ON THE CLIFFORD COLLINEATION, TRANSFORM AND SIMILARITY GROUPS. I.

BEVERLEY BOLT, T. G. ROOM and G. E. WALL

(received 13 May 1960)

1. Introduction

Papers [1] I, II of this projected series lay the algebraic foundations of the theory of the Clifford groups; I deals with the case $p > 2$, II with the case $p = 2$. The present introduction refers to both papers.

Our theory has applications in group theory, geometry and number theory. For example, we prove here that the symplectic group $Sp(2m, p)$ (p an odd prime) has irreducible representations of degrees $\frac{1}{2}(p^m + 1)$ and $\frac{1}{2}(p^m - 1)$, but no irreducible representations of degree k, where $1 < k < \frac{1}{2}(p^m - 1)$, (§ 4.3, thm. 10). Geometrical configurations associated with the Clifford groups have been investigated in the case $p^m = 3^2$ by A. F. Horadam ([4]–[7]), in the case $p^m = 5^2$ by Beverley Bolt ([2]); the locus considered by Horadam is closely related to the system of lines on a cubic surface. The Clifford transform group $\mathscr{CT}_1^+(2^m)$ is the group of automorphs of one of the extreme forms in 2^m variables studied in a recent paper (E. S. Barnes and G. E. Wall [1]). We hope to deal with some of the applications in later papers of this series.

Let p be a prime number, and write $\omega = \exp(2\pi i/p)$. K. Morinaga and T. Nono ([9]), T. G. Room ([10]), have shown that there exist systems of $2m$ complex p^m-rowed matrices U_i such that

$$U_i^p = I, \qquad U_i U_j = \omega U_j U_i \qquad (i < j). \tag{1.1}$$

Moreover, if $V_1, \cdots, V_{2m}$ is a second such system, there exists a complex "transition" matrix M such that

$$MV_i M^{-1} = U_i \qquad (i = 1, \cdots, 2m). \tag{1.2}$$

We regard the system (U_i) as fixed and consider the systems (V_i) in which each member is a scalar multiple of one of the p^{2m} (linearly independent) monomials

$$U_1^{\alpha_1} U_2^{\alpha_2} \cdots U_{2m}^{\alpha_{2m}}. \tag{1.3}$$

[1] Paper I is a development of an unpublished manuscript of Room's, similar in scope to the paper [10] on the case $p = 2$.

The corresponding transition matrices form the *Clifford transform group* $CT(p^m)$. The scalar multiples of the monomials (1.3) form the *Clifford collineation group* $CG(p^m)$. Obviously, CT is the normalizer of CG in the full linear group.

A formal consequence of (1.1) is the identity

$$(1.4) \qquad (\sum_{i=1}^{2m} x_i U_i)^p = (\sum_{i=1}^{2m} x_i^p) I.$$

When $p = 2$, this is the well known matrix factorization of the Euclidean fundamental form, on which the theory of spinors is based. The definition of the spin group resembles that of $CT(2^m)$; the difference is that in the former case one considers systems (V_i) in which each member is a *linear combination of the* U_i. Whereas the spin group is projectively an infinite group, CT is projectively finite.

When $p = 2$, (1.1) has *real* solutions. By admitting only real systems and transition matrices in the definitions, we get the *real Clifford groups* $CG_1(2^m)$ and $CT_1(2^m)$. There are analogous "semi-real" groups $CG_2(2^m)$ and $CT_2(2^m)$, whose definitions need not be given at present.

Let PG denote the projective group determined by a given matrix group G. The central results in our theory are the isomorphisms

$$(1.5) \quad (\text{I, II; thm. } 5) \qquad CT(p^m)/CG(p^m) \cong Sp(2m, p),$$

$$(1.6) \quad (\text{II, thm. } 5^*) \qquad CT_i(2^m)/CG_i(2^m) \cong O_i(2m, 2) \qquad (i = 1, 2),$$

$$(1.7) \quad (\text{I, thm. } 5) \qquad PCT(p^m) \cong ASp(2m, p) \qquad (p > 2),$$

where O_1, O_2 are the two essentially different $2m$-dimensional orthogonal groups over the Galois field $GF(2)$, Sp is the $2m$-dimensional symplectic group over $GF(p)$ and ASp the group of symplectic affine transformations $\alpha \to \alpha T' + t$ $(T \in Sp)$. (1.7) implies the existence of a subgroup $CS(p^m)$ of $CT(p^m)$ such that

$$(1.8) \qquad PCS(p^m) \cong Sp(2m, p) \qquad (p > 2);$$

CS is called the *Clifford similarity group*. There is, in general, no analogue of CS when $p = 2$ (II, thm. 7). CG and CT are irreducible groups (I, II; thm. 1), but CS splits into two irreducible components of degrees $\frac{1}{2}(p^m + 1)$ and $\frac{1}{2}(p^m - 1)$, (I, thm. 6).

The above results are concerned with the *projective* structure of CT. The first question to ask about the *non-projective* structure of a given matrix group G is whether PG can be realized as a subgroup of G; in other words, does there exist a subgroup H of G such that $PH = PG$ and $H \cong PG$? More generally, we ask: for what values of k do there exist subgroups H of G such that $PH = PG$ and H provides a k-valued representation of PG? Such

questions direct attention to the commutator group G' of G; for if $PH = PG$, then $H' = G'$.

Our main results in this direction are as follows. If $p^m \geqq 5$, $P(CT') = PCT$ and CT' provides a k-valued representation of PCT, where $k = p$ when $p > 2$, 4 when $p = 2$ (I, thm. 7; II, thm. 6). $CT_i(2^m)$ has a subgroup $\mathscr{CT}_i(2^m)$ which is projectively equal to $CT_i(2^m)$ and doubly isomorphic to $PCT_i(2^m)$ (II, thm. 6 et seq.). If $p > 2$ and $p^m > 3$, $P(CS') = PCS$ and $CS' \cong PCS \cong Sp$ (I, thm. 8). This last fact is the source of the two representations of Sp mentioned earlier.

For geometrical and other applications it is necessary to determine the elements of CS, CT explicitly, and this is done in I, § 4.1 and II, § 5. The elements of CT', $\mathscr{CT}_i$ are easily deduced from those of CT when $p = 2$ (II, § 5). On the other hand, a rather elaborate determinant evaluation is needed to deduce the elements of CS' from those of CS (I, thm. 9).

The exceptional cases play a more prominent part when $p = 2$ (see II, §§ 4.2, 4.3). The sole exceptional case for odd p, viz. $p^m = 3$, is treated briefly in an Appendix to the present paper.

2. Notation, Preliminaries

2.1 *Notation.*

p	: fixed prime (> 2 in the present paper).
m	: fixed positive integer.
ω	: $\exp(2\pi i/p)$.
C, R, R_0	: complex, real and rational fields.
$GF(q)$	: Galois field with q elements.
S_n, A_n	: symmetric and alternating groups of degree n.
X'	: transpose of a matrix X.
$\bar{X}, X^*$	: conjugate and conjugate transpose of a complex matrix X.
$[x, y]$	: commutator $xyx^{-1}y^{-1}$ of group elements x, y.
G'	: commutator group of a group G.
$\{x, y, \cdots\}$	: subgroup of a group generated by the elements $x, y, \cdots$.

The product of group automorphisms α, β is defined by $(\alpha\beta)(\cdot) = \alpha(\beta(\cdot))$.

Vector spaces. We consider only finite dimensional left vector spaces over commutative fields; let W be such a vector space over a field F. Vectors are printed in Bold type. The product of linear transformations S, T is defined by $(ST)(\cdot) = S(T(\cdot))$.

I	: identity linear transformation (or matrix).
scalar	: elements λ of F; also the corresponding linear transformations λI.

F^* : multiplicative group formed by the non-zero elements of F; also the group formed by the corresponding linear transformation λI.

transvection: linear transformation of the form $Tx = x + g(x)a$, where a is a fixed element of W and $g(x)$ a linear form such that $g(a) = 0$.

Linear groups. Let G, H be groups of non-singular linear transformations on W.

scalar subgroup of G: $F^* \cap G$.

PG : the group of projective transformations determined by G.

G is *projectively equal* to H: $PG = PH$.

$GL(W)$, $SL(W)$: full linear, and special linear, groups on W.

Vector spaces over $GF(p)$.

$\mathfrak{V}_k(p)$: k-dimensional vector space of all row vectors $\alpha = (\alpha_1, \alpha_2, \cdots, \alpha_k)$, $\beta = (\beta_1, \beta_2, \cdots, \beta_k), \cdots$ over $GF(p)$.

$\alpha \cdot \beta$: scalar product $\sum_1^k \alpha_i \beta_i$ of the vectors α, β in $\mathfrak{V}_k(p)$.

e_i : i-th unit vector in $\mathfrak{V}_m(p)$ (having 1 in the i-th place and 0 elsewhere).

ε_i : i-th unit vector in $\mathfrak{V}_{2m}(p)$.

Index to further notation.

§ 2.2: Sp, $\frac{1}{2}Sp$, $f(\alpha, \beta)$.

§ 3.1: V, v_λ, W^α, CG, CT, $\mathscr{CG}$, linear transformation *over a field* F, unitary, projectively unitary.

§ 3.3: $\mathfrak{J}$, $\mathfrak{A}$, ASp.

§ 3.4: CS, J.

§ 4.1: $\mathfrak{V}_T$, X_T, d_T.

§ 4.2: Θ, Ω, sgn T.

2.2 *Symplectic groups.* We set down for reference various properties of the symplectic groups over $GF(p)$; in the present section, p may be 2. For a full account, see Dieudonné ([3]).

Let $F(\alpha, \beta)$ be a non-degenerate skew form on $\mathfrak{V}_{2m}(p)$:

$$F(\alpha, \beta) = \sum_{i,j=1}^{2m} F_{ij} \alpha_i \beta_j, \tag{2.2.1}$$

where

$$F_{ii} = F_{ij} + F_{ji} = 0, \qquad |F_{ij}| \neq 0.$$

The matrices T such that $F(\alpha T', \beta T') \equiv F(\alpha, \beta)$ form the *symplectic group*

https://doi.org/10.1017/S1446788700026379 Published online by Cambridge University Press

$Sp(F)$ of F. A necessary and sufficient condition that $T \in Sp(F)$ is that the rows $t_1, \cdots, t_{2m}$ of T' satisfy the conditions: $F(t_i, t_j) = F_{ij}$ $(i, j = 1, \cdots, 2m)$.

It is well known that F is equivalent to the *canonical* skew form

$$f(\alpha, \beta) = \sum_{i=1}^{m} (\alpha_i \beta_{m+i} - \beta_i \alpha_{m+i}); \tag{2.2.2}$$

i.e.

$$F(\alpha S', \beta S') \equiv f(\alpha, \beta) \tag{2.2.3}$$

for some non-singular matrix S. It is easily seen from (2.2.3) that $Sp(F) = S(Sp(f))S^{-1}$, so that all symplectic groups on $\mathscr{V}_{2m}$ are isomorphic. The standard notation for $Sp(f)$ is $Sp(2m, p)$.

The scalar subgroup of Sp is $\{-I\}$. Hence Sp is isomorphic to PSp when $p = 2$, doubly isomorphic to PSp when $p > 2$. In the latter case we shall write $PSp = \frac{1}{2}Sp$.

(2.2.4) *Structure Theorem. If $p^m \geqq 5$, the only normal subgroups of $Sp(2m, p)$ are $\{I\}$, $\{-I\}$ and $Sp(2m, p)$, and $PSp(2m, p)$ is a non-cyclic simple group. The exceptional groups $Sp(2, 2)$, $\frac{1}{2}Sp(2, 3)$, $Sp(4, 2)$ are isomorphic to S_3, A_4, S_6 respectively.*

(2.2.5) *Witt's Theorem. If $\alpha_1, \cdots, \alpha_s$* and *$\beta_1, \cdots, \beta_s$ are two sets of linearly independent vectors in $\mathscr{V}_{2m}$ such that*

$$F(\alpha_i, \alpha_j) = F(\beta_i, \beta_j) \qquad (i, j = 1, \cdots, s),$$

there exists an element T of $Sp(F)$ such that

$$\alpha_i T' = \beta_i \qquad (i = 1, \cdots, s).$$

(2.2.6) *Corollary. If α, β are non-zero vectors in $\mathscr{V}_{2m}$, there exists an element T of $Sp(F)$ such that $\alpha T' = \beta$. In particular, $Sp(F)$ is an irreducible group.*

The transvections in $Sp(F)$ are the linear transformations

$$\alpha \to \alpha + \lambda F(\alpha, \mathbf{a})\mathbf{a} \qquad (\lambda \mathbf{a} \neq \mathbf{0}). \tag{2.2.7}$$

3. The Clifford Groups

3.1 *The groups CG, $\mathscr{CG}$, CT.* Let $V\,(= V(p^m))$ be a p^m-dimensional vector space over the complex field C. We shall define a family of p^{2m} linear transformations W^{α} on V, the index vector $\alpha = (\alpha_1, \cdots, \alpha_{2m})$ running over $\mathscr{V}_{2m}\,(= \mathscr{V}_{2m}(p))$.

Choose a basis of V and label its p^m members v_{λ} with the elements $\lambda = (\lambda_1, \cdots, \lambda_m)$ of $\mathscr{V}_m$. Write the elements $\alpha, \beta, \cdots$ of $\mathscr{V}_{2m}$ as pairs of elements of $\mathscr{V}_m$:

$$\alpha = (\mathbf{a}_1, \mathbf{a}_2). \qquad \beta = (\mathbf{b}_1, \mathbf{b}_2), \cdots$$

https://doi.org/10.1017/S1446788700026379 Published online by Cambridge University Press

where

$$\boldsymbol{a}_1 = (\alpha_1, \cdots, \alpha_m), \qquad \boldsymbol{a}_2 = (\alpha_{m+1}, \cdots, \alpha_{2m}), \cdots.$$

Then the W^{α} are defined by:

$$W^{\alpha} v_{\lambda} = \omega^{\boldsymbol{a}_1 \cdot (\lambda + \frac{1}{2}\boldsymbol{a}_2)} v_{\lambda + \boldsymbol{a}_2} \quad (\alpha \in \mathscr{V}_{2m},\ \lambda \in \mathscr{V}_m). \tag{3.1.1}$$

It may be verified that

$$W^{\alpha} W^{\beta} = \omega^{\frac{1}{2} f(\alpha, \beta)} W^{\alpha+\beta}, \tag{3.1.2}$$

where $f(\alpha, \beta)$ is the canonical skew form (2.2.2). Hence

$$[W^{\alpha}, W^{\beta}] = \omega^{f(\alpha, \beta)} I, \tag{3.1.3}$$

$$(W^{\alpha})^k = W^{k\alpha} \qquad (k = 1, 2, \cdots). \tag{3.1.4}$$

(3.1.5) *Definition.* The *Clifford collineation group* $CG(p^m)$ is the group formed by the linear transformations $\lambda W^{\alpha} (\lambda \in C^*, \alpha \in \mathscr{V}_{2m})$. The *Clifford transform group* $CT(p^m)$ is the normalizer of $CG(p^m)$ in the full linear group $GL(V)$.

Clearly, $CG' = \{\omega I\}$, $PCG \cong \mathscr{V}_{2m}$, where $\mathscr{V}_{2m}$ is regarded as an additive group. Thus, CG is nilpotent of class 2.

(3.1.6) *Definition.* The *finite Clifford collineation group* $\mathscr{CG}(p^m)$ is the subgroup of $CG(p^m)$ formed by the linear transformations $\omega^k W^{\alpha}$ $(0 \leqq k \leqq p-1, \alpha \in \mathscr{V}_{2m})$.

$\mathscr{CG}$ has order p^{2m+1} and, by (3.1.4), exponent p. Clearly $P\mathscr{CG} = PCG$. $\mathscr{CG}$ is a fully invariant subgroup of CG: $X \in CG$ satisfies $X^p = I$ if, and only if, $X \in \mathscr{CG}$. Hence CT is also the normalizer of $\mathscr{CG}$ in $GL(V)$.

It is easy to determine a system of generators and defining relations for $\mathscr{CG}$. Let $F(\alpha, \beta)$ be the non-degenerate skew form (2.2.1) on $\mathscr{V}_{2m}$. Since $F(\alpha, \beta)$ is equivalent to the canonical form $f(\alpha, \beta)$, there exists a basis $\alpha_1, \cdots, \alpha_{2m}$ of $\mathscr{V}_{2m}$ such that $f(\alpha_i, \alpha_j) = F_{ij}$ $(i, j = 1, \cdots, 2m)$. Therefore, by (3.1.3), (3.1.4),

$$(W^{\alpha_i})^p = I, \qquad [W^{\alpha_i}, W^{\alpha_j}] = \omega^{F_{ij}} I \qquad (i, j = 1, \cdots, 2m).$$

Consider now the abstract group $\mathfrak{G}(F)$ with generators $w_1, \cdots, w_{2m}, w$, and defining relations

$$w_i^p = w^p = [w_i, w] = 1, \quad [w_i, w_j] = w^{F_{ij}} \quad (i, j = 1, \cdots, 2m). \tag{3.1.7}$$

Clearly, $\mathfrak{G}(F)$ is a p-group of order $\leqq p^{2m+1}$. On the other hand, $W^{\alpha_1}, \cdots, W^{\alpha_{2m}}, \omega I$ satisfy the defining relations for $\mathfrak{G}(F)$ and generate the group $\mathscr{CG}$ of order p^{2m+1}. Hence $\mathscr{CG} \cong \mathfrak{G}(F)$.

$\mathscr{CG}$ can be presented in the form (1.1) as follows. Write

$$\left.\begin{aligned} \alpha_{2j-1} &= \varepsilon_j + \sum_{k=1}^{j-1} \varepsilon_{m+k} \\ \alpha_{2j} &= \varepsilon_j + \sum_{k=1}^{j} \varepsilon_{m+k} \end{aligned}\right\} \quad (j = 1, \cdots, m),$$

https://doi.org/10.1017/S1446788700026379 Published online by Cambridge University Press

where ε_i is the i-th unit vector in $\mathscr{V}_{2m}$. Then the linear transformations $U_i = W^{\alpha_i}$ $(i = 1, \cdots, 2m)$ satisfy the required conditions (1.1).

Notation. If X is a linear transformation on V, X_0 the matrix of X with respect to the basis v_λ, then by X, X', X^* we mean the linear transformations whose matrices are $\bar{X}_0$, X_0', X_0^* respectively. X is called *real* if $X = \bar{X}$, *unitary* if $XX^* = I$, a linear transformation *over the field* F when the elements of X_0 are in F. X is called *projectively unitary* when some scalar multiple of it is unitary; an alternative definition is that $XX^* \in C^*$, for then $XX^* = \lambda I$, where λ is necessarily real and positive, so that $\lambda^{-\frac{1}{2}}X$ is unitary. A group of linear transformations on V is called real, unitary, etc. when each of its elements has the corresponding property.

3.2 *Properties of CG, CT.*

LEMMA. *If* $\alpha \neq 0$, *the trace of* W^α *is zero.*

PROOF. When $a_2 \neq 0$ this is clear from (3.1.1). When $a_2 = 0$, $tr\, W^\alpha = \sum_{\lambda \in \mathscr{V}_m} \omega^{a_1 \cdot \lambda} = p^{m-1} \sum_{i=0}^{p-1} \omega^i = 0$, since the non-zero linear form $a_1 \cdot \lambda$ assumes all values equally often.

THEOREM 1. *$\mathscr{CG}$ is an irreducible unitary group.*

PROOF. It is easily seen from (3.1.1) that $\mathscr{CG}$ is unitary. The irreducibility of $\mathscr{CG}$ follows from group character theory, for it is an easy consequence of the lemma that $\sum_{X \in \mathscr{CG}} |tr\, X|^2 = \text{order } \mathscr{CG}$.

The following is a simple direct proof of irreducibility. The linear transformation

$$M_{\lambda,\mu} = p^{-m} \sum_{\nu \in \mathscr{V}_m} \omega^{-\frac{1}{2}\nu \cdot (\mu+\lambda)} W^{(\nu, \mu-\lambda)}$$

maps v_λ into v_μ and every other v_ϱ into zero. Every linear transformation on V is a linear combination of the $M_{\lambda,\mu}$ and so of the W^α.

COROLLARY 1. *C^* is both the centre of CG and the centralizer of CG in $GL(V)$.*

COROLLARY 2. *The group of inner automorphisms of CG is isomorphic to PCG, and so to $\mathscr{V}_{2m}$.*

COROLLARY 3. *Every automorphism of CG which leaves the elements of C^* and PCG fixed is an inner automorphism.*

PROOF. Such an automorphism has the form $\lambda W^\alpha \to \lambda \chi(\alpha) W^\alpha$, where χ is a homomorphism of $\mathscr{V}_{2m}$ into C^*, i.e. a character of $\mathscr{V}_{2m}$. Since there are p^{2m} characters and p^{2m} inner automorphisms, the corollary follows.

THEOREM 2. *CT is a projectively unitary group.*

PROOF. Let $X \in CT$, $Y \in \mathscr{CG}$; then $X^{-1}YX \in \mathscr{CG}$, and by theorem 1 both Y and $X^{-1}YX$ are unitary. Hence $X^{-1}YX = (X^{-1}Y^{-1}X)^* = X^*YX^{*-1}$, and so XX^* commutes with Y. By theorem 1, cor. 1, $XX^* \in C^*$, i.e. X is projectively unitary. Hence CT is projectively unitary.

THEOREM 3. *Every automorphism ψ of CG which leaves the scalars fixed is a similarity over $R_0(\omega)$, i.e. $\psi(X) = TXT^{-1}$ $(X \in CG)$ for some linear transformation T over $R_0(\omega)$.*

PROOF. By the lemma, the representations $X \to X$ and $X \to \psi(X)$ of $\mathscr{C}\mathscr{G}$ have the same character; therefore they are similar over C. Since $\mathscr{C}\mathscr{G}$ is a group over $R_0(\omega)$, they are in fact similar [2] over $R_0(\omega)$. This is equivalent to the theorem.

3.3 *The Structure of CT.* Let $T \in Sp(2m, p)$. Then (3.1.2) shows that the mapping

$$\psi_T(\lambda W^\alpha) = \lambda W^{\alpha T'} \tag{3.3.1}$$

is an automorphism of CG. Let ι_t denote the inner automorphism

$$\iota_t(\lambda W^\alpha) = \lambda W^t W^\alpha (W^t)^{-1}. \tag{3.3.2}$$

LEMMA. *Every automorphism ψ of CG which leaves the scalars fixed has the form $\psi = \iota_t \psi_T$.*

PROOF. Suppose that $\psi(\lambda W^\alpha) = \lambda\rho(\alpha)W^{\sigma(\alpha)}$. By (3.1.3), $\sigma(\alpha) = \alpha T'$, where $T \in Sp$. Then $\psi\psi_T^{-1}$ is an automorphism which leaves the elements of C^* and PCG fixed. The lemma now follows from theorem 1, cor. 3.

THEOREM 4. *Let $\mathfrak{I}(p^m)$ denote the group of inner automorphisms of CG, $\mathfrak{A}(p^m)$ the group formed by the automorphisms of CG which leave the scalars fixed. Let $ASp(2m, p)$ denote the group of symplectic affine transformations*

$$\alpha \to \alpha T' + t \qquad (T \in Sp(2m, p), \quad t \in \mathscr{V}_{2m}). \tag{3.3.3}$$

Then

$$\mathfrak{A}(p^m) \cong ASp(2m, p),$$
$$\mathfrak{A}(p^m)/\mathfrak{I}(p^m) \cong Sp(2m, p).$$

PROOF. If (T, t) is the affine transformation (3.3.3), then

$$(S, s)(T, t) = (ST, tS' + s).$$

By the lemma, $\iota_t\psi_T \leftrightarrow (T, t)$ is a one-to-one correspondence between $\mathfrak{A}$ and ASp. It is easily verified that

$$(\iota_s\psi_S)(\iota_t\psi_T) = \iota_{tS'+s}\psi_{ST},$$

so that this correspondence is an isomorphism and therefore $\mathfrak{A} \cong ASp$.

Under the above isomorphism, $\mathfrak{I}$ corresponds to the normal subgroup $\mathscr{V}$ of ASp formed by the "translations" (I, t). Clearly $ASp/\mathscr{V} \cong Sp$ and therefore $\mathfrak{A}/\mathfrak{I} \cong Sp$.

THEOREM 5.

$$PCT(p^m) \cong ASp(2m, p),$$
$$CT(p^m)/CG(p^m) \cong Sp(2m, p).$$

[2] See, e.g., van der Waerden [11], p. 70.

PROOF. Let

$$\psi_X : \lambda W^\alpha \to X(\lambda W^\alpha)X^{-1}$$

be the automorphism of CG induced by the element X of CT, and consider the homomorphism

$$h : X \to \psi_X$$

of CT into the group of automorphisms of CG. By theorem 3, $h(CT) = \mathfrak{A}$ and by theorem 1, cor. 1, the kernel of h is C^*. Hence $PCT \cong CT/C^* \cong \mathfrak{A} \cong AS\mathfrak{p}$. Also, since $h^{-1}(\mathfrak{J}) = C^*(CG) = CG$, we have $CT/CG \cong \mathfrak{A}/\mathfrak{J} \cong S\mathfrak{p}$.

3.4 *The group CS.*

Definition. The Clifford similarity group $CS(\mathfrak{p}^m)$ is the subgroup of $CT(\mathfrak{p}^m)$ formed by the elements which induce automorphisms (3.3.1) of $CG(\mathfrak{p}^m)$.

It is clear that the automorphisms (3.3.1) form a group isomorphic to $S\mathfrak{p}$, so that $PCS \cong S\mathfrak{p}$. Further, since $S\mathfrak{p}$ is obviously a complement of the translation group $\mathscr{V}$ in $AS\mathfrak{p}$, i.e.

$$(S\mathfrak{p})\mathscr{V} = AS\mathfrak{p}, \qquad S\mathfrak{p} \cap \mathscr{V} = 1,$$

it follows that PCS is a complement of PCG in PCT. We prove now that every complement H of $\mathscr{V}$ in $AS\mathfrak{p}$ is conjugate to $S\mathfrak{p}$ in $AS\mathfrak{p}$. It follows, of course, that every complement of PCG in PCT is conjugate to PCS in PCT.

From the formula

$$(T, \mathbf{t})(-I, \mathbf{0})(T, \mathbf{t})^{-1} = (-I, 2\mathbf{t}),$$

we deduce that (a) $S\mathfrak{p}$ is the centralizer $\mathfrak{C}(-I)$ of $-I = (-I, \mathbf{0})$ in $AS\mathfrak{p}$ and (b) every element $(-I, \mathbf{t})$ is conjugate to $-I$ in $AS\mathfrak{p}$. Now the mapping $\chi : h \to h\mathscr{V}$, is an isomorphism of H onto $AS\mathfrak{p}/\mathscr{V}$. Hence, if $\chi^{-1}((-I)\mathscr{V})) = (-I, 2\mathbf{t})$, we have

$$\begin{aligned} H \subseteq \mathfrak{C}((-I, 2\mathbf{t})) &= (I, \mathbf{t})\mathfrak{C}(-I)(I, \mathbf{t})^{-1} \\ &= (I, \mathbf{t})S\mathfrak{p}(I, \mathbf{t})^{-1}, \end{aligned}$$

and therefore, since H and $S\mathfrak{p}$ are isomorphic,

$$H = (I, \mathbf{t})S\mathfrak{p}(I, \mathbf{t})^{-1},$$

as required.

LEMMA. *CS is the centralizer in CT of the involution*

$$Jv_\lambda = v_{-\lambda} \qquad (\lambda \in \mathscr{V}_m). \tag{3.4.1}$$

PROOF. Since $JW^\alpha J^{-1} = W^{-\alpha}$, J is an element of CS which corresponds to the element $-I$ of $AS\mathfrak{p}$. Therefore, since $S\mathfrak{p}$ is the centralizer of $-I$ in $AS\mathfrak{p}$, CS consists of the elements X of CT which commute projectively with J:

$$XJX^{-1} = \lambda J. \tag{3.4.2}$$

https://doi.org/10.1017/S1446788700026379 Published online by Cambridge University Press

It remains to prove that $\lambda = 1$. Since $J^2 = I$, the only other possibility is $\lambda = -1$.

Let V^+, V^- denote the eigenspaces of J corresponding to the eigenvalues $1, -1$. Since V^+ is spanned by the vectors $v_\lambda + v_{-\lambda}$ and V^- by the vectors $v_\lambda - v_{-\lambda}$, their dimensions are $\frac{1}{2}(p^m + 1)$, $\frac{1}{2}(p^m - 1)$ respectively. If $\lambda = -1$, then we should have $XV^+ = V^-$, which is impossible because V^+, V^- have different dimensions. Therefore $\lambda = 1$ as required.

COROLLARY. *The subspaces V^+, V^- are invariant under CS.*

THEOREM 6. *$CS(p^m)$ is the direct sum of irreducible groups $CS^+(p^m)$, $CS^-(p^m)$ of degrees $\frac{1}{2}(p^m + 1)$, $\frac{1}{2}(p^m - 1)$ respectively.* If $p^m > 3$,

$$PCS^+(p^m) \cong PCS^-(p^m) \cong \tfrac{1}{2}Sp(2m, p).$$

PROOF. Consider the homomorphisms $\iota_+ : X \to X^+$ and $\iota_- : X \to X^-$, where X^+, X^- are the restrictions of $X \in CS$ to the eigenspaces V^+, V^- of J. CS is the direct sum of $CS^+ = \iota_+(CS)$ and $CS^- = \iota_-(CS)$, and these groups have the degrees stated in the theorem. In order to prove that they are irreducible, it is sufficient to prove that the commutator algebra Γ of CS has dimension $\leqq 2$ (the dimension will then be precisely 2 because $I, J \in \Gamma$). Let $Y \in \Gamma$. Since the W^α are linearly independent (theorem 1), Y can be expressed uniquely in the form

$$Y = \sum_{\alpha \in \mathscr{V}_{2m}} \lambda_\alpha W^\alpha.$$

Let $T \in Sp$ and choose $X_T \in CS$ such that $X_T W^\alpha X_T^{-1} = W^{\alpha T'}$. Since Y commutes with X_T, we have

$$\sum \lambda_\alpha W^\alpha = \sum \lambda_\alpha W^{\alpha T'}$$

and therefore $\lambda_\alpha = \lambda_{\alpha T'}$ whenever $\alpha \in \mathscr{V}_{2m}$. Since this is true for all $T \in Sp$, it follows by (2.2.6) that $\lambda_\alpha = \lambda_\beta$ for any two non-zero vectors α and β. Therefore Y is a linear combination of W^0 and $\sum_{\alpha \neq 0} W^\alpha$, so that $\dim \Gamma \leqq 2$ as required.

Let K^+, K^- be the kernels of ι_+, ι_-. It is clear that neither K^+ nor K^- contains scalars other than the identity, and we may therefore identify these groups with subgroups L^+, L^- of Sp. Since J^+ and $(-J)^-$ are the identity transformations on V^+, V^-, both L^+ and L^- contain the element $-I$ of Sp. Suppose now that $p^m > 3$. Then $\frac{1}{2}Sp$ is a simple group, so that the only possibilities for L^+, L^- are $\{-I\}$ and Sp. If L^+ or $L^- = Sp$, then PCS^+ or PCS^- would reduce to the identity, which is impossible because both CS^+ and CS^- are irreducible groups of degree > 1. Therefore $L^+ = L^- = \{-I\}$. It is now easily deduced that $PCS^+ \cong PCS^- \cong \frac{1}{2}Sp$.

3.5 *The commutator group of CT.*

THEOREM 7. *The commutator group CT' of CT has the following properties:*

https://doi.org/10.1017/S1446788700026379 Published online by Cambridge University Press

(i) *CT' is unitary;*
(ii) *CT' is a group over $R_0(\omega)$;*
(iii) *CT' is finite and has scalar subgroup $\{\omega I\}$;*
(iv) *$P(CT') = PCT$ if $p^m > 3$.*

PROOF. (i), (ii) follow from theorems 2, 3 respectively. Let $\lambda I \in CT'$. Then $\lambda \in R_0(\omega)$ and $|\lambda I| = \lambda^{p^m} = 1$. Since every p^k-th root of unity in $R_0(\omega)$ is a power of ω, we have $\lambda I \in \{\omega I\}$. Conversely, $\{\omega I\} = CG' \subset CT'$. Hence $\{\omega I\}$ is the scalar subgroup of CT'. The finiteness of CT' is an immediate consequence of the finiteness of its scalar subgroup.

We prove next that

$$CG \subset C^*(CT'); \tag{3.5.1}$$

i.e., CT' contains an element of the form λW^{α} for every $\alpha \in \mathscr{V}_{2m}$. Write α as the difference $\beta - \gamma$ of non-zero vectors β, γ. By (2.2.6), $\beta = \gamma T'$ for some $T \in Sp$ and therefore $XW^{\gamma}X^{-1} = \mu W^{\beta}$ for some $X \in CT$. Then $[X, W^{\gamma}]$ is an element of CT' of the required form λW^{α}.

Suppose now that $p^m > 3$. Then $Sp' = Sp$ and therefore, by theorem 5,

$$(CT/CG)' = CT/CG,$$

so that

$$(CT')(CG) = CT.$$

Hence, by (3.5.1), $C^*(CT') = CT$ and therefore $P(CT') = PCT$. This proves (iv) and the theorem.

The theorem shows that (when $p^m > 3$) there is a one-to-one correspondence between subgroups H of CT such that $PH = PCT$ and subgroups S of C^* such that $\omega I \in S$. In fact, let $PH = PCT$ and let S be the scalar subgroup of H. Then $H' = CT'$ so that $\omega I \in S$ and $H = S(CT')$.

4. The Commutator Group of CS

The investigation of CS' is more complicated than that of CT' and requires the explicit determination of the elements of CS. Our main result is that $CS' \cong Sp$ $(p^m > 3)$.

4.1 *The elements of CS.* Let $T \in Sp$. We wish to determine an element of CT which induces the automorphism (3.3.1) of CG. It is sufficient to determine a non-zero linear transformation X such that

$$XW^{\alpha} = W^{\alpha T'}X \qquad (\alpha \in \mathscr{V}_{2m}). \tag{4.1.1}$$

For if X_0 is a non-singular solution of (4.1.1), then $X_0^{-1}X$ commutes with every element of CG and therefore, by theorem 1, $X = \lambda X_0$.

Write

$$(\boldsymbol{a}_1, \boldsymbol{a}_2)T' = (\boldsymbol{A}_1, \boldsymbol{A}_2), \quad (\boldsymbol{b}_1, \boldsymbol{b}_2)T' = (\boldsymbol{B}_1, \boldsymbol{B}_2) \quad \cdots \tag{4.1.2}$$

https://doi.org/10.1017/S1446788700026379 Published online by Cambridge University Press

and

$$Xv_\lambda = \sum_{\mu \in \mathscr{V}_m} \xi_{\lambda,\mu} v_\mu.$$

Then (4.1.1) is equivalent to the homogeneous linear system

$$\xi_{\lambda+a_2,\mu+A_2} = \omega^{A_1\cdot(\mu+\frac{1}{2}A_2)-a_1\cdot(\lambda+\frac{1}{2}a_2)}\xi_{\lambda,\mu} \tag{4.1.3}$$
$$((a_1, a_2) \in \mathscr{V}_{2m},\ \lambda, \mu \in \mathscr{V}_m).$$

Since $T \in Sp$, we have, by (4.1.2),

$$a_1 \cdot b_2 - a_2 \cdot b_1 = A_1 \cdot B_2 - A_2 \cdot B_1. \tag{4.1.4}$$

In particular, if $b_2 = a_2$ and $B_2 = A_2$, we deduce that

$$A_1 \cdot A_2 - a_1 \cdot a_2 = B_1 \cdot A_2 - b_1 \cdot a_2.$$

Therefore the value of $A_1 \cdot A_2 - a_1 \cdot a_2$ depends only on a_2 and A_2. A second consequence of (4.1.4) is that

$$\tfrac{1}{2}((A_1 + B_1)\cdot(A_2 + B_2) - (a_1 + b_1)\cdot(a_2 + b_2)) \tag{4.1.5}$$
$$= A_1 \cdot (B_2 + \tfrac{1}{2}A_2) - a_1 \cdot (b_2 + \tfrac{1}{2}a_2) + \tfrac{1}{2}(B_1 \cdot B_2 - b_1 \cdot b_2).$$

Let $\mathscr{V}_T$ denote the subspace of $\mathscr{V}_{2m}$ formed by the vectors (a_2, A_2), where (a_1, a_2) runs over $\mathscr{V}_{2m}$. Then the following is a solution of (4.1.3):

$$\xi_{\lambda,\mu} = \omega^{\frac{1}{2}(A_1\cdot A_2 - a_1\cdot a_2)} \quad \textit{when } (\lambda, \mu) = (a_2, A_2) \in \mathscr{V}_T, \tag{4.1.6}$$
$$\xi_{\lambda,\mu} = 0, \quad \textit{when } (\lambda, \mu) \notin \mathscr{V}_T.$$

For if $(\lambda, \mu) \notin \mathscr{V}_T$ then $(\lambda + a_2, \mu + A_2) \notin \mathscr{V}_T$, so that both sides of (4.1.3) are zero. On the other hand, if $(\lambda, \mu) = (b_2, B_2) \in \mathscr{V}_T$ then (4.1.3) reduces to (4.1.5). The linear transformation defined by (4.1.6) will be denoted by X_T.

It is clear from the form of X_T that $X_T^* = X_{T^{-1}}$. Let

$$\dim \mathscr{V}_T = m + d_T. \tag{4.1.7}$$

Then, if $a \in \mathscr{V}_m$, p^{d_T} is both the number of vectors b such that $(a, b) \in \mathscr{V}_T$ and the number of vectors c such that $(c, a) \in \mathscr{V}_T$; in other words, the matrix $(\xi_{\lambda,\mu})$ of X_T has p^{d_T} non-zero elements in each row and column. It follows from theorem 2 that

$$X_T X_{T^{-1}} = X_T X_T^* = p^{d_T} I. \tag{4.1.8}$$

We note the following alternative characterizations of d_T.

(a) Let $\mathscr{U}_T$ denote the subspace of $\mathscr{V}_m$ formed by the vectors a such that $(a, 0)T'$ has the form $(A, 0)$. Then

$$\dim \mathscr{U}_T = m - d_T. \tag{4.1.9}$$

(b) Let

https://doi.org/10.1017/S1446788700026379 Published online by Cambridge University Press

$$T = \begin{pmatrix} A & B \\ C & D \end{pmatrix},$$

where A, B, C, D are $m \times m$ matrices. Then

$$d_T = \text{rank } C. \tag{4.1.10}$$

(a) follows from the fact that the vectors $(\boldsymbol{a}, \mathbf{0})$ $(\boldsymbol{a} \in \mathscr{U}_T)$ form the kernel of the linear mapping $(\boldsymbol{a}_1, \boldsymbol{a}_2) \to (\boldsymbol{a}_2, \boldsymbol{A}_2)$ of $\mathscr{V}_{2m}$ onto $\mathscr{V}_T$. (b) follows from (a) because $(\boldsymbol{a}, \mathbf{0})T' = (\boldsymbol{a}A', \boldsymbol{a}C')$.

4.2 *Arithmetical Results.*

Write

$$\Theta = \sum_{i=1}^{p} \omega^{i^2}, \tag{4.2.1}$$

$$\Omega = \det (\omega^{ij})_{i,j=1,\cdots,p}.$$

Then

$$\Theta = p^{\frac{1}{2}} (p \equiv 1 \pmod 4), \qquad \Theta = ip^{\frac{1}{2}} (p \equiv 3 \pmod 4), \tag{4.2.2}$$

$$\Omega = \left(\frac{-2}{p}\right) \Theta^p, \tag{4.2.3}$$

where $\left(\frac{-2}{p}\right)$ is Legendre's symbol. See e.g. Landau [8].

LEMMA A. *If $q(\boldsymbol{\lambda})$ is a quadratic form on $\mathscr{V}_k(p)$ and $p^k > 3$, then*

$$\sum_{\boldsymbol{\lambda} \in \mathscr{V}_k} q(\boldsymbol{\lambda}) = 0. \tag{4.2.4}$$

LEMMA B. *If $q(\boldsymbol{\lambda})$ is a quadratic form on $\mathscr{V}_k(p)$, then*

$$\sum_{\boldsymbol{\lambda} \in \mathscr{V}_k} \omega^{q(\boldsymbol{\lambda})} = \pm \Theta^r, \tag{4.2.5}$$

where r is a non-negative integer.

These lemmas follow easily from the fact that $q(\boldsymbol{\lambda})$ is equivalent to a diagonal form $\sum_{i=1}^{k} c_i \lambda_i^2$. We omit the details of the proofs.

If T is a non-singular $k \times k$ matrix over $GF(p)$, we define

$$\text{sgn } T = \left(\frac{\det T}{p}\right).$$

In other words, if $\det T = \gamma^\kappa$, where γ is a generator of the cyclic group $GF(p)^*$, then $\text{sgn } T = (-1)^\kappa$.

LEMMA C. Sgn T *is the sign of the permutation $\boldsymbol{\lambda} \to \boldsymbol{\lambda}T'$ of the p^k elements* of $\mathscr{V}_k$.

PROOF. Let D denote the $k \times k$ diagonal matrix diag $\{\gamma, 1, \cdots, 1\}$, $\sigma(T)$ the sign of the given permutation. Then $T = D^\kappa T_1$, where $\det T_1 = 1$. Since the special linear group is the commutator group of the full linear group, $\sigma(T_1) = 1$, so that $\sigma(T) = \sigma(D)^\kappa$. Now the permutation $\boldsymbol{\lambda} \to \boldsymbol{\lambda}D'$ leaves

p^{k-1} vectors fixed and permutes the remaining $p^{k-1}(p-1)$ vectors in cycles of length $(p-1)$, whence $\sigma(D) = -1$. It follows that $\sigma(T) = (-1)^\kappa = \operatorname{sgn} T$ as required.

LEMMA D. *Let $\lambda T \mu'$ be a non-degenerate bilinear form on $\mathscr{V}_k$, and Y the $p^k \times p^k$ matrix*

$$Y = (\omega^{\lambda T \mu'})_{\lambda, \mu \in \mathscr{V}_k}.$$

Then

$$\det Y = (\operatorname{sgn} T)\Omega^{kp^{k-1}}. \tag{4.2.6}$$

PROOF. Applying the permutation $\lambda \to \lambda T$ to the rows of Y, we have, by lemma C, $\det Y = (\operatorname{sgn} T) \det (\omega^{\lambda \mu'})$. Since $(\omega^{\lambda \mu'}) = (\omega^{\lambda_1 \mu_1} \omega^{\lambda_2 \mu_2} \cdots \omega^{\lambda_k \mu_k})$ is the k-th Kronecker power of the matrix (ω^{ij}), $\det (\omega^{\lambda \mu'}) = \Omega^{kp^{k-1}}$. This gives the lemma.

4.3 *The group CS'.*

LEMMA E. *If $S, T \in Sp$, then*

$$X_S X_T = \lambda_{S,T} X_{ST}$$

where $\lambda_{S,T}$ is a scalar. $\lambda_{S,T}$ has the form $\pm\Theta^k$, where k is an integer $\geqq 0$.

PROOF. The first statement follows from the isomorphism $PCS \cong Sp$. To prove the second, let

$$X_S v_\lambda = \sum \xi'_{\lambda,\mu} v_\mu,$$
$$X_T v_\lambda = \sum \xi_{\lambda,\mu} v_\mu.$$

Then

$$\lambda_{S,T} = \sum_{\mu \in \mathscr{V}_m} \xi_{0,\mu} \xi'_{\mu,0}. \tag{4.3.1}$$

In the notation of § 4.1, the expression $\frac{1}{2}(\boldsymbol{A}_1 \cdot \boldsymbol{A}_2 - \boldsymbol{a}_1 \cdot \boldsymbol{a}_2)$ is a quadratic form $q_T((\boldsymbol{a}_2, \boldsymbol{A}_2))$ on $\mathscr{V}_T$. (4.3.1) can be written

$$\lambda_{S,T} = \sum_{\alpha \in \mathscr{W}} \omega^{q_T(\alpha) - q_{S^{-1}}(\alpha)},$$

where $\mathscr{W}$ is the subspace of $\mathscr{V}_{2m}$ formed by the vectors $(\mathbf{0}, \mu)$ in $\mathscr{V}_T \cap \mathscr{V}_{S^{-1}}$. By lemma B, $\lambda_{S,T}$ has the required form $\pm\Theta^k$.

THEOREM 8. *$CS'(p^m) \cong Sp(2m, p)$ if $p^m > 3$.*

PROOF. If $p^m > 3$, $P(CS') = PCS \cong Sp$. It is therefore sufficient to prove that the scalar subgroup of CS' is the identity.

Let $\lambda I \in CS'$. Then λI can be written in the form

$$X_{T_1}^{\varepsilon_1} X_{T_2}^{\varepsilon_2} \cdots,$$

where each ε_i is ± 1. Since

$$X_S^{-1} = \lambda_{S,S^{-1}}^{-1} X_{S^{-1}},$$

https://doi.org/10.1017/S1446788700026379 Published online by Cambridge University Press

it follows that λ is a product of $\lambda_{S,T}$'s and their inverses. By lemma E, $\lambda = \pm\Theta^k$, where k is a (possibly negative) integer. On the other hand, since $\lambda I \in CT'$, λ is a power of ω. Hence $\lambda I = I$ as required.

We now determine the elements of CS' explicitly. The chief difficulty is to establish the correct sign.

THEOREM 9. *Let $p^m > 3$. Let $T = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in Sp$, where A, B, C, D are $m \times m$ matrices. Since the rank of (C, D) is m and the rank of C is d_T (see (4.1.10)), it is possible to choose $m - d_T$ columns of D which together with the columns of C span $\mathscr{V}_m$; suppose that the columns of D numbered $i_{d_T+1}, i_{d_T+2}, \cdots, i_m$ satisfy this condition. Let M be the $m \times m$ matrix whose i-th column is the i-th column of D when i is one of $i_{d_T+1}, \cdots, i_m$, and the i-th column of C otherwise. Then M is non-singular and*

$$(\operatorname{sgn} M)\left(\left(\frac{2}{p}\right)\Theta\right)^{-d_T} X_T \in CS', \tag{4.3.2}$$

where $\left(\frac{2}{p}\right)$ is Legendre's symbol.

PROOF. It is sufficient to prove that

$$\begin{aligned} \det X_T &= (\operatorname{sgn} M)\left(\left(\frac{2}{p}\right)\Theta\right)^{d_T p^m}, \\ &= (\operatorname{sgn} M)\left(\left(\frac{-1}{p}\right)\Omega\right)^{d_T p^{m-1}}. \end{aligned} \tag{4.3.3}$$

For if this is so, and if Y_T denotes the element (4.3.2), then (a) $\det Y_T = 1$ and (b) $Y_S Y_T = \mu_{S,T} Y_{ST}$, where $\mu_{S,T}$ has the form $\pm\Theta^k$. Hence, by the argument of theorem 8, the group generated by the Y_T has scalar subgroup $\{I\}$ and so coincides with CS'.

We write $d = d_T$. Let $\boldsymbol{a}_i', \boldsymbol{b}_i', \boldsymbol{c}_i', \boldsymbol{d}_i'$ denote the i-th columns, $\boldsymbol{\alpha}_i, \boldsymbol{\beta}_i, \boldsymbol{\gamma}_i, \boldsymbol{\delta}_i$ the i-th rows, of A, B, C, D respectively. As usual, $\boldsymbol{e}_i$ denotes the i-th unit vector of $\mathscr{V}_m$. With $i_{d+1}, \cdots, i_m$ as in the statement of the theorem, the vectors

$$(\boldsymbol{e}_{i_\kappa}, \boldsymbol{d}_{i_\kappa}) \qquad (\kappa = d+1, \cdots, m) \tag{4.3.4}$$

belong to $\mathscr{V}_T$; for $(\mathbf{0}, \boldsymbol{e}_{i_\kappa})T' = (\boldsymbol{b}_{i_\kappa}, \boldsymbol{d}_{i_\kappa})$. Let $\boldsymbol{c}_{i_1}', \boldsymbol{c}_{i_2}', \cdots, \boldsymbol{c}_{i_d}'$ be linearly independent columns of C. By the choice of the $\boldsymbol{d}_i$, the vectors

$$\boldsymbol{c}_{i_\kappa} \quad (\kappa = 1, \cdots, d), \quad \boldsymbol{d}_{i_\kappa} \quad (\kappa = d+1, \cdots, m) \tag{4.3.5}$$

form a basis of $\mathscr{V}_m$. Since $(\boldsymbol{e}_{i_\kappa}, \mathbf{0})T' = (\boldsymbol{a}_{i_\kappa}, \boldsymbol{c}_{i_\kappa})$, the vectors

$$(\mathbf{0}, \boldsymbol{c}_{i_\kappa}) \qquad (\kappa = 1, \cdots, d) \tag{4.3.6}$$

belong to $\mathscr{V}_T$. Let $K = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$; since $T \in Sp$, we have $T'KT = K$, and so

$T^{-1} = K^{-1}T'K$; therefore $T^{-1} = \begin{pmatrix} D' & -B' \\ -C' & A' \end{pmatrix}$. Let $\gamma_{j_1}, \gamma_{j_2}, \cdots, \gamma_{j_d}$ be linearly independent rows of C. Since $(-e_{j_\kappa}, 0)T'^{-1} = (-\delta_{j_\kappa}, \gamma_{j_\kappa})$, the vectors

$$(\gamma_{j_\kappa}, 0) \qquad (\kappa = 1, \cdots, d) \tag{4.3.7}$$

belong to $\mathscr{V}_T$.

Let $(\lambda, \mu) \in \mathscr{V}_T$. Since μ is a linear combination of the vectors (4.3.5), there is a linear combination, say L, of the vectors (4.3.4) and (4.3.6) such that $(\lambda, \mu) - L$ has the form $(\nu, 0)$. Since $(\nu, 0)$ is a linear combination of the vectors (4.3.7), it follows that (λ, μ) is a linear combination of the vectors (4.3.4), (4.3.6), (4.3.7). Therefore these $m + d$ vectors form a basis of $\mathscr{V}_T$. In particular, it follows that the vectors

$$\gamma_{j_\kappa} \quad (\kappa = 1, \cdots, d), \quad e_{i_\kappa} \quad (\kappa = d + 1, \cdots, m) \tag{4.3.8}$$

form a basis of $\mathscr{V}_m$.

Let P and Q be the $m \times m$ matrices whose rows are the vectors (4.3.5) and (4.3.8) respectively. Let $k_1, \cdots, k_d$ be the integers complementary to $i_{d+1}, \cdots, i_m$ in the set $1, 2, \cdots, m$. Since $\det Q \neq 0$, the columns $c'_{k_1}, \cdots, c'_{k_d}$ of C are linearly independent. Altering our original choice of the columns c'_{i_κ} $(\kappa = 1, \cdots, d)$ if necessary, we may therefore suppose that $i_1, \cdots, i_m$ is a permutation of $1, \cdots, m$. Then, on permuting the rows of P so that the subscripts appear in natural order, we get the transpose of the matrix M in the statement of the theorem. Hence M is non-singular. Let $C = (c_{ij})$. Applying the same permutation to the rows of Q we get a matrix whose determinant is the same as that of the $d \times d$ matrix

$$\Gamma = (c_{j_\kappa i_\lambda})_{\kappa, \lambda = 1, \cdots, d}.$$

In the notation of (4.1.6), $\det X_T = \det (\xi_{\lambda, \mu})$. If

$$\lambda = \sum_1^d \nu_\kappa \gamma_{j_\kappa} + \sum_{d+1}^m \nu_\kappa e_{i_\kappa},$$

$$\mu = \sum_1^d \rho_\kappa c_{i_\kappa} + \sum_{d+1}^m \rho_\kappa d_{i_\kappa},$$

then we write $\xi_{\lambda, \mu} = \zeta_{\nu, \varrho}$, where

$$\nu = (\nu_1, \cdots, \nu_m), \qquad \varrho = (\rho_1, \cdots, \rho_m).$$

By lemma C,

$$\det X_T = (\operatorname{sgn} M)(\operatorname{sgn} \Gamma) \det (\zeta_{\nu, \varrho}). \tag{4.3.9}$$

Now, if $(\nu_{d+1}, \cdots, \nu_m) \neq (\rho_{d+1}, \cdots, \rho_m)$ then $(\lambda, \mu) \notin \mathscr{V}_T$ and so $\zeta_{\nu, \varrho} = 0$. Hence, writing

https://doi.org/10.1017/S1446788700026379 Published online by Cambridge University Press

$$\boldsymbol{n} = (\nu_1, \cdots, \nu_d), \quad \boldsymbol{r} = (\rho_1, \cdots, \rho_d), \quad \boldsymbol{s} = (\sigma_{d+1}, \cdots, \sigma_m),$$
$$\zeta_{\boldsymbol{s}} = \det\,(\zeta_{(\boldsymbol{n},\boldsymbol{s}),\,(\boldsymbol{r},\boldsymbol{s})})_{\boldsymbol{n},\boldsymbol{r}\in\mathscr{V}_d},$$

we have

$$\det\,(\zeta_{\boldsymbol{\nu},\boldsymbol{\varrho}}) = \prod_{\boldsymbol{s}\in\mathscr{V}_{m-d}} \zeta_{\boldsymbol{s}}. \tag{4.3.10}$$

Now $\zeta_{(\boldsymbol{n},\boldsymbol{s})(\boldsymbol{r},\boldsymbol{s})}$ has the form

$$\zeta_{(\boldsymbol{n},\boldsymbol{s}),\,(\boldsymbol{r},\boldsymbol{s})} = \omega^{t(\boldsymbol{s},\boldsymbol{n},\boldsymbol{r})},$$
$$t(\boldsymbol{s},\boldsymbol{n},\boldsymbol{r}) = a(\boldsymbol{s}) + b(\boldsymbol{n}) + c(\boldsymbol{r}) + d(\boldsymbol{s},\boldsymbol{n}) + e(\boldsymbol{s},\boldsymbol{r}) + g(\boldsymbol{n},\boldsymbol{r}),$$

where a, b, c are quadratic forms, d, e, g bilinear forms. a, b, c, d, e correspond to constant factors of the rows or columns of $\zeta_{\boldsymbol{s}}$, and it can be seen (with the help of lemma A) that the product of all these factors in $\det\,(\zeta_{\boldsymbol{\nu},\boldsymbol{\varrho}})$ is 1. Hence

$$\det\,(\zeta_{\boldsymbol{\nu},\boldsymbol{\varrho}}) = (\det\,(\omega^{g(\boldsymbol{n},\boldsymbol{r})}))^{p^{m-d}}. \tag{4.3.11}$$

Since

$$(-\sum_1^d \nu_\kappa \boldsymbol{\delta}_{j_\kappa} + \sum_1^d \rho_\kappa \boldsymbol{e}_{i_\kappa},\quad \sum_1^d \nu_\kappa \gamma_{j_\kappa})T' = (-\sum_1^d \nu_\kappa \boldsymbol{e}_{j_\kappa} + \sum_1^d \rho_\kappa \boldsymbol{a}_{i_\kappa},\quad \sum_1^d \rho_\kappa \boldsymbol{c}_{i_\kappa}),$$

we have

$$g(\boldsymbol{n},\boldsymbol{r}) = -\tfrac{1}{2}(\sum_{\kappa,\lambda=1}^d (\boldsymbol{e}_{j_\kappa}\cdot\boldsymbol{c}_{i_\lambda} + \boldsymbol{e}_{i_\lambda}\cdot\gamma_{j_\kappa})\nu_\kappa\rho_\lambda)$$
$$= -\boldsymbol{n}\Gamma\boldsymbol{r}'.$$

Hence, by lemma D,

$$\det\,(\omega^{g(\boldsymbol{n},\boldsymbol{r})}) = (\operatorname{sgn}\,(-\Gamma))\Omega^{dp^{d-1}} \tag{4.3.12}$$
$$= (\operatorname{sgn}\,\Gamma)\left(\left(\frac{-1}{p}\right)\Omega\right)^{dp^{d-1}}$$

The required formula (4.3.3) now follows from (4.3.9), (4.3.11) and (4.3.12).

COROLLARY. *The symplectic group $Sp(2m, p)$ $(p > 2)$ has irreducible representations of degrees $\frac{1}{2}(p^m - 1)$ and $\frac{1}{2}(p^m + 1)$.*

This follows from theorems 6 and 9. If ι_+ and ι_- are the isomorphisms in the proof of theorem 9, we write

$$\iota_+(CS') = CS'^+, \qquad \iota_-(CS') = CS'^-.$$

Theorem 12 shows that

$$\left(\frac{-1}{p}\right)^m J \in CS',$$

where J is the involution (3.4.1). Therefore we have (if $p^m > 3$)

$$CS'^+ \cong \tfrac{1}{2}Sp, \quad CS'^- \cong Sp \quad \text{if } p^m \equiv 1 \pmod 4,$$
$$CS'^+ \cong Sp, \quad CS'^- \cong \tfrac{1}{2}Sp \quad \text{if } p^m \equiv 3 \pmod 4.$$

THEOREM 10. *If $p > 2$, $Sp(2m, p)$ has no irreducible representations of degree k, where $1 < k < \frac{1}{2}(p^m - 1)$.*

PROOF. Let h be an irreducible representation of Sp of character ψ and degree $n > 1$. It is required to prove that $n \geqq \frac{1}{2}(p^m - 1)$. We may, of course, suppose in the proof that $p^m > 3$ and thus that $h(Sp) \cong Sp$ or $\frac{1}{2}Sp$.

Consider the subgroup G of Sp generated by the transvections

$$T_{\boldsymbol{a}} : \boldsymbol{\alpha} \to \boldsymbol{\alpha} + f(\boldsymbol{\alpha}, \boldsymbol{a})\boldsymbol{a},$$

where $\boldsymbol{a}$ runs over the m-dimensional subspace $\mathfrak{V}_m = \{\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \cdots, \boldsymbol{\varepsilon}_m\}$ of $\mathfrak{V}_{2m}$ ($\boldsymbol{\varepsilon}_i$ being the i-th unit vector in $\mathfrak{V}_{2m}$). In general, $T_{\boldsymbol{a}}^p = I$ and $T_{\boldsymbol{a}}T_{\boldsymbol{b}} = T_{\boldsymbol{b}}T_{\boldsymbol{a}}$ when $f(\boldsymbol{a}, \boldsymbol{b}) = 0$, so that G is an elementary abelian p-group. Let

$$\psi(T) = \chi_1(T) + \chi_2(T) + \cdots \quad (T \in G), \tag{4.3.13}$$

where $\chi_1, \chi_2, \cdots$ are irreducible characters of G. We shall prove our theorem by showing that there are at least $\frac{1}{2}(p^m - 1)$ summands in (4.3.13).

Let X be any non-singular linear transformation on $\mathfrak{V}_m$, χ one of the irreducible characters in (4.3.13). By Witt's theorem (2.2.5), we can choose an element S of Sp such that $X\boldsymbol{a} = \boldsymbol{a}S'$ ($\boldsymbol{a} \in \mathfrak{V}_m$). Since $\psi(STS^{-1}) = \psi(T)$, the irreducible character χ_S of G defined by

$$\chi_S(T) = \chi(STS^{-1}) \qquad (T \in G) \tag{4.3.14}$$

is also a summand in (4.3.13). Since $ST_{\boldsymbol{a}}S^{-1} = T_{X\boldsymbol{a}}$, we have

$$\chi_S(T_{\boldsymbol{a}}) = \chi(T_{X\boldsymbol{a}}). \tag{4.3.15}$$

Let $\chi(T_{\boldsymbol{a}}) = \omega^{\phi(\boldsymbol{a})}$. Since χ is multiplicative, and since $T_{\lambda\boldsymbol{a}+\mu\boldsymbol{b}} = T_{\boldsymbol{a}}^{\lambda^2-\lambda\mu}T_{\boldsymbol{b}}^{\mu^2-\lambda\mu}T_{\boldsymbol{a}+\boldsymbol{b}}^{\lambda\mu}$, we have

$$\phi(\lambda\boldsymbol{a} + \mu\boldsymbol{b}) = (\lambda^2 - \lambda\mu)\phi(\boldsymbol{a}) + (\mu^2 - \lambda\mu)\phi(\boldsymbol{b}) + \lambda\mu\phi(\boldsymbol{a} + \boldsymbol{b}),$$

so that ϕ is a quadratic form on $\mathfrak{V}_m$. By (4.3.15), the quadratic form associated with χ_S is

$$\phi_S(\boldsymbol{a}) = \phi(X\boldsymbol{a}). \tag{4.3.16}$$

Since $h(Sp) \cong Sp$ or $\frac{1}{2}Sp$, $h(G) \cong G$ and therefore at least one of the components in (4.3.13) is not the unit representation, i.e. the corresponding quadratic form is not identically zero. In view of (4.3.16), our theorem will follow when we have proved:

(4.3.17) if $\phi(\boldsymbol{a})$ is a non-zero quadratic form on $\mathfrak{V}_m$, there are at least $\frac{1}{2}(p^m - 1)$ different quadratic forms on $\mathfrak{V}_m$ which are equivalent to $\phi(\boldsymbol{a})$.

Let r be the rank of ϕ. If $r = m$, the number N of forms equivalent to ϕ is the order of the full linear group on $\mathfrak{V}_m$ divided by the order of the orthogonal group of ϕ, viz.

$$\tfrac{1}{2}(p^m - 1)(p^{m-2} - 1)(p^{m-4} - 1) \cdots (p - 1)p^{\frac{1}{4}(m^2-1)} \quad (m \text{ odd}),$$
$$\tfrac{1}{2}(p^{\frac{1}{2}m} \pm 1)(p^{m-1} - 1)(p^{m-3} - 1) \cdots (p - 1)p^{\frac{1}{4}m^2} \quad (m \text{ even}).$$

The inequality $N \geqq \frac{1}{2}(p^m - 1)$ is easily verified. Suppose now that $1 \leqq r < m$. Without loss of generality we may suppose that $\phi(\sum_1^m a_i \varepsilon_i) = \sum_1^r k_i a_i^2$, where $k_1, \cdots, k_r$ are non-zero. If $\boldsymbol{u}_1, \cdots, \boldsymbol{u}_m$ is any basis of $\mathscr{V}_m$ then ϕ' defined by $\phi'(\sum_1^m a_i \boldsymbol{u}_i) = \sum_1^r k_i a_i^2$ is equivalent to ϕ. Since the $(m - r)$-dimensional subspace $\{\boldsymbol{u}_{r+1}, \cdots, \boldsymbol{u}_m\}$ consists of the vectors $\boldsymbol{a}$ such that $\phi'(\boldsymbol{\alpha} + \boldsymbol{a}) = \phi'(\boldsymbol{\alpha})$ for all $\boldsymbol{\alpha} \in \mathscr{V}_m$, it follows that ϕ' is different from ϕ'' defined by $\phi''(\sum_1^m a_i \boldsymbol{v}_i) = \sum_1^r k_i a_i^2$ unless $\{\boldsymbol{u}_{r+1}, \cdots, \boldsymbol{u}_m\} = \{\boldsymbol{v}_{r+1}, \cdots, \boldsymbol{v}_m\}$. Also, the $\frac{1}{2}(p - 1)$ forms $\lambda^2\phi'(\boldsymbol{a})$ $(\lambda \neq 0)$ are equivalent to $\phi'(\boldsymbol{a})$ and correspond to the same subspace $\{\boldsymbol{u}_{r+1}, \cdots, \boldsymbol{u}_m\}$. Hence $N \geqq \frac{1}{2}(p - 1)k_{m,m-r}$, where $k_{m,m-r}$ is the number of subspaces of $\mathscr{V}_m$ of dimension $(m - r)$. Let f be the smaller of r and $(m - r)$. Then

$$\begin{aligned}\tfrac{1}{2}(p - 1)k_{m,m-r} &= \tfrac{1}{2}(p - 1)k_{m,f} \\ &= \tfrac{1}{2}(p^m - 1)\frac{(p^{m-1} - 1)(p^{m-2} - 1) \cdots (p^{m-f+1} - 1)}{(p^2 - 1)(p^3 - 1) \cdots (p^f - 1)} \\ &\geqq \tfrac{1}{2}(p^m - 1),\end{aligned}$$

so that $N \geqq \frac{1}{2}(p^m - 1)$. This proves (4.3.17) and the theorem.

Appendix

The results in the exceptional case $p^m = 3$ are as follows.

(1) Sp is isomorphic to the binary tetrahedral group of order 24, Sp' to the quaternion group of order 8. Sp is generated by the two elements

$$(\alpha_1, \alpha_2)S' = (\alpha_1 - \alpha_2, \alpha_2),$$
$$(\alpha_1, \alpha_2)T' = (-\alpha_2, \alpha_1),$$

of orders 3, 4 respectively, Sp' by T, STS^{-1}.

(2) The linear transformations

$$\left.\begin{aligned} Yv_\lambda &= \omega^{\lambda^2-1}v_\lambda, \\ Zv_\lambda &= (\omega^2 - \omega)^{-1}\sum_\mu \omega^{-\lambda\mu}v_\mu, \end{aligned}\right\} \quad (\lambda, \mu = 0, \pm 1)$$

satisfy

$$YW^{\boldsymbol{\alpha}}Y^{-1} = W^{\boldsymbol{\alpha}S'}, \qquad ZW^{\boldsymbol{\alpha}}Z^{-1} = W^{\boldsymbol{\alpha}T'};$$

therefore $\{Y, Z\}$ is a subgroup of CS which is projectively equal to CS. Since

$$Y(v_1 - v_{-1}) = Z(v_1 - v_{-1}) = (v_1 - v_{-1}),$$

$\{Y, Z\}$ is the kernel of the homomorphism ι_- and therefore isomorphic to Sp (see the proof of theorem 6).

https://doi.org/10.1017/S1446788700026379 Published online by Cambridge University Press

(3) CS contains three subgroups isomorphic to Sp, viz. $\{\omega^i Y, Z\}$ $(i = 0, 1, 2)$. (Cf. thm. 8.).

(4) CT contains three subgroups which are projectively equal to CT and have scalar subgroup $\{\omega I\}$, viz. $\{\varepsilon^i Y, Z\}\mathscr{C}\mathscr{G}$ $(i = 0, 1, 2)$, where $\varepsilon = \exp(2\pi i/9)$. Only $\{Y, Z\}\mathscr{C}\mathscr{G}$ is a group over $R_0(\omega)$. (Cf. thm. 7).

References

[1] Barnes, E. S. and Wall, G. E., Some extreme forms defined in terms of Abelian groups, This *Journal* 1 (1959), 47—63.
[2] Bolt, Beverley, Ph.D. Thesis, Sydney University (1959).
[3] Dieudonné, J., *La Géométrie des Groupes classiques* (Springer, 1955).
[4] Horadam, A. F., A locus in [8] invariant under a group of order 51840 × 81, *Quarterly J. Math.* (2) 8 (1957), 241—259.
[5] Horadam A. F., Projection of an invariant locus in [8] from a solid lying on it, *ibidem* (2) 9 (1958), 81—86.
[6] Horadam, A. F., Clifford groups in the plane, *ibidem* (2) 10 (1959), 294—295.
[7] Horadam, A. F., Involutions associated with the Burkhardt configuration in [4], *Canad. J. Math.* 11 (1959), 18—33.
[8] Landau, E., *Vorlesungen über Zahlentheorie*, Bd. 1 (Leipzig, 1927).
[9] Morinaga, K. and Nono, T., On the linearization of a form of higher degree and its representation. *J. Sci. Hiroshima Univ.* A 16 (1952), 13—41.
[10] Room, T. G., A synthesis of the Clifford matrices and its generalization, *Amer. J. Math.* 74 (1952), 967—984.
[11] van der Waerden, B. L., *Gruppen von linearen Transformationen* (Springer, 1935; reprinted Chelsea, 1948).

University of Sydney.