta(P)}S^{-1}$ for all $P \in \mathcal{L}_r(\zeta)$. By Lang's theorem (e.g., [Ca, p.32]) there is $A \in \mathrm{GL}_r(K)$ with $S = A^{-1}\bar{A}$. Then $A\Phi_\zeta(P)A^{-1} = \bar{A}\overline{\Phi_\zeta(P)}\bar{A}^{-1} = \overline{A\Phi_\zeta(P)A^{-1}}$ for all $P \in \mathcal{L}_r(\zeta)$. This proves (b).

§3. Classification of the groups Λ_ζ in the case $\zeta^* = \zeta^{-1}$

From now on we assume the following

HYPOTHESIS (**SYM**): *$r = 2\ell > 10$ is even, and $\zeta^* = \zeta^{-1} \neq \zeta$; the latter means $\zeta_i^{-1} = \zeta_{r-i+1}$ for $i = 1, \ldots, r$, and $\zeta \neq (-1, \ldots, -1)$. We further assume $\zeta_1 \ldots \zeta_\ell \neq 1$.*

The latter condition can always be achieved by permuting $\zeta_1, \ldots, \zeta_r$ by an element of W using (4) (which amounts to replacing Λ_ζ by a conjugate). Note that **(SYM)** implies that $\zeta_1 \cdots \zeta_r = 1$, hence $E_\zeta \subset H_\zeta$.

By **(SYM)** and Proposition 2, the group Λ_ζ leaves a non-degenerate bilinear form f on U invariant.

3.1. THE MAXIMAL ISOTROPIC SUBSPACES U_1 AND U_2. Let $\tilde{U}_1$ (resp., $\tilde{U}_2$) be the subspace of $\tilde{U}$ consisting of the vectors with zeroes in the last (resp., first) ℓ coordinates. Set $\zeta^{(1)} = (\zeta_1, \ldots, \zeta_\ell)$, $\zeta^{(2)} = (\zeta_{\ell+1}, \ldots, \zeta_r)$. Let $H^{(i)}$ be the natural copy of $H_{\zeta^{(i)}}$ in $\tilde{U}_i$. Then $H^{(i)} = H_\zeta \cap \tilde{U}_i$. Since $\zeta_1 \cdots \zeta_\ell \neq 1$ we have $E_{\zeta^{(i)}} \not\subset H_{\zeta^{(i)}}$ (see 2.4). This implies that $E_\zeta \not\subset H^{(1)} \oplus H^{(2)}$, hence

$$H_\zeta = H^{(1)} \oplus H^{(2)} \oplus E_\zeta.$$

Let U_i be the λ_ζ-image of $H^{(i)}$ in U ($\cong H_\zeta/E_\zeta$). Then $U = U_1 \oplus U_2$, and $\dim U_1 = \dim U_2 = \ell - 1$.

Let $\mathcal{L}^+$ be the subgroup of $\mathcal{L}_r$ generated by $P_1, \ldots, P_{\ell-1}$. The map $Q_i \mapsto Q_i Q_{r-i}$ extends to an isomorphism $\mathcal{B}_\ell \to \mathcal{L}^+$. (The inverse of this isomorphism is the restriction to $\mathcal{L}^+$ of the map induced by the embedding of spaces $\mathcal{Q}_\ell \to \mathcal{O}_\ell$, see [SV, §3].) Let $\mathcal{L}^+(\zeta)$ be the subgroup of $\mathcal{L}^+$ corresponding to $\mathcal{B}_\ell(\zeta^{(1)})$ under this isomorphism; then $\mathcal{L}^+(\zeta) = \mathcal{L}^+ \cap \mathcal{B}_r(\zeta)$. Let $\Lambda^+ := \Phi_\zeta(\mathcal{L}^+(\zeta))$. Clearly, $\tilde{U}_1$ and $\tilde{U}_2$ are invariant under $\tilde{\Phi}_\zeta(\mathcal{L}^+(\zeta))$, hence U_1 and U_2 are invariant under Λ^+, and Λ^+ acts on U_1 as the group $\Delta_{\zeta^{(1)}}$.

Hence by Corollary 1 we know that Λ^+, in its action on U_1, induces a group containing $\mathrm{SL}_m(q)$ or $\mathrm{SU}_m(q)$, where $m = \dim U_1 = \ell - 1 > 4$. Thus U_1 is totally isotropic for the invariant form f, since $\mathrm{SL}_m(q)$ and $\mathrm{SU}_m(q)$ do not fix a non-zero bilinear form.

It follows that the action of Λ^+ in $U/U_1 \cong U_2$ is dual to that in U_1. Hence Λ^+ acts irreducibly, faithfully and inequivalently in U_1 and U_2. The latter follows from the fact that the natural representation of $\mathrm{SL}_m(q)$ as well as that of $\mathrm{SU}_m(q)$ is not self-dual. Further, it follows that also U_2 is totally isotropic.

3.2. THE TRANSVECTION B_ℓ. Let $\epsilon_1 = (1, 0, \ldots, 0)$, $\ldots$, $\epsilon_r = (0, \ldots, 0, 1)$ be the unit row vectors of length r. The element $\tilde{B}_\ell = \tilde{\Phi}_\zeta(Q_\ell^2) = \tilde{\Phi}_\zeta(P_\ell^2)$ from 2.5 lies in $\tilde{\Lambda}_\zeta$. Under hypothesis **(SYM)** we get

$$\begin{aligned} \epsilon_j \tilde{B}_\ell &= \epsilon_j \quad \text{for } j \neq \ell, \ell+1, \\ \epsilon_\ell \tilde{B}_\ell &= \zeta_\ell \epsilon_\ell + (\zeta_\ell^{-1} - 1)\epsilon_{\ell+1}, \\ \epsilon_{\ell+1} \tilde{B}_\ell &= \zeta_\ell(\zeta_\ell - 1)\epsilon_\ell + (2 - \zeta_\ell)\epsilon_{\ell+1}. \end{aligned}$$

Thus $\tilde{B}_\ell$ acts on $\tilde{U}$ as a transvection with center spanned by the vector $(\zeta_\ell - 1)\epsilon_\ell + (\zeta_\ell^{-1} - 1)\epsilon_{\ell+1}$ (i.e., $\mathrm{Im}(\tilde{B}_\ell - \mathrm{id})$ is a 1-space spanned by this vector, and this 1-space lies in $\ker(\tilde{B}_\ell - \mathrm{id})$). Then also the element $B_\ell \stackrel{\text{def}}{=} \Phi_\zeta(Q_\ell^2)$ of Λ_ζ acts as a transvection on U.

3.3. PRIMITIVITY.

PROPOSITION 3: *The group Λ_ζ acts primitively in U.*

Proof:

CLAIM 1: *Λ_ζ acts irreducibly.* Since $U = U_1 \oplus U_2$, and the subgroup Λ^+ of Λ_ζ acts irreducibly and inequivalently in U_1 and U_2, it suffices to show that Λ_ζ does not fix U_1 or U_2. This means that $\tilde{\Lambda}_\zeta$ does not fix $H^{(i)} + E_\zeta$. We use the element $\tilde{B}_\ell \in \tilde{\Lambda}_\zeta$ from 3.2.

We consider the case $i = 2$, the case $i = 1$ is similar. Take

$$u = (0, \ldots, 0, u_{\ell+1}, \ldots, u_r)$$

in $H^{(2)}$ with $u_{\ell+1} \neq 0$. Assume the vector $u' = u \cdot \tilde{B}_\ell$ lies in $H^{(2)} + E_\zeta$. Then it lies in $H^{(2)}$ since its first $\ell - 1$ coordinates are zero (by the shape of the matrix $\tilde{B}_\ell$) and each non-zero vector in E_ζ has all coordinates non-zero (see 2.4). Thus the ℓ-th coordinate of u' is also zero. On the other hand, the ℓ-th coordinate of u' equals $\zeta_\ell(\zeta_\ell - 1)u_{\ell+1}$ by 3.2. This is a contradiction (since all ζ_i are different from 0 and 1). This proves Claim 1.

CLAIM 2: Λ_ζ *acts primitively.* Now assume $U = W_1 \oplus \cdots \oplus W_k$ where Λ_ζ permutes the n/k-dimensional spaces W_i transitively, and $k > 1$. This yields a homomorphism ψ from Λ_ζ to the symmetric group S_k. Let Λ' be the subgroup of Λ^+ isomorphic to $\mathrm{SL}_m(q)$ or $\mathrm{SU}_m(q)$. Then also Λ' acts irreducibly and inequivalently in U_1 and U_2. Hence if ψ restricted to Λ' is trivial then $k = 2$ and $W_i = U_i$. But clearly the element $\tilde{B}_\ell$ does not permute $H^{(1)} + E_\zeta$ and $H^{(2)} + E_\zeta$, hence B_ℓ does not permute U_1 and U_2. Thus ψ cannot be trivial on Λ'.

Hence k exceeds the minimal permutation degree of the group Λ'. Since $\Lambda' \cong \mathrm{SL}_m(q)$ or $\cong \mathrm{SU}_m(q)$, and $k \leq 2m$, this contradicts [Co] Table 1.

3.4. NO INVARIANT QUADRATIC FORM.

LEMMA 1: *The group Λ_ζ does not leave a non-zero quadratic form on U invariant.*

Proof: Assume $\Pi \neq 0$ is a Λ_ζ-invariant quadratic form on U. Then its associated bilinear form $(a, b) \mapsto \Pi(a+b) - \Pi(a) - \Pi(b)$ is non-zero (since Λ_ζ is irreducible), hence non-degenerate (again since Λ_ζ is irreducible). Thus we may assume that this bilinear form is the above f. Then f is symmetric.

If q is odd then no transvection on U leaves a non-degenerate symmetric bilinear form invariant. But Λ_ζ contains a transvection by 3.2. Hence q must be even. Then f is a non-degenerate symplectic form.

We use the notation from 3.1. For $i = 1, 2$ let $u^{(i)}$ (resp., $E^{(i)}$) be the natural copy of $u(\zeta^{(i)})$ (resp., $E_{\zeta^{(i)}}$) in $\tilde{U}_i$. Thus $u^{(1)} = (1 - \zeta_1, \ldots, 1 - \zeta_\ell, 0, \ldots, 0)$, $u^{(2)} = (0, \ldots, 0, 1 - \zeta_{\ell+1}, \ldots, 1 - \zeta_r)$ and $u(\zeta) = u^{(1)} + u^{(2)}$ (see 2.4). Also $E^{(i)} = \langle u^{(i)} \rangle$, $E_\zeta = \langle u(\zeta) \rangle$, of course. We have $\tilde{U}_i = H^{(i)} + E^{(i)}$ since $\zeta_1 \cdots \zeta_\ell \neq 1$, and $H_\zeta = H^{(1)} + H^{(2)} + E_\zeta$.

The space $\langle \epsilon_\ell, \epsilon_{\ell+1}, u^{(1)}, u^{(2)} \rangle$ is $\tilde{B}_\ell$-invariant by 3.2 (since it contains the center of $\tilde{B}_\ell$). Thus also the 3-space

$$\tilde{D} \stackrel{\text{def}}{=} \langle \epsilon_\ell, \epsilon_{\ell+1}, u^{(1)}, u^{(2)} \rangle \cap H_\zeta$$

is $\tilde{B}_\ell$-invariant. Let D be the λ_ζ-image of $\tilde{D}/E_\zeta$ ($\subset H_\zeta/E_\zeta$). Then D is a B_ℓ-invariant 2-space in U. Using the element $x_1 \in D$ from below, we see that B_ℓ

does not act trivially in D. Hence the center $C = \mathrm{Im}(B_\ell - \mathrm{id})$ of B_ℓ is contained in D; and D is not contained in the axis $\ker(B_\ell - \mathrm{id})$ of B_ℓ. Since the axis of a symplectic transvection is the full perpendicular space of its center, it follows that f does not vanish on D. Since f is symplectic, the 2-space D is f-nondegenerate.

Now consider again the quadratic form Π. It vanishes on U_i $(i = 1, 2)$, since $\mathrm{SL}_m(q)$ and $\mathrm{SU}_m(q)$ do not leave a non-zero quadratic form invariant (see 3.1). Hence $X_i \overset{\text{def}}{=} U_i \cap D$ is a Π-isotropic subspace of D. To compute X_i, consider the vectors

$$x^{(1)} = (\zeta_1 \cdots \zeta_\ell - 1)\zeta_1^{-1} \cdots \zeta_{\ell-1}^{-1}\epsilon_\ell + u^{(1)} \quad \text{and} \quad x^{(2)} = (\zeta_1^{-1} \cdots \zeta_\ell^{-1} - 1)\epsilon_{\ell+1} + u^{(2)}.$$

They satisfy $x^{(1)} \in \langle \epsilon_\ell, u^{(1)} \rangle \cap H^{(1)} \subset \tilde{D}$ and $x^{(2)} \in \langle \epsilon_{\ell+1}, u^{(2)} \rangle \cap H^{(2)} \subset \tilde{D}$. Since U_i is the (isomorphic) λ_ζ-image of $H^{(i)}$, it follows that the λ_ζ-image x_i of $x^{(i)}$ lies in $U_i \cap D = X_i$, and $x_i \neq 0$. Since X_i is a Π-isotropic subspace of D we have $\dim X_i \leq 1$, hence $X_i = \langle x_i \rangle$. Also $X_1 \neq X_2$ (since $U_1 \cap U_2 = 0$).

The 2-space D is f-nondegenerate, hence contains at most two Π-isotropic 1-spaces. Thus X_1, X_2 are exactly those, hence must be interchanged by B_ℓ. The condition $x_1 \cdot B_\ell \in \langle x_2 \rangle$ means $x^{(1)} \cdot \tilde{B}_\ell \in \langle x^{(2)}, u(\zeta) \rangle$. A simple calculation using 3.2 yields that the latter holds iff $\zeta_\ell = \zeta_1 \cdots \zeta_{\ell-1}$.

Thus a necessary condition for the existence of Π is that

$$\zeta_\ell = \zeta_1 \cdots \zeta_{\ell-1}.$$

However, if Λ_ζ leaves a quadratic form on U invariant, then the same holds for Λ_{ζ^π} for each $\pi \in W = \kappa(\mathcal{L}_r)$ (see 1.3). Indeed, $\tilde{\Lambda}_{\zeta^\pi}$ is conjugate $\tilde{\Lambda}_\zeta$ in $\mathrm{GL}_r(q)$ by formula (4), hence also Λ_{ζ^π} is conjugate Λ_ζ in $\mathrm{GL}_n(q)$.

Thus we must have $\zeta_{\pi(\ell)} = \zeta_{\pi(1)} \cdots \zeta_{\pi(\ell-1)}$ for all $\pi \in W$ with $\zeta_{\pi(1)} \cdots \zeta_{\pi(\ell)} \neq 1$; in particular, for all $\pi \in S_\ell$. This implies $\zeta_1 = \cdots = \zeta_\ell$ and $\zeta_1^{\ell-2} = 1$. Now choose $\pi \in W$ with $\zeta_{\pi(1)} = \zeta_1^{-1}$, $\zeta_{\pi(2)} = \zeta_2^{-1}$, $\zeta_{\pi(j)} = \zeta_j$ otherwise. Then $\zeta_{\pi(1)} \cdots \zeta_{\pi(\ell)} \neq 1$, but we do not have $\zeta_{\pi(1)} = \cdots = \zeta_{\pi(\ell)}$. This contradiction completes the proof of Lemma 1.

3.5. APPLICATION OF KANTOR'S THEOREM. So far our methods have been rather elementary. Now we use a stronger tool: Kantor's classification [Ka] of the primitive subgroups of $\mathrm{GL}_n(q)$ that contain a transvection. This yields our main result:

THEOREM 1: *Let $r = 2\ell > 10$ and let q be a prime power. Let $n = r - 2$. Let $\zeta_1, \ldots, \zeta_r$ be generators of the field $\mathbf{F}_q$ with $\zeta_i \neq 0, 1$ for all i. Assume $(\zeta_1^{-1}, \ldots, \zeta_r^{-1}) = (\zeta_r, \ldots, \zeta_1) \neq (-1, \ldots, -1)$. Let $\zeta = (\zeta_1, \ldots, \zeta_r)$. Then Λ_ζ is*

conjugate in $\mathrm{GL}_n(q)$ *to either* $\mathrm{Sp}_n(q)$ *or* $\mathrm{Sp}_n(\sqrt{q})$. *The latter case occurs if and only if* q *is a square and all* ζ_i *have norm 1 over* $\mathbf{F}_{\sqrt{q}}$.

Proof: We know that Λ_ζ acts primitively on U and leaves a non-degenerate bilinear form f on U invariant. Further, Λ_ζ contains a transvection by 3.2. Let G be the normal subgroup of Λ_ζ generated by the conjugates of this transvection. Then G acts irreducibly on U. By [Wa1] for q odd and by [Po, Thm. 1] for q even, it follows that G is as in case (T1), (T2) or (T3) of Kantor's theorem [Ka, Th. II].

In case (T3), q is even and $G = S_{n+1}$ or $G = S_{n+2}$, acting on the n-dimensional space U as on the non-trivial irreducible constituent of its natural permutation module. Thus the image of G in the projective group of U is self-normalizing, which means that $\Lambda_\zeta \mathbf{F}_q^*/\mathbf{F}_q^* \cong S_{n+1}$ or $\cong S_{n+2}$. Restricting to the subgroup Λ' we obtain a contradiction similarly as in Proposition 3. Thus case (T3) cannot occur.

In case (T2), q is even and G is conjugate $O_n^{\pm}(q_0)$, where q is a power of q_0. Thus G leaves a non-degenerate quadratic form II on U invariant, hence also the associated bilinear form

$$f'(x,y) = \mathrm{II}(x+y) + \mathrm{II}(x) + \mathrm{II}(y). \tag{8}$$

Since G acts absolutely irreducibly on U, f' is a scalar multiple of f, the above Λ_ζ-invariant form. Since G is normal in Λ_ζ (and II is the only G-invariant quadratic form on U, up to scalar multiples), the group Λ_ζ fixes II up to scalar multiples. Since Λ_ζ fixes f, hence f', it actually fixes II (by (8)). But this is excluded by Lemma 1.

Thus we are in case (T1). This means that G is conjugate to $\mathrm{SL}_n(q_0)$, $\mathrm{SU}_n(q_0)$ or $\mathrm{Sp}_n(q_0)$, where q is a power of q_0. Since the first two groups do not fix a non-zero bilinear form, it follows that $G = \mathrm{Sp}_n(q_0)^\alpha$ for some $\alpha \in \mathrm{GL}_n(q)$. Since $\mathrm{Sp}_n(q_0)^\alpha$ fixes a unique bilinear form on U (up to scalar multiples), this form equals the Λ_ζ-invariant form f. Thus

$$\mathrm{Sp}_n(q_0)^\alpha = G \lhd \Lambda_\zeta \leq \mathrm{Sp}_n(q)^\alpha. \tag{9}$$

Thus the centralizer of G in $\mathrm{GL}_n(q)$ is $\mathbf{F}_q^*$, the group of scalars. Since Λ_ζ fixes a non-zero bilinear form, we have $\Lambda_\zeta \cap \mathbf{F}_q^* = \pm 1$, hence $\Lambda_\zeta/\{\pm 1\}$ embeds into $\mathrm{Aut}(G)$ via conjugation. Consider again the subgroup $\Lambda' \cong \mathrm{SL}_m(q)$ or $\cong \mathrm{SU}_m(q)$ of Λ_ζ from the proof of Proposition 3. Since $\mathrm{Out}(G)$ is abelian and Λ' is perfect, we get that $\Lambda' \subset G$.

Consider an element d of Λ' acting in U_1 as the diagonal matrix $\mathrm{diag}(t, 1, \ldots, 1)$; then d acts in U_2 dually as $\mathrm{diag}(t^{-1}, 1, \ldots, 1)$. Since Λ' induces $\mathrm{SL}_m(q)$ or $\mathrm{SU}_m(q)$ on U_1, such d exists where t generates the field $\mathbf{F}_q$ over its prime field. Since $d \in G \subset \mathrm{GL}_n(q_0)^\alpha$, the eigenvalues of d are permuted by the absolute Galois group of $\mathbf{F}_{q_0}$. Thus $t^{q_0} = t$ or $t^{q_0} = t^{-1}$, hence $t^{q_0^2} = t$ in any case. It follows that $q_0 = q$ or $q_0^2 = q$.

If q is a square and $\zeta^* = \bar{\zeta}$ as in Proposition 2(b), then there is $A \in \mathrm{GL}_n(K)$ with $\Xi := \Lambda_\zeta^A \subset \mathrm{GL}_n(\sqrt{q})$. The group Ξ fixes a non-degenerate bilinear form over K, unique up to scalar multiples. Thus in its action on the space of bilinear forms over K, Ξ has a 1-dimensional eigenspace for the eigenvalue 1. Since $\Xi \subset \mathrm{GL}_n(\sqrt{q})$, this eigenspace is defined over $\mathbf{F}_{\sqrt{q}}$. Hence Ξ lies in a conjugate of $\mathrm{Sp}_n(\sqrt{q})$. Thus $|\Lambda_\zeta| = |\Xi| \leq |\mathrm{Sp}_n(\sqrt{q})| \leq |G|$. Since $G \leq \Lambda_\zeta$ it follows that $\Lambda_\zeta = G = \mathrm{Sp}_n(\sqrt{q})^\alpha$.

If q and ζ are not as in the preceding paragraph, then for $\zeta^{(1)} = (\zeta_1, \ldots, \zeta_\ell)$ we are not in the case that q is a square and all entries of $\zeta^{(1)}$ have norm 1 over $\mathbf{F}_{\sqrt{q}}$. In this case it follows as in [V2], Theorem 1, that $\Delta_{\zeta^{(1)}}$ ($\cong \Lambda^+$) contains $\mathrm{SL}_m(q)$. Thus we can take $\Lambda' \cong \mathrm{SL}_m(q)$. Then we can choose the above d such that $t^{q_0} \neq t^{-1}$. Then $t^{q_0} = t$ by the above, thus $q_0 = q$. Then clearly $\Lambda_\zeta = G = \mathrm{Sp}_n(q)^\alpha$ from (9).

§4. Galois realizations of symplectic groups

Corollary 4.2 of [SV] gives conditions that force the image H of Λ_ζ in $\mathrm{PGL}_n(q)$ to occur as a Galois group over $\mathbb{Q}$. The first condition is that H is self-normalizing in $\mathrm{PGL}_n(q)$. This holds if q is even and Λ_ζ is conjugate to $\mathrm{Sp}_n(q)$ or $\mathrm{Sp}_n(\sqrt{q})$. Besides conditions assumed in Theorem 1 there is one further condition: The tuple ζ is W-rational, i.e., for each integer m prime to $q-1$ the elements $\zeta_1^m, \ldots, \zeta_\ell^m$ are a permutation of $\zeta_1^{\epsilon_1}, \ldots, \zeta_\ell^{\epsilon_\ell}$ with $\epsilon_i = \pm 1$.

To construct such ζ, assume $q = 4^s$ is a power of 4. Let h be the number of generators of the (cyclic) group $\mathbf{F}_q^*$ (resp., of the group S of all elements of $\mathbf{F}_q^*$ of norm 1 over $\mathbf{F}_{\sqrt{q}}$). Assume $\ell \geq h$. Take $\zeta_1, \ldots, \zeta_h$ to be the generators of $\mathbf{F}_q^*$ (resp., of S), and take the remaining ζ_i's with $i \leq \ell$ to be equal to some fixed element of order 3. Finally, choose $\zeta_{r-i+1} = \zeta_i^{-1}$ for $i \leq \ell$. Then if $\ell > 5$ the hypothesis of Theorem 1 holds, and thus we get $\Lambda_\zeta \cong \mathrm{Sp}_n(q)$ if $q > 4$ (resp., $\Lambda_\zeta \cong \mathrm{Sp}_n(\sqrt{q})$ if s is odd). Also ζ is W-rational. Now given any $f \geq 1$, set $s = f/2$ (i.e., $q = 2^f$) if f is even and $s = f$ (i.e., $q = 4^f$) otherwise. Let ϕ denote Euler's ϕ-function. Then we get

THEOREM 2: *The simple group* $\mathrm{Sp}_n(2^f)$, $1 \leq f \neq 2$, $n \geq 10$, *occurs as a Galois group over* $\mathbb{Q}$ *(actually, it has a* GAL*-realization over* $\mathbb{Q}$*) if* $n \geq 2\phi(2^f - 1)$ *for even* f *and* $n \geq 2\phi(2^f + 1)$ *for odd* f.

For the notion of GAL-realization see also [V4], Ch. 8. It remains to justify the GAL-realization in Theorem 2. We get it from Corollary 4.2 of [SV] for even f, since the centralizer of $H = \mathrm{PSp}_n(q)$ in $\mathrm{P\Gamma L}_n(q)$ is trivial, and $[\mathrm{Aut}(H) : \mathrm{Inn}(H)] = f$. If f is odd, we have to modify that Corollary. Let I be the subgroup of index two of $\mathrm{P\Gamma L}_n(q)$ with $\mathrm{PGL}_n(q) \subset I$. It also suffices that the centralizer of $H = \mathrm{PSp}_n(\sqrt{q})$ in I is trivial, and $[\mathrm{Aut}(H) : \mathrm{Inn}(H)] = [I : \mathrm{PGL}_n(q)]$. The proof is the same.

Remark 3: For the groups $\mathrm{Sp}_n(2)$, the bound in Theorem 2 can be improved to be $n \geq 6$, using $q = 4$ and $\zeta = (t, \ldots, t, t^{-1}, \ldots, t^{-1})$ with $t^3 = 1$ (done by [GAP]). The group $\mathrm{Sp}_4(2) \cong S_6$ of course also occurs regularly over $\mathbb{Q}$, but we don't get a GAL-realization because of the exceptional outer automorphism. Thus all groups $\mathrm{Sp}_n(2)$ occur regularly over $\mathbb{Q}$. This improves a result of Häfner [H] who showed this for all n such that $n+1$ is a prime having 2 as a primitive root mod $n+1$.

Remark 4: The group $\mathrm{Sp}_n(4)$ has a GAL-realization over $\mathbb{Q}$ if $n \geq 6$ satisfies $n \equiv 2 \bmod 4$. Indeed, then $r = n+2$ is divisible by 4, say $r = 4r_0$, and we get a W-rational tuple ζ with $\zeta_1 = \cdots = \zeta_{r_0}$ of order 5 in $\mathbf{F}_{16}$. Then $\Lambda_\zeta \cong \mathrm{Sp}_n(4)$ for $n \geq 10$ by Theorem 1; for $n = 6$ use [GAP].

Appendix: Irreducibility of Λ_ζ

For possible later use, we give here a proof for the irreducibility of Λ_ζ in the general case, only assuming $\zeta_1 \cdots \zeta_r = 1$ (but not the hypothesis $\zeta^* = \zeta^{-1}$ from §3). This would be a first step in proving that Λ_ζ is between a special and general linear (resp., unitary) group if $\zeta^* \neq \zeta^{-1}$.

PROPOSITION: *Suppose* $\ell \geq 4$, $\zeta_1 \cdots \zeta_r = 1$ *and* $\zeta \neq \zeta^*$. *Then* $\tilde{\Lambda}_\zeta$ *acts irreducibly in* H_ζ / E_ζ.

Proof: We use the notation from §3. Let $\mathcal{L}_*$ be the subgroup of $\mathcal{B}_r$ generated by $P_1, \ldots, P_{\ell-1}$. Let $\mathcal{L}^* = \mathcal{L}_* \cap \mathcal{B}^{(r)}$. The map $Q_i \mapsto Q_i Q_{r-i}$ extends to an isomorphism $\mathcal{B}_\ell \to \mathcal{L}_*$. This induces an isomorphism $\mathcal{B}^{(\ell)} \to \mathcal{L}^*$. Identify $\mathcal{L}^*$ with $\mathcal{B}^{(\ell)}$ via this isomorphism.

The representation $\tilde{\Phi}_\zeta$ restricted to $\mathcal{L}^* \cong \mathcal{B}^{(\ell)}$ leaves $\tilde{U}_i$ invariant (for $i = 1, 2$). It yields the representation $\tilde{\Phi}_{\zeta^{(1)}}$ of $\mathcal{B}^{(\ell)}$ on $\tilde{U}_1$ (where we identify $\tilde{U}_i$ with the

space of row vectors of length ℓ by dropping the last resp., first, ℓ coordinates). On $\tilde{U}_2$ we obtain the representation $\tilde{\Phi}_{\zeta^{(2)}} \circ \rho_0$, where ρ_0 is the restriction to $\mathcal{B}^{(\ell)}$ of the (inner) automorphism ρ_ℓ of $\mathcal{B}_\ell$ with $\rho_\ell(Q_i) = Q_{\ell-i}$ (see 1.1). Set $\Lambda = \tilde{\Phi}_\zeta(\mathcal{L}^*)$. From Proposition 1, the non-trivial, proper subspaces of $\tilde{U}_i$ invariant under Λ are exactly $E^{(i)}$ and $H^{(i)}$. Note that $H^{(i)} \subset H_\zeta$.

If $\zeta_1 \cdots \zeta_\ell = 1$ then $E^{(i)} \subset H^{(i)}$ (by 2.4). Then the representation of $\mathcal{L}^* \cong \mathcal{B}^{(\ell)}$ in $H^{(i)}/E^{(i)}$ induced by $\tilde{\Phi}_\zeta$ is equivalent to $\Phi_{\zeta^{(1)}}$, respectively, $\Phi_{\zeta^{(2)}} \circ \rho_0$ (see 2.6). From §1.1 and formula (4) we get

$$\Phi_{\zeta^{(2)}} \circ \rho_0(Q) = \Phi_{\zeta^{(2)}}(R_\ell^{-1} Q R_\ell) = T \Phi_{(\zeta^{(2)})^*}(Q) T^{-1}, \quad Q \in \mathcal{B}^{(\ell)}$$

where $R_\ell \in \mathcal{B}_\ell$ satisfies $\rho_\ell(Q) = R_\ell^{-1} Q R_\ell$ for all $Q \in \mathcal{B}_\ell$ (see 1.1) and $T = \Phi(R_\ell^{-1}, \zeta^{(2)})$ and $(\zeta^{(2)})^* \stackrel{\text{def}}{=} (\zeta^{(2)})^{\kappa(R_\ell^{-1})} = (\zeta_r, \ldots, \zeta_{\ell+1})$.

Since $\zeta \neq \zeta^*$ we have $\zeta^{(1)} \neq (\zeta^{(2)})^*$. Hence the restrictions to $\mathcal{B}^{(\ell)}$ of $\Phi_{\zeta^{(1)}}$ and of $\Phi_{(\zeta^{(2)})^*}$ are not equivalent by [V2, Cor. 4] (note $\ell \geq 4$). Thus $H^{(1)}/E^{(1)}$ and $H^{(2)}/E^{(2)}$ are non-isomorphic Λ-modules. They are irreducible by Proposition 1. (When speaking of Λ-modules we mean $\mathbf{F}_q[\Lambda]$-modules, to be precise.)

In the other case $\zeta_1 \cdots \zeta_\ell \neq 1$, $H^{(1)}$ and $H^{(2)}$ are irreducible Λ-modules, and one can similarly show that they are non-isomorphic.

CASE 1: *If $\zeta_1 \cdots \zeta_\ell \neq 1$ then the Proposition holds.*

Proof: In this case $H_\zeta = H^{(1)} + H^{(2)} + E_\zeta$. Hence any proper Λ-submodule of H_ζ that properly contains E_ζ must equal $H^{(i)} + E_\zeta$ for $i = 1$ or $i = 2$. Thus it suffices to show that $H^{(i)} + E_\zeta$ is not $\tilde{\Lambda}_\zeta$-invariant. This is as in the proof of Proposition 3.

CASE 2: If $\zeta_1 \cdots \zeta_\ell = 1$ then we can permute the ζ_i using formula (4) to reduce to Case 1. (Note that not all ζ_i are equal because we assumed $\zeta^* \neq \zeta$.)

References

[Br] E. Brieskorn, *Die Fundamentalgruppe des Raumes der regulären Orbits einer endlichen komplexen Spiegelungsgruppe*, Inventiones Mathematicae **12** (1971), 57–61.

[Ca] R. W. Carter, *Finite Groups of Lie Type – Conjugacy Classes and Complex Characters*, Wiley, Chichester, 1985.

[Co] B. Cooperstein, *Minimal degree for a permutation representation of a classical group*, Israel Journal of Mathematics **30** (1978), 213–235.

[H] F. Häfner, *Einige orthogonale und symplektische Gruppen als Galoisgruppen über* $\mathbb{Q}$, Mathematische Annalen **292** (1992), 587–618.

[Ka] W. M. Kantor, *Subgroups of classical groups generated by long root elements*, Transactions of the American Mathematical Society **248** (1979), 347–379.

[MM] G. Malle and H. Matzat, *Inverse Galois Theory*, book manuscript.

[Po] H. Pollatsek, *Irreducible groups generated by transvections over finite fields of characteristic 2*, Journal of Algebra **39** (1976), 328–333.

[GAP] M. Schönert et al., *Groups, Algorithms and Programming*, Lehrstuhl D für Mathematik, RWTH, Aachen, Germany.

[SV] K. Strambach and H. Völklein, *The symplectic braid group and Galois realizations*, in *Proceedings of the 1995 Luminy Conference on "Moduli Spaces in the Inverse Galois Problem"* (P. Lochak and L. Schneps, eds.), to appear in the Lecture Notes of the London Mathematical Society series, Cambridge University Press.

[V1] H. Völklein, $\mathrm{GL}_n(q)$ *as Galois group over the rationals*, Mathematische Annalen **293** (1992), 163–176.

[V2] H. Völklein, *Braid group action through* $\mathrm{GL}_n(q)$ *and* $U_n(q)$, *and Galois realizations*, Israel Journal of Mathematics **82** (1993), 405–427.

[V3] H. Völklein, *Braid group action, embedding problems and the groups* $\mathrm{PGL}(n,q)$, $\mathrm{PU}(n,q^2)$, Forum Mathematicum **6** (1994), 513–535.

[V4] H. Völklein, *Groups as Galois Groups – An Introduction*, Cambridge Studies in Advanced Mathematics **53**, Cambridge University Press, 1996.

[Wa1] A. Wagner, *Groups generated by elations*, Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg **41** (1974), 190–205.

[Wa2] A. Wagner, *Collineation groups generated by homologies of order greater than 2*, Geometriae Dedicata **7** (1978), 387–398.