Can. J. Math., Vol. XXIX, No. 2, 1977, pp. 333–348

IRREDUCIBLE AUTOMORPHISMS OF CERTAIN p-GROUPS

D. Ž. DJOKOVIĆ AND J. MALZAN

Introduction. The chief purpose of this paper is to find all pairs (G, θ) where G is a finite special p-group, and θ is an automorphism of G acting trivially on the Frattini subgroup and irreducibly on the Frattini quotient. This problem arises in the context of describing finite groups having an abelian maximal subgroup. In fact, we solve a more general problem for a wider class of p-groups, which we call *special F-groups*, where F is a finite field of characteristic p. We point out that if p is odd, then an F-group has exponent p. On the other hand, every special 2-group is also a special $GF(2)$-group.

As a byproduct of our theory of F-groups we obtain an interesting result about non-singular subspaces of alternating matrices over finite fields (Theorems 10 and 12). These results can be stated in terms of alternating forms. Analogous results are obtained for quadratic forms over $GF(2^n)$ (Theorem 13). Theorems of this type are known for matrices over reals, complexes or quaternions [**1**; **2**].

We conclude with an open problem about non-degenerate F-groups (Section 5).

Notation.

$Z(G)$ = the centre of a group G,
$\Phi(G)$ = the Frattini subgroup of G,
G' = the commutator subgroup of G,
$N_G(H)$ = the normalizer of H in G,
$C_H(a)$ = the centralizer of an element $a \in G$ in the subgroup H of G.
If H is a subgroup of G then

$$\text{core}(H) = \bigcap_{x \in G} xHx^{-1}.$$

$|S|$ = the number of elements of a finite set S.

$G = N \prec H$ is the semi-direct product of N and H with $N \lhd G$. It will always be clear from the context how H acts on N.

A group H of automorphisms of a group G is *regular* if for every $\alpha \in H$, $\alpha \neq 1$, the centralizer

$$C_G(\alpha) = \{x \in G | \alpha(x) = x\}$$

of α in G is trivial.

Received March 11, 1976 and in revised form, November 9, 1976. This research was supported by NRC grants A-5285 and A-7263.

https://doi.org/10.4153/CJM-1977-037-8 Published online by Cambridge University Press

p will always denote a prime number. We say that a finite group is a p'-group if $|G|$ is not divisible by p.

A finite p-group is called *special* if either it is elementary abelian or nilpotent of class two with $Z(P) = P' = \Phi(P)$. If, moreover, $|\Phi(P)| = p$ then P is called *extra-special*. See [**6**, Chapter 5] or [**7**, Chapter III, § 13] for the basic properties of these groups.

1. The structure of G. In this section G will denote a finite group having an abelian maximal subgroup A. In the case where $A \lhd G$ we have $(G : A) = p$ where p is a prime. The structure of such groups is known [**8**]. Hence we will only be interested in the case when A is not normal in G.

First we show how one can construct finite groups G having an abelian subgroup A which is not normal in G.

Let P be a non-trivial special p-group (of exponent p if p is odd) admitting a cyclic p'-group of automorphisms H which is trivial on $\Phi(P)$ and acts irreducibly and non-trivially on $\bar{P} = P/\Phi(P)$. Let D be an abelian p-group containing a copy of $\Phi(P)$. Define $K = (D \times P)/R$ where R consists of all (x, x^{-1}) for $x \in \Phi(P)$. We extend the action of H to $D \times P$ and K by specifying that it acts trivially on D. Now let B be an abelian p'-group admitting an epimorphism $f\colon B \to H$. Let $G = K \prec B$ where B acts on K via f. The subgroup $A = BD$ of G is abelian and proper. We claim that it is maximal in G. Indeed, if M is a subgroup of G containing A properly then $M \cap P$ contains $\Phi(P)$ properly and the irreducibility of $\bar{P}$ under the action of B implies that $M \cap P = P$. Hence $M \supset AP = G$.

We claim that A is not normal in G. Otherwise it follows from $A = B \times D$ that B is normal in G. Hence $G = B \times K$, contradicting that B acts non-trivially on K.

We prove next that there are no other examples.

THEOREM 1. *Let G be a finite group having an abelian maximal subgroup A which is not normal in G. Then*

(i) $N_G(A) = A$, $Z(G) = \mathrm{core}(A)$, *and* $A \cap xAx^{-1} = Z(G)$ *for all* $x \in G \backslash A$;

(ii) $(G : A) = p^n$ *for some prime* p.

Let $A = B \times D$ where D is the p-Sylow subgroup of A and B its unique p'-complement. Then

(iii) $Z(G) = B_0 \times D$ *where* $B_0 = B \cap Z(G)$,

(iv) *there exists a special p-subgroup P of G such that $P \lhd G$, $P \not\subset A$, $G = AP$, $A \cap P = D \cap P = \Phi(P)$, and P has exponent p when p is odd, 2 or 4 when $p = 2$.*

(v) *B acts irreducibly and non-trivially on $\bar{P} = P/\Phi(P)$ and the kernel of this action is B_0;*

(vi) *$\bar{B} = B/B_0$ is cyclic;*

(vii) *DP is a p-group and $G = (DP) \prec B$.*

https://doi.org/10.4153/CJM-1977-037-8 Published online by Cambridge University Press

Proof. It is clear from our hypotheses that $N_G(A) = A$. We have $Z(G) \subset N_G(A) = A$. On the other hand if $x \in G \backslash A$ then $xAx^{-1} \neq A$. Hence A and xAx^{-1} centralize $A \cap xAx^{-1}$ and generate G, implying that $\text{core}(A) \subset A \cap xAx^{-1} \subset Z(G)$. Thus (i) is proved.

Let $\bar{A} = A/Z(G)$, $\bar{G} = G/Z(G)$. It follows from (i) that $\bar{A}$ is a maximal subgroup of $\bar{G}$, $N_{\bar{G}}(\bar{A}) = \bar{A}$ and that $\bar{A}$ has trivial intersection with each of its conjugates. Hence, by [**6**, Theorem 7.7, p. 39] $\bar{G}$ is a Frobenius group with complement $\bar{A}$. By [**6**, Theorem 3.1, p. 339] we have $\bar{G} = \bar{N} \leftthreetimes \bar{A}$ where $\bar{N}$ is nilpotent and $|\bar{A}|$ divides $|\bar{N}| - 1$. Since $\bar{N}$ is a direct product of its Sylow subgroups and $\bar{N}$ is maximal in $\bar{G}$ it follows that $\bar{N}$ is a non-trivial p-group for some prime p. Since $(G : A) = (\bar{G} : \bar{A}) = |\bar{N}|$ the assertion (ii) is proved.

Since $\bar{A}$ divides $|\bar{N}| - 1 = p^n - 1$ (say) it follows that $\bar{A}$ is a p'-group, i.e., $Z(G) \supset D$ and (iii) is proved. Let N be the pre-image of $\bar{N}$ in G, and let S_p be the Sylow p-subgroup of N. Then $S_p \supset D$, $N = Z(G)S_p = B_0 \times S_p$, $S_p \lhd G$ and $G = AS_p$. By [**6**, Theorem 3.8, p. 183] there exists a special p-subgroup P of S_p such that P is B-invariant and B acts irreducibly and non-trivially on $\bar{P} = P/\Phi(P)$. Thus $P \not\subset A$, $P \lhd G$, $G = AP$.

We claim that $\Phi(P) \subset A$ Otherwise we have $G = A\Phi(P)$, $\Phi(P) \lhd G$ and $P = \Phi(P)(A \cap P)$. By a well-known property of the Frattini subgroup this implies that $P = A \cap P$, which is a contradiction. Hence $\Phi(P) \subset A \cap P \subset P$ and since B acts irreducibly on $\bar{P}$ we must have $\Phi(P) = A \cap P$.

Assume now that p is odd. (If $p = 2$, it is immediate that P has exponent 2 or 4, by definition.) By [**6**, Lemma 3.9, p. 183] the elements $x \in P$ satisfying $x^p = 1$ form a subgroup P_1 of P. We have $\Phi(P) \subset P_1 \subset P$ and so by irreducibility of $\bar{P}$ we must have either $P_1 = \Phi(P)$ or $P_1 = P$. The first possibility is ruled out because P is a non-trivial special p-group and p is odd. Thus $P_1 = P$, i.e., P has exponent p.

Hence we have proved (iv) and the first part of (v). Assume that $a \in B$ acts trivially on $\bar{P}$. Then $\langle Z(G), a \rangle$ is normalized by A and P and hence it lies in $\text{core}(A) = Z(G)$. Thus $a \in Z(G) \cap B = B_0$ and (v) is proved.

Let $a \in B$ be such that $\bar{C} = C_{\bar{P}}(a)$ is non-trivial. Let C be the pre-image of $\bar{C}$ in P. Since B is abelian it is clear that B normalizes C. Since $P \cap A \subsetneq C \subset P$ we must have $C = P$ by the irreducibility of $\bar{P}$. Thus a acts trivially in $\bar{P}$ and by (v) we have $a \in B_0$. This proves that $\bar{B}$ is a regular p'-group of automorphisms of $\bar{P}$. By [**6**, Theorem 3.14, p. 187] $\bar{B}$ is cyclic and (vi) is proved.

It is clear that (vii) holds because $D \subset Z(G)$, D is a p-group and consequently DP is a p-group normal in G.

The theorem is proved.

It is clear that the problem of constructing finite groups G having an abelian maximal subgroup A is now reduced to the following problem:

Construct all pairs (P, θ) where P is a non-trivial special p-group (of exponent p if p is odd) and θ is a p'-automorphism of P fixing $\Phi(P)$ elementwise and acting irreducibly on $\bar{P} = P/\Phi(P)$.

https://doi.org/10.4153/CJM-1977-037-8 Published online by Cambridge University Press

We shall solve this problem completely in the remaining part of this paper. In fact, we solve this problem for a somewhat larger class of groups which we call F-groups (F being a field).

2. F-groups. Let F be any field, and let V_0 and V_1 be F-vector spaces. Let also ϕ: $V_0 \times V_0 \to V_1$ be an F-bilinear form. We construct a group $V = V_0 \times V_1$ having the following multiplication:

$$(x, y)(x', y') = (x + x', y + y' + \phi(x, x')).$$

This is a group because ϕ is a normalized 2-cocycle. The elements $(0, y)$ in V form a subgroup of V, canonically isomorphic with V_1. Further, $V_1 \subset Z(V)$ and V_0 is canonically isomorphic with V/V_1. The group V will be called in this paper an *F-group*. Whenever we refer to an F-group V we shall regard V_0, V_1 and $\phi = \phi_V$ as part of the structure of V.

In V we have $(x, y) = (x, 0)(0, y)$, $(x, y)^{-1} = (-x, -y + \phi(x, x))$ and hence the commutator

$$\begin{aligned}[(x, y), (x', y')] &= [(x, 0), (x', 0)] \\ &= (-x, \phi(x, x))(-x', \phi(x', x'))(x, 0)(x', 0) \\ &= (-x-x', \phi(x, x) + \phi(x', x') \\ &\quad + \phi(x, x'))(x + x', \phi(x, x')) \\ &= (0, \phi(x, x') - \phi(x', x)).\end{aligned}$$

Further, it is easy to check that

$$V' \subset \Phi(V) \subset V_1 \subset Z(V).$$

Given two F-groups V and W, we shall say that a homomorphism θ: $V \to W$ is an *F-homomorphism* if $\theta(V_1) \subset W_1$ and the induced map θ_0: $V_0 \to W_0$ and the restriction θ_1: $V_1 \to W_1$ are F-linear.

We shall denote by $\mathrm{Aut}(V; F)$ the group of F-automorphisms of V.

If F has characteristic p, an odd prime, then every non-trivial F-group has exponent p. This follows directly by computation. If $p = 2$, then every non-trivial F-group has exponent 4 or 2.

For each bilinear function ϕ we define

$$\phi'(x, y) = \phi(x, y) - \phi(y, x).$$

We shall say that an F-group V is *special* if V_1 is generated (as a vector space or, equivalently, as a group) by the image of ϕ_V', where ϕ_V is the bilinear function associated with V.

Definition 1. Let ϕ: $V_0 \times V_0 \to V_1$ be an F-bilinear map. Then we shall say that ϕ is *non-degenerate* if for every non-zero linear function ψ: $V_1 \to F$ the composite bilinear form $\psi \circ \phi$ is non-degenerate. Similarly, if Q: $V_0 \to V_1$ is a quadratic map of F-vector spaces V_0 and V_1 then we shall say that Q is

https://doi.org/10.4153/CJM-1977-037-8 Published online by Cambridge University Press

non-degenerate if the bilinear map $Q(x + y) - Q(x) - Q(y)$ is non-degenerate. We shall say that an F-group V is *non-degenerate* if the bilinear map ϕ_V' is non-degenerate.

Our definition of non-degenerate quadratic maps is analogous to the definition of non-degenerate quadratic forms given in Bourbaki [**3**, Definition 2, p. 54]. Some other authors call such quadratic forms *non-defective* if char $F = 2$. See, for instance [**5**, p. 33].

LEMMA 2. *Every non-degenerate F-group V is a special F-group.*

Proof. Assume that V is not special. Then there exists a non-zero linear form $\psi\colon V_1 \to F$ such that $V' \subset \mathrm{Ker}(\psi)$. Hence $\psi \circ \phi' = 0$, contradicting that V is non-degenerate.

LEMMA 3. *If V is a non-degenerate F-group, then $V' = \Phi(V) = V_1 \subset Z(V)$. If also $V_1 \neq 0$, then $V_1 = Z(V)$.*

Proof. From the previous lemma V is a special F-group, and so $V' = V_1$. It follows that $V' = \Phi(V) = V_1$.

If $V_1 \neq 0$, and $(x, y) \in Z(V)$, then also $(x, 0) \in Z(V)$, and therefore $\phi'(x, z) = \phi(x, z) - \phi(z, x) = 0$ for all $z \in V_0$. Since $V_1 \neq 0$ we can choose a non-zero linear form $\psi\colon V_1 \to F$, and since $\psi \circ \phi'$ is non-degenerate, we must have $x = 0$, completing the proof.

LEMMA 4. *Let p be an odd prime. If P is a p-group of exponent p with a central subgroup P_1 such that P/P_1 is abelian then P is a $GF(p)$-group.*

Proof. We may consider $P_0 = P/P_1$ and P_1 as $GF(p) = F$-vector spaces. First, we choose a family of elements $a_i \in P$ ($i \in I$, I totally ordered) such that the $\bar{a}_i \in P_0$ form a basis of P_0. Then the elements

$$a_{i_1}^{\alpha_1} \ldots a_{i_k}^{\alpha_k}, \quad i_1 < i_2 < \ldots < i_k, \alpha_i \in F$$

are coset representatives for $P_1 \subset P$. The 2-cocycle ϕ associated with this extension can be computed as follows:

$$(1) \quad a_{i_1}^{\alpha_1} \ldots a_{i_k}^{\alpha_k} a_{i_1}^{\beta_1} \ldots a_{i_k}^{\beta_k} = a_{i_1}^{\alpha_1+\beta_1} \ldots a_{i_k}^{\alpha_k+\beta_k} \prod_{r>s} [a_{i_r}, a_{i_s}]^{\alpha_r\beta_s}.$$

Using now additive notation we have

$$\phi(\alpha_1\bar{a}_{i_1} + \ldots + \alpha_k\bar{a}_{i_k}, \beta_1\bar{a}_{i_1} + \ldots + \beta_k\bar{a}_{i_k}) = \sum_{r>s} \alpha_r\beta_s[a_{i_r}, a_{i_s}].$$

Hence ϕ is F-bilinear, and it is now clear that P is isomorphic to the $GF(p)$-group built using P_0, P_1 and ϕ.

LEMMA 5. *Let P be a 2-group with a central subgroup P_1 of exponent 2 such that P/P_1 is of exponent 2. Then P is a $GF(2)$-group.*

Proof. Again, we may consider $P_0 = P/P_1$ and P_1 as $GF(2) = F$-vector spaces, and choose a family of elements $a_i \in P$ ($i \in I$, I totally ordered) such

https://doi.org/10.4153/CJM-1977-037-8 Published online by Cambridge University Press

that the $\bar{a}_i \in P_0$ form a basis of P_0. The elements

$$a_{i_1}^{\alpha_1} \ldots a_{i_k}^{\alpha_k}, \quad i_1 < i_2 < \ldots < i_k, \alpha_i = 0, 1$$

are coset representatives for $P_1 \subset P$. In order to compute the 2-cocycle ϕ we can use formula (1) of the previous lemma noting that if for some index i, $\alpha_i = \beta_i = 1$, then

$$a_{i_1}^{\alpha_1+\beta_1} \ldots a_{i_k}^{\alpha_k+\beta_k}$$

is not in general a coset representative. In this case, however, if we let $a_i^2 = b_i$, then $b_i \in P_1$ and

$$a_{i_r}^{\alpha_r+\beta_r} = a_{i_r}^{\gamma_r} b_{i_r}^{\alpha_r\beta_r}$$

where $\gamma_r = 0, 1$ and $\gamma_r \equiv \alpha_r + \beta_r \bmod 2$. Hence in this case

$$\phi(\alpha_1\bar{a}_{i_1} + \ldots + \alpha_k\bar{a}_{i_k}, \beta_1\bar{a}_{i_1} + \ldots + \beta_k\bar{a}_{i_k}) = \sum_{r=1}^{k} \alpha_r\beta_r b_{i_r} + \sum_{r>s} \alpha_r\beta_s[a_{i_r}, a_{i_s}].$$

Thus again ϕ is F-bilinear, and we are done.

LEMMA 6. *If V and W are F-groups, and $\theta\colon V \to W$ is an F-homomorphism then*

$$\theta(x, y) = (\theta_0(x), \theta_1(y) + \theta_{01}(x))$$

where $\theta_i\colon V_i \to W_i$, $i = 0, 1$, are F-linear maps, and $\theta_{01}\colon V_0 \to W_1$ is a quadratic map such that we have

(2) $\quad \phi_W' \circ (\theta_0 \times \theta_0) = \theta_1 \circ \phi_V'$

and

(3) $\quad \theta_{01}(x + x') - \theta_{01}(x) - \theta_{01}(x') = \phi_W(\theta_0(x), \theta_0(x')) - \theta_1(\phi_V(x, x'))$.

In particular, $\phi_W(\theta_0(x), \theta_0(x')) - \theta_1(\phi_V(x, x'))$ is a symmetric bilinear map. If $\operatorname{char}(F) = 2$, then this map is alternating. Conversely, if θ_0, θ_1 and θ_{01} satisfy these conditions, then $\theta \in \operatorname{Aut}(V; F)$.

Proof. From $\theta(x, y) = \theta(x, 0) \cdot \theta(0, y) = \theta(x, 0) \cdot (0, \theta_1(y))$ and the definition of θ_0 it follows that $\theta(x, y)$ has the form given in the Lemma. Equation (2) follows from

$$\phi_W'(\theta_0(x), \theta_0(x')) = [(\theta_0(x), \theta_{01}(x)), (\theta_0(x'), \theta_{01}(x'))] = \theta([(x, 0), (x', 0)]) = \theta_1(\phi_V'(x, x')).$$

Equation (3) follows from

$$\theta((x, 0)(x', 0)) = \theta((x + x', \phi_V(x, x')) = (\theta_0(x + x'), \theta_1(\phi_V(x, x')) + \theta_{01}(x + x')),$$

https://doi.org/10.4153/CJM-1977-037-8 Published online by Cambridge University Press

and

$$\theta(x, 0) \cdot \theta(x', 0) = (\theta_0(x), \theta_{01}(x))(\theta_0(x'), \theta_{01}(x')) = (\theta_0(x) + \theta_0(x'), \theta_{01}(x) + \theta_{01}(x') + \theta_W(\theta_0(x), \theta_0(x')))$$

The converse is straightforward.

3. Irreducible automorphisms of finite F-groups. For the rest of this paper the field F and all the groups will be assumed to be finite.

Definition 2. If V is an F-group we denote by $\mathrm{Aut}_0(V; F)$ the subgroup of $\mathrm{Aut}(V; F)$ consisting of those F-automorphisms which fix all the elements of $V_1 \subset V$.

PROPOSITION 7. *If V is a special F-group admitting an automorphism $\theta \in \mathrm{Aut}_0(V; F)$ such that the induced automorphism $\theta_0 \in \mathrm{Aut}(V_0)$ is irreducible as an F-linear transformation, then V is non-degenerate.*

Proof. By equation (2) of Lemma 6, it follows that ϕ' is preserved by θ_0.

Let ψ be a non-zero linear form on V_1. By the irreducibility of θ_0 if follows that $\mathrm{Ker}(\psi \circ \phi') = 0$ or V_0 because θ_0 preserves the form $\psi \circ \phi'$. We have $\mathrm{Ker}(\psi \circ \phi') \neq V_0$ because otherwise $\mathrm{Im}(\phi') \subset \mathrm{Ker}(\psi)$ contradicting the hypothesis that V is a special F-group. Hence $\mathrm{Ker}(\psi \circ \phi') = 0$ and $\psi \circ \phi'$ is non-degenerate.

This completes the proof of the proposition.

Definition 3. Let $f(X)$ be a monic irreducible polynomial over a finite field $F = GF(q)$, $q = p^n$. An *F-representation* of $f(X)$ is a pair (V, θ) where V is a special F-group, $\theta \in \mathrm{Aut}_0(V; F)$, θ has p' order, and the induced automorphism θ_0 has $f(X)$ as its characteristic polynomial. (This last implies that θ_0 is irreducible on V_0).

Definition 4. If (V, θ) and (W, ω) are F-representations of $f(X)$ then a morphism $(V, \theta) \to (W, \omega)$ is an F-homomorphism $\sigma: V \to W$ such that $\omega \circ \sigma = \sigma \circ \theta$.

Let (V, θ) be an F-representation of $f(X)$ and let N be a subgroup of V_1. Then $\bar{V} = V/N$ is also a non-degenerate F-group, the induced automorphism $\bar{\theta}$ of $\bar{V}$ is in $\mathrm{Aut}_0(\bar{V}; F)$ and $(\bar{V}, \bar{\theta})$ is also an F-representation of $f(X)$. We say that $(\bar{V}, \bar{\theta})$ is a *quotient* of (V, θ).

PROPOSITION 8. *If V is a non-degenerate F-group, and if $V_1 \neq 0$, then the dimension of V_0 is even.*

Proof. Let ψ be any non-zero linear form from V_1 to F. By Definition 1, ϕ_V' is non-degenerate. Therefore $\psi \circ \phi_V'$ is a non-degenerate alternating form from V_0 to F, and this implies that the dimension of V_0 is even.

It follows from Proposition 8 that if $f(X)$ is an irreducible polynomial of odd degree and (V, θ) is an F-representation of f, then $V_1 = 0$, and $V = V_0$.

https://doi.org/10.4153/CJM-1977-037-8 Published online by Cambridge University Press

We introduce some notation. Let

$$f(X) = X^m + \alpha_1 X^{m-1} + \ldots + \alpha_m.$$

If $\alpha_m \neq 0$ we define

$$\tilde{f}(X) = \alpha_m{}^{-1} X^m f(X^{-1})$$

noting that if $f(X)$ is irreducible and $\tilde{f} = f$, then $\alpha_m = 1$ and m must be even, unless $m = 1$.

We also define the $(m-1) \times (m-1)$ matrix $M(f)$ as

$$M(f) = \begin{bmatrix} \alpha_m & & & 0 \\ \alpha_{m-1} & \alpha_m & & \\ \vdots & \ddots & \ddots & \\ \alpha_2 & \alpha_3 & \ldots & \alpha_m \end{bmatrix} - \begin{bmatrix} \alpha_{m-2} & \alpha_{m-3} & & \alpha_0 \\ & \ddots & \iddots & \\ & \ddots & & \\ \alpha_1 & \alpha_0 & & 0 \\ \alpha_0 & & & \end{bmatrix}$$

where $\alpha_0 = 1$.

We denote by $r(f)$ the rank of $M(f)$. We shall prove later that when $f(X)$ is irreducible in $F[X]$ then

$$r(f) = \begin{cases} m-1 & \text{if } \tilde{f} \neq f \\ m/2 - 1 & \text{if } \tilde{f} = f \text{ and } m > 1. \end{cases}$$

THEOREM 9. *Given any monic irreducible polynomial $f(X) \in F[X]$ there exists an F-representation (V, θ) of $f(X)$ which is universal in the following sense: Every F-representation of $f(X)$ is isomorphic to a quotient of (V, θ). This universal F-representation (V, θ) is unique up to isomorphism. Also,* $\dim(V_0) = m = \deg(f)$, *and* $\dim(V_1) = m - 1 - r(f)$.

Proof. Recall that $F = GF(q)$, $q = p^n$. Let V_0 and U be F-vector spaces with bases $a_0, a_1, \ldots, a_{m-1}$ and $b_1, \ldots, b_{m-1}$ respectively. Let $\boldsymbol{b}$ be the column vector whose coordinates are the vectors $b_1, \ldots, b_{m-1}$. Then $M(f)\boldsymbol{b}$ is an $(m-1)$-tuple of vectors in U. Let N be the F-subspace spanned by the vectors $M(f)\boldsymbol{b}$ and let $V_1 = U/N$. For $x \in V$ we let $\bar{x} = x + N$.

Let ϕ be the bilinear map from $V_0 \times V_0$ to V_1 defined by

$$\phi(a_i, a_j) = \begin{cases} 0 & \text{if } i < j \\ b_{j-i} & \text{if } i \geqq j \end{cases}$$

where $b_0 = 0$ if $p \neq 2$, and, if $p = 2$,

$$b_0 = f(1)^{-2}\left(\sum_{i=1}^{m-1} b_i(\alpha_1 \alpha_{i+1} + \alpha_2 \alpha_{i+2} + \ldots + \alpha_{m-i}\alpha_m)\right).$$

We construct an F-group $V = V_0 \times V_1$ using this ϕ.

https://doi.org/10.4153/CJM-1977-037-8 Published online by Cambridge University Press

Let an F-automorphism θ_0 of V_0 be defined by

$$\theta_0(a_i) = a_{i+1} \quad \text{for } 0 \leqq i \leqq m-2$$
$$\theta_0(a_{m-1}) = -\alpha_m a_0 - \alpha_{m-1}a_1 - \ldots - \alpha_1 a_{m-1} \quad (= a_m, \text{ say}).$$

Note that the characteristic polynomial of θ_0 is $f(X)$ and hence θ_0 is irreducible as an F-linear automorphism of V_0.

We claim that $\phi(\theta_0(x), \theta_0(x')) - \phi(x, x')$ is symmetric. This is equivalent to the statement that $\phi'(x, x')$ is θ_0-invariant. Since ϕ' is alternating, it suffices to check that $\phi'(\theta_0(a_i), \theta_0(a_j)) = \phi'(a_i, a_j)$ for $0 \leqq i < j \leqq m-1$. Thus we have to show that $\phi'(a_{i+1}, a_{j+1}) = \phi'(a_i, a_j)$, $0 \leqq i < j \leqq m-1$. This is clear if $j \neq m-1$. If $j = m-1$, this equation becomes

$$\phi'(a_{i+1}, -\alpha_m a_0 - \alpha_{m-1}a_1 - \ldots - \alpha_1 a_{m-1}) = \bar{b}_{m-1-i}$$

or

$$\alpha_m \bar{b}_{i+1} + \alpha_{m-1}\bar{b}_i + \ldots + \alpha_{m-i}\bar{b}_1 \quad -\alpha_{m-i-2}\bar{b}_1 - \ldots - \alpha_1 \bar{b}_{m-i-2} = \bar{b}_{m-1-i}.$$

This follows from the definition of V_1 as a quotient.

In case $p = 2$ we must check further that the form $\phi(\theta_0(x), \theta_0(x')) - \phi(x, x')$ is alternating. It is enough to check that

$$\phi(\theta_0(a_i), \theta_0(a_i)) = \phi(a_i, a_i) \quad \text{for } 0 \leqq i \leqq m-1.$$

This is clear unless $i = m-1$. In that case we need to show that $\phi(a_m, a_m) = \bar{b}_0$, i.e.,

$$\phi\left(\sum_{i=0}^{m-1} \alpha_{m-i}a_i, \sum_{j=0}^{m-1} \alpha_{m-j}a_j\right) = \bar{b}_0, \quad \text{i.e.,} \quad \sum_{0 \leqq i < j \leqq m-1} \alpha_{m-i}\alpha_{m-j}\bar{b}_{j-i} = f(1)^2 \bar{b}_0$$

which follows from our definition of b_0.

Since this bilinear map is symmetric and, if $p = 2$, alternating, there exists a quadratic map $\theta_{01} : V_0 \to V_1$ such that

$$\theta_{01}(x + x') - \theta_{01}(x) - \theta_{01}(x') = \phi(\theta_0(x), \theta_0(x')) - \phi(x, x');$$

see [**3**, Proposition 2, p. 55] for the case of quadratic forms. Now we define θ by

$$\theta(x, y) = (\theta_0(x), \theta_{01}(x) + y).$$

It is a straightforward check that $\theta \in \mathrm{Aut}_0(V; F)$. Since $f(X)$ is irreducible, the order k of θ_0 is a p'-number. Hence the order of θ is of the form $p^r k$. Then if $\theta' = \theta^{p^s}$, where s is chosen so that $s \geqq r$ and $p^s \equiv 1 \bmod k$, θ' will have order k. Thus, by replacing θ by θ', if necessary, we may assume that θ is a p'-element. Therefore, (V, θ) is an F-representation of $f(X)$. Also $\dim(V_0) = m$, $\dim(V_1) = m - 1 - r(f)$.

We claim that (V, θ) is universal. Let (W, ω) be any F-representation of $f(X)$. We can assume that $W_0 = V_0$, and $\omega_0 = \theta_0$. Define a linear map $\tau: U \to W_1$ by

$$\tau(b_i) = \phi_W'(a_0, a_i) \quad \text{for } 1 \leqq i \leqq m-1.$$

https://doi.org/10.4153/CJM-1977-037-8 Published online by Cambridge University Press

We claim that $N \subset \mathrm{Ker}(\tau)$. For all integers k we write $a_k = \theta_0{}^k(a_0)$, consistent with the notation for a_i used above. We compute

$$\begin{aligned} c_i &= \tau(\alpha_{m-i+1}b_1 + \ldots + \alpha_m b_i - \alpha_{m-i-1}b_1 - \ldots - \alpha_0 b_{m-i}) \\ &= \phi_W{}'(a_0, \alpha_{m-i+1}a_1 + \ldots + \alpha_m a_i - \alpha_{m-i-1}a_1 - \ldots - \alpha_0 a_{m-i}) \\ &= \phi_W{}'(a_0, \alpha_{m-i+1}a_1 + \ldots + \alpha_m a_i) - \phi_W{}'(a_0, \alpha_{m-i-1}a_1 + \ldots + \alpha_0 a_{m-i}). \end{aligned}$$

Now by equation (2) of Lemma 6, $\phi_W{}'$ is θ_0-invariant, and so

$$\begin{aligned} &\phi_W{}'(a_0, \alpha_{m-i+1}a_1 + \ldots + \alpha_m a_i) \\ &\quad = -\phi_W{}'(a_1, \alpha_{m-i+1}a_0) - \phi_W{}'(a_2, \alpha_{m-i+2}a_0) - \ldots - \phi_W{}'(a_i, \alpha_m a_0) \\ &\quad = -\phi_W{}'(a_0, \alpha_{m-i+1}a_{-1} + \alpha_{m-i+2}a_{-2} + \ldots + \alpha_m a_{-i}) \\ &\quad = -\phi_W{}'(a_0, \alpha_m a_{-i} + \ldots + \alpha_{m-i+1}a_{-1}) \end{aligned}$$

so that

$$\begin{aligned} c_i &= -\phi_W{}'(a_0, \alpha_m a_{-i} + \ldots + \alpha_0 a_{m-i}) \\ &= -\phi_W{}'(a_0, \theta_0{}^{-i}(\alpha_m a_0 + \alpha_{m-1}a_1 + \ldots + \alpha_0 a_m)) \\ &= -\phi_W{}'(a_0, \theta_0{}^{-i}(0)) = 0. \end{aligned}$$

Since this is true for all i, $1 \leqq i \leqq m-1$, we conclude that $N \subset \mathrm{Ker}(\tau)$. Let σ_1 be the τ-induced map from $V_1 = U/N \to W_1$.

The bilinear map $\sigma_1(\phi_V(x, x')) - \phi_W(x, x')$ is symmetric because $\sigma_1 \circ \phi_V{}' = \phi_W{}'$ by definition of τ and σ_1. If $p = 2$ we claim that this map is alternating. Thus we have to verify that

$$\sigma_1(\phi_V(a_i, a_i)) = \phi_W(a_i, a_i) \quad \text{for } 0 \leqq i \leqq m-1.$$

But $\sigma_1(\phi_V(a_i, a_i)) = \sigma_1(\bar{b}_0) = \tau(b_0)$ and since

$$(a_i, 0)^2 = (0, \phi_W(a_i, a_i)),$$

$$(\omega(a_i, 0))^2 = ((\theta_0(a_i), \omega_{01}(a_i))^2 = (0, \phi_W(a_{i+1}, a_{i+1}))$$

it follows that $\phi_W(a_i, a_i)$ is independent of i. Thus we just have to justify the single equality $\tau(b_0) = \phi_W(a_0, a_0)$. Since

$$\sum_{i=0}^{m} \alpha_{m-i}a_i = 0$$

we have

$$\begin{aligned} 0 &= \phi_W\left(\sum_{i=0}^{m} \alpha_{m-i}a_i, \sum_{j=0}^{m} \alpha_{m-j}a_j\right) \\ &= \sum_{i,j=0}^{m} \alpha_{m-i}\alpha_{m-j}\phi_W(a_i, a_j) \\ &= \sum_{0 \leqq i < j \leqq m} \alpha_{m-i}\alpha_{m-j}\phi_W{}'(a_i, a_j) + f(1)^2\phi_W(a_0, a_0). \end{aligned}$$

https://doi.org/10.4153/CJM-1977-037-8 Published online by Cambridge University Press

Using the identity

$$\sum_{0\leqq i\leqq m-1} \alpha_{m-i}\alpha_0 \phi_W'(a_i, a_m) = \phi_W'\left(\sum_{i=0}^{m} \alpha_{m-i}a_i, a_m\right) = 0$$

the preceding equality gives

$$f(1)^{-2} \sum_{0\leqq i<j\leqq m-1} \alpha_{m-i}\alpha_{m-j}\phi_W'(a_i, a_j) = \phi_W(a_0, a_0).$$

The left hand side of this equality is $\tau(b_0)$, since

$$b_0 = f(1)^{-2} \sum_{0\leqq i<j\leqq m-1} \alpha_{m-i}\alpha_{m-j}b_{j-i}.$$

Hence we have $\tau(b_0) = \phi_W(a_0, a_0)$ and the map $\sigma_1(\phi_V(x, x')) - \phi_W(x, x')$ is shown to be alternating when $p = 2$.

It follows that there exists a quadratic map σ_{01}: $V_0 \to W_1$ such that

$$\sigma_{01}(x + x') - \sigma_{01}(x) - \sigma_{01}(x') = \sigma_1(\phi_V(x, x')) - \phi_W(x, x').$$

Now we define σ: $V \to W$ by $\sigma(x, y) = (x, \sigma_1(y) + \sigma_{01}(x))$. It is easy to check that σ is an F-homomorphism and consequently σ: $(V, \theta) \to (W, \omega)$ is a morphism. Since σ is onto and $\mathrm{Ker}(\sigma) \subset V_1$ the F-representation (W, ω) is a quotient of (V, θ). Thus (V, θ) is a universal representation.

By a dimension argument it is clear that the universal F-representation is unique up to isomorphism.

The theorem is proved.

4. Universal representations. In this section we compute $r(f)$. In the course of this we prove a theorem about maximal non-singular subspaces of the space of alternating matrices over a finite field.

As before, $q = p^n$. $S_p(2m, q)$ is the symplectic group, consisting of $2m \times 2m$ matrices X with elements from the field $F = GF(q)$ satisfying ${}^tXJX = J$ where

$$J = \begin{pmatrix} 0 & I_m \\ -I_m & 0 \end{pmatrix}.$$

We shall consider these matrices X as operators on the space of column vectors $F^{2m} = V_0$. We shall use $M_s(F) = M_s(q)$ to denote the set of all $s \times s$ matrices over F, and by $K_s(F) = K_s(q)$ the set of all alternating matrices over F.

THEOREM 10. *If $A \in M_{2m}(q)$ has irreducible characteristic polynomial $f(X)$ then the space $K(A; q) = \{X \in K_{2m}(q); {}^tAXA = X\}$ has dimension m if $f = \tilde{f}$ and 0 if $f \neq \tilde{f}$. As well, if $0 \neq X \in K(A, q)$ then X is non-singular.*

Proof. Let $X \in K(A; q)$, $X \neq 0$. Note that $\mathrm{Ker}(X)$ is A-invariant because $v \in V_0$ and $Xv = 0$ imply that $0 = Xv = ({}^tAXA)v = {}^tAX(Av)$ and $X(Av) = 0$. By the irreducibility of A and $X \neq 0$ we must have $\mathrm{Ker}(X) = 0$, i.e., X is non-singular. Now ${}^tAXA = X$ and so ${}^tA = XA^{-1}X^{-1}$, ${}^tA$ and A^{-1} are

https://doi.org/10.4153/CJM-1977-037-8 Published online by Cambridge University Press

similar, and the characteristic polynomial f of A satisfies $f = \tilde{f}$. Therefore if $f \neq \tilde{f}$ we have $K(A; q) = 0$.

Assume then that $f = \tilde{f}$. Let $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_{2m}$ be the distinct roots of $f(X)$. They are all in $F(\alpha) = GF(q^{2m})$. Then A is similar in $M_{2m}(q^{2m})$ to the diagonal matrix D with diagonal entries $\alpha_1, \alpha_2, \ldots, \alpha_{2m}$. The dimension of $K(D; q^{2m})$ over $F(\alpha)$ is the same as the dimension of $K(A; q)$ over F [**4**, (29, 5), p. 200]. A matrix $X \in K_{2m}(q^{2m})$ belongs to $K(D; q^{2m})$ if and only if $DXD = X$, i.e., $\alpha_i\alpha_j\xi_{ij} = \xi_{ij}$ where $X = (\xi_{ij})$. We may assume, since $f = \tilde{f}$, that $\alpha_{m+i} = \alpha_i^{-1}$ for $1 \leqq i \leqq m$. The above equations imply that $\xi_{ij} = 0$ unless $j - i = \pm m$. Now it is clear that

$$\dim_{F(\alpha)} K(D; q^{2m}) = \dim_F (K(A, q)) = m.$$

LEMMA 11. *For each finite field $F = GF(q)$, and each positive integer $2m$ there exists an irreducible polynomial $f(X)$ in $F[X]$ of degree $2m$ such that $f = \tilde{f}$.*

Proof. Let $L = GF(q^{2m})$. The multiplicative group of L has order $q^{2m} - 1$. Let α be an element of L of order $q^m + 1$. Let $f(X)$ be the minimal polynomial of α over F. Then $L = F(\alpha)$, since if $F(\alpha)$ has order q^r then we must have $q^m + 1 | q^r - 1$ and since $r | 2m$ it follows that $r = 2m$. Also $\alpha^{-1} = \alpha^{q^m}$ is also a root of $f(X)$. Therefore $f = \tilde{f}$ and the lemma is proven.

Definition 5. A subspace L of $M_s(F)$ is called *non-singular* if every non-zero matrix in L is non-singular.

THEOREM 12. *In $K_{2m}(q)$ the dimension of a non-singular subspace is $\leqq m$. This upper bound is always achieved.*

Proof. Let S be a non-singular subspace of $K_{2m}(q)$. By choosing a basis $X_1, \ldots, X_k$ we can express any X in S as

$$X = \alpha_1 X_1 + \ldots . + \alpha_k X_k.$$

Then $\det(X) = (\mathrm{Pf}(X))^2$ where $\mathrm{Pf}(X)$ is the pfaffian of X. $\mathrm{Pf}(X)$ is a homogeneous polynomial in the α_i of degree m. If $k > m$ then by Chevalley's theorem [**9**, p. 13] the polynomial $\mathrm{Pf}(X)$ has a non-trivial zero, contradicting the hypothesis that S is non-singular. Therefore $\dim(S) \leqq m$.

By the previous lemma, a polynomial $f(X)$ of the desired kind can always be found. Let $A \in M_{2m}(q)$ have characteristic polynomial $f(X)$. Then $\dim K(A, q) = m$, $K(A, q)$ is non-singular, and the upper bound is achieved, as claimed.

We remark that the problem of finding maximum dimension for real non-singular subspaces of symmetric, skew-symmetric, etc. matrices has been considered for real, complex and quaternionic matrices [**1**; **2**].

The set of all upper triangular matrices in $M_s(F) = M_s(q)$ will be denoted by $T_s(F) = T_s(q)$.

https://doi.org/10.4153/CJM-1977-037-8 Published online by Cambridge University Press

THEOREM 13. *If $A \in M_{2m}(q)$, $q = 2^n$, has irreducible characteristic polynomial $f(X)$, then the space $T(A; q) = \{X \in T_{2m}(q),\ {}^tAXA \equiv X \bmod K_{2m}(q)\}$ has dimension m if $f = \tilde{f}$, 0 if $f \neq \tilde{f}$. As well, if $X \in T(A; q)$ and $X \neq 0$ then $X + {}^tX$ is non-singular.*

Proof. Suppose $0 \neq X \in T(A; q)$. Then ${}^tAXA = X + B$ with B alternating and so ${}^tA\,{}^tXA = {}^tX + B$. Adding,

$$ {}^tA(X + {}^tX)A = X + {}^tX $$

and so, as in the proof of Theorem 10, $X + {}^tX$ is either 0 or non-singular.

It remains to show that $X + {}^tX \neq 0$ or, equivalently, that X is not diagonal. We can assume that A has the form

$$ \begin{bmatrix} 0 & & & & & & \alpha_{2m} \\ 1 & 0 & & & & & \\ & 1 & 0 & & & & \\ & & 1 & & & & \\ & & & \ddots & & & \\ & & & & \ddots & & \\ & & & & & & \\ 0 & & & & & 1 & \alpha_1 \end{bmatrix} $$

and that the diagonal matrix X has diagonal entries $\xi_1, \xi_2, \ldots, \xi_{2m}$. By equating the diagonal entries of ${}^tAXA$ and X we get that

$$ \xi_1 = \xi_2 = \ldots = \xi_{2m} $$

and

$$ \xi_{2m} = \alpha_{2m}{}^2\xi_1 + \alpha_{2m-1}{}^2\xi_2 + \ldots + \alpha_1{}^2\xi_{2m} $$

so that $f(1)^2\xi_1 = 0$, and the ξ_i are 0. This is a contradiction, and so $X + {}^tX$ is non-singular.

Let α be a root of $f(X)$. Then $F(\alpha) = GF(q^{2m})$ and A is similar (in $M_{2m}(q^{2m})$) to a diagonal matrix D with diagonal entries $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_{2m}$. If $f = \tilde{f}$ then these may be taken as $\alpha_1, \ldots, \alpha_m, \alpha_1{}^{-1}, \ldots, \alpha_m{}^{-1}$ while if $f \neq \tilde{f}$ then $\alpha_i \neq \alpha_j{}^{-1}$ for all i and j. The dimension of $T(D, q^{2m})$ over $F(\alpha)$ is the same as the dimension of $T(A, q)$ over F. Matrices $X \in T(D, q^{2m})$ satisfy

$$ DXD \equiv X \bmod K_{2m}(q^{2m}). $$

If $X = (\xi_{ij})$, then $\alpha_i\alpha_j\xi_{ij} = \xi_{ij}$ where $\alpha_k = \alpha_{k-m}{}^{-1}$ if $k > m$ and $f = \tilde{f}$, and $\alpha_i\alpha_j \neq 1$ for all i, j if $f \neq \tilde{f}$. If $f = \tilde{f}$, $\xi_{ij} = 0$ unless $j - i = m$, and these may be chosen arbitrarily, while if $f \neq \tilde{f}$, $\xi_{ij} = 0$ for all i, j. Hence

$$ \dim_{F(\alpha)} T(D; q^{2m}) = \dim_F T(A; q) = \begin{cases} m & \text{if } f = \tilde{f} \\ 0 & \text{if } f \neq \tilde{f}. \end{cases} $$

THEOREM 14. *Let (V, θ) be a universal F-representation for a monic irreducible polynomial $f(X)$ of degree k over the field $F = GF(q)$. If $f \neq \tilde{f}$ then $\dim(V_1) = 0$ while if $f = \tilde{f}$ then k is even, $k = 2m$, and $\dim(V_1) = m$.*

https://doi.org/10.4153/CJM-1977-037-8 Published online by Cambridge University Press

Proof. If k is odd then $f \neq \tilde{f}$ and $\dim(V_1) = 0$ by Propositions 7 and 8. Assume, then, that k is even. If $V_1 \neq 0$, then let ψ: $V_1 \to F$ be a non-zero linear form. Then $\psi \circ \phi_V'$ is an alternating bilinear form which is invariant under θ_0. Theorem 10 implies $f = \tilde{f}$, and $\dim(V_1) \leqq m$.

Take $V_0 = F^{2m}$, considered as column vectors. We choose a matrix $A \in M_{2m}(q), A = \theta_0$, having characteristic polynomial $f(X)$. We take $V_1 = K(A, q)^*$ if q is odd, and $V_1 = T(A, q)^*$ if $q = 2^n$, where * denotes the dual. We define a bilinear map ϕ: $V_0 \times V_0 \to V_1$ as follows: $\phi(x, y)$ is the linear function on V_1 defined by

$$\phi(x, y)(X) = {}^t xXy \in F.$$

Using this ϕ we define the F-group $V = V_0 \times V_1$.

If q is odd we define $\theta(x, g) = (Ax, g)$. It is easy to check that $\theta \in \mathrm{Aut}_0(V; F)$.

If $q = 2^n$ we must check that the form $\phi(A(x), A(y)) - \phi(x, y)$ is symmetric. This is equivalent to the claim that ϕ' is A-invariant. This follows from

$$\begin{aligned}\phi'(Ax, Ay)(X) = {}^t x {}^t AXAy - {}^t y {}^t AXAx &= {}^t x {}^t A(X + {}^t X)Ay \\ &= {}^t x(X + {}^t X)y = \phi'(x, y)(X).\end{aligned}$$

We also claim that the form $\phi(A(x), A(y)) - \phi(x, y)$ is alternating. This follows from

$$(\phi(Ax, Ax) - \phi(x, x))(X) = {}^t x {}^t AXAx - x {}^t Xx = 0$$

because ${}^t AXA - X$ is alternating.

Thus there is a quadratic map θ_{01}: $V_0 \to V_1$ satisfying $\theta_{01}(x + y) - \theta_{01}(x) - \theta_{01}(y) = \phi(A(x), A(y)) - \phi(x, y)$ and we define θ: $V \to V$ by

$$\theta(x, g) = (Ax, g + \theta_{01}(x)).$$

By Lemma 6, $\theta \in \mathrm{Aut}_0(V; F)$.

We claim that V is a special F-group. It is enough to show that

$$\phi'(x, y)(X) = 0 \text{ for all } x, y \in V_0 \Rightarrow X = 0.$$

But

$$\phi'(x, y)(X) = {}^t x {}^t AXAy - {}^t y {}^t AXAx = {}^t x {}^t A(X - {}^t X)Ay = 0$$

for all x, y implies $X = {}^t X$. But if q is odd, X is skew-symmetric and we have $X = 0$. If $q = 2^n$, and $X = {}^t X$ then, since X is triangular, X must be diagonal. By Theorem 13, this cannot happen unless $X = 0$.

We require as well that θ have p' order. If it does not, then we replace θ with an appropriate power of θ, as in the proof of Theorem 9.

Clearly (V, θ) is the universal F-group for $f(X)$ which we require, since $\dim(V_1) = m$ and, by Theorem 12, $\dim(V_1) \leqq m$.

THEOREM 15. *If $f(X)$ and $g(X)$ are irreducible polynomials of degree $2m$ over F, satisfying $f = \tilde{f}$ and $g = \tilde{g}$, and if (V, θ) and (W, ω) are the universal F-representations of f and g respectively, then V and W are F-isomorphic.*

https://doi.org/10.4153/CJM-1977-037-8 Published online by Cambridge University Press

Proof. Choose $A \in M_{2m}(q)$ having characteristic polynomial $f(X)$. Since A is irreducible, its centralizer in $M_{2m}(q)$ is $F[A]$. It is clear that $F[A]$ is a finite field with q^{2m} elements. We may assume without loss that $f(X)$ is such that A has order $q^m + 1$. By the proof of Lemma 11, this can be done. There is an element B in $F[A]$ whose minimal polynomial over F is $g(X)$. It follows that B is irreducible.

Suppose now that q is odd. We claim that

$$K(A; q) \subset K(B; q).$$

By [**7**, Satz 9.23, p. 228] and the fact that the characteristic polynomial of B satisfies $g = \tilde{g}$ so that B is conjugate to an element of $\mathrm{Sp}(2m, q)$, $B^{q^m+1} = 1$ and so $B = A^s$ for some s. It is now clear that

$$K(A; q) \subset K(B; q).$$

Similarly, if $q = 2^n$.

$$T(A; q) \subset T(B; q).$$

By Theorems 10 and 13 these spaces have the same dimension and so $K(A; q) = K(B; q)$ if q is odd, and $T(A; q) = T(B; q)$ if $q = 2^n$.

It is clear from the construction of the universal F-representation in Theorem 14 that V and W are F-isomorphic.

5. An open question. Let $V = V(2m, q)$ be the non-degenerate $F = GF(q)$-group with $\dim V_0 = 2m$, $\dim V_1 = m$ such that there exists $\theta \in \mathrm{Aut}_0(V; F)$ which induces an F-irreducible linear automorphism θ_0 in V_0. (We have seen in the previous section that such a group is unique up to F-isomorphism.) Recall that $V(2m, q)$ is a non-degenerate F-group.

Question 1. If W is a non-degenerate $GF(q)$-group, q odd, $\dim W_0 = 2m$ is it true that W is an F-quotient of $V(2m, q)$?

This question is equivalent to the following question about matrices:

Question 2. Let L be a subspace of $K_{2m}(q)$, q odd, such that if $X \neq 0$, $X \in L$ then X is non-singular. Is it true that there exists $A \in M_{2m}(q)$ having irreducible characteristic polynomial and satisfying ${}^tAXA = X$ for all $X \in L$?

We conjecture that the answers are affirmative.

It is interesting to remark that if $V = V(2m, 2)$ then the quadratic forms $\psi \circ Q_V$, where $Q_V(x) = \phi_V(x, x)$ and $\psi: V_1 \to GF(2)$ is any non-zero linear form, are all of (-1)-type (see [**7**, p. 248]).

References

1. J. F. Adams, Peter D. Lax and Ralph S. Phillips, *On matrices whose real linear combinations are non-singular*, Proc. Amer. Math. Soc. *16* (1965), 318–322, and a *Correction* to this in the same journal *17* (1966), 945–947.

https://doi.org/10.4153/CJM-1977-037-8 Published online by Cambridge University Press

2. Y.-H. Au-Yeung, *On matrices whose non-trivial real linear combinations are non-singular* Proc. Amer. Math. Soc. *29* (1971), 17–22.
3. N. Bourbaki, *Algèbre*, Chap. 9 (Hermann, Paris 1959).
4. C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras* (Interscience Publishers, New York 1966).
5. J. Dieudonné, *La géometrie des groupes classiques* (Springer-Verlag, Berlin 1963).
6. D. Gorenstein, *Finite groups* (Harper and Row, New York 1968).
7. B. Huppert, *Endliche Gruppen I* (Springer-Verlag, New York 1967).
8. L. A. Nazarova and A. V. Roiter, *Finitely generated modules over a dyad of two local Dedekind rings, and finite groups with an abelian normal divisor of index p*. Math. USSR-Izvestija *3* (1969), 65–86.
9. J-P. Serre, *Cours d'arithmétique* (Presses Universitaires de France, Paris 1970).

University of Waterloo,
Waterloo, Ontario

https://doi.org/10.4153/CJM-1977-037-8 Published online by Cambridge University Press