SUZUKI 2-GROUPS

BY
Graham Higman

1. Introduction

In this paper we shall determine all groups G of order a power of 2 which possess automorphisms ξ that permute their involutions cyclically. The determination is complete, except that we do not exclude the possibility that two or more of the groups that we list may be isomorphic. The investigation is perhaps not without interest simply as an example of the use of linear methods in p-group theory; but the main motivation for it is that some result along these lines is needed by Suzuki in his classification [4] of ZT-groups. It is a pleasure to acknowledge that this paper is, in a direct way, a fruit of the special year in Group Theory organized by the Department of Mathematics at the University of Chicago.[1]

A 2-group with only one involution, that is, a cyclic or generalised quaternion group obviously has the property under discussion; and an abelian group has it if and only if it is a direct product of cyclic 2-groups all of the same order. It is convenient to exclude these cases from the beginning, and define a *Suzuki 2-group* as a non-abelian 2-group with more than one involution, having a cyclic group of automorphisms which permutes its involutions transitively.

Evidently, the involutions of a Suzuki 2-group G all belong to its center, and so constitute, with the identity, an elementary abelian subgroup $\Omega_1(G)$ of order $q = 2^n, n > 1$. We shall show that $\Omega_1(G) = Z(G) = \Phi(G) = G'$, so that G is of exponent 4 and class 2. The automorphism ξ which permutes cyclically the $q - 1$ involutions evidently has order divisible by $q - 1$. We shall show that ξ can be taken to have order precisely $q - 1$, and so to be regular. The order of G is either q^2 or q^3.

In many ways, it would be more satisfactory to impose on G the simpler, weaker condition that the involutions of G are permuted transitively by the full automorphism group of G. Possibly such a relaxation would not bring in any large class of new groups; but the condition seems to be very hard to handle. However, a little of our argument extends to the general case, and this part has been stated for that case.

The methods used are similar to those involving the associated Lie ring (cf. e.g. [2]), but we shall not construct this ring explicitly. The setup, which we shall presuppose, is as follows. If H is a subgroup of the 2-group G, and K a normal subgroup of H with elementary abelian factor group H/K,

Received October 3, 1961.

[1] My part in which was supported by grants from the National Science Foundation and the Esso Education Foundation.

then H/K can be considered as a vector space over the field $\mathfrak{F}_2$ of two elements. If H_i/K_i, $i = 1, 2, 3$, are three such spaces, with $[H_1, H_2] \subset H_3$, and $[H_1, K_2]$, $[H_2, K_1]$, $[H_1, H_2, H_1]$, and $[H_1, H_2, H_2]$ all contained in K_3, then the map $(h_1, h_2) \rightarrow [h_1, h_2] = h_1^{-1}h_2^{-1}h_1 h_2$ induces a bilinear map from the spaces H_1/K_1, H_2/K_2 to H_3/K_3. If $H_1 = H_2$, the map is skew-symmetric; and, under conditions which we shall not specify precisely, triple products formed in this way satisfy the Jacobi identity. In particular, for $i \geqq 1$, let $L_i = H_i/H_i^2 H_{i+1}$, where $H_1, H_2, \cdots$ is the lower central series of G; and for any vector space V let $\mathfrak{L}^i(V)$ be the component homogeneous of degree i in the free Lie algebra generated by V. Then there is a linear map, induced by commutation, from $\mathfrak{L}^i(L_1)$ to L_i. Because all these maps are linear, they have natural extensions when the base field is extended. Moreover, if X is a group of automorphisms of G, and the subgroups involved admit X, then the vector spaces are all X-modules, and the linear mappings are module homomorphisms.

Naturally, besides the commutator structure, we have also to consider the power structure of G. Let H_i/K_i $(i = 1, 2)$ be elementary factors in G, such that $H_1^2 \subset H_2$, $K_1^2 \subset K_2$, and $[H_1, K_1] \subset K_2$. Then the map $h \rightarrow h^2$ induces a map $v \rightarrow v^{(2)}$ of H_1/K_1 into H_2/K_2. The identity $g^{-1}h^{-1}gh = g^{-2}(gh^{-1})^2h^2$ shows that $[H_1, H_1] \subset H_2$, so that the product $[u, v]$ is defined from H_1/K_1 to H_2/K_2, and furthermore (remembering that the characteristic is 2) that

$$(u + v)^{(2)} = u^{(2)} + v^{(2)} + [u, v].$$

Thus $v \rightarrow v^{(2)}$ is not in general a linear map, so there need be no natural extension of it if the base field is extended. The mapping is linear if $[H_1, H_1] \subset K_2$, in particular, if H_1 is abelian. In any case, if all the groups involved admit the automorphism group X, then for ξ in X, $(u\xi)^{(2)} = u^{(2)}\xi$.

2. Detailed statement of results

As we have said, a Suzuki 2-group G has a central and elementary abelian Frattini subgroup $\Phi(G) = \Omega_1(G)$. It is easy to see that in this case the isomorphism class of G is determined by the vector spaces $G/\Phi(G)$ and $\Phi(G)$, together with the map $v \rightarrow v^{(2)}$ of $G/\Phi(G)$ onto $\Phi(G)$. Indeed, if $g_1, \cdots, g_m$ are independent generators of G, and $h_1, \cdots, h_n$ of $\Phi(G)$, an element of G can be written uniquely in the form $g_1^{\alpha_1} \cdots g_m^{\alpha_m} h_1^{\beta_1} \cdots h_n^{\beta_n}$, where the α_i and β_j are 0 or 1. Since the h_j are of order 2 and central, to multiply two such expressions we need only to know g_i^2 for $i = 1, 2, \cdots, m$, and $[g_i, g_j]$ for $1 \leqq i < j \leqq m$, both of which the map $v \rightarrow v^{(2)}$ tells us. Moreover, it is clear that any choice of g_i^2 and $[g_i, g_j]$ gives a group, from which it follows that in general the only conditions that the map $v \rightarrow v^{(2)}$ must satisfy are that $(u + v)^{(2)} + u^{(2)} + v^{(2)}$ is bilinear, and that the images $v^{(2)}$ span the whole of $\Phi(G)$. Similar considerations show that if ρ, σ are linear maps of $G/\Phi(G)$ and $\Phi(G)$ onto themselves such that $(u\rho)^{(2)} = u^{(2)}\sigma$, then there is an automorphism of G which induces the map ρ on $G/\Phi(G)$ and the map σ on $\Phi(G)$.

In the case when G is a Suzuki 2-group, $\Phi(G)$ contains $q = 2^n$ elements, and can be identified with the additive group of the field $\mathfrak{F}_q$ of q elements. We use ζ for the general element of $\mathfrak{F}_q$, when it is identified with $\Phi(G)$. When G has order q^2, $G/\Phi(G)$ can also be identified with $\mathfrak{F}_q$. To distinguish $G/\Phi(G)$ from $\Phi(G)$, elements of $\mathfrak{F}_q$ will be enclosed in brackets when they represent elements of $G/\Phi(G)$, and the general element will be written (α). In the cases when G is of order q^3, elements of $G/\Phi(G)$ will be identified with pairs (α, β) of elements of $\mathfrak{F}_q$. The cases that arise are given in the following table.

Column I	Column II	Column III
$A(n, \theta)$	$(\alpha)^{(2)} = \alpha^{\theta+1}$	$\theta \neq 1$
$B(n, \theta, \varepsilon)$	$(\alpha, \beta)^{(2)} = \alpha^{\theta+1} + \varepsilon\alpha\beta^{\theta} + \beta^{\theta+1}$	$\varepsilon \neq \rho^{-1} + \rho^{\theta}$
$C(n, \varepsilon)$	$(\alpha, \beta)^{(2)} = \alpha^{\theta+1} + \varepsilon\alpha^{1/2}\beta^{2\theta} + \beta^{2}$	$2\theta^2 = 1, \quad \varepsilon \neq \rho^{-1} + \rho^{2\theta+1}$
$D(n, \theta, \varepsilon)$	$(\alpha, \beta)^{(2)} = \alpha^{\theta+1} + \varepsilon\alpha^{\theta 3}\beta^{\theta} + \beta^{\theta 2+1}$	$\theta^5 = 1, \quad \theta \neq 1,$ $\varepsilon \neq \rho^{-1} + \rho^{\theta 4+\theta-1}$

Column IV

$(\alpha) \to (\lambda\alpha),$	$\zeta \to \lambda^{\theta+1}\zeta$
$(\alpha, \beta) \to (\lambda\alpha, \lambda\beta),$	$\zeta \to \lambda^{\theta+1}\zeta$
$(\alpha, \beta) \to (\lambda\alpha, \lambda^{(\theta+1)/2}\beta),$	$\zeta \to \lambda^{\theta+1}\zeta$
$(\alpha, \beta) \to (\lambda\alpha, \lambda^{\theta 4-\theta 2+1}\beta),$	$\zeta \to \lambda^{\theta+1}\zeta$

Column V

$(\alpha, \zeta)(\gamma, \eta) = (\alpha + \gamma, \zeta + \eta + \alpha\gamma^{\theta})$
$(\alpha, \beta, \zeta)(\gamma, \delta, \eta) = (\alpha + \gamma, \beta + \delta, \zeta + \eta + \alpha\gamma^{\theta} + \varepsilon\alpha\delta^{\theta} + \beta\delta^{\theta})$
$(\alpha, \beta, \zeta)(\gamma, \delta, \eta) = (\alpha + \gamma, \beta + \delta, \zeta + \eta + \alpha\gamma^{\theta} + \varepsilon\alpha^{1/2}\delta^{2\theta} + \beta\delta)$
$(\alpha, \beta, \zeta)(\gamma, \delta, \eta) = (\alpha + \gamma, \beta + \delta, \zeta + \eta + \alpha\gamma^{\theta} + \varepsilon\alpha^{\theta 3}\delta^{\theta} + \beta\delta^{\theta 2})$

In this table, the first column contains a name for the group described. The second column gives the map induced by squaring; here θ is an automorphism of $\mathfrak{F}_q$ of odd order, which is subject to the conditions, if any, stated in the third column; and ε is a nonzero element of $\mathfrak{F}_q$, which is subject to the conditions stated in the third column. ($\varepsilon \neq \rho^{-1} + \rho^{\theta}$, for instance, means that there is no element ρ of $\mathfrak{F}_q$ for which $\varepsilon = \rho^{-1} + \rho^{\theta}$.) Groups $A(n, \theta)$ will exist whenever $\mathfrak{F}_q$ has a nontrivial automorphism of odd order, that is, whenever n is not a power of 2. Groups $B(n, \theta, \varepsilon)$ exist for all $n \geqq 2$, since here, and in the remaining cases, a counting argument shows that ε can always be chosen to meet the requirements. Groups $C(n, \varepsilon)$ exist whenever an automorphism θ exists satisfying $2\theta^2 = 1$, that is, for odd n. θ is then unique, which is why it is not specified in the symbol naming the group. Groups $D(n, \theta, \varepsilon)$ exist whenever n is divisible by 5.

It is easy to check that, with the above specifications, $(u + v)^{(2)} + u^{(2)} + v^{(2)}$ is bilinear and not identically zero, so that we have in each case genuinely defined a group, and that group is not abelian. To verify that these are indeed Suzuki 2-groups, we use the fourth column of the table. This specifies linear transformations of $G/\Phi(G)$ and $\Phi(G)$ onto themselves, which commute with the square map, and so are induced by an automorphism of G. We note that, since θ is of odd order, the map $\lambda \to \lambda^{\theta+1}$ is invertible. For if $\theta^k = 1$, k odd, there is a map ψ such that $(\theta + 1)\psi = \theta^k + 1 = 2$, and $\lambda \to \lambda^2$ is certainly invertible. Thus if λ is a generator of the cyclic group $\mathfrak{F}_q^*$, so is $\lambda^{\theta+1}$, and the automorphism in question permutes cyclically the nonzero elements of $\Phi(G)$. Thus to verify that G is a Suzuki group, we only have to show that $\Phi(G)$ contains all involutions, that is, that $(u)^{(2)} = 0$ implies $u = 0$. We leave this verification, and the verification that the maps in the fourth column really do commute with the square mapping, to the reader.

All these groups have rather obvious representations as groups of triangular matrices with elements in $\mathfrak{F}_q$, the relevant automorphisms being obtained by transformation by diagonal matrices. For instance, the matrices

$$\begin{bmatrix} 1 & \alpha & \zeta \\ & 1 & \alpha^\theta \\ & & 1 \end{bmatrix}$$

form a group isomorphic to $A(n, \theta)$, the relevant automorphism being induced by

$$\begin{bmatrix} 1 & & \\ & \lambda & \\ & & \lambda^{1+\theta} \end{bmatrix}.$$

In this way, we can obtain a description of the elements of $A(n, \theta)$ by pairs (α, ζ) of elements of $\mathfrak{F}_q$, and of elements of the other groups by triples (α, β, ζ), with the multiplication shown in the last column of the table.

Our main theorem is

THEOREM 1. *Every Suzuki 2-group is isomorphic to one of the groups $A(n, \theta)$, $B(n, \theta, \varepsilon)$, $C(n, \varepsilon)$, and $D(n, \theta, \varepsilon)$.*

It is not hard to see that $A(n, \theta)$ is isomorphic to $A(n, \theta^{-1})$, $B(n, \theta, \varepsilon)$ to $B(n, \theta^{-1}, \varepsilon)$, and $D(n, \theta, \varepsilon)$ to $D(n, \theta^i, \varepsilon)$ for $i = 2, 3, 4$. We shall show that $A(n, \varphi)$ is not isomorphic to $A(n, \theta)$ unless $\varphi = \theta^{\pm 1}$, but we shall not attempt to determine when groups of the other three series are isomorphic.

3. Involutions equivalent under the full automorphism group

In this section G is a non-abelian 2-group with more than one involution, with an automorphism group X which permutes its involutions transitively.

LEMMA 1. *An abelian X-subgroup A of G is a direct product of cyclic groups of the same order 2^e. The only X-subgroups of A are the groups A^{2^s}, $s = 0, 1, \cdots, e$.*

If A were not a direct product of cyclic groups of the same order, it would contain involutions of different heights, whereas the restriction of X to A permutes the involutions transitively. If 2^e is the exponent of A, the subgroup $A^{2^{e-1}}$ of involutions is clearly an irreducible X-module; and since in an abelian group the power mappings are linear, so is $A^{2^{s-1}}/A^{2^s}$, for all s. The second part of the lemma follows immediately.

In what follows we shall be concerned with an abelian normal X-subgroup A of G, and a normal X-subgroup C which covers A, in the lattice of normal X-subgroups. Then $A \geqq \Phi(C) \geqq \Phi(A)$; and by Lemma 1, there are no X-subgroups strictly between A and $\Phi(A)$. Thus either $\Phi(C) = A$ or $\Phi(C) = \Phi(A)$. The first of these possibilities has to be deferred to a later section; but the second can be dealt with under our present assumptions.

LEMMA 2. *If A is an abelian normal X-subgroup of G, which is not* 1, *then for no element u of G not in A is both $u^2 \in A^2$ and $[u, A] \subset A^4$.*

Assume that both $[u, A] \subset A^4$ and $u^2 \in A^2$. By the first of these statements, there is an automorphism α of A such that, for a in A, $u^{-1}au = a^{1+4\alpha}$, and hence $(au^{-1})^2 = a^{2+4\alpha}u^{-2}$. Because A is a 2-group, the endomorphism $1 + 2\alpha$ is invertible, so that a can be chosen so that $a^{2+4\alpha}$ is any element of A^2, in particular u^2. Then $(au^{-1})^2 = 1$. But A contains all the involutions in G, so that au^{-1}, and therefore u, belongs to A.

LEMMA 3. *Let A be a normal abelian X-subgroup of G, and C a normal X-subgroup covering A. If $\Phi(C) = \Phi(A)$, then A has exponent at most* 4.

By assumption, $[C, A]$ is contained in $\Phi(A) = A^2$, so that for u in C we have $u^{-1}au = a^{1-2\eta}$, where $\eta = \eta(u)$ is an endomorphism of A. Then

$$u^{-2}au^2 = a^{(1-2\eta)^2} = a^{1-4\eta+4\eta^2}.$$

Since $u^2 \in A$, and A is abelian, we have $4(\eta - \eta^2) = 0$. Let $\bar{\eta} = \bar{\eta}(u)$ be the linear transformation of A/A^2 induced by η. Then if A has exponent greater than 4, we must have $\bar{\eta} = \bar{\eta}^2$, so that $\bar{\eta}$ is idempotent.

If v is a second element of C, we have

$$1 - 2\eta(uv) = (1 - 2\eta(u))(1 - 2\eta(v)),$$

whence $\bar{\eta}(uv) = \bar{\eta}(u) + \bar{\eta}(v)$. Since each of $\bar{\eta}(uv)$, $\bar{\eta}(u)$, and $\bar{\eta}(v)$ is idempotent, this gives $\bar{\eta}(u)\bar{\eta}(v) + \bar{\eta}(v)\bar{\eta}(u) = 0$, which, the characteristic being 2, says that $\bar{\eta}(u)$ and $\bar{\eta}(v)$ commute. Thus the transformations $\bar{\eta}(u)$ for u in C form a set of commuting idempotents, and they have therefore a common eigenvector. But X permutes the nonzero vectors of A/A^2 transitively, and permutes the transformations $\bar{\eta}(u)$ among themselves; so that every vector in A/A^2 is an eigenvector for all $\bar{\eta}(u)$; that is, each $\bar{\eta}(u)$ is either 0 or 1.

As we have seen, $\bar{\eta}(uv) = \bar{\eta}(u) + \bar{\eta}(v)$, so that $\bar{\eta}$ is a homomorphism of C into the additive group of the endomorphism ring of A/A^2. If u belongs to the kernel of $\bar{\eta}$, $[u, A] \subset A^2$; and since we are assuming $\Phi(C) = \Phi(A)$, we also have $u^2 \in A^2$. By Lemma 2, u belongs to A. That is, the kernel of $\bar{\eta}$ is A. Since its image has order 2, C/A has order 2. Let u belong to C but not to A. Then $\eta = \eta(u)$ does not depend on the choice of u, and so commutes with the elements of X. For a in A, $(ua)^2 = u^2a^{2-2\eta}$. If $u^2 \in A^{2-2\eta}$, we can choose a so that $(ua)^2 = 1$, whereas all involutions of G are in A. If $u^2 \notin A^{2-2\eta}$, then B, the group generated by the squares of elements of C not in A, is cyclic over $A^{2-2\eta}$. B obviously admits X, and so does $A^{2-2\eta}$, since η commutes with the elements of X. Thus we have a contradiction to Lemma 1, and the theorem is proved.

4. Some auxiliary lemmas

In this section we prove some lemmas about a non-abelian 2-group H with an automorphism ξ of odd order satisfying the following conditions. Let $H = H_1, H_2, H_3, \cdots$ be the lower central series of H, and put

$$L_i = H_i/H_i^2 H_{i+1}.$$

Then we assume that ξ transforms L_1 irreducibly, and permutes transitively the vectors of L_2. We shall assume also that L_2 has $q = 2^n$ elements, $n \geqq 2$. Suppose that L_1 has order 2^m. If λ is an eigenvalue of the transformation of L_1 induced by ξ, then L_1 is isomorphic to $\mathfrak{K} = \mathfrak{F}_2(\lambda)$, the field of 2^m elements, because it is irreducible. The eigenvalues of ξ on L_1 are the conjugates $\lambda_i = \lambda^{2^i}, i = 0, 1, \cdots, m-1$. In the vector space $L_1 \otimes \mathfrak{K}$ obtained from L_1 by extending the base field to $\mathfrak{K}$, we can choose a basis $u_0, u_1, \cdots, u_{m-1}$, such that $u_i\xi = \lambda^{2^i}u_i$; and we can furthermore suppose that $u_0, u_1, \cdots, u_{m-1}$ are conjugate over $\mathfrak{F}_2$, so that the elements of L_1 are precisely the elements $\sum \alpha^{2^i}u_i$, for α in $\mathfrak{K}$. We shall have frequent occasion to choose a basis in this sort of way in what follows; we shall describe the process as "choosing a conjugate basis for L_1 adapted to ξ." If $u_0, \cdots, u_{m-1}$ is a conjugate basis for L_1 adapted to ξ, the products $[u_{a_1}, u_{a_2}, \cdots, u_{a_i}]$ span $L_i \otimes \mathfrak{K}$, $i = 2, 3, \cdots$.

LEMMA 4 (Gorenstein-Thompson, cf. Gorenstein [1]). *L_1 and L_2 are not ξ-isomorphic.*

Assume the contrary. Then $m = n$, and λ is a primitive $(2^n - 1)$-st root of unity. $L_2 \otimes \mathfrak{K}$ is spanned by the elements $[u_i, u_j]$, $0 \leqq i < j \leqq n-1$, and $[u_i, u_j]\xi = \lambda^{2^i+2^j}[u_i, u_j]$. Thus the eigenvalues of ξ on L_2 are found among the numbers $\lambda^{2^i+2^j}$, $0 \leqq i < j \leqq n - 1$. If L_1 and L_2 are ξ-isomorphic, λ is among these eigenvalues, so that for some i, j in $0 \leqq i < j \leqq n - 1$, $\lambda = \lambda^{2^i+2^j}$. Since $2^i + 2^j - 1 < 2^n - 1$, this contradicts the fact that λ is a primitive $(2^n - 1)$-st root of unity.

COROLLARY. *If $\mathfrak{K}$ is any extension field of $\mathfrak{F}_2$, $L_2 \otimes \mathfrak{K}$ has no ξ-$\mathfrak{F}_2$-subspace ξ-isomorphic to L_1.*

If it had, the transformations induced by ξ on L_1 and L_2 would have a common eigenvalue, and L_1 and L_2, being both irreducible, would be isomorphic.

LEMMA 5. *If $H^2 = H_2$, the map of L_1 into L_2 induced by squaring is*

$$\left(\sum \alpha^{2^i} u_i\right)^{(2)} = \sum\nolimits_{i<j} \alpha^{2^i+2^j}[u_i, u_j].$$

The square map satisfies

$$(u\xi)^{(2)} = u^{(2)}\xi,$$

$$(u + v)^{(2)} = u^{(2)} + v^{(2)} + [u, v],$$

and these equations characterize it among mappings of L_1 into $L_2 \otimes \mathfrak{K}$, for any extension field $\mathfrak{K}$ of $\mathfrak{F}_2$. For if the map $u \to u^*$ satisfies similar conditions, by subtraction the map $u \to u^{(2)} - u^*$ is a ξ-homomorphism. Since L_1 is irreducible, it is either an isomorphism or the zero map, and it cannot be an isomorphism by the corollary to Lemma 4. Thus $u^* = u^{(2)}$ as required. That is, it is only necessary to verify that the proposed map has these properties, which is straightforward.

LEMMA 6. *If $H^2 = H_2$, then L_3 is not ξ-isomorphic to L_2.*

Assume that it is. The first step is to show that the order of ξ on L_1 is the same as its order on L_2 or L_3. Suppose indeed that η is a power of ξ which induces the identity on L_2 and on L_3. Then for x in L_1 and y in L_2, we have

$$[x, y] = [x, y]\eta = [x\eta, y\eta] = [x\eta, y],$$

so that $[x(1 - \eta), y] = 0$, that is, $[L_1(1 - \eta), L_2] = 0$. But $L_1(1 - \eta)$ is a ξ-subspace of L_1, and cannot be the whole of L_1, since that would imply $L_3 = [L_1, L_2] = 0$, which is not so. Thus $L_1(1 - \eta) = 0$, so that η induces the identity on L_1 also, as asserted. Thus we again have $m = n$, and λ a primitive $(2^n - 1)$-st root of unity. Since L_1 and L_2 both have order 2^n, n is at least 3. We may furthermore assume that n is odd, since otherwise $2^n - 1$ is divisible by 3, and a suitable power of ξ induces a fixed-point-free automorphism of order 3 in the group H/H_4 of class 3, which is impossible (Neumann [3]).

The eigenvalues of ξ on L_2 are found among the numbers $\lambda^{2^i+2^j}$, $0 \leqq i < j \leqq n - 1$, and since L_2 is irreducible, they form a single conjugate class over $\mathfrak{F}_2$, that is, they are the numbers $\lambda^{2^s(1+2^r)}$ for some fixed r, and for

$s = 0, 1, \cdots, n-1$. It follows that $[u_i, u_j] = 0$ unless $i - j \equiv \pm r \pmod{n}$.

$L_3 \otimes \mathfrak{K}$ is spanned by the products $[[u_i, u_j], u_k]$, and

$$[[u_i, u_j], u_k]\xi = \lambda^{2^i+2^j+2^k}[[u_i, u_j], u_k].$$

If i, j, k are distinct numbers between 0 and $n - 1$, $2^i + 2^j + 2^k$ is not congruent (mod $2^n - 1$) to any number $2^a + 2^b$, and so $\lambda^{2^i+2^j+2^k}$ is not an eigenvalue of ξ on L_2, and hence not on the isomorphic space L_3 either. It follows that $[[u_i, u_j], u_k] = 0$. There remain products $[[u_i, u_j], u_j]$. Some of these, also, are eigenvectors for multipliers which are not eigenvalues, and so are zero. But the possible eigenvalue $\lambda^{2^i+2^j}$ will arise, in general, from two such products, $[[u_i, u_{j-1}], u_{j-1}]$ and $[[u_j, u_{i-1}], u_{i-1}]$, where if necessary subscripts are taken mod n, though there will be only one such product if $i - j = \pm 1$. If there are two products, at most one of them is nonzero. For $[u_a, u_b] \neq 0$, $0 \leqq a < b \leqq n - 1$, implies $b - a = r$ or $b - a = n - r$. Thus if $j > i$, $[[u_i, u_{j-1}], u_{j-1}]$ and $[[u_j, u_{i-1}], u_{i-1}]$ are both nonzero only if $j - i - 1$ and $j - i + 1$ are, in either order, r and $n - r$. But this would imply $n = 2(j - i)$, whereas n is odd.

We use finally the fact that $[u^{(2)}, u] = 0$ for any u in L_1. Taking $u = \sum u_i$, and using Lemma 5, we obtain

$$\sum_{i<j} \sum_k [[u_i, u_j], u_k] = 0.$$

Since eigenspaces belonging to different eigenvalues are independent, we can pick out of this sum the terms belonging to the eigenvalue $\lambda^{2^i+2^j}$, and equate them to zero. In case $j = i \pm 1$, there is only one such term, and this must therefore be zero. In general, we obtain

$$[[u_i, u_{j-1}], u_{j-1}] + [[u_j, u_{i-1}], u_{i-1}] = 0,$$

and since we have already seen that at least one of these products is zero, both must be.

Thus the assumption that L_3 is isomorphic to L_2 leads to the conclusion that $L_3 = 0$, a contradiction.

5. Application to Suzuki 2-groups

If G is a Suzuki 2-group, and A is an abelian normal ξ-subgroup of G, then as H of the previous section we may take any non-abelian normal ξ-subgroup C of G covering A.

LEMMA 7. *Let A be a normal abelian ξ-subgroup of G, and C a normal ξ-subgroup which covers A. If $A = \Phi(C)$, but $C' \leqq A^2$, then C is abelian.*

The ξ-composition factors of C in A are all isomorphic under a power mapping, and so are those in C/C', since $C/\Phi(C)$ is irreducible. Under the hypotheses of the lemma, these sets overlap, so that all ξ-composition factors of C are isomorphic. If C is non-abelian, this contradicts Lemma 4.

Lemma 8. *Let A be a normal abelian ξ-subgroup of G, and C a normal ξ-subgroup which covers A. If $C' = A$, then A has exponent at most* 2.

Suppose not. Since C/C' has exponent 2, the same is true of all the factors of the lower central series of C. By Lemma 1, the lower central series can only be $C, A, A^2, A^4, \cdots$. But then the factors $L_2 = A/A^2$ and $L_3 = A^2/A^4$ are isomorphic under a power mapping, which contradicts Lemma 6.

Lemma 9. *If A is a maximal normal abelian ξ-subgroup of G, then A has exponent at most* 4, *and contains* $\Phi(G)$.

Since G is non-abelian, there exists a normal ξ-subgroup C which covers A. The hypotheses of Lemmas 3, 7, and 8 together include all possibilities, so the conclusion of one or other must apply. It cannot be that C is abelian, since A is maximal, so A has exponent at most 4.

If A does not contain $\Phi(G)$, we can take $C = AB$, where $B \subset \Phi(G)$. By Lemma 1, the proper ξ-subgroup $[G, A]$ of A is contained in A^2. Thus $[g, A] \subset A^2$, whence $[g^2, A] \subset A^4$. Since the squares generate $\Phi(G)$, we have $[b, A] \subset A^4$ for any b in $\Phi(G)$, in particular, for b in B but not in A. By Lemma 2, $b^2 \notin A^2$, so that $\Phi(C) = A$. By Lemma 7, $C' < A$ implies C abelian, so that $C' = A$, and by Lemma 8, A is of exponent 2, whence $A = \Omega_1(G)$. Since A is a maximal abelian normal ξ-subgroup, it is the only nontrivial abelian normal ξ-subgroup. Thus $A = Z(G)$, and G has class 2 (since a group of greater class has two distinct nontrivial abelian terms in its lower central series). Thus G is its own second center, and since $Z(G)$ has exponent 2, so has $G/Z(G) = G/A$. That is, A contains $\Phi(G)$ after all.

6. Concluding computations

It follows immediately from Lemma 9 that G has exponent not exceeding 8 and class not exceeding 3. To obtain the precise results stated in Section 1, and the complete list of groups in Section 2, we have to resort to computation. We shall obtain the groups in order of increasing ξ-length (= length of ξ-composition series).

As always, we denote the order of $\Omega_1(G)$ by q. The order of the automorphism ξ must necessarily be divisible by $q - 1$, and it is no loss of generality to assume that its order is divisible only by primes dividing $q - 1$. In what follows we shall make this assumption. In the case of ξ-length 2, the main burden of the proof is to show that this implies that ξ has order precisely $q - 1$. We begin with a lemma that isolates the necessary field theory.

Lemma 10. *Let $\mathfrak{K}$ be a field of characteristic* 2, *$\mathfrak{L}$ a proper extension of odd degree. For any integer r and for any ε in $\mathfrak{L}$, there exists $\alpha \neq 0$ in $\mathfrak{L}$ such that the trace of $\alpha^{1+2^r}\varepsilon$ in $\mathfrak{L}$ is zero.*

We denote the trace by $\operatorname{tr}(\alpha^{1+2^r}\varepsilon)$. Let $\mathfrak{L}$ have order 2^m, and let $\mathfrak{K}$ have order 2^n, so that m is an odd multiple of n. The multiplicative group $\mathfrak{L}^*$ of $\mathfrak{L}$

is cyclic of order $2^m - 1$, so that as α runs through $\mathfrak{L}^*$, the values taken by α^{1+2^r} are the same as those taken by α^u, where u is the highest common factor $(1 + 2^r, 2^m - 1)$. Now if $(r, m) = r_0$, $(1 + 2^r, 2^m - 1)$ is 1 if m is an odd multiple of r_0, and is $1 + 2^{r_0}$ if m is an even multiple of r_0. In the first case, α^{1+2^r}, and therefore $\alpha^{1+2^r}\varepsilon$ can be any element of $\mathfrak{L}^*$, and the lemma is trivial. Thus we may suppose we are in the second case, and also that $r = r_0$; that is, we may suppose that $2r$ divides m.

Next we write $\varepsilon = \varepsilon_1 \varepsilon_2$, where the multiplicative order of ε_1 is prime to $2^r + 1$, and the multiplicative order of ε_2 is divisible only by prime factors of $2^r + 1$. Then ε_1 is of the form β^{2^r+1}, so that the set of elements $\alpha^{2^r+1}\varepsilon$ is the same as the set of elements $\alpha^{2^r+1}\varepsilon_2$. Thus we may suppose $\varepsilon = \varepsilon_2$, so that ε is a product of p^a-th roots of unity, for various primes p dividing $2^r + 1$, and exponents a. For such a prime p, a p-th root of unity belongs to the field of 2^{2r} elements, and a p^a-th root to an extension of this field of odd degree. Thus if $\mathfrak{L}_0$ is the greatest subfield of $\mathfrak{L}$ which is an extension of odd degree of the field of 2^{2r} elements, we may assume that ε belongs to $\mathfrak{L}_0$.

Let $\mathfrak{L}_{00}$ be the subfield of $\mathfrak{L}_0$ such that the degree of $\mathfrak{L}_0$ over $\mathfrak{L}_{00}$ is 2. Then $\mathfrak{L}_{00}$ is an extension of odd degree of the field of 2^r elements, so that the map $\alpha \rightarrow \alpha^{2^r}$ is an automorphism of it of odd order, and the map $\alpha \rightarrow \alpha^{2^r+1}$ restricted to it is invertible. That is, among the elements $\alpha^{2^r+1}\varepsilon$ are to be found all elements $\gamma\varepsilon$, for γ in $\mathfrak{L}_{00}$. The map $\gamma \rightarrow \mathrm{tr}(\gamma\varepsilon)$ maps $\mathfrak{L}_{00}$ into $\mathfrak{L}_0 \cap \mathfrak{K} = \mathfrak{K}_0$ say; and it is linear over $\mathfrak{L}_{00} \cap \mathfrak{K} = \mathfrak{K}_{00}$. Now the degree of $\mathfrak{L}$ over $\mathfrak{K}$ is odd, whereas its degree over $\mathfrak{L}_{00}$ is a power of 2. It follows that the degree of $\mathfrak{L}_{00}$ over $\mathfrak{K}_{00}$ is the same as the degree of $\mathfrak{L}$ over $\mathfrak{K}$, and so is at least 3. But the degree of $\mathfrak{K}_0$ over $\mathfrak{K}_{00}$ is at most 2. Hence the $\mathfrak{K}_{00}$-linear map $\gamma \rightarrow \mathrm{tr}(\gamma\varepsilon)$ must have a kernel; that is, we can choose α, even in $\mathfrak{L}_{00}$, so that $\alpha \neq 0$ but $\mathrm{tr}(\alpha^{2^r+1}\varepsilon) = 0$, as required.

LEMMA 11. *A Suzuki 2-group of ξ-length 2 is isomorphic to some $A(n, \theta)$.*

The sole composition series of G is $G > \Phi(G) > 1$. Let λ be an eigenvalue of ξ on $G/\Phi(G)$. By assumption, λ is an $a(q - 1)$-st root of unity, where primes dividing a also divide $q - 1$, and it is a corollary that $\mathfrak{L} = \mathfrak{F}_2(\lambda)$ is an extension of odd degree of $\mathfrak{K}$, the field of q elements. Let the order of $\mathfrak{L}$ be 2^m, and let $u_0, u_1, \cdots, u_m$ be a conjugate basis adapted to ξ, with $u_0\xi = \lambda u_0$. Because the products $[u_i, u_j]$ span $\Phi(G) \otimes \mathfrak{L}$, and $[u_i, u_j]$ is conjugate to $[u_0, u_{j-i}]$, there is an r such that $[u_0, u_r] \neq 0$. Then λ^{2^r+1} is an eigenvalue of ξ on $\Phi(G)$, and so is a primitive $(q - 1)$-st root of unity. We observe that it cannot happen that $m = 2r$. For then λ^{2^r+1} would belong to the field of 2^r elements, and so $\mathfrak{F}_2(\lambda)$ would be of even degree over $\mathfrak{F}_2(\lambda^{2^r+1})$.

We next show that $[u_i, u_j] = 0$ unless $i - j \equiv \pm r \pmod{m}$. Indeed, if $[u_i, u_j] \neq 0$, $\lambda^{2^i+2^j}$ is an eigenvalue of ξ on $\Phi(G)$, and so is $\lambda^{2^s(1+2^r)}$ for some s. Thus $2^s(1 + 2^r) - 2^i - 2^j$ is divisible by the order of λ, and in particular by $2^n - 1$. This implies that, perhaps after interchanging i and j, $i \equiv r + s \pmod{n}$ and $j \equiv s \pmod{n}$. Now λ^{1+2^r} is a $(2^n - 1)$-st root of unity, so that if $s \equiv t \pmod{n}$, $\lambda^{2^s(1+2^r)} = \lambda^{2^t(1+2^r)}$. Thus we may assume that in fact $i = r + s$. But then $\lambda^{2^s(1+2^r)} = \lambda^{2^i+2^j}$ gives $\lambda^{2^s} = \lambda^{2^j}$, and since λ generates the field of 2^m elements, $j \equiv s \pmod{m}$. Thus $i - j \equiv r \pmod{m}$, (possibly after interchanging i and j), as required.

It follows that a conjugate base $v_0, v_1, \cdots, v_{n-1}$ can be chosen for $\Phi(G)$ so that, for some ε in $\mathfrak{L}$, $[u_i, u_{i+r}] = \varepsilon^{2^i} v_i$, and $[u_i, u_j] = 0$, $i - j \not\equiv \pm r \pmod{m}$, where, as in what follows, subscripts on u's are taken mod m, and on v's, mod n. We are now in a position to compute the effect of the square mapping on the general element $\sum \alpha^{2^i} u_i$ of $G/\Phi(G)$, using Lemma 5. The result is

$$\begin{aligned}(\textstyle\sum \alpha^{2^i} u_i)^{(2)} &= \textstyle\sum_{0 \leqq i<j<m} \alpha^{2^i+2^j}[u_i, u_j] \\ &= \textstyle\sum_{i=0}^{m-1} \alpha^{2^i(1+2^r)}[u_i, u_{i+r}] \\ &= \textstyle\sum_{i=0}^{m-1} \alpha^{2^i(1+2^r)} \varepsilon^{2^i} v_i \\ &= \textstyle\sum_{i=0}^{n-1} \gamma^{2^i} v_i ,\end{aligned}$$

where $\gamma = \operatorname{tr}(\alpha^{1+2^r}\varepsilon)$, using the fact that $v_i = v_{i+n} = \cdots$. If $\mathfrak{L}$ is a proper extension of $\mathfrak{K}$, then by Lemma 10 we can choose $\alpha \neq 0$ in $\mathfrak{L}$ so that $\gamma = 0$; that is, we can choose $u \neq 0$ in $G/\Phi(G)$ such that $u^{(2)} = 0$. This means that there are involutions in G not in $\Phi(G)$, and G is not a Suzuki 2-group. We conclude that $\mathfrak{L} = \mathfrak{K}$, that is, that the order of ξ is exactly $q - 1$. Moreover, in this case the symbol "tr" is superfluous; and by choice of v_i, we can take $\varepsilon = 1$. The square map becomes $(\sum \alpha^{2^i} u_i)^{(2)} = \sum \alpha^{2^i(1+2^r)} v_i$. If we identify $\sum \alpha^{2^i} u_i$ with (α) and $\sum \zeta^{2^i} v_i$ with ζ, this is the square map appropriate to $A(n, \theta)$, with θ the automorphism $\alpha \to \alpha^{2^r}$. This automorphism must be of odd order, because λ^{1+2^r} must be a primitive $(q - 1)$-st root of unity. Thus G is isomorphic to some $A(n, \theta)$, as asserted.

If now G is any Suzuki 2-group, and X is a ξ-subgroup of ξ-length 2, X is either a Suzuki 2-group, in which case it is isomorphic to some $A(n, \theta)$, by Lemma 11, or it is abelian, in which case it is a direct sum of n cyclic groups of order 4. Clearly, we can unify the two cases by writing $A(n, 1)$ for this latter group; this is indeed the group that we get if we take $\theta = 1$ in the definition of $A(n, \theta)$; the only reason why the stipulation $\theta \neq 1$ was made in the definition was that Suzuki 2-groups are assumed non-abelian. Thus in any case we can choose a conjugate basis $x_0, x_1, \cdots, x_{n-1}$ for $X/\Phi(X)$, adapted to ξ, and a conjugate basis $v_0, v_1, \cdots, v_{n-1}$ for $\Phi(X)$ $(= \Omega_1(G))$ such that the square map from $X/\Phi(X)$ to $\Phi(X)$ is $(\sum \alpha^{2^i} x_i)^{(2)} = \sum \zeta^{2^i} v_i$, where $\zeta = \alpha^{1+\theta}$. We notice that in fact the basis $v_0, \cdots, v_{n-1}$ can be chosen first, and then the basis $x_0, \cdots, x_{n-1}$ to satisfy these requirements. Indeed if the given bases satisfy our requirement, so do $\lambda x_0, \lambda^2 x_1, \cdots, \lambda^{2^{n-1}} x_{n-1}$ and $\mu v_0, \mu^2 v_1, \cdots, \mu^{2^{n-1}} v_{n-1}$ for any choice of λ and $\mu = \lambda^{1+\theta}$, and since μ is then arbitrary, $\mu v_0, \cdots, \mu^{2^{n-1}} v_{n-1}$ is an arbitrary conjugate basis of $\Phi(X)$ adapted to ξ. In particular, if Y is a second ξ-subgroup of G of ξ-length 2, we can choose a basis $y_0, \cdots, y_{n-1}$ for $Y/\Phi(Y)$, so that the square mapping in Y is also in the normal form. Lastly, since the square mapping determines the commutator map, we see, comparing X with the group constructed in the proof of Lemma 11, that if θ is $\alpha \to \alpha^{2^r}$, then $[x_i, x_{i+r}] = u_i$, and $[x_i, x_j] = 0$ if $j \neq i \pm r$, assuming $\theta \neq 1$.

LEMMA 12. *A Suzuki 2-group of ξ-length 3 is isomorphic to some $B(n, \theta, \varepsilon)$, $C(n, \varepsilon)$, or $D(n, \theta, \varepsilon)$.*

If G is such a group, we observe first that $\Phi(G)$ is elementary abelian. For it is abelian by Lemma 9, and if it contains two steps of the ξ-composition series of G, G covers it. Then Lemmas 7 and 8 show that either $\Phi(G)$ is of exponent 2 or G is abelian, neither of which is true.

Thus the factor $G/\Phi(G)$ contains two steps of the ξ-composition series, so that $G = XY$, where each of X, Y is of ξ-length 2. Let X be isomorphic to $A(n, \theta)$, and Y to $A(n, \varphi)$, where it may or may not be the case that $\theta \neq \varphi$. We choose conjugate bases $x_0, \cdots, x_{n-1}$ for $X/\Phi(G)$, $y_0, \cdots, y_{n-1}$ for $Y/\Phi(G)$, and $v_0, \cdots, v_{n-1}$ for $\Phi(G)$ so that the square mappings in X and Y are given by

$$\left(\sum \alpha^{2^i} x_i\right)^{(2)} = \sum \zeta^{2^i} v_i, \quad \text{and} \quad \left(\sum \beta^{2^i} y_i\right)^{(2)} = \sum \zeta^{2^i} v_i,$$

where $\zeta = \alpha^{\theta+1} = \beta^{\varphi+1}$. To complete the description of G, we have to determine the products $[x_i, y_j]$. These products cannot all be zero. For that would mean that X and Y commute elementwise. However, for any $g \neq 1$ in $\Phi(G)$ we can choose x in X, y in Y so that $x^2 = y^2 = g$. If x, y commute, this means that $(xy^{-1})^2 = 1$, whereas all involutions are in $\Phi(G)$. On the other hand, if $x_0 \xi = \lambda x_0$, and $y_0 \xi = \mu y_0$, $[x_i, y_j]$ can be nonzero only if $\lambda^{2^i} \mu^{2^j}$ is an eigenvalue of ξ on $\Phi(G)$. We play these facts off against one another, to find out which pairs (θ, φ) can occur, and what the structure of G then is. It is convenient to proceed by cases.

Suppose first that $\theta = \varphi = 1$. Then $X/\Phi(G)$, $Y/\Phi(G)$, and $\Phi(G)$ are all ξ-isomorphic. From the fact that the square mapping takes the form $\left(\sum \alpha^{2^i} x_i\right)^{(2)} = \sum \zeta^{2^{i+1}} v_i$, and similarly in Y, it follows that if $x_i \xi = \lambda^{2^i} x_i$, then $y_i \xi = \lambda^{2^i} y_i$, and $v_i \xi = \lambda^{2^{i+1}} v_i$. Thus $[x_i, y_j] = 0$ if $i \neq j$, since $\lambda^{2^i + 2^j}$ is not conjugate to λ, but $[x_i, y_i] = \varepsilon^{2^i} v_i$, for some ε not 0 in $\mathfrak{F}_q$, since $[x_i, y_i]$, like v_i, belongs to the eigenvalue $\lambda^{2^{i+1}}$. The formula

$$(u + v)^{(2)} = u^{(2)} + v^{(2)} + [u, v]$$

enables us now to show that

$$\left(\sum \alpha^{2^i} x_i + \sum \beta^{2^i} y_i\right)^{(2)} = \sum \zeta^{2^i} v_i,$$

where $\zeta = \alpha^2 + \varepsilon\alpha\beta + \beta^2$. We cannot have $\varepsilon = \rho + \rho^{-1}$, for any $\rho \neq 0$ in $\mathfrak{F}_q$, since this would imply $\zeta = 0$ if $\alpha = \beta\rho$, so there would be involutions outside $\Phi(G)$. Thus G is isomorphic to $B(n, 1, \varepsilon)$ for a permitted ε.

Take next the case $\theta = \varphi \neq 1$. Here $X/\Phi(G)$ and $Y/\Phi(G)$ are ξ-isomorphic to one another, but not to $\Phi(G)$. We may assume the conjugate bases chosen so that $x_0 \xi = \lambda x_0$, $y_0 \xi = \lambda y_0$. If θ is $\alpha \rightarrow \alpha^{2^r}$, then $[x_i, x_{i+r}] = [x_{i+r}, x_i] = v_i$, and $[x_i, x_j] = 0$ otherwise; so that the eigenvalue corresponding to v_i is $\lambda^{2^i(1+2^r)}$. It follows that $\lambda^{2^i(1+2^s)}$ is an eigenvalue of ξ on $\Phi(G)$ only if $s = \pm r$, and hence that $[x_i, y_j] = 0$ if $|j - i| \neq r$. We now note that, whenever $\theta = \varphi$, the groups X, Y are not uniquely determined; we can, in fact replace y_0 by a suitable multiple of $\rho x_0 + y_0$, for any ρ in $\mathfrak{F}_q$, and, of course, y_i by $\rho^{2^i} x_i + y_i$. Since $[x_r, x_0] \neq 0$, we can choose ρ so that $[x_r, \rho x_0 + y_0] = 0$. That is, we may assume that $[x_i, y_{i-r}] = 0$, so that the only nonzero products $[x_i, y_j]$ are given by $[x_i, y_{i+r}] = \varepsilon^{2^i} v_i$, for some ε in $\mathfrak{F}_q$. We can now compute the square mapping, and obtain

$$\left(\sum \alpha^{2^i} x_i + \sum \beta^{2^i} y_i\right)^{(2)} = \sum \zeta^{2^i} v_i,$$

where $\zeta = \alpha^{1+2^r} + \varepsilon \alpha \beta^{2^r} + \beta^{1+2^r}$. If $\varepsilon = \rho^{-1} + \rho^{2^r}$, then $\zeta = 0$ when $\alpha = \beta\rho$, so that G is not a Suzuki 2-group. Thus G is a group $B(n, \theta, \varepsilon)$ with θ the map $\alpha \rightarrow \alpha^{2^r}$.

Thirdly, suppose that θ is $\alpha \rightarrow \alpha^{2^r}$, $r \neq 0$, but φ is the identity. We note that since $A(n, \theta)$ and $A(n, \theta^{-1})$ are isomorphic, we may suppose that $0 < r \leqq \frac{1}{2}n$. For some primitive $(2^n - 1)$-st root of unity λ, we have $x_i \xi = \lambda^{2^i} x_i$, $y_i \xi = \lambda^{2^{i-1}(1+2^r)} y_i$, and $v_i \xi = \lambda^{2^i(1+2^r)} v_i$. There exists a subscript s such that $[x_0, y_s] \neq 0$, from which it follows that $\lambda^{1+2^{s-1}(1+2^r)}$ is an eigenvalue of ξ on $\Phi(G)$, and so is $\lambda^{2^t(1+2^r)}$ for some t. Now $2^a + 2^b + 2^c \equiv 2^d + 2^e \pmod{2^n - 1}$ has only the trivial solution $a \equiv b \equiv d - 1$, $c \equiv e \pmod{n}$, and the solutions obtained from it by permuting a, b, and c, and d and e. Of the six solutions of the congruence $1 + 2^{s-1}(1 + 2^r) \equiv 2^t(1 + 2^r)$ obtained in this way, two give an immediate contradiction (e.g., $0 \equiv s - 1 \equiv t - 1$, $s - 1 + r \equiv t + r \pmod{n}$ is contradictory), and two imply $r \equiv 0 \pmod{n}$, which is not so. The remaining cases are $s \equiv r + 2$, $t \equiv 1$, $2r + 1 \equiv 0 \pmod{n}$, and $s \equiv 1$, $t \equiv r$, $2r - 1 \equiv 0 \pmod{n}$. The second conflicts with the requirement that $0 < r \leqq \frac{1}{2}n$, leaving only the first. We see at once that n is odd, and that $\theta : \alpha \rightarrow \alpha^{2^r}$ satisfies $2\theta^2 = 1$. The only nonzero products $[x_i, y_j]$ are given by $[x_i, y_{i+r+2}] = \varepsilon^{2^{i+1}} v_{i+1}$ for some ε in $\mathfrak{F}_q$. We can compute the square mapping $\left(\sum \alpha^{2^i} x_i + \sum \beta^{2^i} y_i\right)^{(2)} = \sum \zeta^{2^i} v_i$, where $\zeta = \alpha^{1+2^r} + \alpha^{1/2} \beta^{2^{r+1}} + \beta^2$. The usual argument shows that $\varepsilon \neq \rho^{-1} + \rho^{2^{r+1}+1}$, and so G is a group $C(n, \varepsilon)$.

Finally, we must consider the case when X, Y are nonisomorphic and nonabelian. This requires θ, φ to be $\alpha \rightarrow \alpha^{2^r}$ and $\alpha \rightarrow \alpha^{2^s}$, where r, s, $r + s$, and $r - s$ are nonzero mod n. Then $x_i \xi = \lambda^{2^i} x_i$, $y_i \xi = \mu^{2^i} y_i$, and $v_\imath = \nu^{2^i} v_i$, where ν is a primitive $(2^n - 1)$-st root of unity, and $\nu = \lambda^{1+2^r} = \mu^{1+2^s}$. We can choose i, j so that $[x_i, y_j]$ is a nonzero multiple of v_0, which implies that $\lambda^i \mu^j = \nu$, or $2^i(1 + 2^s) + 2^j(1 + 2^r) \equiv (1 + 2^r)(1 + 2^s) \pmod{2^n - 1}$. The right-hand side is the sum of the powers 2^0, 2^r, 2^s, 2^{r+s} whose exponents are distinct mod n, hence the exponents on the left must be equal to them, in some order. If, for instance, $i \equiv 0$, and so $i + s = s$, we find that j, $j + r$

are congruent, in either order, to r, $r + s$, so that $r \equiv \pm s$, which is impossible. Similar arguments exclude all possibilities except

$$i = s, \qquad i + s = r, \qquad j = r + s, \qquad j + r = 0,$$

and

$$i = r + s, \qquad i + s = 0, \qquad j = r, \qquad j + r = s.$$

The first case comes from the second by interchanging r and s, and i and j; that is, by interchanging X and Y, so it does not yield a different group. The second gives $5r = 0$, $s = 2r$, $i = 3r$, $j = r$. The nonzero products are given by $[x_{i+3r}, y_{i+r}] = \varepsilon^{2^i} v_i$, for some ε in $\mathfrak{F}_q$. The square mapping is $(\sum \alpha^{2^i} x_i + \sum \beta^{2^i} y_i)^{(2)} = \sum \zeta^{2^i} v_i$, with $\zeta = \alpha^{1+2^r} + \varepsilon \alpha^{2^{3r}} \beta^{2^r} + \beta^{1+2^{2r}}$. The range of ε is limited as usual, so that G is a group $D(n, \theta, \varepsilon)$.

LEMMA 13. *There exists no Suzuki 2-group of ξ-length greater than* 3.

We note that it is sufficient to exclude ξ-length 4. For a group of length greater than 4 contains a normal ξ-subgroup of length 4, which cannot be abelian, by Lemma 9, and so is a Suzuki 2-group.

If the length is 4, there are two *a priori* possibilities, according as $\Phi(G)$ has exponent 4 or exponent 2. We take the first case first. Since $\Phi(G)$ then accounts for two steps of the ξ-composition series, there are two in $G/\Phi(G)$, so that $G = XY$, where X, Y are of ξ-length 3. Each of X, Y contains $\Phi(G)$, which is of type $A(n, 1)$, and so is either of type $B(n, 1, \varepsilon)$ or $C(n, \varepsilon)$.

We choose conjugate bases, adapted to ξ, $x_0, \cdots, x_{n-1}$ in $X/\Phi(G)$, $y_0, \cdots, y_{n-1}$ in $Y/\Phi(G)$, $u_0, \cdots, u_{n-1}$ in $\Phi(G)/\Phi^2(G)$, and $v_0, \cdots, v_{n-1}$ in $\Phi(G)$. We note that $\Phi(X) = \Phi(Y) = \Phi^2(G)$, so that products $[x_i, x_j]$ and $[y_i, y_j]$, evaluated in $\Phi(G)/\Phi^2(G)$, are to be reckoned zero. Thus the Jacobi identity gives $[[y_k, x_i], x_j] = [[y_k, x_j], x_i]$, if double products are evaluated in $\Phi(G)/\Phi^2(G)$, and triple products in $\Phi^2(G)$, and similarly with x's and y's interchanged. We shall use these relations to show that $[x_i, y_j] = 0$ for all i, j. This disposes of this case, for it shows that $[X, Y] \subset \Phi^2(G)$, which combined with $\Phi(X) = \Phi(Y) = \Phi^2(G)$, gives $\Phi(G) = \Phi^2(G)$, a contradiction.

First, if X, Y are both groups $B(n, 1, \varepsilon)$, then for some primitive $(2^n - 1)$-st root of unity λ, $x_i \xi = \lambda^{2^i} x_i$, $y_i \xi = \lambda^{2^i} y_i$, $u_i \xi = \lambda^{2^i} u_i$, and $v_i = \lambda^{2^{i+1}} v_i$; and $[x_i, u_i] = \varepsilon^{2^i} v_i$, $[y_i, u_i] = \eta^{2^i} v_i$, for some nonzero ε and η. The usual eigenvalue argument shows that $[x_i, y_j] = 0$ if $i \neq j$, and that $[x_i, y_i]$ is a multiple of u_{i+1}. But then $[x_i, y_i] \neq 0$ implies $[[x_i, y_i], y_{i+1}] \neq 0$, whereas $[[x_i, y_{i+1}], y_i] = 0$.

Next suppose that X is a $C(n, \varepsilon)$, but Y is a $B(n, 1, \varepsilon)$. Then $n = 2r + 1$, and for a suitable $(2^n - 1)$-st root of unity λ, $x_i \xi = \lambda^{2^i} x_i$, $y_i \xi = \lambda^{2^i(1+2^r)} y_i$, $u_i \xi = \lambda^{2^i(1+2^r)} u_i$, and $v_i \xi = \lambda^{2^{i+1}(1+2^r)} v_i$; and $[u_i, x_{i+r}] = \varepsilon^{2^i} v_{i+r}$, and $[u_i, y_i] = \eta^{2^i} v_i$ for nonzero ε, η. The only products $[x_i, y_j]$ which can be nonzero are products such as $[x_i, y_{i-r}]$, which is a multiple of u_{i+1}. Then if $[x_i, y_{i-r}] \neq 0$, we have $[[y_{i-r}, x_i], x_{i-r}] \neq 0$, whereas $[[y_{i-r}, x_{i-r}], x_i] = 0$.

Finally, if X and Y are both $C(n, \varepsilon)$, the bases satisfy $x_i \xi = \lambda^{2^i} x_i$, $y_i \xi = \lambda^{2^i} y_i$, $u_i \xi = \lambda^{2^i(1+2^r)} u_i$, and $v_i \xi = \lambda^{2^i(1+2^r)} v_i$; and $[u_i, x_{i+r}]$ and $[u_i, y_{i+r}]$ are nonzero multiples of v_{i-r}. The only products $[x_i, y_j]$ which can be nonzero are products such as $[x_i, y_{i+r}]$ and $[y_i, x_{i+r}]$, which are multiples of u_i. Then $[x_i, y_{i+r}] \neq 0$ implies $[[y_{i+r}, x_i], x_{i+r}] \neq 0$, whereas $[[y_{i+r}, x_{i+r}], x_i] = 0$; and similarly with x's and y's interchanged.

This disposes of the possibility that $\Phi(G)$ has exponent 4. If $\Phi(G)$ has exponent 2, then $G = XYW$, where each of X, Y, W is of ξ-length 2, and so is isomorphic to $A(n, \theta)$ for some θ. We observe first that it is not possible for X, Y, W to be all nonisomorphic. Indeed, each of XW, YW is one of the groups listed in Lemma 12, and it is merely a matter of checking through the list to see that, if X, Y, W are all nonisomorphic, this implies that W is $A(5, \theta)$ where θ is $\alpha \to \alpha^4$. Since the argument is symmetric, X, Y are also isomorphic to $A(5, \theta)$, and we have a contradiction.

Assume, then, that X, Y are isomorphic, and choose conjugate bases adapted to ξ, $x_0, \cdots, x_{n-1}$ in $X/\Phi(G)$, $y_0, \cdots, y_{n-1}$ in $Y/\Phi(G)$, $w_0, \cdots, w_{n-1}$ in $W/\Phi(G)$, and $v_0, \cdots, v_{n-1}$ in $\Phi(G)$. Exclude, for the moment, the case when X, Y, W are all isomorphic and non-abelian. Then it is, again, a matter of checking through the list of possible groups XW to see that there is in each case precisely one value of i for which $[x_0, w_i]$ or $[y_0, w_i]$ is nonzero, and that, for this value, $[x_0, w_i]$ and $[y_0, w_i]$ are multiples of the same v_j. Thus we can choose $u_0 = \alpha x_0 + \beta y_0$, with α, β not both zero, so that $[u_0, w_i] = 0$, and so $[u_0, w_j] = 0$ for all j. Then u_0 and its conjugates span a ξ-invariant subspace of $G/\Phi(G)$, corresponding to a ξ-invariant subgroup U of ξ-length 2, which commutes elementwise with W. Since $U \neq W$, we obtain an element of order 2 outside $\Phi(G)$, which is a contradiction.

In the case when X, Y, W are all isomorphic and non-abelian, there is an integer r such that the possible nonzero products $[x_0, w_i]$ or $[y_0, w_i]$ are $[x_0, w_r]$ and $[y_0, w_r]$, which are multiples of v_0, and $[x_0, w_{-r}]$ and $[x_0, w_{-r}]$, which are multiples of v_{-r}. In this case $[w_0, w_r]$ is a nonzero multiple of v_0, and $[w_0, w_{-r}]$ of v_{-r}, and all other products $[w_0, w_i]$ are zero. Then we can choose α, β, γ with α, β not both zero, so that if $u_0 = \alpha x_0 + \beta y_0 + \gamma w_0$, $[u_0, w_r] = [u_0, w_{-r}] = 0$, and hence $[u_0, w_i] = 0$ for all i, from which point the proof is completed as before.

Thus Lemma 13 is proved, and with it, the main theorem.

7. Loose ends

In this final section, we deal with two matters left over. They are not, perhaps, of major importance, and proofs will be given in outline only.

First, as we have said, we do not intend to deal with possible isomorphisms between groups $B(n, \theta, \varepsilon)$, $C(n, \varepsilon)$, and $D(n, \theta, \varepsilon)$; but we do want to deal in this way with the groups $A(n, \theta)$. We abandon the restrictions that $\theta \neq 1$, and that θ is of odd order, and prove the following theorem.

THEOREM 2. *$A(n, \theta)$ is isomorphic to $A(n, \varphi)$ only if $\varphi = \theta^{-1}$.*

$A(n, \theta)$ is abelian only if $\theta = 1$, and contains involutions outside its Frattini subgroup if θ is of even order, but not if it is of odd order. Thus we may assume that neither θ nor φ is 1, and that both have odd, or both have even order. Interchanging θ and φ if necessary, and supposing that $\varphi \neq \theta^{\pm 1}$, it follows that we may suppose the order of θ to be at least 4.

Let θ be $\alpha \to \alpha^{2^r}$, and let φ be $\alpha \to \alpha^{2^s}$. It is clear that if $G = A(n, \theta)$ is isomorphic to $A(n, \varphi)$, there is an automorphism η of G, of order $2^n - 1$, which induces a transformation of $G/\Phi(G)$ with an eigenvalue μ, and a transformation of $\Phi(G)$ with an eigenvalue μ^{2^s+1}. The automorphism ξ of G which gives it its $A(n, \theta)$ structure has eigenvalue λ on $G/\Phi(G)$ and λ^{2^r+1} on $\Phi(G)$, and λ^{2^s+1} is not a conjugate of λ^{2^r+1}, since $s \not\equiv \pm r \pmod n$. It follows that η cannot induce the same transformation on $G/\Phi(G)$ as ξ does, and similarly, that it cannot induce the same transformation as any power of ξ. Thus to prove the theorem, it is sufficient to show that if X is the group of transformations of $G/\Phi(G)$ induced by automorphisms of G, X has only one cyclic subgroup of order $2^n - 1$.

If we choose a conjugate basis $u_0, u_1, \cdots, u_{n-1}$ for $G/\Phi(G)$, adapted to ξ, the only nonzero products $[u_i, u_j]$ are $v_i = [u_i, u_{i+r}]$, $i = 0, \cdots, n-1$, and these are linearly independent. It is clear that if we put $V = G/\Phi(G) \otimes \mathfrak{K}_q$, $[u_i, V]$ has dimension 2. But if $u = \sum \lambda_i u_i$, it is not hard to see that the matrix of coefficients of the forms $[u, u_i]$, can be transformed, by a permutation of rows and columns, into a diagonal sum of blocks

$$\begin{bmatrix} \mu_0 & -\mu_2 & 0 & \cdots & 0 & 0 \\ 0 & \mu_1 & -\mu_3 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \mu_{k-2} & -\mu_0 \\ -\mu_1 & 0 & 0 & \cdots & 0 & \mu_{k-1} \end{bmatrix},$$

where $\mu_0, \cdots, \mu_{k-1}$ are a selection of $\lambda_0, \cdots, \lambda_{n-1}$, and k is the additive order of $r \pmod n$. This is the same as the multiplicative order of θ, and so, by assumption, is at least 4, from which, again, it is not hard to see that if two or more of $\lambda_0, \cdots, \lambda_{k-1}$ are different from zero, the rank of the coefficient matrix is at least 3, that is, the dimension of $[u, V]$ is at least 3. Transformations in X clearly preserve the dimension of $[u, V]$, and so they must act monomially on $u_0, u_1, \cdots, u_{n-1}$. Since they must also map conjugate vectors into conjugate vectors, X is generated by the elements $g : u_i \to u_{i+1}$, and $h : u_i \to \lambda^{2^i} u_i$, λ a primitive $(2^n - 1)$-st root.

Clearly, $g^n = h^{2n-1} = 1$, $g^{-1}hg = h^2$. In any cyclic subgroup Z of X we can choose a generator $g^{n/d}h^i$, where d is a divisor of n. Then Z has order dividing $d(2^{n/d} - 1)$, which is less than $2^n - 1$, unless $d = 1$, which implies $Z = \{h\}$. That is, X has only one cyclic subgroup of order $2^n - 1$, as asserted.

Finally, the main theorem raises rather obviously the question of what can be said about p-groups satisfying similar conditions, for p odd. Here both the answer and the arguments leading to it are simpler.

THEOREM 3. *If p is odd, a p-group with an automorphism permuting its subgroups of order p cyclically is abelian.*

Let G be such a group, and ξ the automorphism. Evidently, a maximal abelian ξ-invariant normal subgroup A of G is a direct product of cyclic groups of the same order, and its only ξ-invariant subgroups are its powers A^{p^i}. We may, without loss of generality, assume that G covers A, in arguing by contradiction.

First, we prove that if $g \notin A$, $g^p \notin A^p$. Since $[G, A]$ is a proper ξ-invariant subgroup of A, $[G, A] \subset A^p$, so that for g in G, $g^{-1}ag = a^{1+p\alpha}$, where α is an endomorphism of A. Then $(ag)^p = g^p a^\psi$, where

$$\psi = 1 + (1 + p\alpha) + (1 + p\alpha)^2 + \cdots + (1 + p\alpha)^{p-1} = p(1 + p\beta)$$

for some endomorphism β of A, p being odd. If, for g outside A, g^p belongs to A^p, then we can choose a in A so that $(ag)^p = 1$, for $1 + p\beta$ is invertible. This is a contradiction.

Now the map from G/A to A/A^p induced by $g \rightarrow g^p$ is linear, since

$$(xy)^p \equiv x^p y^p \pmod{(G')^p H_p},$$

where H_p is the p-th term of the lower central series, and both $(G')^p$ and H_p are contained in A^p; and it is therefore a ξ-homomorphism. The fact that $g^p \in A^p$ implies $g \in A$ shows that it is an isomorphism, and since A/A^p is, as always, irreducible, the image must be the whole of A/A^p. Thus G/A is ξ-isomorphic to A/A^p, and since power mappings in an abelian group are always linear, the ξ-composition factors of G are all isomorphic.

This contradicts the fact that G is non-abelian, by an argument of the type used in proving Lemma 4. Indeed, ξ has order a multiple of

$$p^{n-1} + p^{n-2} + \cdots + 1,$$

the number of cyclic subgroups of an elementary abelian group of order p^n, whereas if G/A were ξ-isomorphic to any submodule of $G'/(G')^p H_3$, ξ could not have order greater than $p^{n-1} + p^{n-2} - 1$.

REFERENCES

1. D. GORENSTEIN, *On finite groups of the form ABA*, Canadian J. Math., vol. 14 (1962), pp. 195–236.
2. G. HIGMAN, *Lie ring methods in the theory of finite nilpotent groups*, Proceedings of the International Congress of Mathematicians 1958 (Edinburgh), Cambridge University Press, 1960, pp. 307–312.
3. B. H. NEUMANN, *Groups with automorphisms that leave only the neutral element fixed*, Arch. Math., vol. 7 (1956), pp. 1–5.

4. M. Suzuki, *On a class of doubly transitive groups*, Ann. of Math. (2), vol. 75 (1962), pp. 105–145.

University of Chicago
Chicago, Illinois
University of Oxford
Oxford, England