ISRAEL JOURNAL OF MATHEMATICS 82 (1993), 405–427

BRAID GROUP ACTION VIA $\mathrm{GL}_n(q)$ AND $\mathrm{U}_n(q)$, AND GALOIS REALIZATIONS

BY

HELMUT VÖLKLEIN*

Department of Mathematics, University of Florida
Gainesville, FL 32611, USA
and
Universität Erlangen, Germany

Dedicated to Prof. J. G. Thompson

ABSTRACT

We determine the braid group action on generating systems of a group that is the semi-direct product of a finite vector space with a group of scalars. This leads to Galois realizations of certain groups $\mathrm{GL}_n(q)$ and $\mathrm{PU}_n(q)$.

Introduction

A new criterion for realizing groups as Galois groups was given in [V1]. This criterion involves a transitivity condition for the braid group action on certain generating systems of a finite group G. If this condition and others are satisfied, then a certain subgroup of $\mathrm{Aut}(G)$ occurs as a Galois group over the rationals $\mathbb{Q}$ (even as Galois group of a regular extension of $\mathbb{Q}(x)$).

The criterion was applied in [V1] to a group G that is the semi-direct product of a finite vector space $V = \mathbb{F}_q^n$ with a group Z of scalars. As a result, the group $\mathrm{GL}_n(q)$ was realized as Galois group over $\mathbb{Q}$ for certain values of n and q. All conditions from the criterion but the braid group transitivity were easy to check. For this transitivity, one needs to determine the subgroup Δ_ζ of $\mathrm{GL}_n(q)$

* Partially supported by an NSA grant.
This work was done while the author was a fellow of the Institute for Advanced Studies in Jerusalem.
Received March 10, 1992

generated by certain explicit matrices (coming from the elementary braids). Even though stronger than necessary conditions on q and n were imposed (essentially $n \geq 3q$) to keep this group-theoretic problem manageable, its solution occupied much of the paper [V1].

The present paper contains a more systematic study of the above group-theoretic situation. The original goal was to find the exact conditions on q and n under which the above criterion would realize $\mathrm{GL}_n(q)$ over $\mathbb{Q}$. It was expected that the group Δ_ζ would usually contain $\mathrm{SL}_n(q)$, with one known exception in the case that $q = p$ is a prime (and $Z =< -1 >$). This exceptional case yields $\Delta_\zeta = \mathrm{Sp}_n(p)$ (the symplectic group).

Surprisingly, it turned out that Δ_ζ is a unitary group in many cases. This will lead to Galois realizations of certain unitary groups. The necessary group-theoretic work is contained in the present paper. However, one also needs a modification of the above criterion. Since this requires methods quite different from those of the present paper, it will be developed in later work.

Theorem 1 of the present paper gives the classification of the groups Δ_ζ that arise from the braid group action. The proof is given in part 1 of the paper. Important steps are to show that Δ_ζ is irreducible (§1.3), and to construct invariant bilinear and hermitian forms (§1.4). The proof is then completed by appealing to a result of Wagner [Wa] that classifies primitive linear groups containing non-involutory homologies.

In part 2 we apply Theorem 1 to give Galois realizations for certain groups $\mathrm{GL}_n(q)$ and $\mathrm{PU}_n(q)$. This is based on the criterion from [V1], and on an extended version of this criterion (to appear in [V2]).

§1. Classifying the groups Δ_ζ

§1.1. Nielsen classes and braid group action.

Fix an integer $r \geq 3$. Let G be a finite group. Let $\mathcal{E}_r$ denote the set of r-tuples $(g_1, ..., g_r) \in G^r$ with the following properties: $g_1 \cdots g_r = 1$, the group G is generated by $g_1, ..., g_r$, and $g_i \neq 1$ for all i.

The free group F_{r-1} on generators $Q_1, ..., Q_{r-1}$ acts on $\mathcal{E}_r$ by the following rule: The element Q_i $(1 \leq i \leq r-1)$ sends $(g_1, ..., g_r)$ to

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

We let F_{r-1} act from the right, so Q_iQ_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 of $\mathcal{E}_r$ (for $i = 1, ..., r-2$); same for the elements Q_iQ_j and Q_jQ_i with $|i-j| \geq 2$. Hence the action of F_{r-1} induces an action of the *Artin braid group* $\mathcal{B}_r$ on $\mathcal{E}_r$, 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 $\mathcal{B}_r$.

Let $\mathbf{C} = (C_1, ..., C_r)$ be an r-tuple of conjugacy classes of G. We let $\mathcal{E}(\mathbf{C})$ be the set of all $(g_1, ..., g_r) \in \mathcal{E}_r$ with $g_i \in C_i$ for all i. Further, the Nielsen class $\mathrm{Ni}(\mathbf{C})$ is defined to be the set of all $(g_1, ..., g_r) \in \mathcal{E}_r$ for which there is a permutation $\pi \in S_r$ with $g_{\pi(i)} \in C_i$ for all i.

Clearly, the set $\mathrm{Ni}(\mathbf{C})$ is invariant under the above action of $\mathcal{B}_r$. Each element $Q \in \mathcal{B}_r$ sends the set $\mathcal{E}(\mathbf{C})$ to $\mathcal{E}({}^{\kappa(Q)}\mathbf{C})$, where $\kappa : \mathcal{B}_r \to S_r$ is the (surjective) homomorphism sending Q_i to the transposition $(i, i+1)$. In particular, the kernel $\mathcal{B}^{(r)}$ of the map $\kappa : \mathcal{B}_r \to S_r$ – called the **pure braid group** – fixes the set $\mathcal{E}(\mathbf{C})$.

§1.2. BRAID GROUP ACTION THROUGH THE MATRICES $\Phi(Q, \zeta)$.

Fix an integer $n \geq 2$ and set $r = n + 2$. Let q be a power of the prime p, and let $\mathbb{F}_q$ be the finite field with q elements. Let $Z = < \eta_1, ..., \eta_r >$ be a subgroup of the multiplicative group $\mathbb{F}_q^*$, where $\eta_1 ... \eta_r = 1$ and $\eta_i \neq 1$ for all i. Assume further $\mathbb{F}_q = \mathbb{F}_p(\eta_1, ..., \eta_r)$.

In the following, $\zeta_1, ..., \zeta_r$ will always be some permutation of $\eta_1, ..., \eta_r$. Set $\zeta = (\zeta_1, ..., \zeta_r)$, $\eta = (\eta_1, ..., \eta_r)$. If $(\zeta_1, ..., \zeta_r) = (\eta_{\pi(1)}, ..., \eta_{\pi(r)})$ with $\pi \in S_r$, then we write $\zeta = {}^{\pi}\eta$ for short.

Let V be the elementary abelian group $\mathbb{F}_q^n$. Let $G \stackrel{\mathrm{def}}{=} V \times^s Z$ be the semi-direct product of V and Z (where Z acts on V via scalar multiplication). We write the elements of G as pairs $[v, z]$ with $v \in V$, $z \in Z$. For $i = 1, ..., r$, let $C(\zeta_i)$ be the conjugacy class of G consisting of all $[v, \zeta_i]$, $v \in V$. Set $\mathbf{C}_\zeta \stackrel{\mathrm{def}}{=} (C(\zeta_1), ..., C(\zeta_r))$, and $\mathcal{E}(\zeta) \stackrel{\mathrm{def}}{=} \mathcal{E}(\mathbf{C}_\zeta)$ (see §1.1 for notation).

LEMMA 1: *Each element of $\mathcal{E}(\zeta)$ is conjugate under V to exactly one element of the form*

$$(*) \qquad ([0, \zeta_1], [v_1, \zeta_2], ..., [v_{n+1}, \zeta_r]), \quad v_i \in V.$$

Define $\lambda_1, ..., \lambda_n \in Z$ by setting $\lambda_i = \zeta_{i+1}^{-1} \cdots \zeta_{n+1}^{-1}$. Then an element of the *form (*) lies in* $\mathcal{E}(\zeta)$ *if and only if* $v_1, ..., v_n$ *is an* $\mathbb{F}_q$*-basis of* V*, and* $v_{n+1} = -\lambda_1 v_1 - \cdots - \lambda_n v_n$.

The proof of the lemma is straightforward (details omitted).

For each matrix $B \in \mathrm{GL}_n(q)$ and each permutation ζ of η, let $F(B,\zeta)$ denote the element of the form (*), where $v_1, ..., v_n$ are the column vectors of the matrix B, and v_{n+1} is given in terms of $v_1, ..., v_n$ and ζ as in the Lemma. Note that from the definitions in §1.1, the set $\mathrm{Ni}(\mathbf{C}_\eta)$ is the union of the sets $\mathcal{E}(\zeta)$, as ζ runs over the permutations of η. It follows that each element of $\mathrm{Ni}(\mathbf{C}_\eta)$ is V-conjugate to exactly one element of the form $F(B,\zeta)$. This yields a 1-1 correspondence between the quotient $\mathrm{Ni}(\mathbf{C}_\eta)/V$ and the set of pairs (B,ζ), where $B \in \mathrm{GL}_n(q)$, and ζ is any permutation of η.

Thus the action of the braid group $\mathcal{B}_r$ on $\mathrm{Ni}(\mathbf{C}_\eta)/V$ (via (1)) induces an action on the set of pairs (B,ζ). Denote this action by $(B,\zeta) \mapsto (B,\zeta)^Q$ $(Q \in \mathcal{B}_r)$. Let $e_1, ..., e_n$ be the standard basis of $V = \mathbb{F}_q^n$ (i.e., e_1 is the vector with entries $1, 0, ..., 0$ etc.). Straightforward computations yield:

LEMMA 2: *For* $i = 1, ..., r-1$*, and for each pair* (B,ζ) *as above, we have*

$$(B,\zeta)^{Q_i} \;=\; (B\ \Phi_i(\zeta), {}^{(i,i+1)}\zeta)$$

where $(i, i+1)$ *is the transposition switching* i *and* $i+1$*, and* $\Phi_i(\zeta) \in \mathrm{GL}_n(q)$ *is the following matrix:*

(a) *For* $i = 2, ..., n$*, the matrix* $\Phi_i(\zeta)$ *has* j*-th column* e_j *for* $j \notin \{i, i-1\}$*, has* $(i-1)$*-st column* e_i *and* i*-th column* $\zeta_{i+1}^{-1} e_{i-1} + \zeta_{i+1}^{-1}(\zeta_i - 1)e_i$.

(b) *The matrix* $\Phi_1(\zeta)$ *has first column* $\zeta_2^{-1}(\zeta_2 - 1)^{-1}(1-\zeta_1)e_1$ *and* j*-th column* $(\zeta_2 - 1)^{-1}(1 - \zeta_{j+1})e_1 + e_j$ *for* $j = 2, ..., n$.

(c) *The matrix* $\Phi_{n+1}(\zeta)$ *has* j*-th column* e_j *for* $j = 1, ..., n-1$*, and* n*-th column* $-\lambda_1 e_1 - \cdots - \lambda_n e_n$ *with* $\lambda_1, ..., \lambda_n$ *as in Lemma 1.*

Recalling that the elements of $\mathcal{B}_r$ act from the right, we get

$$(B,\zeta)^{Q_i Q_j} \;=\; (B\ \Phi_i(\zeta)\ \Phi_j({}^{(i,i+1)}\zeta),\ {}^{(i,i+1)}({}^{(j,j+1)}\zeta)). \tag{2}$$

In general, since the Q_i's generate $\mathcal{B}_r$, it follows that for each $Q \in \mathcal{B}_r$ and for each ζ there is unique $\Phi(Q,\zeta) \in \mathrm{GL}_n(q)$ such that

$$(B,\zeta)^Q \;=\; (B\ \Phi(Q,\zeta), {}^{\kappa(Q)}\zeta) \tag{3}$$

for all $B \in \mathrm{GL}_n(q)$. Thereby $\kappa : \mathcal{B}_r \to S_r$ is the natural surjection from §1.1 (sending Q_i to the transposition $(i, i+1)$).

We get the rules:

$$\text{(4)} \qquad \Phi(QQ', \zeta) = \Phi(Q,\zeta)\ \Phi(Q', {}^{\kappa(Q)}\zeta), \quad \Phi(Q^{-1}, \zeta) = \Phi(Q, {}^{\kappa(Q)^{-1}}\zeta)^{-1},$$

$$\text{(5)} \qquad \Phi(QQ'Q^{-1}, \zeta) = \Phi(Q,\zeta)\ \Phi(Q', {}^{\kappa(Q)}\zeta)\ \Phi(Q,\zeta)^{-1},$$

Let $\mathcal{B}_r(\zeta)$ be the group of all $Q \in \mathcal{B}_r$ with ${}^{\kappa(Q)}\zeta = \zeta$. The group $\mathcal{B}_r(\zeta)$ is the stabilizer in $\mathcal{B}_r$ of the set $\mathcal{E}(\zeta)$ (see (3)), and it contains the pure braid group $\mathcal{B}^{(r)} = \ker(\kappa)$. Each $Q \in \mathcal{B}_r(\zeta)$ sends the pair (B,ζ) to $(B\ \Phi(Q,\zeta),\zeta)$ (see (3)). Hence the map $\Phi_\zeta : \mathcal{B}_r(\zeta) \to \mathrm{GL}_n(q)$ sending Q to $\Phi(Q,\zeta)$ is a homomorphism. The image of this homomorphism is a subgroup of $\mathrm{GL}_n(q)$ that we denote by Δ_ζ. We clearly have :

COROLLARY 1: *The braid group $\mathcal{B}_r$ acts transitively on the set $Ni(\mathbf{C}_\eta)/V$ (via (1)) if and only if $\Delta_\zeta = \mathrm{GL}_n(q)$.*

If these equivalent conditions hold, and ζ is rational (see §2), then by [V1] the group $\mathrm{GL}_n(q)$ $(= \Delta_\zeta)$ is a Galois group over $\mathbb{Q}(x)$. (Without the rationality condition, we get it only as a Galois group over $\mathbb{Q}_{ab}(x)$). But we also get Galois realizations for Δ_ζ (or some related groups) in certain cases when it is a proper subgroup of $\mathrm{GL}_n(q)$ (see §2).

Before we can go further with this, we need a classification of the groups Δ_ζ. This is given in the following theorem. Thereby, we view $V = \mathbb{F}_q^n$ as $\mathbb{F}_q$-vector space of column vectors, on which the group $\mathrm{GL}_n(q)$ acts by left multiplication; and q is a power of the prime p.

THEOREM 1: *Let $\zeta_1, \ldots, \zeta_r$ be generators of the finite field $\mathbb{F}_q$ satisfying $\zeta_1 \cdots \zeta_r = 1$ and $\zeta_i \neq 1$ for all i. Set $\zeta = (\zeta_1, \ldots, \zeta_r)$ and $n = r-2$. Suppose $n \geq 2$. Let Δ_ζ be the image of the homomorphism $\Phi_\zeta : \mathcal{B}_r(\zeta) \to \mathrm{GL}_n(q)$. Then Δ_ζ acts absolutely irreducibly on $V = \mathbb{F}_q^n$. Furthermore:*

(a) *Δ_ζ leaves a non-zero bilinear form on V invariant if and only if $q = p$ is a prime, n is even and $\zeta = (-1, \ldots, -1)$. In this case,*

$$\Delta_\zeta = \mathrm{Sp}_n(p).$$

(b) *Δ_ζ leaves a non-zero hermitian form on V invariant if and only if $q = q_0^2$ is a square and all ζ_i have norm 1 over $\mathbb{F}_{q_0}$. In this case,*

$$\mathrm{SU}_n(q) \le \Delta_\zeta \le \mathrm{U}_n(q)$$

with possible exceptions (E1)–(E4) below.

(c) *If ζ is not as in (a) or (b), and if $n > 2$, then*

$$\mathrm{SL}_n(q) \le \Delta_\zeta \le \mathrm{GL}_n(q)$$

with exceptions (E3) and (E4).

Let $\bar{\Delta}_\zeta$ denote the image of Δ_ζ in $\mathrm{PGL}_n(q)$.

(d) *If $n = 2$ then $\bar{\Delta}_\zeta$ is (conjugate to) $\mathrm{PSL}_2(q_0)$ or $\mathrm{PGL}_2(q_0)$, $q \in \{q_0, q_0^2\}$, with exceptions (E1) and (E2).*

The exceptional cases are as follows:

(E1) *$n = 2$ and $\zeta = (t, t, -t^{-1}, -t^{-1})$ (up to permutation) with $t^4 \neq 1$. In this case, $\bar{\Delta}_\zeta$ is dihedral of order $2m$, with m prime to q.*

(E2) *$n = 2$, and $\bar{\Delta}_\zeta \cong A_4, S_4$ or A_5. If $p > 5$ then $\zeta_i\zeta_j \neq 1$ for all $i \neq j$.*

(E3) *$n = 3$, $p > 3$ and $\zeta = (-\epsilon, -\epsilon, -\epsilon, -\epsilon, \epsilon^{-1})$ with $\epsilon^3 = 1$ (up to permutation). In this case, $\bar{\Delta}_\zeta \cong \mathrm{PU}_3(4) \cong \mathbb{F}_3^2 \times^s \mathrm{SL}_2(3)$.*

(E4) *$n = 4$, $p > 3$ and $\zeta = (-\epsilon, -\epsilon, -\epsilon, -\epsilon, -\epsilon, -\epsilon)$ with $\epsilon^3 = 1$, $\epsilon \neq 1$. In this case, $\bar{\Delta}_\zeta \cong \mathrm{PSU}_4(4) \cong \mathrm{PSp}_4(3)$.*

Thereby $\mathrm{Sp}_n(q)$ (resp., $\mathrm{U}_n(q)$) denotes the invariance group in $\mathrm{GL}_n(q)$ of a non-degenerate symplectic (resp., hermitian) form on V. And $\mathrm{SU}_n(q)$ is the intersection of $\mathrm{U}_n(q)$ and $\mathrm{SL}_n(q)$.

Remark 1: The case $n = 2$

If $\zeta = (t, t, t, t)$ with $t^4 = 1$, but $t^2 \neq 1$, then case (E3) occurs with type S_4. If $\zeta = (s, s, s, -1)$ with $s^3 = -1$, but $s \neq -1$, then case (E3) occurs with type A_4. Further, to compare (a), (b) with (d) note the isomorphisms $\mathrm{SU}_2(q_0^2) \cong \mathrm{SL}_2(q_0)$ and $\mathrm{Sp}_2(q) \cong \mathrm{SL}_2(q)$.

Remark 2: The groups in (E3) and (E4) were classically studied in low-dimensional linear group theory (e.g., [Mi], and the remarks in [Wa]; the group in (E4) belongs to the 27 lines on a cubic surface). It will be interesting to explore their Galois-theoretic significance.

The proof of Theorem 1 occupies the rest of §1. The idea is to apply a theorem of Wagner [Wa] that classifies primitive linear groups containing non-involutory homologies. In §1.3 we prove that Δ_ζ is primitive, and in §1.4 we construct the invariant bilinear resp. hermitian form.

For the rest of §1, we assume that ζ, n and q satisfy the hypothesis of Theorem 1. Instead of Δ_ζ we write Δ, for short.

§1.3. Δ IS IRREDUCIBLE.

For $i = 1, ..., n+1$ we have $Q_i^2 \in \mathcal{B}^{(r)} \subset \mathcal{B}_r(\zeta)$. Hence the matrix $B_i \stackrel{\text{def}}{=} \Phi(Q_i^2, \zeta)$ lies in Δ. By (4) we have

$$B_i \;=\; \Phi_i(\zeta)\; \Phi_i({}^{(i,i+1)}\zeta).$$

Let Γ be the subgroup of Δ generated by the matrices $B_1, ..., B_n$. The goal of this section is to prove:

PROPOSITION 1: *Γ and Δ act absolutely irreducibly in the $\mathbb{F}_q$-vector space V.*

From now on we consider $V = \mathbb{F}_q^n$ as $\mathbb{F}_q$-vector space of column vectors, on which the matrix group $\mathrm{GL}_n(q)$ acts by left multiplication. For elements $v, w, ...$ of V we let $< v, w, ... >$ denote the subspace spanned by these elements. Call an element $P \neq 1$ of $\mathrm{GL}_n(q)$ a **perspectivity** if it fixes a hyperplane of V elementwise. This hyperplane is then called the **axis** of P, and the 1-dimensional space $\mathrm{Im}(P-1)$ is called the **center** of P.

Recall that an irreducible subgroup of $\mathrm{GL}_n(q)$ that contains a perspectivity is absolutely irreducible (see e.g., [Wa, Lemma 2.1]). Since the B_i's are perspectivities by the following Lemma, Proposition 1 follows once we have shown that Γ is irreducible.

From Lemma 2 one computes that the matrices B_i have the following form:

LEMMA 3: *B_i is a perspectivity that acts with eigenvalue $\zeta_i^{-1}\zeta_{i+1}^{-1}$ on its center (for $i = 1, ..., n+1$). More precisely:*

(a) *For $i = 2, ..., n$ the matrix B_i has j-th column e_j for $j \notin \{i, i-1\}$, has $(i-1)$-st column*

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

and has i-th column

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

Thus B_i is a perspectivity with center spanned by

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

and with axis spanned by the e_j *with* $j \notin \{i, i-1\}$ *together with the vector*

$$e_{i-1} + \zeta_i e_i.$$

(b) *The matrix* B_1 *has first column* $\zeta_1^{-1}\zeta_2^{-1}e_1$ *and* j*-th column*

$$\zeta_2^{-1}(1-\zeta_{j+1})e_1 + e_j$$

for $j = 2, ..., n$. *Thus* B_1 *is a perspectivity with center* $< e_1 >$.

(c) *The matrix* B_{n+1} *has* j*-th column* e_j *for* $j = 1, ..., n-1$, *and has* n*-th column*

$$(1-\zeta_{n+1})\,(\zeta_1\, e_1 + \zeta_1\zeta_2\, e_2 + \ldots + \zeta_1 \ldots \zeta_{n-1}\, e_{n-1}) + \zeta_{n+1}^{-1}\zeta_{n+2}^{-1}\, e_n,$$

Thus B_{n+1} *is a perspectivity with axis* $< e_1, ..., e_{n-1} >$.

LEMMA 4: B_{i-1} *does not fix the center of* B_i *for* $i = 2, ..., n$.

Proof: For $3 \le i \le n$ it is clear from Lemma 3 that B_{i-1} does not fix the center of B_i.

It remains to show that B_1 does not fix the center of B_2. From Lemma 3(a) we see that the center of B_2 is spanned by the vector

$$w = (1-\zeta_3)\, e_1 + (\zeta_2 - 1)\, e_2.$$

Clearly $< w >$ cannot equal the center $< e_1 >$ of B_1. Hence if the perspectivity B_1 fixes the 1-space $< w >$, then $< w >$ must lie on the axis of B_1, i.e., $B_1 w = w$. This equation $B_1 w = w$ is equivalent to:

$$\zeta_1^{-1}\zeta_2^{-1}(1-\zeta_3) + \zeta_2^{-1}(1-\zeta_3)\,(\zeta_2 - 1) = (1-\zeta_3).$$

This simplifies to

$$(\zeta_1^{-1} - 1)\,(\zeta_3 - 1) = 0.$$

This contradiction concludes the proof of Lemma 5. ∎

Set $V_i \stackrel{\text{def}}{=} < e_1, ..., e_i >$ for $i = 1, ..., n$.

LEMMA 5: *For $i = 1, ..., n$ let S_i denote the intersection of V_i and the axes of $B_1, ..., B_i$. Then $S_i \neq 0$ if and only if $\zeta_1 \cdots \zeta_{i+1} = 1$.*

Proof: From Lemma 3 (a) one checks easily that the intersection of V_i and the axes of $B_2, ..., B_i$ is 1-dimensional, spanned by the vector

$$e_1 + \zeta_2 e_2 + \zeta_2\zeta_3 e_3 + \cdots + \zeta_2\zeta_3\cdots\zeta_i e_i.$$

Thus if $S_i \neq 0$, then S_i must be spanned by the above vector, and so this vector must be fixed by B_1. Conversely, the latter condition implies $S_i \neq 0$. It is equivalent to the equation

$$\zeta_1^{-1}\zeta_2^{-1} + \zeta_2^{-1}(1-\zeta_3)\,\zeta_2 + \cdots + \zeta_2^{-1}(1-\zeta_{i+1})\,\zeta_2\zeta_3\cdots\zeta_i = 1$$

This simplifies to the condition $\zeta_1 \cdots \zeta_{i+1} = 1$. ∎

For $i = 1, ..., n$ let Γ_i be the group generated by $B_1, ..., B_i$. From Lemma 3 we see that the group Γ_i fixes the space $V_i = \langle e_1, ..., e_i \rangle$.

LEMMA 6: *If $\zeta_1 \cdots \zeta_{i+1} \neq 1$ then Γ_i acts irreducibly in V_i $(1 \leq i \leq n)$.*

(By Lemma 4, the converse also holds for $i > 1$).

Proof (of Lemma 6): By way of contradiction, assume the Lemma is false. Hence there is some $j \geq 2$ such that $\zeta_1...\zeta_{j+1} \neq 1$, and Γ_j acts reducibly in V_j. Take j to be minimal with this property. Then there exists a non-zero, proper subspace E of V_j that is fixed by Γ_j. Furthermore, the space S_j from Lemma 5 is zero.

Case 1: $\zeta_1 \cdots \zeta_j \neq 1$.
In this case Γ_{j-1} acts irreducibly in V_{j-1}, hence $E \cap V_{j-1} = 0$ or $E = V_{j-1}$. The latter cannot occur, since B_j does not fix V_{j-1}. Hence E is a 1-space with $V_j = V_{j-1} + E$.

The centers of $B_1, ..., B_{j-1}$ are contained in V_{j-1}, hence they cannot equal E. By Lemma 4, E is also distinct from the center of B_j. Hence E lies on the axes of $B_1, ..., B_j$. Thus the intersection of V_j and these axes is non-zero. But this intersection is the space S_j, which is zero—contradiction.

Case 2: $\zeta_1 \cdots \zeta_j = 1$.
Then $\zeta_1 \cdots \zeta_{j-1} \neq 1$. Assume first $j > 2$. Then Γ_{j-2} acts irreducibly in V_{j-2}. Hence $E \cap V_{j-2} = 0$ or E contains V_{j-2}. The latter cannot occur, since $V_{j-2} + B_{j-1}(V_{j-2}) = V_{j-1}$ and $V_{j-1} + B_j(V_{j-1}) = V_j$. Hence $E \cap V_{j-2} = 0$. This

implies that E cannot contain the center of B_i for $i \leq j-2$, hence E lies on the axis of B_i.

If E does not lie on the axis of B_{j-1} then the center C of B_{j-1} lies on E; then $C \subset E \cap V_{j-1}$, hence $C = E \cap V_{j-1}$ (since E intersects V_{j-2} trivially). But then C is fixed by B_{j-2}, contradicting Lemma 4. Thus E lies also on the axis of B_{j-1}. Hence the intersection of E with the axis of B_j is contained in S_j. Since $S_j = 0$, it follows that E is the center of B_j. Hence B_{j-1} fixes the center of B_j, contradicting Lemma 4. This settles the case $j > 2$. The case $j = 2$ follows with the reasoning from Case 1. ∎

The proof of Proposition 1 is now complete, because $\zeta_1 \cdots \zeta_{n+1} = \zeta_{n+2}^{-1} \neq 1$, hence Γ is irreducible by Lemma 6.

Recall that a linear group is called **primitive** if it is irreducible, and does not permute the summands in any non-trivial direct sum decomposition of the underlying vector space.

COROLLARY 2: *If $n > 2$ then Δ acts primitively in V.*

Proof: First we prove:

CLAIM 1: *Δ contains two non-involutory perspectivities that do not commute.*

Proof: One sees easily that there must be three distinct indices i, j, k with $\zeta_i\zeta_j \neq -1 \neq \zeta_j\zeta_k$, unless $\zeta_1 = \cdots = \zeta_r = \sqrt{-1}$ (and $p \neq 2$). In the latter case, Δ contains the non-commuting perspectivities $\Phi_1(\zeta)$ and $\Phi_2(\zeta)$ of order 4 (Lemma 2). Thus we may assume that not all ζ_i equal $\sqrt{-1}$. By (5) we may then further assume $\zeta_1\zeta_2 \neq -1 \neq \zeta_2\zeta_3$. Then B_1 and B_2 are perspectivities with the desired properties (Lemma 3). (Note that if two perspectivities commute, then they fix each others centers). This proves Claim 1.

Now assume $V = W_1 \oplus ... \oplus W_m$, where Δ permutes $W_1, ..., W_m$ transitively. We have to show $m = 1$.

Let d be the dimension of the W_j. If $d > 1$ then W_1 intersects the axis of each B_i non-trivially, hence B_i fixes W_1. Since $\Gamma = < B_1, ..., B_n >$ is irreducible, it follows that $m = 1$, as desired. Thus we may assume $d = 1$. Then we have:

CLAIM 2: *Any non-involutory perspectivity from Δ fixes $W_1, ..., W_m$.*

Proof: Let P be a perspectivity in Δ that does not fix all W_j, say $P(W_1) = W_2$. We follow the argument in [Wa, Lemma 2.1]: The center C of P lies on $W_1 \oplus W_2$, hence P fixes $W_1 \oplus W_2$, and therefore switches W_1 and W_2. Thus P^2 fixes W_1 and W_2. Hence $C = W_1$ or $C = W_2$ — a contradiction — unless $P^2 = 1$. This proves Claim 2.

Since Claim 2 contradicts Claim 1, the proof of Corollary 2 is now complete. ∎

§1.4. THE INVARIANT HERMITIAN FORM.

Set $\zeta^{-1} \stackrel{\text{def}}{=} (\zeta_1^{-1}, \ldots, \zeta_r^{-1})$. The goal of this section is to prove:

PROPOSITION 2: *$\Phi_{\zeta^{-1}}$ is the dual of Φ_ζ. More precisely, there is a non-degenerate, $\mathbb{F}_q$-bilinear pairing $<,>: V \times V \to \mathbb{F}_q$ such that for all $Q \in \mathcal{B}_r(\zeta)$, $v, w \in V$ we have*

$$< \Phi_\zeta(Q) \cdot v, \Phi_{\zeta^{-1}}(Q) \cdot w > \; = \; < v, w > .$$

COROLLARY 3: (a) *If $\zeta = (-1, \ldots, -1)$ then $q = p$ is an odd prime, n is even and*

$$\Delta = \mathrm{Sp}_n(p).$$

(b) *If $q = q_0^2$ is a square and all ζ_i have norm 1 over $\mathbb{F}_{q_0}$, then Δ leaves a non-degenerate hermitian form on V invariant.*

Proof: (a) Assume $\zeta = (-1, \ldots, -1)$. Then the non-degenerate bilinear form $<,>$ from Proposition 2 is invariant under Δ. Furthermore, $q = p$ because $\mathbb{F}_q = \mathbb{F}_p(\zeta_1, \ldots, \zeta_r)$; p is odd because all $\zeta_i \neq 1$, and n is even because $\zeta_1 \cdots \zeta_r = 1$ (and $n = r - 2$).

Further we have $\mathcal{B}_r(\zeta) = \mathcal{B}_r$, hence $\Delta = < \Phi_1(\zeta), \ldots, \Phi_r(\zeta) >$. From Lemma 2 we see that the $\Phi_i(\zeta)$ are now transvections (i.e., perspectivities with incident center and axis); because of (2) it suffices to check this for $\Phi_1(\zeta)$. Hence Δ is an irreducible subgroup of $\mathrm{GL}_n(p)$, $p \neq 2$, generated by transvections. By a theorem of McLaughlin [McL], it follows that Δ equals $\mathrm{Sp}_n(p)$ or $\mathrm{SL}_n(p)$. The latter case is ruled out (for $n > 2$) because Δ leaves a non-zero bilinear form invariant. This proves (a).

(b) Denote the automorphism of order 2 of $\mathbb{F}_q$ by $t \mapsto \bar{t}$. Extend the action of this automorphism to column vectors and matrices by applying it to the coordinates.

The hypothesis yields $\bar{\zeta} = \zeta^{-1}$. Hence $\overline{\Phi(Q, \zeta)} = \Phi(Q, \bar{\zeta}) = \Phi(Q, \zeta^{-1})$ for all $Q \in \mathcal{B}_r$. (By (4) it suffices to check the first equality for $Q = Q_i$, in which case it follows from Lemma 2 because $\Phi(Q_i, \zeta) = \Phi_i(\zeta)$). In particular, we get

$$\overline{\Phi_\zeta(Q)} = \Phi_{\zeta^{-1}}(Q)$$

for all $Q \in \mathcal{B}_r(\zeta)$. This implies that Δ leaves the sesqui-linear form $(,)$ invariant that is defined as follows: $(v,w) = < v, \bar{w} >$ for all $v, w \in V$, where $<,>$ is the bilinear form from Proposition 2. (Clearly $(,)$ is linear in v and semi-linear in w.)

Since Δ is absolutely irreducible (Proposition 1), it follows that the form $(,)$ is hermitian or anti-hermitian. Multiplying by a suitable scalar, if necessary, we get it hermitian. This proves (b). ∎

Remark 2: The symplectic form from case (a) can be written down explicitly: Set (e_i, e_j) equal to $1, -1$, or 0 if $i < j$, $i > j$ or $i = j$, respectively (for $i, j = 1, ..., n$). This yields a non-zero symplectic form on V. A computation using Lemma 2 shows that this form is invariant under Δ_ζ, $\zeta = (-1, ..., -1)$.

When trying to do the same for the hermitian form from case (b), one sees quickly that the computations get too complicated. Thus a more conceptual approach is needed: The invariant pairing from Proposition 2 arises from the fact that the product of the entries of an r-tuple is invariant under the braiding action. This can be worked out as follows.

Constructing an invariant of $\Phi_\zeta \otimes \Phi_{\zeta^{-1}}$: Consider $W = V \oplus V$. For $w \in W$, let w' and w'' denote its projections: $w = (w', w'')$. Define the set $\tilde{W}$ as the cartesian product of W and $V \otimes V$, and make it into a group by defining

$$(w_1, \chi_1) \cdot (w_2, \chi_2) \;=\; (w_1 + w_2,\ \chi_1 + \chi_2 + w_1' \otimes w_2'')$$

for $w_1, w_2 \in W$, $\chi_1, \chi_2 \in V \otimes V$. The group $\tilde{W}$ is a central extension of W by $V \otimes V$:

$$V \otimes V \to \tilde{W} \to W$$

where the first map is the embedding $\chi \mapsto (0, \chi)$, and the second map is projection.

Consider the natural action of $\mathrm{GL}_n(q) \times \mathrm{GL}_n(q)$ on $W = V \oplus V$ (where (g,h) sends (u,v) to $(g(u), h(v))$) and on $V \otimes V$ (where (g,h) sends $u \otimes v$ to $g(u) \otimes h(v)$). These actions extend naturally to an action on $\tilde{W}$, commuting with the maps in the above central extension.

Embed Z (the group of scalars from §1.1) into $\mathrm{GL}_n(q) \times \mathrm{GL}_n(q)$ by letting ζ_i send (u,v) to $(\zeta_i u, \zeta_i^{-1} v)$. Then Z centralizes $V \otimes V$. Set $H = W \times^s Z$, $\tilde{H} = \tilde{W} \times^s Z$. Since Z centralizes $V \otimes V$, we get the central extension

$$V \otimes V \to \tilde{H} \to H$$

where the second map is the identity on Z and restricts to the projection map $\tilde{W} \to W$. The action of $\mathrm{GL}_n(q)\times\mathrm{GL}_n(q)$ extends further to H and $\tilde{H}$, centralizing Z and commuting with the maps in the above central extension.

The map $\tilde{H} \to H$ induces a bijection between the p'-elements (i.e., elements of order prime to p) of $\tilde{H}$ and of H (because the kernel is a central p-group). Under this bijection, each r-tuple

$$\mathbf{h} = ([0,\zeta_1],[w_1,\zeta_2],\dots,[w_{n+1},\zeta_r]) \in H^r$$

corresponds to some r-tuple $\tilde{\mathbf{h}} \in \tilde{H}^r$. This correspondence commutes with the braiding action of $\mathcal{B}_r$ on these r-tuples.

Now take specifically $w_i = (e_i, e_i)$ for $i = 1,\dots,n$, and

$$w_{n+1} = (-\sum_{i=1}^{n} \lambda_i e_i, -\sum_{i=1}^{n} \lambda_i^{-1} e_i),$$

with $\lambda_1,\dots,\lambda_n$ as in Lemma 1. Consider the maps $P', P'' : H = W \times^s Z \to G = V \times^s Z$, where P' (resp., P'') sends $[w,\zeta_i]$ to $[w',\zeta_i]$ (resp., $[w'',\zeta_i^{-1}]$). Under these maps, the above r-tuple $\mathbf{h} \in H^r$ is mapped to the r-tuples $F(E_n,\zeta)$ and $F(E_n,\zeta^{-1})$, respectively (where E_n denotes the identity matrix in $\mathrm{GL}_n(q)$, and $F(B,\zeta)$ is the r-tuple from Lemma 1). In particular, it follows by Lemma 1 that the product of the entries of the r-tuple $\mathbf{h}$ is 1. Hence for the lifted r-tuple $\tilde{\mathbf{h}}$ the corresponding product is some element of the kernel $V \otimes V$ that we denote by Π.

Claim 1: *Π is invariant under* $\Phi_\zeta \otimes \Phi_{\zeta^{-1}}$.

Proof: Consider the map $\Phi_\zeta \times \Phi_{\zeta^{-1}} : \mathcal{B}_r(\zeta) \to \mathrm{GL}_n(q)\times\mathrm{GL}_n(q)$. By the above, this lifts to an action of $\mathcal{B}_r(\zeta)$ on H and $\tilde{H}$; for $Q \in \mathcal{B}_r(\zeta)$, denote the induced automorphism of H and $\tilde{H}$ by $\Phi_H(Q)$ and $\Phi_{\tilde{H}}(Q)$, respectively. It follows that $\Phi_{\tilde{H}}(Q)$ restricts to the map $\Phi_\zeta(Q) \otimes \Phi_{\zeta^{-1}}(Q)$ on $V \otimes V$.

Each $Q \in \mathcal{B}_r(\zeta)$, in its braiding action, sends the r-tuple $F(E_n,\zeta)$ to $F(\Phi_\zeta(Q), \zeta)$, and sends $F(E_n,\zeta^{-1})$ to $F(\Phi_{\zeta^{-1}}(Q),\zeta^{-1})$ (this is immediate from the definitions in §1.1). Via the maps P', P'' it follows that Q, in its braiding action, sends $\mathbf{h}$ to the r-tuple obtained by applying $\Phi_H(Q)$ to the entries of $\mathbf{h}$. Then Q, in its braiding action, also sends $\tilde{\mathbf{h}}$ to the r-tuple obtained by applying $\Phi_{\tilde{H}}(Q)$ to the entries of $\tilde{\mathbf{h}}$. This holds because the map $\tilde{H} \to H$ is a bijection on the p'-elements, and commutes with the braiding action of Q as well as with the action through $\Phi_{\tilde{H}}$ and Φ_H.

Since the product of the entries of an r-tuple is invariant under the braiding action, it follows that $\Pi = \Phi_{\tilde{H}}(Q) \cdot \Pi = \Phi_\zeta(Q) \otimes \Phi_{\zeta^{-1}}(Q) \cdot \Pi$. This proves Claim 1. ∎

Consider the natural isomorphisms

$$V \otimes V \cong (V \otimes V)^{**} \cong (V^* \otimes V^*)^* \cong \{V^* \times V^* \to \mathbb{F}_q \ \text{bilinear}\}$$

where $*$ denotes $\mathbb{F}_q$-dual. Via these isomorphisms, the invariant $\Pi \in V \otimes V$ yields a dual pairing between Φ_ζ^* and $\Phi_{\zeta^{-1}}^*$ (in the sense of Proposition 2). Because Δ_ζ is irreducible, this pairing is non-degenerate if $\Pi \neq 0$. Then Φ_ζ^* is dual to $\Phi_{\zeta^{-1}}^*$, hence is equivalent to $\Phi_{\zeta^{-1}}$. Thus Proposition 2 now follows from

CLAIM 2: $\Pi \neq 0$.

Proof: Recall that the w_i occurring in the r-tuple $\mathbf{h}$ were chosen such that $w_i' = w_i'' = e_i$ for $i = 1, ..., n$, and $w_{n+1}' = -\sum_{i=1}^n \lambda_i e_i$, $w_{n+1}'' = -\sum_{i=1}^n \lambda_i^{-1} e_i$. Set $\chi_0 = w_{n+1}' \otimes w_{n+1}''$.

The element $[w_i, \zeta_{i+1}] \in H$ lifts to a unique p'-element $[\tilde{w}_i, \zeta_{i+1}] \in \tilde{H}$, for $i = 1, ..., n+1$. Write $\tilde{w}_i$ in the form (w_i, χ_i) with $\chi_i \in V \otimes V$. Then $\chi_i \in < w_i' \otimes w_i'' >$ because $(\tilde{w}_i, \zeta_{i+1})$ is a p'-element. Now we compute:

$$\begin{aligned}\Pi &= [0, \zeta_1]\ [\tilde{w}_1, \zeta_2] ... [\tilde{w}_{n+1}, \zeta_r] \\ &= (\zeta_2^{-1} ... \zeta_{r-1}^{-1} w_1, \chi_1) \cdots (\zeta_{r-1}^{-1} w_n, \chi_n)(w_{n+1}, \chi_{n+1}).\end{aligned}$$

Omitting the first coordinate (which gives 0), we continue as follows:

$$\begin{aligned}\Pi = &\ \chi_1 + \cdots + \chi_{n+1} + \sum_{1 \le \nu < \mu \le n} c_{\nu\mu}\ e_\nu \otimes e_\mu \ - w_{n+1}' \otimes w_{n+1}'' \\ = &\ \chi_1 + \cdots + \chi_n + \sum_{1 \le \nu < \mu \le n} c_{\nu\mu}\ e_\nu \otimes e_\mu \ + \chi_{n+1} - \chi_0\end{aligned}$$

for certain non-zero $c_{\nu\mu} \in \mathbb{F}_q$.

Note $\chi_{n+1} - \chi_0 \in < \chi_0 >$ from the above. If $\chi_{n+1} - \chi_0 = 0$ then clearly $\Pi \neq 0$, because $\chi_i \in < e_i \otimes e_i >$ for $i = 1, ..., n$. If $\chi_{n+1} - \chi_0 \neq 0$, then $e_2 \otimes e_1$ occurs with non-zero coefficient in Π, because it occurs with non-zero coefficient in $\chi_0 = (\sum \lambda_i e_i) \otimes (\sum \lambda_i^{-1} e_i)$. Hence $\Pi \neq 0$ in either case. This proves Claim 2.

§1.5. Φ_ζ DETERMINES ζ.

In the following we need some geometrical language. The projective space of rank n over the finite field $\mathbb{F}_q$, denoted $\mathbf{P}^{n-1}(q)$, is the lattice of all (non-trivial) subspaces of the vector space $\mathbb{F}_q^n$. The 1-spaces are called points.

LEMMA 7: *Set* $P_1 = < e_1 >$ *(= the center of* B_1*), and* $P_2 = < e_2 >$ *(= the center of* $\Phi_\zeta(Q_2Q_1^2Q_2^{-1})$*, cf. (5)). Further,* Q_1 *(resp.,* Q_2*) is the intersection of* V_2 *with the axis of* B_1 *(resp.,* B_2*). If* $\zeta_1\zeta_2 \neq 1$ *then the cross ratio of the 4 points* $Q_1, P_2, P_1, B_1(P_2)$ *is* $\zeta_1^{-1}\zeta_2^{-1}$*, and the cross ratio of the 4 points* Q_1, P_2, P_1, Q_2 *is:*

$$(\zeta_3 - \zeta_1^{-1}\zeta_2^{-1})(\zeta_3 - 1)^{-1}.$$

Proof: We use that for any two linearly independent vectors a, b and non-zero scalars μ, ν the cross ratio of the 4 points $< a >$, $< a + b >$, $< b >$ and $< \mu a + \nu b >$ is $\mu^{-1}\nu$. We omit the details (straightforward from Lemma 3). ∎

Let $\mathcal{B}_{1,2}$ be the normal subgroup of $\mathcal{B}_r$ generated by the conjugates of Q_1^2 and Q_2^2. Let $\Phi_{1,2}(\zeta)$ be the restriction of Φ_ζ to $\mathcal{B}_{1,2}$.

COROLLARY 4: *Suppose* $\tilde{\zeta} = (\tilde{\zeta}_1, ..., \tilde{\zeta}_r)$ *is another* r*-tuple with the properties of* ζ *from Theorem 1. Assume that* $\Phi_{1,2}(\tilde{\zeta})$ *is equivalent to* $\Phi_{1,2}(\zeta)$ *(i.e., there is* $T \in \mathrm{GL}_n(q)$ *such that* $\Phi_{\tilde{\zeta}}(Q) = T\,\Phi_\zeta(Q)\,T^{-1}$ *for all* $Q \in \mathcal{B}_{1,2}$*). Then* $\tilde{\zeta} = \zeta$*.*

Proof: Since $B_1 = \Phi_\zeta(Q_1^2)$ and $\Phi_{\tilde{\zeta}}(Q_1^2)$ have the same eigenvalues, we get $\zeta_1\zeta_2 = \tilde{\zeta}_1\tilde{\zeta}_2$ (Lemma 3). From (5) it follows that if $\Phi_{1,2}(\zeta)$ and $\Phi_{1,2}(\tilde{\zeta})$ are equivalent, then also $\Phi_{1,2}({}^\pi\zeta)$ and $\Phi_{1,2}({}^\pi\tilde{\zeta})$ are equivalent, for each $\pi \in S_r$. It follows that $\zeta_i\zeta_j = \tilde{\zeta}_i\tilde{\zeta}_j$ for all $i \neq j$.

If $\zeta_i\zeta_j = 1$ for all $i \neq j$ then $\zeta = (-1, ..., -1) = \tilde{\zeta}$. Thus we may assume $\zeta_1\zeta_2 \neq 1$. Since T preserves cross ratios, it now follows from Lemma 7 that $\zeta_3 = \tilde{\zeta}_3$. Then $\zeta = \tilde{\zeta}$ by the above. ∎

COROLLARY 5: *The following are equivalent:*

(i) Δ *leaves a non-degenerate bilinear (resp., hermitian) form on* V *invariant.*

(ii) $\Phi_\zeta(\mathcal{B}_{1,2})$ *leaves a non-degenerate bilinear (resp., hermitian) form on* V *invariant.*

(iii) *We have* $\zeta = (-1, ..., -1)$ *(resp.,* $q = q_0^2$ *is a square, and all* ζ_i *have norm 1 over* $\mathbb{F}_{q_0}$*).*

If $n > 2$ then it suffices to assume in (ii) *that $\Phi_\zeta(\mathcal{B}_{1,2})$ leaves the form invariant up to scalar multiples.*

Proof: By Corollary 3, (iii) implies (i). Further (i) implies (ii) trivially.

Now we show that (ii) implies (iii). If the invariant form is bilinear, then $\Phi_{1,2}(\zeta)$ is equivalent to its dual. Hence $\Phi_{1,2}(\zeta)$ is equivalent to $\Phi_{1,2}(\zeta^{-1})$ (Proposition 2). It follows that $\zeta = \zeta^{-1}$, hence $\zeta = (-1, ..., -1)$ (Corollary 4).

Now assume q is a square. If the invariant form is hermitian, then $\Phi_{1,2}(\zeta)$ is dual to $\Phi_{1,2}(\bar{\zeta})$. (Notation as in the proof of Corollary 3). Hence $\Phi_{1,2}(\bar{\zeta})$ is equivalent to $\Phi_{1,2}(\zeta^{-1})$ (Proposition 2), and so $\bar{\zeta} = \zeta^{-1}$ (Corollary 4). Thus the ζ_i are as in (iii). This proves that (ii) implies (iii).

It remains to prove the last assertion in Corollary 5. For this it suffices to show that the given form f, invariant under $\Phi_\zeta(\mathcal{B}_{1,2})$ up to scalar multiples, is actually invariant. We need only show that f is invariant under all perspectivities P in $\Phi_\zeta(\mathcal{B}_{1,2})$, since $\Phi_\zeta(\mathcal{B}_{1,2})$ is generated by perspectivities (clear from its definition and (5)). But f does not vanish on the axis of P, since $n > 2$ and the axis is a hyperplane. Thus P cannot transform f into a non-trivial scalar multiple (because P acts as identity on its axis). Hence P leaves f invariant, as claimed. ∎

We derive another corollary that we need in the next section. First we return for a moment to the set-up of §1.2. From the definitions it follows immediately that

$$\mathcal{B}_r({}^{\kappa(Q)}\zeta) \;=\; Q^{-1}\, \mathcal{B}_r(\zeta)\, Q$$

for each $Q \in \mathcal{B}_r$. Thus (5) yields for $\zeta' = {}^{\kappa(Q)}\zeta$:

$$\Delta_{\zeta'} \;=\; \Phi(Q,\zeta)^{-1}\; \Delta_\zeta\; \Phi(Q,\zeta). \tag{6}$$

Since $\kappa : \mathcal{B}_r \to S_r$ is surjective, it follows that for any $\zeta' = {}^{\pi}\zeta$ ($\pi \in S_r$) the group $\Delta_{\zeta'}$ is conjugate Δ_ζ.

COROLLARY 6: *Suppose $n > 2$, and Δ leaves a subspace $\mathbf{P} \cong \mathbf{P}^{n-1}(q')$ of $\mathbf{P}^{n-1}(q)$ invariant. Then $q = q'$ and $\mathbf{P} = \mathbf{P}^{n-1}(q)$.*

Proof: If $\zeta_i\zeta_j = 1$ for all $i \neq j$ then $\zeta = (-1, ..., -1)$, hence q is a prime (Corollary 3) and then trivially $q = q'$. Thus we may assume $\zeta_1\zeta_2 \neq 1$ (using (6)).

The center and axis of each perspectivity from Δ lie in $\mathbf{P}$ (since $n > 2$). The cross ratio of any 4 collinear points of $\mathbf{P}$ lies in $\mathbb{F}_{q'}$. These two facts, together with Lemma 7, yield that $\zeta_1\zeta_2$, and then also ζ_3, lies in $\mathbb{F}_{q'}$. Using (6), it follows that all ζ_i lie in $\mathbb{F}_{q'}$. Hence $q = q'$ (since the ζ_i generate $\mathbb{F}_q$). ∎

§1.6. THE CASE $n > 2$.

A perspectivity is called a transvection if the center lies on the axis; otherwise it is called a homology. The image of such an element in $\mathrm{PGL}_n(q)$ is again called a homology etc..

We use the following result of Wagner [Wa]. For simplicity, we state the result only under the additional hypothesis that the group leaves no proper subspace of $\mathbf{P}^{n-1}(q)$ invariant.

THEOREM (Wagner): *Suppose $\bar{\Delta}$ is a primitive subgroup of $\mathrm{PGL}_n(q)$, $n > 2$, that contains homologies of order > 2. Assume $\bar{\Delta}$ leaves no proper subspace $\mathbf{P} \cong \mathbf{P}^{n-1}(q')$ of $\mathbf{P}^{n-1}(q)$ invariant. Then either q is a square and*

$$\mathrm{PSU}_n(q) \;\le\; \bar{\Delta} \;\le\; \mathrm{PU}_n(q),$$

or

$$\mathrm{PSL}_n(q) \;\le\; \bar{\Delta} \;\le\; \mathrm{PGL}_n(q)$$

or $n = 3$, q is odd, $\bar{\Delta} \cong \mathrm{PU}_3(4)$, or $n = 4$, q is odd, $\bar{\Delta} \cong \mathrm{PSU}_4(4)$. In the two exceptional cases, Δ contains no homology of order > 3.

Now we can prove:

PROPOSITION 3: *Suppose $n > 2$. Exclude the two exceptional cases from Wagner's theorem (in the case $n \le 4$). Then the following holds:*

(b) *If $q = q_0^2$ is a square and all ζ_i have norm 1 over $\mathbb{F}_{q_0}$, then*

$$\mathrm{SU}_n(q) \;\le\; \Delta_\zeta \;\le\; \mathrm{U}_n(q).$$

(c) *If ζ is not as in* (b), *and $\zeta \ne (-1,\dots,-1)$, then*

$$\mathrm{SL}_n(q) \;\le\; \Delta_\zeta \;\le\; \mathrm{GL}_n(q).$$

Proof: From (6) and Lemma 3 we see that Δ contains a non-involutory homology unless $\zeta_i\zeta_j = \pm 1$ for all $i \ne j$. The latter implies $\zeta_i^2\zeta_j^2 = 1$ for all $i \ne j$, hence $\zeta_1^2 = \dots = \zeta_r^2 = \pm 1$. If this value is $+1$, then $\zeta = (-1,\dots,-1)$, a case that is not under consideration (see Corollary 3; in this case, actually Δ contains no homologies). If $\zeta_1^2 = \ldots = \zeta_r^2 = -1$ (and $p \neq 2$), then we may assume $\zeta_1 = \zeta_2 = \sqrt{-1}$ (by (6)), hence Δ contains a homology of order 4, namely $\Phi_1(\zeta)$ (Lemma 2).

Hence we may assume Δ contains a non-involutory homology. Together with Corollary 2 and Corollary 6, it follows that the image $\bar{\Delta}$ of Δ in $\mathrm{PGL}_n(q)$ satisfies the hypothesis of Wagner's theorem. Since we excluded the exceptional cases, Wagner's theorem implies that $\bar{\Delta}$ either contains $\mathrm{PSL}_n(q)$, or lies between $\mathrm{PSU}_n(q)$ and $\mathrm{PU}_n(q)$. Thus the group $\Delta\mathbb{F}_q^*$ contains $\mathrm{SL}_n(q)$ or $\mathrm{SU}_n(q)$. Since the latter groups are generated by transvections, we have even $\mathrm{SL}_n(q)$ or $\mathrm{SU}_n(q)$ contained in Δ.

Assume now that ζ is as in (b), hence $\Delta \leq \mathrm{U}_n(q)$ (Corollary 3). Then Δ cannot contain $\mathrm{SL}_n(q)$, hence $\mathrm{SU}_n(q) \leq \Delta$. This proves (b).

Finally, assume Δ does not contain $\mathrm{SL}_n(q)$. Then by the above, $\bar{\Delta}$ lies between $\mathrm{PSU}_n(q)$ and $\mathrm{PU}_n(q)$. It follows that Δ preserves the corresponding hermitian form up to scalar multiples. Then ζ is as in (b) (by Corollary 5). This proves (c). ∎

LEMMA 8: *If one of the exceptional cases from Wagner's Theorem occurs for the image of Δ_ζ in $\mathrm{PGL}_n(q)$, then $p > 3$, and ζ is as in (E3) or (E4) from Theorem 1.*

Proof: Assume one of the exceptional cases occurs. Then q is odd, and by [Wa, Lemma 3.1] the group Δ contains no transvection. This implies $\zeta_i\zeta_j \neq 1$ for all $i \neq j$ (Lemma 3 and (6)).

Since Δ contains no homology of order > 3, we have $\zeta_i\zeta_j$ of multiplicative order ≤ 3 for all $i \neq j$ (Lemma 3 and (6)); further, if $\zeta_i = \zeta_j$ for $i \neq j$ then $-\zeta_i$ has order ≤ 3 (Lemma 2 and (6)). Thus clearly $p \neq 3$. Let ϵ be a primitive third root of unity in $\bar{\mathbb{F}}_q$. We get for all $i \neq j$:

(i) $\zeta_i\zeta_j$ *equals* -1 *or* $\epsilon^{\pm 1}$.

(ii) *If* $\zeta_i = \zeta_j$ *then* $\zeta_i = -\epsilon^{\pm 1}$.

By (i) the ζ_i's can take at most 4 different values. Because $r \geq 5$ it follows that they cannot be all distinct. Thus by (ii) we may assume $\zeta_1 = -\epsilon$. (Interchanging ϵ and ϵ^{-1} if necessary). Then (i) implies $\zeta_i \in \{-\epsilon, \epsilon^{-1}, -1\}$ for all i. Thereby, ϵ^{-1} and -1 cannot occur both (by (i)), and each of them occurs at most once (by (ii)). Thus after re-labelling we get $\zeta_1 = \cdots = \zeta_{r-1} = -\epsilon$ and $\zeta_r \in \{-\epsilon, \epsilon^{-1}, -1\}$.

Since $\zeta_1 \cdots \zeta_r = 1$ we must have $\zeta_r = \epsilon^{-1}$ if $r = 5$, and $\zeta_r = -\epsilon$ if $r = 6$. This proves the claim. ∎

The converse to Lemma 8 has been checked by computer (calculating over the integers in the field of third roots of unity). Together with Proposition 3, Corollary 3 and Corollary 5, this completes the proof of Theorem 1 in the case $n > 2$.

§1.7. THE CASE $n = 2$.

In this section we assume $n = 2$ (hence $r = 4$). Let $\bar{\Delta}$ denote the image of Δ in $\mathrm{PGL}_2(q)$. Let $\bar{\mathbb{F}}_q$ be an algebraic closure of $\mathbb{F}_q$.

If $\zeta_i\zeta_j = -1$ for all $i \neq j$ then $p \neq 2$ and $\zeta_1 = \cdots = \zeta_4 = \sqrt{-1}$. In this case one finds that $\bar{\Delta} \cong S_4$, hence case (E2) of Theorem 1 occurs. Now assume not all ζ_i equal $\sqrt{-1}$. Then without loss of generality, $\zeta_1\zeta_2 \neq -1$ (by (6)). We can further assume $\zeta_2\zeta_3 \neq -1$ unless $\zeta_1 = \zeta_2 = -\zeta_3^{-1} = -\zeta_4^{-1}$; this exceptional case gives (E1) of Theorem 1.

Assume now $\zeta_1\zeta_2 \neq -1 \neq \zeta_2\zeta_3$. Since $\zeta_1\zeta_2 \neq -1$ we have $B_1^2 \neq 1$, hence B_1^2 is a perspectivity with the same center and axis as B_1 (see Lemma 3). Thus B_1^2 fixes the same subspaces of $V \otimes \bar{\mathbb{F}}_q$ as B_1. Analogously, we get the same for B_2. Since $\Gamma = < B_1, B_2 >$ acts absolutely irreducibly in V (Proposition 1), it follows that the same holds for $< B_1^2, B_2^2 >$. Hence Δ acts primitively in $V \otimes \bar{\mathbb{F}}_q$. By Dickson's list of subgroups of $\mathrm{PSL}_2(q)$ (see [Wa, Appendix]) it follows that $\bar{\Delta}$ is A_4, S_4, A_5, $\mathrm{PSL}_2(q_0)$ or $\mathrm{PGL}_2(q_0)$, where q is a power of q_0. (Note that $\bar{\Delta} \leq \mathrm{PSL}_2(q^2)$.)

Case 1: $\bar{\Delta}$ is A_4, S_4 or A_5.

Then all perspectivities in Δ have order ≤ 5, hence all $\zeta_i\zeta_j$, $i \neq j$, have multiplicative order ≤ 5. Thus, if $p > 5$ then Δ cannot contain non-trivial unipotent elements (that have p-power order), hence $\zeta_i\zeta_j \neq 1$ for all $i \neq j$ by Lemma 3 (and (5)). Hence we are in case (E2) of Theorem 1.

Case 2: $\bar{\Delta}$ is (conjugate to) $\mathrm{PSL}_2(q_0)$ or $\mathrm{PGL}_2(q_0)$.

The fixed points in $\mathbf{P}^1(\bar{\mathbb{F}}_q)$ of any element of $\mathrm{PGL}_2(q_0)$ are rational over $\mathbb{F}_{q_0^2}$. It follows that if $\bar{\Delta}$ lies in a conjugate of $\mathrm{PGL}_2(q_0)$, then the axes and centers of the perspectivities in Δ are points of $\mathbf{P}^1(\bar{\mathbb{F}}_q)$ any four of which have their cross ratio in $\mathbb{F}_{q_0^2}$. By (6) and Lemma 7 it follows that all ζ_i lie in $\mathbb{F}_{q_0^2}$, hence $q_0 = q$ or $q_0^2 = q$.

We have shown that $\bar{\Delta}$ is $\mathrm{PSL}_2(q_0)$ or $\mathrm{PGL}_2(q_0)$, with $q_0 = q$ or $q_0^2 = q$. This proves (d) of Theorem 1. The first assertions in (a) and (b) of Theorem 1 were proved in Corollary 5. Corollary 3 proves the rest of (a). Now assume ζ is as in (b), hence $\Delta \leq \mathrm{U}_2(q)$. Then certainly $q_0 \neq q$, hence $q_0^2 = q$. Thus Δ is a subgroup of $\mathrm{U}_2(q)$ mapping onto $\mathrm{PSU}_2(q)$ ($\cong \mathrm{PSL}_2(q_0)$) or $\mathrm{PU}_2(q)$ ($\cong \mathrm{PGL}_2(q_0)$). It follows that Δ contains $\mathrm{SU}_2(q)$ (since $\mathrm{SU}_2(q)$ ($\cong \mathrm{SL}_2(q_0)$) is generated by transvections). This proves (b) of Theorem 1. The proof of Theorem 1 is now complete.

§2. Galois realizations for Δ_ζ

§2.1. REALIZATIONS FOR $\mathrm{GL}_n(q)$.

In recent approaches to the Inverse Galois Problem, one tries to realize finite groups as Galois groups of regular extensions $L/\mathbb{Q}(x)$ (where "regular" means that $\mathbb{Q}$ is algebraically closed in L). If a finite group H is isomorphic to such a Galois group, we say for short that H **occurs regularly over $\mathbb{Q}$**. In [V1, Theorem 2 and 3] general criteria for realizing groups in this way (over $\mathbb{Q}$ and other number fields) are given. Applying these criteria to the group $G = V \times^s Z$ (from §1.2), together with the r-tuple of conjugacy classes represented by $\zeta_1, ..., \zeta_r$, we obtain the following Theorem 2.

Let $\zeta_1, ..., \zeta_r$ be generators of the finite field $\mathbb{F}_q$ satisfying $\zeta_1 ... \zeta_r = 1$ and $0 \neq \zeta_i \neq 1$ for all i. Set $\zeta = (\zeta_1, ..., \zeta_r)$, $Z = <\zeta_1, ..., \zeta_r>$ and $n = r - 2$. Suppose $n \geq 2$. Recall that ζ is called *rational* if $\zeta_1^m, ..., \zeta_r^m$ is a permutation of $\zeta_1, ..., \zeta_r$ for each integer m that is prime to $q - 1$. Let Δ_ζ be the image of the homomorphism $\Phi_\zeta : \mathcal{B}_r(\zeta) \to \mathrm{GL}_n(q)$.

THEOREM 2 ([V1]): *Let S be a subgroup of $\mathbb{F}_q^*$ that is either trivial or contains Z. If ζ is rational, and $\Delta_\zeta S = \mathrm{GL}_n(q)$, then the group $\mathrm{GL}_n(q)/S$ occurs regularly over $\mathbb{Q}$.*

From Theorem 1, it is easy to give conditions on n and q that imply the existence of rational ζ with $\Delta_\zeta S = \mathrm{GL}_n(q)$. We give some reasonable conditions like this in the following Lemma. As one sees from the proof, these conditions could easily be further refined to cover more groups $\mathrm{GL}_n(q)$ and $\mathrm{PGL}_n(q)$. Let φ denote Euler's φ-function, and let again $\bar{\Delta}_\zeta$ be the image of Δ_ζ in $\mathrm{PGL}_n(q)$.

LEMMA 9: (i) *Assume $q > 4$ is either odd or a power of 4. If n is even and $n \geq \varphi(q-1)$ then there is rational ζ with $\Delta_\zeta = \mathrm{GL}_n(q)$.*

(ii) *Assume $q = p$ is a prime, and $(n, p-1) = 2$. If $p \equiv 7$ (mod 12) or $p \equiv 5$ (mod 8) then there is rational ζ with $\bar{\Delta}_\zeta = \mathrm{PGL}_n(p)$.*

Proof: (i) Choose ζ_1 such that $-\zeta_1$ generates the multiplicative group $\mathbb{F}_q^*$. Let $\zeta_1, \dots, \zeta_s$ be the generators of the cyclic group $< \zeta_1 >$. Note $s \le \varphi(q-1) \le n = r-2$. Thus there are at least 2 more ζ_i's to choose: Take them to be -1 if q is odd, and elements of order 3 if q is a power of 4 (with each of the two elements of order 3 occurring the same number of times). This yields a rational r-tuple $\zeta = (\zeta_1, \dots, \zeta_r)$ with the properties given before Theorem 2.

It remains to show that $\Delta_\zeta = \mathrm{GL}_n(q)$. By Lemma 3 (and (5)), Δ_ζ contains an element of determinant $\zeta_r\zeta_1 = -\zeta_1$ (= a generator of $\mathbb{F}_q^*$) if q is odd. If q is even, the group $< \zeta_1 >= \mathbb{F}_q^*$ is cyclic of odd order, hence the $\zeta_1^i\zeta_1^j$ with i, j prime to $q-1$, $i \not\equiv j$ (mod $q-1$), generate $< \zeta_1 >$; further, these $\zeta_1^i\zeta_1^j$ occur as determinants of elements of Δ_ζ (again by Lemma 3 and (5)). It follows that det: $\Delta_\zeta \to \mathbb{F}_q^*$ is surjective.

Clearly, ζ is not as in (a), (b), (E4),(E5) of Theorem 1. Hence if $n > 2$ then Δ_ζ contains $\mathrm{SL}_n(q)$ (by Theorem 1). Thus $\Delta_\zeta = \mathrm{GL}_n(q)$ (by the previous paragraph).

If $n = 2$ then our hypothesis implies $q = 5$; then the unipotent elements of $\mathrm{GL}_n(q)$ have order 5, and Δ_ζ contains such an element by Lemma 3. Thus $\bar{\Delta}_\zeta$ contains $\mathrm{PSL}_n(q) = \mathrm{PSL}_2(5) \cong A_5$, either by (d) or (E2) of Theorem 1. Hence Δ_ζ contains $\mathrm{SL}_2(5)$, and the claim follows as above.

(ii) If $p \equiv 7$ (mod 12) (resp., $p \equiv 5$ (mod 8)), let ζ_1 be an element of order 3 (resp., 4), let $\zeta_2 = \zeta_1^{-1}$, and take the remaining ζ_i's to be -1. Then clearly ζ is a rational r-tuple with the properties given before Theorem 2.

We may exclude the case $n = 2, p = 5$ (since this is covered by (i)). Then ζ is not as in (a),(b), (E2)-(E5) of Theorem 1, hence $\bar{\Delta}_\zeta$ contains $\mathrm{PSL}_n(p)$. Further, Δ_ζ contains an element of determinant $-\zeta_1$ (by Lemma 3). But $-\zeta_1$ is a non-square in $\mathbb{F}_p^*$ in either case. Hence $\bar{\Delta}_\zeta = \mathrm{PGL}_n(p)$. (Note that $\mathrm{PSL}_n(p)$ has index 2 in $\mathrm{PGL}_n(p)$ because $(n, p-1) = 2$). ∎

The case (i) allows to improve Theorem 1 of [V1].

COROLLARY A: *If n and q are as in* (i) *(resp.* (ii)*) of the above Lemma, then the group $\mathrm{GL}_n(q)$ (resp., $\mathrm{PGL}_n(q)$) occurs regularly over $\mathbb{Q}$. In particular, if $q > 4$ is a power of 4, and $n \ge \varphi(q-1)$ is even and prime to $q-1$, then the simple group $\mathrm{PSL}_n(q) = \mathrm{PGL}_n(q)$ occurs regularly over $\mathbb{Q}$.*

Examples: The group $\mathrm{GL}_n(5)$ occurs regularly over $\mathbb{Q}$ for all even $n \geq 2$. Also, $\mathrm{GL}_n(16)$ for all even $n \geq 6$. (The proof of Lemma 9 shows that for even q actually the bound $n \geq \varphi(q-1) - 2$ works). The latter groups modulo their center are simple if n is prime to 15.

§2.2. Realizations of unitary groups.

In forthcoming work [V2], we will generalize Theorem 2 as follows:

Theorem 2′: *Let S be a subgroup of $\mathbb{F}_q^*$. If ζ is rational, and $\Delta_\zeta S/S$ is self-normalizing in $\mathrm{GL}_n(q)/S$, then $\Delta_\zeta S/S$ occurs regularly over $\mathbb{Q}$.*

Since the group $\mathrm{PU}_n(q)$ is self-normalizing in $\mathrm{PGL}_n(q)$, we get Galois realizations for $\mathrm{PU}_n(q)$ under similar conditions on n and q as in Corollary A. First we need the analogue of Lemma 9.

Lemma 10: (i) *Let $q = p^{2s}$ with p a prime, s a positive integer. Assume either q or s is odd. If $n \geq 4$ is even and $n \geq \varphi(\sqrt{q}+1)$, then there is rational ζ with $\Delta_\zeta = U_n(q)$.*

(ii) *Assume $q = p^2$, and $(n, p+1) = 2$. If $p \equiv 5$ (mod 12) or $p \equiv 3$ (mod 8) then there is rational ζ with $\bar{\Delta}_\zeta = \mathrm{PU}_n(p^2)$.*

Proof: The construction is analogous to that in Lemma 9.
(i) Choose ζ_1 such that $-\zeta_1$ generates the group S_q of elements of $\mathbb{F}_q^*$ that have norm 1 over $\mathbb{F}_{\sqrt{q}}$. Let again $\zeta_1, \ldots, \zeta_s$ be the generators of the cyclic group $< \zeta_1 >$. Note $s \leq \varphi(\sqrt{q}+1) \leq n = r-2$. Take the remaining ζ_i's as in Lemma 9. Then ζ is a rational r-tuple with all ζ_i of norm 1 over $\mathbb{F}_{\sqrt{q}}$. Thus case (b) of Theorem 1 occurs. As in Lemma 9 one sees that det: $\Delta_\zeta \to S_q$ is surjective. This implies $\Delta_\zeta = \mathrm{U}_n(q)$.
(ii) Choose ζ as in the proof of Lemma 9(ii). Then ζ is again a rational r-tuple with the properties given before Theorem 2. Further, case (b) of Theorem 1 occurs. (The case $n = 2$, $p = 5$ is done as in Lemma 9.)

As in Lemma 9, Δ_ζ contains an element of determinant $-\zeta_1$. But $-\zeta_1$ is a non-square in S_q (since S_q has order $p+1$). Hence $\bar{\Delta}_\zeta = \mathrm{PU}_n(p^2)$. (Note that $\mathrm{PSU}_n(p^2)$ has index 2 in $\mathrm{PU}_n(p^2)$ because $(n, p+1) = 2$). ∎

Corollary B: *If n and q are as in* (i) *or* (ii) *of Lemma 10, then the group $\mathrm{PU}_n(q)$ occurs regularly over $\mathbb{Q}$. In particular, if $q = 2^{2s}$ with odd s, and $n \geq 4$ is even, $n \geq \varphi(\sqrt{q}+1)$ and n is prime to $\sqrt{q}+1$, then the simple group $\mathrm{PSU}_n(q) = \mathrm{PU}_n(q)$ occurs regularly over $\mathbb{Q}$.*

Example: The group $PU_n(4)$ occurs regularly over $\mathbf{Q}$ for all even $n \geq 4$. This group is simple if n is not divisible by 3.

Remark: In view of the isomorphism $PU_2(p^2) \cong PGL_2(p)$, the cases (ii) of Corollary A and B imply the following: The group $PGL_2(p)$ occurs regularly over Q for all primes p with $p \not\equiv \pm 1 \pmod{24}$. This was shown in [MM] using the rigidity method. It is quite remarkable that we get the same congruence condition here, although the present method is quite different.

References

[MM] G. Malle and B.H. Matzat, *Realisierung von Gruppen $PSL_2(\mathbf{F}_p)$ als Galoisgruppen über* $\mathbf{Q}$, Math. Annalen **272** (1985), 549–565.

[McL] J. McLaughlin, *Some groups generated by transvections*, Arch. Math. **18** (1967), 364–368.

[Mi] M.H. Mitchell, *Determination of the finite quaternary linear groups*, Trans. Am. Math. Soc. **14** (1913), 123–142.

[V1] H. Völklein, *$GL_n(q)$ as Galois group over the rationals*, Math. Annalen **293** (1992), 163–176.

[V2] H. Völklein, *Braid group action, embedding problems and the groups* $PGL_n(q)$, $PU_n(q^2)$, preprint.

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