Advances in Group Theory and Applications
© 2016 AGTA - www.advgrouptheory.com/journal
2 (2016), pp. 31–65 ISSN: 2499-1287
DOI: 10.4399/97888548970144

Extraspecially Irreducible Groups [1]

R. Dark — A.D. Feldman — M.D. Pérez-Ramos

(*Received Jan. 24, 2016; Accepted Feb. 29, 2016 — Communicated by M.R. Dixon*)

Gewidmet Herrn Professor Dr. Hermann Heineken
zu seinem 80. Geburtstag

Abstract

Given distinct prime numbers q and r, we construct a semidirect product CR with $R \lhd CR$, where C is a cyclic group of order q, and R is an extraspecial r-group, such that C centralizes R', and R is minimal among the extraspecial normal subgroups of CR. We also calculate the automorphism group of CR, and we investigate certain situations in which an automorphism fixes a nontrivial element of R/R'.

Mathematics Subject Classification (2010): 20D99
Keywords: finite group; extraspecial group

1 Introduction

Extraspecial groups play a useful role in the theory of finite groups (see [1, Chapter 2, Section 8], [6, III(13.10)], [8, IX(2.6)]). This is particularly true for questions which involve representation theory [11, Theorems 3.5, 4.4, 7.3 and 8.4], and in many cases one is led to investigate a subgroup CR with $R \lhd CR$, where C is cyclic, R is

[1] The first author is grateful to the University of Valencia for its hospitality. The third author has been supported by Proyecto MTM2014-54707-C3-1-P Ministerio de Economía y Competitividad, Spain

extraspecial and $[R, C] = R$, $[R', C] = 1$. In this paper, we consider the case when C is of prime order, and R is minimal among the extraspecial normal subgroups of CR. We use the theory of Galois fields to give an explicit construction of such groups CR, and to derive some of their properties. The construction was motivated by the proof of a result about the injectors for certain Fitting classes in a finite solvable group [3], and some of our results are designed to be used in this proof.

The layout of the paper is as follows. In the remainder of this section we state some known results which will be used later, and in Section 2 we construct the groups CR. In Section 3 we show that CR is unique (up to isomorphism), and in Section 4 we find the automorphism group of CR. Finally in Section 5 we prove some results about automorphisms fixing a nontrivial element of R/R', which are used in our application [3].

Notation — If n is a natural number, let $\mathbb{C}_n$ be the cyclic (multiplicative) group of order n, and let $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ be the additive group of integers modulo n. If also r is a prime number, let $\mathbb{F}_{r^n}$ be the Galois field of order r^n, and write $\mathbb{F}_{r^n}^+$ and $\mathbb{F}_{r^n}^\times$ for the additive and multiplicative groups of $\mathbb{F}_{r^n}$ respectively. Then $\mathbb{F}_{r^n}^+$ is elementary abelian of order r^n, and $\mathbb{F}_{r^n}^\times \cong \mathbb{C}_{r^n-1}$.

Lemma 1.1

(a) [5, B (9.3.b) and (9.8.c)] *Let W be a module which is C-faithful and $\mathbb{F}_r C$-irreducible, where C is a finite abelian group (and r is a prime number). Then $C = \langle c \rangle \cong \mathbb{C}_n$ is cyclic with $r \nmid n$, and $\dim_{\mathbb{F}_r} W = k$ where k is the order of r modulo n.*

(b) [5, B (9.8.b)] *More explicitly, assuming the hypotheses and conclusions of (a), there exist an $\mathbb{F}_r$-isomorphism $\theta : W \to \mathbb{F}_{r^k}^+$, and an element γ which is a primitive n-th root of 1 in $\mathbb{F}_{r^k}^\times$, such that $(\xi c)^\theta = \gamma \xi^\theta$ $(\xi \in W)$. Thus C permutes the set $W - 0$ semiregularly.*

(c) *With the notation of (b), form the $\mathbb{F}_{r^k}C$-module $W_1 = \mathbb{F}_{r^k} \otimes_{\mathbb{F}_r} W$. Then there is an $\mathbb{F}_{r^k}$-basis $\{\xi_0, \xi_1, \dots, \xi_{k-1}\}$ of W_1 such that $\xi_i c = \gamma^{r^i} \xi_i$ $(i \in \mathbb{Z}_k)$.*

Proof — The statements (a) and (b) are proved in the given references.

(c) Let

$$\chi(x) = x^k - \alpha_{k-1}x^{k-1} - \ldots - \alpha_1 x - \alpha_0$$

be the minimum polynomial of γ over $\mathbb{F}_r$, and take vectors $v_i \in W$ such that $v_i^\theta = \gamma^i$ $(0 \leqslant i < k)$. Then $\{v_0, v_1, \ldots, v_{k-1}\}$ is an $\mathbb{F}_r$-basis of W, and the matrix of c with respect to this basis is the companion matrix

$$M = \begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & \ddots & \ddots & \\ & & & 0 & 1 \\ \alpha_0 & \alpha_1 & \cdots & \alpha_{k-2} & \alpha_{k-1} \end{pmatrix}$$

Moreover $\chi(x)$ is the characteristic polynomial of M, so γ is an eigenvalue for the action of c on W. Hence the other eigenvalues are the images γ^{r^i} $(i \in \mathbb{Z}_k)$ under the Galois group of $\mathbb{F}_{r^k}$ over $\mathbb{F}_r$. We get the result by choosing eigenvectors $\xi_i \in W_1$ with eigenvalue γ^{r^i}. □

Lemma 1.2 *Let r be a prime number.*

(a) [5, B (12.9)] *If k is a natural number, then there is an affine semilinear group B_0C_0W with $C_0 \lhd B_0C_0$, $W \lhd B_0C_0W$ and $B_0 \cap C_0 = B_0C_0 \cap W = 1$, where*

$$B_0 = \langle b_0 \rangle \cong \mathbb{C}_k, \quad C_0 = \langle c_0 \rangle \cong \mathbb{C}_{r^k-1}, \quad c_0^{b_0} = c_0^r.$$

Also $W = \mathbb{F}_{r^k}^+$ is a module which is B_0C_0-faithful and $\mathbb{F}_rC_0$-irreducible, and there is a generator γ_0 of $\mathbb{F}_{r^k}^\times$ such that

$$\omega b_0 = \omega^r, \quad \omega c_0 = \gamma_0 \omega \ \ (\omega \in W).$$

(b) [5, B (12.4)] *Suppose n is a natural number with $r \nmid n$, and let k be the order of r modulo n. Let CW be a semidirect product with $W \lhd CW$ and $C \cap W = 1$, such that $C \cong \mathbb{C}_n$ and W is a module which is C-faithful and $\mathbb{F}_rC$-irreducible. Then CW is unique (up to isomorphism), and $|W| = r^k$. Hence CW can be embedded in the group C_0W constructed in* (a), *with $C = C_0^{(r^k-1)/n}$. Moreover if $\Theta_0 = \mathrm{Aut}(CW)$ and $\Psi_0 = N_{\Theta_0}(C)$, then $B_0C_0 \leqslant \Psi_0$.*

(c) [6, II (3.11)] *Using the notation of* (b), *$\Theta_0 = \Psi_0W$ is a semidirect product, with $W \lhd \Theta_0$ and $\Psi_0 \cap W = 1$. Also $\Psi_0 = B_0C_0$.*

(d) [10, (2.35)] *If* $L \leqslant B_0C_0$ *with* $C_W(L) \neq 0$*, then* $L \leqslant B_0^c$ *for some element* $c \in C_0$*. Moreover* W *has an* $\mathbb{F}_r$*-basis which is permuted regularly by* B_0*.*

Proof — (a) This is proved in the given reference.

(b) The uniqueness is a consequence of Lemma 1.1(b) (and is generalized in the given reference), while the other statements follow from (a).

(c) Clearly C is a Hall r'-subgroup of CW, and $CW \lhd \Theta_0$, so Frattini's argument shows that $\Theta_0 = \Psi_0 \cdot CW = \Psi_0 W$ [6, I (7.8)]. Also

$$\Psi_0 \cap W = N_W(C) = C_W(C) = 1.$$

To prove the last equation, suppose $\phi \in \Psi_0$; because of (b) it suffices to deduce that $\phi \in B_0C_0$. As in Lemma 1.1(b) $W = \mathbb{F}_{r^k}^+$, and the notation can be chosen so that

$$\gamma = \gamma_0^{(r^k-1)/n}, \quad \lambda^{c^i} = \gamma^i\lambda \quad (\lambda \in \mathbb{F}_{r^k},\ i \in \mathbb{Z}_n).$$

Now ϕ preserves the addition in W, so

$$(\lambda+\mu)^\phi = \lambda^\phi + \mu^\phi, \quad (\alpha\lambda)^\phi = \alpha\lambda^\phi \quad (\lambda, \mu \in \mathbb{F}_{r^k},\ \ \alpha \in \mathbb{F}_r).$$

If $1^\phi = \gamma_0^s$, then $1^{\phi c_0^{-s}} = \gamma_0^{-s}1^\phi = 1$. Since $c_0^{-s} \in C_0$, we can replace ϕ by ϕc_0^{-s}, and arrange that $1^\phi = 1$. Since $C^\phi = C$, there is an integer h such that $c^\phi = c^h$. Suppose $\lambda, \mu \in \mathbb{F}_{r^k}$, and note that $\mathbb{F}_r[\gamma] = \mathbb{F}_{r^k}$, so $\lambda = \sum_{i\in\mathbb{Z}_k} \alpha_i\gamma^i$ with $\alpha_i \in \mathbb{F}_r$. Now

$$\begin{aligned}
\gamma^{i\phi} &= 1^{c^i\phi} = 1^{\phi c^{ih}} = 1^{c^{ih}} = \gamma^{ih}, \\
\lambda^\phi &= \left(\sum_{i\in\mathbb{Z}_k} \alpha_i\gamma^i\right)^\phi = \sum_{i\in\mathbb{Z}_k} \alpha_i\gamma^{i\phi} = \sum_{i\in\mathbb{Z}_k} \alpha_i\gamma^{ih}, \\
(\lambda\mu)^\phi &= \left(\sum_{i\in\mathbb{Z}_k} \alpha_i\gamma^i\mu\right)^\phi = \left(\sum_{i\in\mathbb{Z}_k} \alpha_i\mu^{c^i}\right)^\phi = \sum_{i\in\mathbb{Z}_k} \alpha_i\mu^{c^i\phi} \\
&= \sum_{i\in\mathbb{Z}_k} \alpha_i\mu^{\phi c^{ih}} = \sum_{i\in\mathbb{Z}_k} \alpha_i\gamma^{ih}\mu^\phi = \lambda^\phi\mu^\phi,
\end{aligned}$$

which proves that $\phi \in \operatorname{Aut}\mathbb{F}_{r^k} = B_0$.

(d) Choose an element $\delta \in C_W(L) - 0$, and suppose $\delta = \gamma_0^t$. Then $L \leqslant C_{B_0C_0}(\gamma_0^t) = C_{B_0C_0}(1)^{c_0^t} = B_0^c$, where $c = c_0^t$. Finally the given reference shows that $\mathbb{F}_{r^k}$ has a normal $\mathbb{F}_r$-basis $\{\lambda_0, \lambda_1, \ldots, \lambda_{k-1}\}$, with $\lambda_i = \lambda_0^{r^i}$. Then $\lambda_i b_0 = \lambda_{i+1}$ $(i \in \mathbb{Z}_k)$. □

Remark — In Sections 2, 3, 4 and 5 we prove results corresponding to Lemma 1.2 (a), (b), (c) and (d) respectively, when the elementary abelian group W is replaced by an extraspecial group R. The constructions in Section 2 are inspired by Lemma 1.3, and use Lemma 1.4.

Definitions — (a) Let X be a (right) FG-module, where F is a field and G is a group. Then the *dual* FG-*module* is defined to be the vector space $X^* = \mathrm{Hom}_F(X, F)$, with action

$$\xi(\lambda g) = (\xi g^{-1})\lambda \quad (\xi \in X,\ \lambda \in X^*,\ g \in G).$$

(b) Let Q be a finite group which acts on an extraspecial r-group R (where r is a prime number) and take

$$Z = Z(R) = R' \cong \mathbb{C}_r.$$

Then R will be called *extraspecially* Q-*irreducible* if it satisfies the following conditions:

(i) $[R, Q] = R$;

(ii) $[Z, Q] = 1$;

(iii) there is no extraspecial subgroup R_0 such that $Z < R_0 < R$ and $R_0 \lhd QR$.

Lemma 1.3 ([2, Lemma 14], [7, Satz 2]) *Let Q be a finite r'-group which acts on an extraspecial r-group R (where r is a prime number). Take*

$$Z = \langle z \rangle = Z(R) = R' \cong \mathbb{C}_r,$$

and form the $\mathbb{F}_rQ$-module $W = R/Z$. Suppose $[R, Q] = R$ and $[Z, Q] = 1$.

(a) *Then R can be written as a central product $R = R_1 \circ R_2 \circ \ldots \circ R_n$ of extraspecially Q-irreducible groups R_i, with $R_i' = R_i \cap R_j = Z$ and $[R_i, R_j] = 1$ when $i \neq j$.*

(b) *If R is extraspecially Q-irreducible, then W satisfies one of the following conclusions:*

(i) *W is* $\mathbb{F}_r Q$*-irreducible, and if* $r \neq 2$ *then* $R^r = 1$*;*

(ii) $W = X_1 \oplus X_2$ *where* X_1 *and* X_2 *are* $\mathbb{F}_r Q$*-irreducible, with* $X_1 = X_2^*$*, and if* $D_i/Z = X_i$ *then* $D_i' = D_i^r = 1$ $(i = 1, 2)$*. Moreover if* $d_i \in D_i$*, with* $Zd_1 = \lambda \in X_2^*$ *and* $Zd_2 = \xi \in X_2$*, then the notation can be chosen so that* $[d_2, d_1] = z^{\xi,\lambda}$*.*

Proof — (a) Note that W is completely $\mathbb{F}_r Q$-reducible by Maschke's theorem [5, A (11.5)], so this is proved in the first reference.

(b) The required facts are proved in the first reference, except for the statements that $R^r = 1$ when $r \neq 2$ in case (i), and that $D_i^r = 1$ in case (ii). If $r \neq 2$ in case (i), then there is an $\mathbb{F}_r Q$-homomorphism

$$\theta : W \to Z$$

defined by taking $(Zd)^\theta = d^r$ $(d \in R)$. But $[W, Q] = W$, so W has no quotient module centralized by Q, whereas $[Z, Q] = 1$, and hence θ must be the zero homomorphism. Similarly in case (ii) $D_i' = 1$, so there are $\mathbb{F}_r Q$-homomorphisms $\theta_i : X_i \longrightarrow Z$ defined by taking $(Zd_i)^{\theta_i} = d_i^r$ $(d_i \in D_i)$. As before $[X_i, Q] = X_i$, so θ_i is the zero homomorphism $(i = 1, 2)$. □

Lemma 1.4 ([5, A (20.6)], [9, §1A]) *Suppose* W *and* Z *are additive abelian groups, and let* $f : W \times W \to Z$ *be a biadditive map. Put* $E = W \times Z$*, and define a binary operation on* E *by taking*

$$(\omega, \lambda)(\zeta, \mu) = (\omega + \zeta, \lambda + \mu + f(\omega, \zeta)) \quad (\omega, \zeta \in W,\ \lambda, \mu \in Z).$$

Then E *is a group, with*

$$(\omega, \lambda)^n = \left(n\omega, n\lambda + \tfrac{1}{2}n(n-1)f(\omega, \omega)\right) \quad (n \in \mathbb{Z}),$$
$$[(\omega, \lambda), (\zeta, \mu)] = (0, f(\omega, \zeta) - f(\zeta, \omega)).$$

Proof — The operation is associative, with

$$(\omega, \lambda)(\zeta, \mu)(\eta, \nu) =$$
$$= (\omega + \zeta + \eta,\ \lambda + \mu + \nu + f(\omega, \zeta) + f(\omega, \eta) + f(\zeta, \eta)).$$

Also $(0, 0)$ is the identity, and $(\omega, \lambda)^{-1} = (-\omega, -\lambda + f(\omega, \omega))$. The required formulae follow from these facts. □

2 Constructions

In this section we prove results corresponding to Lemma 1.2(a), when the elementary abelian group W is replaced by an extraspecial group R. The constructions are inspired by Lemma 1.3, and use Lemma 1.4.

Definitions — (a) Suppose n is an even number, and consider the group $C_\infty = \langle c_0, c_1 \rangle$ with defining relations

$$c_0^4 = c_1^n = 1,\ c_0^2 = c_1^{n/2}$$

and $c_1^{c_0} = c_1^{-1}$. Then C_∞ will be called a *quasiquaternion group*. Put $C_1 = \langle c_1 \rangle$, and note that $\langle c_0 \rangle \cong \mathbb{C}_4$, $C_1 \cong \mathbb{C}_n$, $C_1 \lhd C_\infty$ and $|C_\infty| = 2n$. If further $n = n_0 n_1$ where n_0 is a power of 2 and $2 \nmid n_1$, then $\langle c_0 \rangle C_1^{n_1}$ is a (generalized) quaternion group of order $2n_0$ (or cyclic of order 4 when $n_0 = 2$), and $C_1^{n_0} \cong \mathbb{C}_{n_1}$ with

$$\langle c_0 \rangle C_1^{n_1} \cdot C_1^{n_0} = C_\infty \text{ and } \langle c_0 \rangle C_1^{n_1} \cap C_1^{n_0} = 1.$$

Moreover the element $y = c_0^2 = c_1^{n/2}$ is the unique involution in C_∞ [6, III (8.2.b)].

(b) Suppose E is a finite r-group (where r is a prime number). If $[d, E] = E'$ for every element $d \in E - E'$, then E is called a *Camina r-group* [4, Section 1]. Note that if further $E^r \leqslant E' = Z(E)$ and $Z < E'$ with $|E'/Z| = r$, then E/Z is extraspecial [5, A (20.3)].

Lemma 2.1 *Suppose r is an odd prime number, and k is a natural number. Then there is a group $BC_\infty R$ such that $C_\infty \lhd BC_\infty$, $R \lhd BC_\infty R$, and $B \cap C_\infty = BC_\infty \cap R = 1$, where $C_\infty = \langle c_0, c_1 \rangle$ is a quasiquaternion group of order $2(r^k - 1)$, and*

$$B = \langle b \rangle \cong \mathbb{C}_k,\quad \langle c_0 \rangle \cong \mathbb{C}_4,\quad C_1 = \langle c_1 \rangle \cong \mathbb{C}_{r^k-1},$$
$$c_0^2 = c_1^{(r^k-1)/2},\quad c_0^b = c_0,\quad c_1^b = c_1^r,\quad c_1^{c_0} = c_1^{-1}.$$

Also $R = D_1 D_2$ is an extraspecial r-group such that

$$Z = Z(R) = R' = D_1 \cap D_2 \cong \mathbb{C}_r,$$

$R^r = D_i' = 1$ *and* $|D_i| = r^{k+1}$ $(i = 1, 2)$. *Moreover if $W = R/Z$ and $X_i = D_i/Z$ are regarded as additive abelian groups, then X_1 and X_2 are* *modules which are* BC_1*-faithful and* $\mathbb{F}_r C_1$*-irreducible, and*

$$X_i b = X_i c_1 = X_i, \quad X_i c_0 = X_{3-i} \ (i = 1, 2), \quad Z = Z(BC_\infty R).$$

Proof — Take

$$X_1 = X_2 = Z_1 = \mathbb{F}^+_{r^k}, \quad W = X_1 \oplus X_2,$$
$$f(\xi_1 \oplus \xi_2, \eta_1 \oplus \eta_2) = \xi_2 \eta_1 \in Z_1 \quad (\xi_i, \eta_i \in X_i),$$

and define $E = W \times Z_1$ as in Lemma 1.4. Put

$$Y_i = \{(\xi, \lambda) : \xi \in X_i, \lambda \in Z_1\} \quad (i = 1, 2),$$

and identify Z_1 with the subgroup $\{(0, \lambda) : \lambda \in Z_1\}$. Then

$$(\xi_1 \oplus \xi_2, \lambda)^r = (0, 0),$$
$$[(\xi_1 \oplus \xi_2, \lambda), (\eta \oplus 0, \mu)] = (0, \xi_2 \eta),$$
$$[(\xi_1 \oplus \xi_2, \lambda), (0 \oplus \eta, \mu)] = (0, -\xi_1 \eta).$$

Hence $[d, E] = Z_1$ for every element $d \in E - Z_1$, so E is a Camina r-group with $E' = Z_1$, and $E^r = Y_i' = 1$ $(i = 1, 2)$. Let γ_1 be a generator of $\mathbb{F}^\times_{r^k}$, and take

$$(\xi_1 \oplus \xi_2, \lambda)^b = (\xi_1^r \oplus \xi_2^r, \lambda^r),$$
$$(\xi_1 \oplus \xi_2, \lambda)^{c_0} = (\xi_2 \oplus (-\xi_1), \lambda - \xi_1 \xi_2),$$
$$(\xi_1 \oplus \xi_2, \lambda)^{c_1} = ((\gamma_1 \xi_1) \oplus (\gamma_1^{-1} \xi_2), \lambda),$$
$$B = \langle b \rangle, \quad C_\infty = \langle c_0, c_1 \rangle, \quad C_1 = \langle c_1 \rangle.$$

Then

$$b, c_0, c_1 \in \operatorname{Aut} E, \quad b^k = c_0^4 = c_1^{r^k - 1} = 1, \quad c_0^2 = c_1^{(r^k-1)/2},$$
$$c_0^b = c_0, \quad c_1^b = c_1^r, \quad c_1^{c_0} = c_1^{-1},$$
$$X_i b = X_i c_1 = X_i, \quad X_i c_0 = X_{3-i} \ (i = 1, 2), \quad Z_1 = Z(C_\infty E),$$

and X_1, X_2 are modules which are BC_1-faithful and $\mathbb{F}_r C_1$-irreducible.

Let $\{\lambda_0, \lambda_1, \ldots, \lambda_{k-1}\}$ be a normal $\mathbb{F}_r$-basis of $\mathbb{F}_{r^k}$, with $\lambda_i = \lambda_0^{r^i}$ $(i \in \mathbb{Z}_k)$ [10, (2.35)]. Then $Z_1 = \mathbb{F}^+_{r^k}$ has a corresponding basis which is permuted regularly by B. Consider an element

$$\lambda = \sum_{i \in \mathbb{Z}_k} \alpha_i \lambda_i \in Z_1$$

with $\alpha_i \in \mathbb{F}_r$, and define $\rho : Z_1 \to \mathbb{F}_r$ by taking

$$\rho(\lambda) = \sum_{i \in \mathbb{Z}_k} \alpha_i.$$

Put $Z_0 = \operatorname{Ker} \rho$, $R = E/Z_0$, $D_i = Y_i/Z_0$ and $Z = Z_1/Z_0$. Then

$$Z_0 = [Z_1, B] \lhd BC_\infty E,$$

so $BC_\infty R$ has the required properties. □

Remark — Let $\tau_0 : \mathbb{F}_{r^k}^+ \to \mathbb{F}_r^+$ be the $\mathbb{F}_r$-linear trace map, with

$$\tau_0(\mu) = \sum_{i \in \mathbb{Z}_k} \mu^{r^i}.$$

Using the above notation for λ and ρ, we get

$$\tau_0(\lambda) = \sum_{i \in \mathbb{Z}_k} \alpha_i \tau_0(\lambda_i) = \sum_{i \in \mathbb{Z}_k} \alpha_i \tau_0(\lambda_0) = \rho(\lambda)\tau_0(\lambda_0).$$

Thus $\rho(\lambda) = \tau_0(\lambda)/\tau_0(\lambda_0)$, so ρ is a constant multiple of τ_0.

Lemma 2.2 *Suppose k is a natural number. Then there is a group $BC_\infty R$ such that $C_\infty \lhd BC_\infty$, $R \lhd BC_\infty R$, and $B \cap C_\infty = BC_\infty \cap R = 1$, where $C_\infty = \langle c_0, c_1 \rangle$ is a dihedral group of order $2(2^k - 1)$, and*

$$B = \langle b \rangle \simeq \mathbb{C}_k, \quad \langle c_0 \rangle \simeq \mathbb{C}_2, \quad C_1 = \langle c_1 \rangle \simeq \mathbb{C}_{2^k - 1},$$
$$c_0^b = c_0, \quad c_1^b = c_1^2, \quad c_1^{c_0} = c_1^{-1}.$$

Also $R = D_1 D_2$ is an extraspecial 2-group with

$$Z = Z(R) = R' = D_1 \cap D_2 \simeq \mathbb{C}_2,$$

$D_i^2 = D_i' = 1$, $|D_i| = 2^{k+1}$ $(i = 1, 2)$. *Moreover if $W = R/Z$ and $X_i = D_i/Z$ are regarded as additive abelian groups, then X_1 and X_2 are modules which are BC_1-faithful and $\mathbb{F}_2 C_1$-irreducible, and*

$$X_i b = X_i c_1 = X_i, \quad X_i c_0 = X_{3-i} \ (i = 1, 2), \quad Z = Z(BC_\infty R).$$

Proof — We can copy the proof of Lemma 2.1 as follows. Take

$$X_1 = X_2 = Z_1 = \mathbb{F}_{2^k}^+, \quad W = X_1 \oplus X_2,$$
$$f(\xi_1 \oplus \xi_2, \eta_1 \oplus \eta_2) = \xi_2 \eta_1 \in Z_1 \quad (\xi_i, \eta_i \in X_i),$$

and define $E = W \times Z_1$ as in Lemma 1.4. Put
$$Y_i = \{(\xi, \lambda) : \xi \in X_i,\ \lambda \in Z_1\} \quad (i = 1, 2),$$
and identify Z_1 with the subgroup $\{(0, \lambda) : \lambda \in Z_1\}$. Then

$$\begin{gathered}
(\xi_1 \oplus \xi_2, \lambda)^2 = (0, \xi_1\xi_2),\\
(\xi \oplus 0, \lambda)^2 = (0 \oplus \xi, \lambda)^2 = (0, 0)\\
[(\xi_1 \oplus \xi_2, \lambda),\ (\eta \oplus 0, \mu)] = (0, \xi_2\eta),\\
[(\xi_1 \oplus \xi_2, \lambda),\ (0 \oplus \eta, \mu)] = (0, \xi_1\eta).
\end{gathered}$$

Hence $[d, E] = Z_1$ for every element $d \in E - Z_1$, so E is a Camina 2-group with $E' = Z_1$, and $Y_i^2 = Y_i' = 1$ $(i = 1, 2)$. Let γ_1 be a generator of $\mathbb{F}_{2^k}^{\times}$, and take

$$\begin{gathered}
(\xi_1 \oplus \xi_2, \lambda)^b = (\xi_1^2 \oplus \xi_2^2, \lambda^2),\\
(\xi_1 \oplus \xi_2, \lambda)^{c_0} = (\xi_2 \oplus \xi_1, \lambda + \xi_1\xi_2),\\
(\xi_1 \oplus \xi_2, \lambda)^{c_1} = ((\gamma_1\xi_1) \oplus (\gamma_1^{-1}\xi_2), \lambda),\\
B = \langle b \rangle, \quad C_\infty = \langle c_0, c_1 \rangle, \quad C_1 = \langle c_1 \rangle.
\end{gathered}$$

Then

$$\begin{gathered}
b, c_0, c_1 \in \operatorname{Aut} E, \quad b^k = c_0^2 = c_1^{2^k - 1} = 1,\\
c_0^b = c_0, \quad c_1^b = c_1^2, \quad c_1^{c_0} = c_1^{-1},\\
X_i b = X_i c_1 = X_i, \quad X_i c_0 = X_{3-i} \ (i = 1, 2), \quad Z_1 = Z(C_\infty E),
\end{gathered}$$

and X_1, X_2 are modules which are BC_1-faithful and $\mathbb{F}_2 C_1$-irreducible.

Let $\{\lambda_0, \lambda_1, \ldots, \lambda_{k-1}\}$ be a normal $\mathbb{F}_2$-basis of $\mathbb{F}_{2^k}$, with $\lambda_i = \lambda_0^{2^i}$ $(i \in \mathbb{Z}_k)$ [10, (2.35)]. Then $Z_1 = \mathbb{F}_{2^k}^{+}$ has a corresponding basis which is permuted regularly by B. Consider an element

$$\lambda = \sum_{i \in \mathbb{Z}_k} \alpha_i \lambda_i \in Z_1$$

with $\alpha_i \in \mathbb{F}_2$, and define $\rho : Z_1 \to \mathbb{F}_2$ by taking

$$\rho(\lambda) = \sum_{i \in \mathbb{Z}_k} \alpha_i.$$

Put $Z_0 = \operatorname{Ker} \rho$, $R = E/Z_0$, $D_i = Y_i/Z_0$ and $Z = Z_1/Z_0$. Then $Z_0 = [Z_1, B] \lhd BC_\infty E$, so $BC_\infty R$ has the required properties. □

Remark As in Lemma 2.1, let $\tau_0 : \mathbb{F}_{2^k}^+ \to \mathbb{F}_2^+$ be the trace map, with

$$\tau_0(\mu) = \sum_{i \in \mathbb{Z}_k} \mu^{2^i}.$$

Using the above notation for λ and ρ, we get $\rho(\lambda) = \tau_0(\lambda)/\tau_0(\lambda_0)$, so ρ is a constant multiple of τ_0.

Definition Suppose r is an odd prime number, and k is an even number, and consider the group $B_\infty = \langle b_1, c_1 \rangle$ with defining relations $b_1^{2k} = c_1^{r^{k/2}+1} = 1$,

$$b_1^k = c_1^{(r^{k/2}+1)/2} \text{ and } c_1^{b_1} = c_1^r.$$

Then B_∞ will be called a *hyperquaternion group*. Put

$$B = \langle b_1 \rangle \simeq \mathbb{C}_{2k} \text{ and } C_1 = \langle c_1 \rangle \simeq \mathbb{C}_{r^{k/2}+1},$$

and observe that $C_1 \lhd B_\infty$ and $|B_\infty| = k(r^{k/2} + 1)$. Also

$$c_1^{b_1^{k/2}} = c_1^{r^{k/2}} = c_1^{-1},$$

so $C_\infty = \langle b_1^{k/2}, c_1 \rangle$ is a quasiquaternion group. If $2 \nmid k/2$ then $B = B^4 \times B^{k/2}$, so $B_\infty = B^4 C_\infty$ with $B^4 \cap C_\infty = 1$. On the other hand, if $2 \mid k/2$ then $r^{k/2} \equiv 1$ modulo 4, so

$$2 \nmid (r^{k/2} + 1)/2 \text{ and } C_1 = C_1^{(r^{k/2}+1)/2} \times C_1^2,$$

and therefore $B_\infty = BC_1^2$ with $B \cap C_1^2 = 1$. In both cases, the element $y = b_1^k = c_1^{(r^{k/2}+1)/2}$ is the unique involution in B_∞.

Lemma 2.3 *Suppose* r *is an odd prime number, and* k *is an even number. Then there is a group* $B_\infty R$ *such that* $R \lhd B_\infty R$ *and* $B_\infty \cap R = 1$, *where* $B_\infty = \langle b_1, c_1 \rangle$ *is a hyperquaternion group of order* $k(r^{k/2} + 1)$, *with*

$$B = \langle b_1 \rangle \simeq \mathbb{C}_{2k}, \quad C_1 = \langle c_1 \rangle \simeq \mathbb{C}_{r^{k/2}+1},$$
$$b_1^k = c_1^{(r^{k/2}+1)/2}, \quad c_1^{b_1} = c_1^r.$$

Also R *is an extraspecial* r*-group with* $Z = Z(R) = R' \simeq \mathbb{C}_r$, $R^r = 1$ *and* $|R| = r^{k+1}$. *Moreover if* $W = R/Z$ *is regarded as an additive abelian* *group, then* W *is a module which is* $B_\infty C_1$*-faithful and* $\mathbb{F}_r C_1$*-irreducible, and* $Z = Z(B_\infty R)$.

Proof — Define $\mathbb{F}_{r^{k/2}}$-homomorphisms $\sigma, \tau : \mathbb{F}^+_{r^k} \to \mathbb{F}^+_{r^k}$ by the equations $\sigma(\omega) = \omega - \omega^{r^{k/2}}$, $\tau(\omega) = \omega + \omega^{r^{k/2}}$ $(\omega \in \mathbb{F}_{r^k})$, and take

$$W = \mathbb{F}^+_{r^k}, \quad Z_1 = \operatorname{Img}\sigma = \operatorname{Ker}\tau,$$
$$f(\omega, \zeta) = \tfrac{1}{2}\sigma(\omega\zeta^{r^{k/2}}) \in Z_1 \quad (\omega, \zeta \in W).$$

Define $E = W \times Z_1$ as in Lemma 1.4, and identify Z_1 with the subgroup $\{(0, \lambda) : \lambda \in Z_1\}$. Then

$$(\omega, \lambda)^r = (0, 0), \quad [(\omega, \lambda), (\zeta, \mu)] = (0, \sigma(\omega\zeta^{r^{k/2}})).$$

Hence $[d, E] = Z_1$ for every element $d \in E - Z_1$, so E is a Camina r-group with $E' = Z_1$, and $E^r = 1$. Let γ_0 be a generator of $\mathbb{F}^\times_{r^k}$, and suppose r_1 is an odd number; in the present proof we can take $r_1 = 1$, but in the proof of Theorem 5.4 it will be convenient to choose a different value for r_1. Note that if $\lambda \in Z_1$, then

$$\tau(\lambda^r) = \tau(\lambda)^r = 0 \text{ and } \tau(\gamma_0^{r^{k/2}+1}\lambda) = \gamma_0^{r^{k/2}+1}\tau(\lambda) = 0,$$

so λ^r and $\gamma_0^{r^{k/2}+1}\lambda$ are both in $\operatorname{Ker}\tau = Z_1$. We can therefore define

$$(\omega, \lambda)^b = (\omega^r, \lambda^r), \ (\omega, \lambda)^{c_0} = (\gamma_0\omega, \gamma_0^{r^{k/2}+1}\lambda) \ (\omega \in W, \lambda \in Z_1),$$
$$b_1 = bc_0^{r_1(r-1)/2}, \quad c_1 = c_0^{r^{k/2}-1}, \quad B_\infty = \langle b_1, c_1\rangle, \quad C_1 = \langle c_1\rangle,$$
$$\gamma_1 = \gamma_0^{r^{k/2}-1}, \quad \delta = \gamma_0^{-r_1(r^{k/2}+1)/2}.$$

Then $b, c_0 \in \operatorname{Aut} E$ and

$$\gamma_0^{r^k-1} = 1, \quad b^k = c_0^{r^k-1} = 1, \quad c_0^b = c_0^{b_1} = c_0^r,$$
$$\gamma_1^{r^{k/2}+1} = 1, \quad (\omega, \lambda)^{c_1} = (\gamma_1\omega, \lambda), \quad c_1^{r^{k/2}+1} = 1, \quad c_1^{b_1} = c_1^r,$$
$$b_1^i = b^i c_0^{r_1(r^i-1)/2} \quad (i \geqslant 0),$$
$$b_1^k = b^k c_0^{r_1(r^k-1)/2} = (c_1^{(r^{k/2}+1)/2})^{r_1} = c_1^{(r^{k/2}+1)/2},$$
$$\delta^{r^{k/2}} = \gamma_0^{-r_1(r^k+r^{k/2})/2} = \gamma_0^{-r_1(r^k-1)/2}\delta = (-1)^{r_1}\delta = -\delta, \ \delta \in Z_1,$$
$$Z_1 = Z(C_1E),$$

and W is a module which is $B_\infty C_1$-faithful and $\mathbb{F}_r C_1$-irreducible, while $Z_1 = \mathbb{F}_{r^{k/2}}\delta$ is the 1-dimensional $\mathbb{F}_{r^{k/2}}$-subspace of $\mathbb{F}_{r^k}$ spanned by δ.

Let $\{\lambda_0, \lambda_1, \dots, \lambda_{(k/2)-1}\}$ be a normal $\mathbb{F}_r$-basis of $\mathbb{F}_{r^{k/2}}$ with $\lambda_i = \lambda_0^{r^i}$ $(i \in \mathbb{Z}_{k/2})$ [10, (2.35)], and take $\lambda'_i = \lambda_i\delta \in Z_1$ $(i \in \mathbb{Z}_{k/2})$. Then $\{\lambda'_0, \lambda'_1, \dots, \lambda'_{(k/2)-1}\}$ is an $\mathbb{F}_r$-basis of Z_1, and

$$\begin{aligned}(0, \lambda'_i)^b &= (0, \lambda_i^r\delta^r)^{c_0^{r_1(r-1)/2}} = (0, \lambda_{i+1}\delta^r\gamma_0^{r_1(r-1)(r^{k/2}+1)/2}) \\ &= (0, \lambda_{i+1}\delta^r\delta^{-(r-1)}) = (0, \lambda'_{i+1}) \quad (i \in \mathbb{Z}_{k/2}),\end{aligned}$$

so $\{\lambda'_0, \lambda'_1, \dots, \lambda'_{(k/2)-1}\}$ is permuted regularly by $B/B^{k/2}$. Consider an element $\lambda = \sum_{i\in\mathbb{Z}_{k/2}} \alpha_i\lambda'_i \in Z_1$ with $\alpha_i \in \mathbb{F}_r$, and define $\rho : Z_1 \to \mathbb{F}_r$ by taking

$$\rho(\lambda) = \sum_{i\in\mathbb{Z}_{k/2}} \alpha_i.$$

Put $Z_0 = \operatorname{Ker}\rho$, $R = E/Z_0$ and $Z = Z_1/Z_0$. Then $Z_0 = [Z_1, B] \lhd B_\infty E$, so $B_\infty R$ has the required properties. □

Remark As in Lemma 2.1, let $\tau_0 : \mathbb{F}_{r^{k/2}} \to \mathbb{F}_r$ be the trace map, with

$$\tau_0(\mu) = \sum_{i\in\mathbb{Z}_{k/2}} \mu^{r^i},$$

and define an $\mathbb{F}_r$-linear map $\tau_1 : Z_1 \to \mathbb{F}_r$ by taking $\tau_1(\lambda) = \tau_0(\lambda\delta^{-1})$ $(\lambda \in Z_1)$. Using above notation for λ and ρ, we get

$$\tau_1(\lambda) = \sum_{i\in\mathbb{Z}_{k/2}} \alpha_i\tau_1(\lambda'_i) = \sum_{i\in\mathbb{Z}_{k/2}} \alpha_i\tau_0(\lambda_i) = \rho(\lambda)\tau_0(\lambda_0),$$

so $\rho(\lambda) = \tau_1(\lambda)/\tau_0(\lambda_0)$, and hence ρ is a constant multiple of τ_1.

Lemma 2.4 *Suppose* k *is an even number. Then there is a group* BC_1R *such that*

$$C_1 \lhd BC_1,\ R \lhd BC_1R \text{ and } B \cap C_1 = BC_1 \cap R = 1,$$

with $|BC_1| = k(2^{k/2} + 1)$, *where*

$$B = \langle b\rangle \simeq \mathbb{C}_k, \quad C_1 = \langle c_1\rangle \simeq \mathbb{C}_{2^{k/2}+1}, \quad c_1^b = c_1^2.$$

Also R *is an extraspecial 2-group with* $Z = Z(R) = R' \simeq C_2$ *and* $|R| = 2^{k+1}$. *Moreover if* $W = R/Z$ *is regarded as an additive abelian group, then* W *is a module which is* BC_1*-faithful and* $\mathbb{F}_2C_1$*-irreducible and* $Z = Z(BC_1R)$.

Proof — Define the $\mathbb{F}_{2^{k/2}}$-linear trace map $\tau : \mathbb{F}^+_{2^k} \to \mathbb{F}^+_{2^{k/2}}$ by taking

$$\tau(\omega) = \omega + \omega^{2^{k/2}} \quad (\omega \in \mathbb{F}_{2^k}),$$

and note that τ is epimorphic [10, (2.23.iii)]. Choose $\epsilon \in \mathbb{F}_{2^k}$ with $\tau(\epsilon) = 1$, and take

$$W = \mathbb{F}^+_{2^k}, \quad Z_1 = \operatorname{Img}\tau = \operatorname{Ker}\tau = \mathbb{F}^+_{2^{k/2}},$$
$$f(\omega, \zeta) = \tau(\epsilon\omega\zeta^{2^{k/2}}) \in Z_1 \quad (\omega, \zeta \in W).$$

Define $E = W \times Z_1$ as in Lemma 1.4, and identify Z_1 with the subgroup $\{(0, \lambda) : \lambda \in Z_1\}$. Then

$$(\omega, \lambda)^2 = (0, \tau(\epsilon)\omega^{2^{k/2}+1}) = (0, \omega^{2^{k/2}+1}),$$
$$[(\omega, \lambda), (\zeta, \mu)] = (0, \tau(\epsilon\omega\zeta^{2^{k/2}} + \epsilon\omega^{2^{k/2}}\zeta))$$
$$= (0, \tau(\epsilon\omega\zeta^{2^{k/2}} + \epsilon^{2^{k/2}}\omega\zeta^{2^{k/2}})) = (0, \tau(\omega\zeta^{2^{k/2}})).$$

Hence $[d, E] = Z_1$ for every element $d \in E - Z_1$, so E is a Camina 2-group with $E' = Z_1$. Let γ_0 be a generator of $\mathbb{F}^\times_{2^k}$, and put

$$\epsilon_1 = \epsilon^{2^{k/2}+1}, \quad \gamma_1 = \gamma_0^{2^{k/2}-1},$$

with

$$\epsilon^2 + \epsilon + \epsilon_1 = \epsilon^2 + (\epsilon + \epsilon^{2^{k/2}})\epsilon + \epsilon^{2^{k/2}+1} = 0.$$

Suppose $(\omega, \lambda)^b = (\omega^2, \lambda^2 + f'(\omega))$, and note that $b \in \operatorname{Aut} E$ provided

$$f'(\omega + \zeta) + f'(\omega) + f'(\zeta) = \epsilon_1\tau(\omega\zeta^{2^{k/2}})^2$$
$$= \epsilon_1(\omega^2\zeta^{2\cdot 2^{k/2}} + \omega^{2\cdot 2^{k/2}}\zeta^2).$$

We therefore take $f'(\omega) = \epsilon_1\omega^{2(2^{k/2}+1)}$, and define

$$(\omega, \lambda)^b = (\omega^2, \lambda^2 + \epsilon_1\omega^{2(2^{k/2}+1)}), \quad (\omega, \lambda)^{c_1} = (\gamma_1\omega, \lambda),$$
$$B = \langle b\rangle, \quad C_1 = \langle c_1\rangle.$$

Then $b, c_1 \in \operatorname{Aut} E$ and

$$(\omega,\lambda)^{b^j} = (\omega^{2^j}, \lambda^{2^j} + \textstyle\sum_{i=0}^{j-1} \epsilon_1^{2^i} \omega^{2^j(2^{k/2}+1)}) \ \ (j \in \mathbb{Z}_k),$$
$$\epsilon_1^{2^i} = \epsilon_1^{2^{i+(k/2)}}, \quad \gamma_1^{2^{k/2}+1} = 1, \quad b^k = c_1^{2^{k/2}+1} = 1, \quad c_1^b = c_1^2,$$
$$Z_1 = Z(C_1 E),$$

and W is a module which is BC_1-faithful and $\mathbb{F}_2 C_1$-irreducible.

Let

$$\{\lambda_0, \lambda_1, \ldots, \lambda_{(k/2)-1}\}$$

be a normal $\mathbb{F}_2$-basis of $\mathbb{F}_{2^{k/2}}$ with $\lambda_i = \lambda_0^{2^i}$ $(i \in \mathbb{Z}_{k/2})$ [10, (2.35)]. Then $Z_1 = \mathbb{F}_{2^{k/2}}^+$ has a corresponding basis which is permuted regularly by $B/B^{k/2}$. Finally consider an element

$$\lambda = \sum_{i \in \mathbb{Z}_{k/2}} \alpha_i \lambda_i \in Z_1$$

with $\alpha_i \in \mathbb{F}_2$, and define $\rho : Z_1 \to \mathbb{F}_2$ by taking

$$\rho(\lambda) = \sum_{i \in \mathbb{Z}_{k/2}} \alpha_i.$$

Put $Z_0 = \operatorname{Ker} \rho$, $R = E/Z_0$ and $Z = Z_1/Z_0$. Then $Z_0 = [Z_1, B] \lhd BC_1 E$, so $BC_1 R$ has the required properties. □

Remark As in Lemma 2.1, let $\tau_0 : \mathbb{F}_{2^{k/2}}^+ \to \mathbb{F}_2^+$ be the trace map, with $\tau_0(\mu) = \sum_{i \in \mathbb{Z}_{k/2}} \mu^{2^i}$. Using the above notation for λ and ρ, we get $\rho(\lambda) = \tau_0(\lambda)/\tau_0(\lambda_0)$, so ρ is a constant multiple of τ_0.

3 Uniqueness

In this section we prove results corresponding to Lemma 1.2(b), when the elementary abelian group W is replaced by an extraspecial group R.

Lemma 3.1 *Suppose* r *is a prime number, and* n *is a natural number with* $r \nmid n$, *and let* k *be the order of* r *modulo* n. *Let* CR *be a group, with* $R \lhd CR$ *and* $C \cap R = 1$, *where* $C \simeq \mathbb{C}_n$ *and* R *is a* C*-faithful extraspecial* r*-group. Put* $Z = Z(R) = R' \simeq \mathbb{C}_r$, *and assume that* R *satisfies* *the conditions in Lemma 1.3*(b - ii), *with* $[R, C] = R$ *and* $[Z, C] = 1$ *(but* R *need not be extraspecially* C*-irreducible). Then* CR *is unique (up to isomorphism), and* $|R| = r^{2k+1}$.

Proof — The conditions in Lemma 1.3(b - ii) imply that CR can be constructed as follows. Let CX_2 be the group described in Lemma 1.1(b) (so X_2 is a module which is C-faithful and $\mathbb{F}_r C$-irreducible), and take $X_1 = X_2^*$ and $Z = \mathbb{F}_r^+$. Note that $D_i' = D_i^r = [Z, C] = 1$, and that D_i is completely $\mathbb{F}_r C$-reducible by Maschke's theorem [5, A (11.5)]. Hence $D_i = X_i \times Z$, with binary operation

$$(\xi, \alpha)(\eta, \beta) = (\xi + \eta, \alpha + \beta),$$

and action

$$(\xi, \alpha)^c = (\xi c, \alpha)(\xi, \eta \in X_i, \alpha, \beta \in Z, c \in C, i = 1, 2).$$

Suppose $(\lambda, \gamma), (\mu, \delta) \in D_1$, and $(\xi, \alpha), (\eta, \beta) \in D_2$, and $c \in C$. If $d_1 = (\lambda, \gamma)$, $d_2 = (\xi, \alpha)$ and $z = (0, 1) \in D_2$, then

$$\begin{aligned}
[(\xi, \alpha), (\lambda, \gamma)] &= [d_2, d_1] = z^{\xi\lambda} = (0, 1)^{\xi\lambda} = (0, \xi\lambda),\\
(\xi, \alpha)^{(\lambda,\gamma)} &= (\xi, \alpha)[(\xi, \alpha), (\lambda, \gamma)] = (\xi, \alpha)(0, \xi\lambda)\\
&= (\xi, \alpha + \xi\lambda),
\end{aligned}$$

$$\begin{aligned}
((\xi, \alpha)(\eta, \beta))^{(\lambda,\gamma)} &= (\xi + \eta, \alpha + \beta)^{(\lambda,\gamma)} = (\xi + \eta, \alpha + \beta + \xi\lambda + \eta\lambda)\\
&= (\xi, \alpha + \xi\lambda)(\eta, \beta + \eta\lambda) = (\xi, \alpha)^{(\lambda,\gamma)}(\eta, \beta)^{(\lambda,\gamma)},\\
(\xi, \alpha)^{(\lambda,\gamma)(\mu,\delta)} &= (\xi, \alpha + \xi\lambda)^{(\mu,\delta)} = (\xi, \alpha + \xi\lambda + \xi\mu)\\
&= (\xi, \alpha)^{(\lambda+\mu,\gamma+\delta)},\\
(\xi, \alpha)^{(\lambda,\gamma)c} &= (\xi, \alpha + \xi\lambda)^c = (\xi c, \alpha + (\xi c)(\lambda c))\\
&= (\xi c, \alpha)^{(\lambda c,\gamma)} = (\xi, \alpha)^{c(\lambda,\gamma)^c}.
\end{aligned}$$

Finally if $R = D_1 D_2 = X_1 X_2 Z$ (with $D_1 \cap D_2 = Z$), then CR has the required properties. Moreover CX_2 is unique by Lemma 1.2(b), and hence CR is also unique (up to isomorphism). □

Lemma 3.2 *Suppose* q *and* r *are distinct prime numbers, and let* k *be the order of* r *modulo* q. *Let* CR *be a group with* $R \lhd CR$ *and* $C \cap R = 1$, *where* $C \simeq \mathbb{C}_q$ *and* R *is a* C*-faithful extraspecial* r*-group. Put*

$$Z = Z(R) = R' \simeq \mathbb{C}_r,$$

and assume that R *is extraspecially* C*-irreducible, with* $[R, C] = R$ *and* $[Z, C] = 1$*. Put*

$$\Gamma = \mathrm{Aut}(CR),\ \Theta = C_\Gamma(Z) \text{ and } \Psi = N_\Theta(C),$$

and suppose $2 \nmid k$.

(a) *The group* CR *is unique (up to isomorphism), and* R *is of type* (ii) *in Lemma 1.3*(b) *with* $|R| = r^{2k+1}$.

(b) *If* $r \neq 2$*, then* $BC_\infty \leqslant \Psi$*, where* $BC_\infty R$ *is the group constructed in Lemma 2.1.*

(c) *If* $r = 2$*, then* $BC_\infty \leqslant \Psi$*, where* $BC_\infty R$ *is the group constructed in Lemma 2.2.*

Proof — Note that $2 \mid \dim_{\mathbb{F}_r}(R/Z)$ (because R is extraspecial), but $2 \nmid k$, so it is clear that R is not of type (i). Then (a) is a consequence of Lemma 3.1, while (b) and (c) follow from Lemmas 2.1 and 2.2 respectively, with $C = C_1^{(r^k-1)/q} \simeq \mathbb{C}_q$. □

Proposition 3.3 *Suppose* r *is a prime number, and* k *is an even number. Then there is a group* C_1R *with* $R \lhd C_1R$ *and* $C_1 \cap R = 1$*, where*

$$C_1 = \langle c_1 \rangle \simeq \mathbb{C}_{r^{k/2}+1}.$$

Also $R = D_1D_2 = R_1 \circ R_2$ *is an extraspecial* r*-group, with*

$$Z = Z(R) = R' = D_1 \cap D_2 = R_1 \cap R_2 \simeq \mathbb{C}_r,$$

$D_i^r = D_i' = [R_1, R_2] = 1$, R_i is extraspecial and $|D_i| = |R_i| = r^{k+1}$ $(i = 1, 2)$. Moreover if $W = R/Z$, $X_i = D_i/Z$ and $W_i = R_i/Z$ are regarded as additive abelian groups, then X_i and W_i are modules which are C_1-faithful and $\mathbb{F}_rC_1$-irreducible $(i = 1, 2)$ with

$$W = X_1 \oplus X_2 = W_1 \oplus W_2,\ X_1 \simeq X_2^* \text{ and } Z = Z(C_1R).$$

Proof — First suppose $r \neq 2$, and define $\mathbb{F}_{r^{k/2}}$-homomorphisms $\sigma, \tau : \mathbb{F}_{r^k}^+ \to \mathbb{F}_{r^k}^+$ by the equations

$$\sigma(\omega) = \omega - \omega^{r^{k/2}}, \tau(\omega) = \omega + \omega^{r^{k/2}} \quad (\omega \in \mathbb{F}_{r^k}).$$

Take

$$W_1 = W_2 = \mathbb{F}_{r^k}^+, \quad W = W_1 \oplus W_2, \quad Z_1 = \operatorname{Img}\sigma = \operatorname{Ker}\tau,$$
$$X_1 = \{\omega \oplus \omega : \omega \in W_1\}, \quad X_2 = \{\omega \oplus (-\omega) : \omega \in W_1\},$$
$$f(\omega_1 \oplus \omega_2, \zeta_1 \oplus \zeta_2) = \tfrac{1}{2}\sigma(\omega_1 \zeta_1^{r^{k/2}} - \omega_2 \zeta_2^{r^{k/2}}) \in Z_1$$

with $\omega_i, \zeta_i \in W_i$. Define $E = W \times Z_1$ as in Lemma 1.4, put

$$E_i = \{(\omega, \lambda) : \omega \in W_i,\ \lambda \in Z_1\} \text{ and } Y_i = \{(\xi, \lambda) : \xi \in X_i,\ \lambda \in Z_1\}$$

$(i = 1, 2)$, and identify Z_1 with the subgroup $\{(0, \lambda) : \lambda \in Z_1\}$. Then

$$\begin{aligned}
&(\omega_1 \oplus \omega_2, \lambda)^r = (0, 0),\\
&[(\omega_1 \oplus \omega_2, \lambda), (\zeta_1 \oplus \zeta_2, \mu)] = (0, \sigma(\omega_1 \zeta_1^{r^{k/2}} - \omega_2 \zeta_2^{r^{k/2}})),\\
&[(\omega \oplus 0, \lambda), (0 \oplus \zeta, \mu)] = (0, 0),\\
&[(\omega \oplus \omega, \lambda), (\zeta \oplus \zeta, \mu)] = (0, 0),\\
&[(\omega \oplus (-\omega), \lambda), (\zeta \oplus (-\zeta), \mu)] = (0, 0),\\
&[(\omega_1 \oplus \omega_2, \lambda), (\zeta \oplus 0, \mu)] = (0, \sigma(\omega_1 \zeta^{r^{k/2}})),\\
&[(\omega_1 \oplus \omega_2, \lambda), (0 \oplus \zeta, \mu)] = (0, -\sigma(\omega_2 \zeta^{r^{k/2}})),\\
&[(\omega \oplus \omega, \lambda), (\zeta \oplus (-\zeta), \mu)] = (0, 2\sigma(\omega \zeta^{r^{k/2}})).
\end{aligned}$$

As in Section 2, we get $[d, E] = [d_i, E_i] = Z_1$ for all elements $d \in E - Z_1$ and $d_i \in E_i - Z_1$ $(i = 1, 2)$. Hence E, E_1 and E_2 are Camina r-groups with

$$E' = E_i' = [Y_1, Y_2] = Z_1 \text{ and } E^r = [E_1, E_2] = Y_i' = 1.$$

Let γ_0 be a generator of $\mathbb{F}_{r^k}^\times$, define

$$\gamma_1 = \gamma_0^{r^{k/2}-1},$$
$$(\omega_1 \oplus \omega_2, \lambda)^{c_1} = ((\gamma_1 \omega_1) \oplus (\gamma_1 \omega_2), \lambda) \quad (\omega_i \in W_i,\ \lambda \in Z_1),$$

and note that W_i and X_i are modules which are C_1–faithful and $\mathbb{F}_r C_1$-irreducible. Choose $Z_0 < Z_1$ with $|Z_1/Z_0| = r$, and take

$$R = E/Z_0,\ R_i = E_i/Z_0,\ D_i = Y_i/Z_0 \text{ and } Z = Z_1/Z_0.$$

Then $D_i' = 1$ $(i = 1, 2)$ and $[D_1, D_2] = Z$, and hence $X_1 \simeq X_2^*$, so $C_1 R$

has the required properties.

Next suppose $r = 2$, and define the $\mathbb{F}_{2^{k/2}}$-linear trace map

$$\tau : \mathbb{F}_{2^k}^{+} \to \mathbb{F}_{2^{k/2}}^{+}$$

by the equation $\tau(\omega) = \omega + \omega^{2^{k/2}}$ $(\omega \in \mathbb{F}_{2^k})$. Choose $\epsilon \in \mathbb{F}_{2^k}$ with $\tau(\epsilon) = 1$ [10, (2.23.iii)], and let γ_0 be a generator of $\mathbb{F}_{2^k}^{\times}$. Take

$$\begin{gathered} W_1 = W_2 = \mathbb{F}_{2^k}^{+}, \quad W = W_1 \oplus W_2, \\ Z_1 = \operatorname{Img}\tau = \operatorname{Ker}\tau = \mathbb{F}_{2^{k/2}}^{+}, \quad \gamma_1 = \gamma_0^{2^{k/2}-1}, \\ X_1 = \{\omega \oplus \omega : \omega \in W_1\}, \quad X_2 = \{\omega \oplus (\gamma_1\omega) : \omega \in W_1\}, \\ f(\omega_1 \oplus \omega_2, \zeta_1 \oplus \zeta_2) = \tau(\epsilon\omega_1\zeta_1^{2^{k/2}} + \epsilon\omega_2\zeta_2^{2^{k/2}}) \in Z_1 \end{gathered}$$

with $\omega_i, \zeta_i \in W_i$. Define $E = W \times Z_1$ as in Lemma 1.4, put

$$E_i = \{(\omega, \lambda) : \omega \in W_i,\ \lambda \in Z_1\} \text{ and } Y_i = \{(\xi, \lambda) : \xi \in X_i,\ \lambda \in Z_1\}$$

$(i = 1, 2)$, and identify Z_1 with the subgroup $\{(0, \lambda) : \lambda \in Z_1\}$. Then

$$\begin{aligned} &(\omega_1 \oplus \omega_2, \lambda)^2 = (0, \omega_1^{2^{k/2}+1} + \omega_2^{2^{k/2}+1}), \\ &(\omega \oplus \omega, \lambda)^2 = (\omega \oplus (\gamma_1\omega), \lambda)^2 = (0, 0), \\ &[(\omega_1 \oplus \omega_2, \lambda), (\zeta_1 \oplus \zeta_2, \mu)] = (0, \tau(\omega_1\zeta_1^{2^{k/2}} + \omega_2\zeta_2^{2^{k/2}})), \\ &[(\omega \oplus 0, \lambda), (0 \oplus \zeta, \mu)] = (0, 0), \\ &[(\omega \oplus \omega, \lambda), (\zeta \oplus \zeta, \mu)] = (0, 0), \\ &[(\omega \oplus (\gamma_1\omega), \lambda), (\zeta \oplus (\gamma_1\zeta), \mu)] = (0, 0), \\ &[(\omega_1 \oplus \omega_2, \lambda), (\zeta \oplus 0, \mu)] = (0, \tau(\omega_1\zeta^{2^{k/2}})), \\ &[(\omega_1 \oplus \omega_2, \lambda), (0 \oplus \zeta, \mu)] = (0, \tau(\omega_2\zeta^{2^{k/2}})), \\ &[(\omega \oplus \omega, \lambda), (\zeta \oplus (\gamma_1\zeta), \mu)] = (0, \tau((1 + \gamma_1^{-1})\omega\zeta^{2^{k/2}})). \end{aligned}$$

As in Section 2, we get $[d, E] = [d_i, E_i] = Z_1$ for all elements $d \in E - Z_1$ and $d_i \in E_i - Z_1$ $(i = 1, 2)$. Hence E, E_1 and E_2 are Camina 2-groups with

$$E' = E_i' = [Y_1, Y_2] = Z_1 \text{ and } [E_1, E_2] = Y_i^2 = Y_i' = 1.$$

Define

$$(\omega_1 \oplus \omega_2, \lambda)^{c_1} = ((\gamma_1\omega_1) \oplus (\gamma_1\omega_2), \lambda) \quad (\omega_i \in W_i,\ \lambda \in Z_1),$$

and note that W_i and X_i are modules which are C_1-faithful and $\mathbb{F}_2C_1$-irreducible. Choose $Z_0 < Z_1$ with $|Z_1/Z_0| = 2$, and take $R = E/Z_0$,

$R_i = E_i/Z_0$, $D_i = Y_i/Z_0$ and $Z = Z_1/Z_0$. As before $D_i^2 = D_i' = 1$ $(i = 1, 2)$ and $[D_1, D_2] = Z$, and hence $X_1 \simeq X_2^*$, so C_1R has the required properties. □

Notation — Write $q^t \parallel n$ to mean that $q^t \mid n$ but $q^{t+1} \nmid n$ (where n and t are natural numbers, and q is a prime number).

Proposition 3.4 *Suppose q and r are distinct prime numbers, and let k be the order of r modulo q. Suppose CR is a group with $R \lhd CR$ and $C \cap R = 1$, where $C \simeq \mathbb{C}_q$, and R is a C-faithful extraspecial r-group. Put $Z = Z(R) = R' \simeq \mathbb{C}_r$, and assume that R is extraspecially C-irreducible, with $[R, C] = R$ and $[Z, C] = 1$. Put $\Gamma = \mathrm{Aut}(CR)$ and $\Theta = C_\Gamma(Z)$, $\Psi = N_\Theta(C)$, and suppose $2 \mid k$.*

(a) *The group CR is unique (up to isomorphism), and R is of type* (i) *in Lemma 1.3*(b) *with $|R| = r^{k+1}$.*

(b) *If $r \neq 2$, then $B_\infty \leqslant \Psi$, where $B_\infty R$ is the group constructed in Lemma 2.3.*

(c) *If $r = 2$, then $BC_1 \leqslant \Psi$, where BC_1R is the group constructed in Lemma 2.4.*

Proof — (a) Note that $q \neq 2$ and $q \nmid r^{k/2} - 1$, and hence $q \mid r^{k/2} + 1$. First suppose R is of type (ii) in Lemma 1.3(b). Let C_1R be the group constructed in Proposition 3.3, and take $C = C_1^{(r^{k/2}+1)/q} \simeq \mathbb{C}_q$. Then $R = D_1D_2$ satisfies the conditions in Lemma 1.3(b - ii), so CR is the unique such group by Lemma 3.1. But $R = R_1 \circ R_2$ is extraspecially C-reducible, which contradicts the hypothesis. This shows that R must be of type (i), and it remains to prove the uniqueness. Put

$$\Delta = \mathrm{Aut}\, R, \quad \Lambda = C_\Delta(Z), \quad W = R/Z, \quad \Omega = C_\Lambda(W).$$

Then Lemmas 2.3 and 2.4 imply that there is a group C_2R such that $q^t \parallel r^{k/2} + 1$ and

$$C_2 = C_1^{(r^{k/2}+1)/q^t} \simeq \mathbb{C}_{q^t}, \quad C = C_2^{q^{t-1}} \simeq \mathbb{C}_q, \quad C_2 \leqslant \Lambda.$$

First suppose $r \neq 2$. Then $R^r = 1$ by Lemma 1.3(b - i), and hence $\Omega = W$ and $\Lambda/\Omega \simeq \mathrm{Sp}_k(r)$ ([5, A (20.8)], [12, Theorem 1(a)]). Moreover

$$|\Lambda| = r^k r^{(k/2)^2}(r^2 - 1)(r^4 - 1)\ldots(r^k - 1),$$

and therefore $q^t \parallel |\Lambda|$. Thus $C_2 \in \mathrm{Syl}_q \Lambda$, and it follows from Sylow's theorem that Λ has a unique conjugacy class of subgroups of order q. Now suppose C_0R_0 is any group with $R_0 \lhd C_0R_0$ and $C_0 \cap R_0 = 1$, where $C_0 \simeq \mathbb{C}_q$ and R_0 is an extraspecially C_0-irreducible r-group of type (i), such that $[R_0, C_0] = R_0$ and $[R_0', C_0] = 1$. Then $\left|R_0/R_0{}'\right| = r^k$ by Lemma 1.1(a), so $|R_0| = r^{k+1}$. Also $R_0^r = 1$, so R_0 can be identified with R. Hence C_0 is identified with a subgroup of Λ, so C_0 is conjugate to C in Λ, and $C_0R_0 \simeq CR$.

Next suppose $r = 2$. Then $\Omega = W$ and $\Lambda/\Omega \simeq O_k^{\pm}(r)$ ([5, A (20.8)], [12, Theorem 1(c)]), and hence

$$|\Lambda| = 2^k 2^{(k/2)^2-(k/2)+1}(2^2-1)(2^4-1)\dots(2^{k-2}-1)(2^{k/2}\mp 1).$$

Therefore $C_2 \in \mathrm{Syl}_q \Lambda$ (and $\Lambda/\Omega = O_k^-(r)$), and the result follows, as before.

The statements (b) and (c) are consequences of Lemmas 2.3 and 2.4 respectively. □

4 Automorphisms

In this section we prove results corresponding to Lemma 1.2(c), when the elementary abelian group W is replaced by an extraspecial group R. Throughout the section, we assume the following hypothesis.

Hypothesis *Suppose* q *and* r *are distinct prime numbers, and let* k *be the order of* r *modulo* q. *Take* CR *as in Lemma 3.2 if* $2 \nmid k$, *and as in Proposition 3.4 if* $2 \mid k$, *and put*

$$Z = Z(CR) = R' \simeq \mathbb{C}_r,$$
$$\Gamma = \mathrm{Aut}(CR), \quad \Theta = C_\Gamma(Z), \quad \Psi = N_\Theta(C),$$
$$W = R/Z, \quad \Theta_0 = \mathrm{Aut}(CW), \quad \Psi_0 = N_{\Theta_0}(C).$$

Given an element $\theta \in \Theta$, *define a homomorphism* $\pi : \Theta \to \Theta_0$ *by taking* θ^π *to be the induced automorphism of* $CW = CR/Z$.

Lemma 4.1 *Assume the above Hypothesis. Then:*

(a) $\Theta \lhd \Gamma$ *and* $\Gamma/\Theta \simeq \mathbb{C}_{r-1}$;

(b) $\Theta = \Psi W$ *is a semidirect product, with* $W \lhd \Theta$ *and* $\Psi \cap W = 1$;

(c) *the restricted map* $\pi_\Psi : \Psi \to \Psi_0$ *is monomorphic.*

Proof — (a) Let α and z be generators of $\mathbb{F}_r^\times$ and Z respectively. Clearly $\Theta \lhd \Gamma$, and $\Gamma/\Theta \leqslant \operatorname{Aut} Z \simeq \mathbb{C}_{r-1}$, so it suffices to find an element $a \in \Gamma$ such that $z^a = z^\alpha$. If $r = 2$, then $\alpha = 1$ and $\Gamma = \Theta$, so the result is clear, and we may therefore assume that $r \neq 2$.

First suppose $2 \nmid k$, and use the notation of Lemma 2.1. Define $a \in \operatorname{Aut} E$ by taking $(\xi_1 \oplus \xi_2, \lambda)^a = (\xi_1 \oplus (\alpha\xi_2), \alpha\lambda)$, and note that $c_1^a = c_1$, so $a \in \operatorname{Aut}(CE)$. Moreover $\rho(\alpha\lambda) = \alpha\rho(\lambda)$ $(\lambda \in Z_1)$, so a normalizes Z_0. Hence a induces the required automorphism of $Z_1/Z_0 = Z$, and in this case $\Gamma = A\Theta$ is a semidirect product, with $A = \langle a \rangle \simeq \mathbb{C}_{r-1}$ and $A \cap \Theta = 1$.

Next suppose $2 \,\big|\, k$, and use the notation of Lemma 2.3. Define

$$a = c_0^{(r^{k/2}-1)/(r-1)} \quad \text{and} \quad \gamma_1 = \gamma_0^{(r^{k/2}-1)/(r-1)}.$$

Then we can take $\alpha = \gamma_1^{r^{k/2}+1}$, and we get $(\omega, \lambda)^a = (\gamma_1\omega, \alpha\lambda)$, with $c_1^a = c_1$ and $a \in \operatorname{Aut}(CE)$. Also $\rho(\alpha\lambda) = \alpha\rho(\lambda)$ $(\lambda \in Z_1)$, so a normalizes Z_0. Hence a induces the required automorphism of Z.

(b) Clearly C is a Hall r'-subgroup of CW, and $CW \lhd \Theta$, so Frattini's argument shows that $\Theta = \Psi \cdot CW = \Psi W$ [5, I (6.3.b)]. Also $\Psi \cap W = N_W(C) = C_W(C) = 1$.

(c) Put

$$\Psi_1 = \operatorname{Ker} \pi_\Psi = N_\Theta(C) \cap C_\Gamma(CR/Z),$$

and note that $[C, \Psi_1] \leqslant C \cap Z = 1$. Given elements $\theta_1 \in \Psi_1$ and $\xi = Zx \in W$, we can therefore define a map $\lambda \in \operatorname{Hom}_{\mathbb{F}_r C}(W, Z)$ by taking $\xi\lambda = [x, \theta_1] = x^{-1}x^{\theta_1}$. But $\operatorname{Hom}_{\mathbb{F}_r C}(W, Z) = 0$, and hence $\lambda = 0$, so $\theta_1 = 1$. □

Lemma 4.2 *If* $q = 2$*, then* $k = 1$ *and* $|R| = r^3$, $W = X_1 \oplus X_2$*, where the modules* X_1 *and* X_2 *are* $\mathbb{F}_r C$*-isomorphic to each other. Moreover* $\Psi = SL_2(r)$.

Proof — Clearly $k = 1$, so R is of type (ii) by Lemma 3.2(a). In fact $C = \langle c \rangle \simeq \mathbb{C}_2$ and $R = \langle d_1, d_2 \rangle$, with $R' \neq R^r = 1$, $|R| = r^3$ and $d_i^c = d_i^{-1}$ $(i = 1, 2)$. Hence $\Psi = Sp_2(r) = SL_2(r)$ [5, A (20.8)]. □

Theorem 4.3 *Suppose* $2 \nmid k$.

(a) *If* $q \neq 2$ *and* $r \neq 2$*, then* $\Psi = BC_\infty$ *as in Lemma 2.1.*

(b) *If* $r = 2$*, then* $\Psi = BC_\infty$ *as in Lemma 2.2.*

Proof — We can prove (a) and (b) together, as follows. Note that R is of type (ii) by Lemma 3.2(a), and $BC_\infty \leqslant \Psi$ by Lemma 3.2(b) and (c). Conversely suppose $\theta \in \Psi$; we must deduce that $\theta \in BC_\infty$. Let $\gamma = \gamma_0^{(r^k-1)/q}$ be a primitive q-th root of 1 in $\mathbb{F}_{r^k}^\times$, where γ_0 is a generator of $\mathbb{F}_{r^k}^\times$. As in Lemma 1.1(c), the eigenvalues for the action of c on X_2 are $\gamma, \gamma^r, \gamma^{r^2}, \dots, \gamma^{r^{k-1}}$ (in $\mathbb{F}_{r^k}$), and hence the eigenvalues for the action of c on $X_1 = X_2^*$ are

$$\gamma^{-1}, \gamma^{-r}, \gamma^{-r^2}, \dots, \gamma^{-r^{k-1}}$$

[8, VII (8.2)]. If X_1 and X_2 are $\mathbb{F}_r$-isomorphic, then

$$\{\gamma^{r^i} : i \in \mathbb{Z}_k\} = \{\gamma^{-r^i} : i \in \mathbb{Z}_k\},$$

so there is an integer $t \in \mathbb{Z}_k$ such that $\gamma = \gamma^{-r^t}$. Then $\gamma^{r^t+1} = 1$, so $q \mid r^t + 1$. Thus $q \mid (r^t - 1)(r^t + 1) = r^{2t} - 1$, and hence $k \mid 2t$. But $2 \nmid k$, so $k \mid t$, which implies that $t = 0$. Therefore $\gamma = \gamma^{-1}$, so $\gamma^2 = 1$. This contradicts the fact that $q \neq 2$, and proves that $X_1 \not\cong X_2$. It follows that X_1 and X_2 are the $\mathbb{F}_r C_1$-homogeneous components of W [5, B (3.4)], so Ψ permutes the set $\{X_1, X_2\}$, and we put

$$\Psi_2 = N_\Psi(X_2) = N_\Psi(X_1).$$

If $X_1^\theta = X_2$, then $X_1^{\theta c_0} = X_1$, so we can replace θ by θc_0 if necessary, and arrange that $\theta \in \Psi_2$.

As in Lemma 1.2(b), put $\Theta_1 = \mathrm{Aut}(CX_1)$ and $\Psi_1 = N_{\Theta_1}(C)$. As in the Hypothesis, given an element $\theta_2 \in \Psi_2$, define a homomorphism $\pi_2 : \Psi_2 \to \Psi_1$ by taking $\theta_2^{\pi_2}$ to be the induced automorphism of CX_2. Note that

$$\mathrm{Ker}\,\pi_2 \leqslant C_{\Psi_2}(X_2) = C_{\Psi_2}(X_2^*) = C_{\Psi_2}(X_1) = C_{\Psi_2}(W) = 1$$

by Lemma 4.1 (c), so π_2 is monomorphic. Now $BC_1 \leqslant \Psi_2$ by Lemma 3.2 (b) and (c), and $B_0C_0 = \Psi_1$ by Lemma 1.2(c). Using the definitions of b and c_1 in the proof of Lemmas 2.1 and 2.2, we get $(BC_1)^{\pi_2} = B_0C_0 = \Psi_1$, so π_2 is also epimorphic. Thus π_2 is an isomorphism, and therefore $\theta \in \Psi_2 = BC_1$. □

Theorem 4.4 [6, II (9.23)] *Suppose* $2 \mid k$.

(a) *If* $r \neq 2$, *then* $\Psi = B_\infty$ *as in Lemma 2.3.*

(b) *If* $r = 2$*, then* $\Psi = BC_1$ *as in Lemma 2.4.*

Proof — As in Theorem 4.3, we can prove (a) and (b) together, as follows. Note that R is of type (i) by Proposition 3.4(a), and as in Lemma 1.2(b) put $\Theta_0 = \mathrm{Aut}(CW)$ and $\Psi_0 = N_{\Theta_0}(C)$. As in the Hypothesis, given an element $\theta \in \Psi$, define a homomorphism $\pi : \Psi \to \Psi_0$ by taking θ^π to be the induced automorphism of $CW = CR/Z$. In case (a) we define B as in the proof of Lemma 2.3, and in both cases, we get $BC_1 \leqslant \Psi$ by Proposition 3.4 (b) and (c). Also $B_0C_0 = \Psi_0$ by Lemma 1.2(c), and it follows from the definition of B in the proof of Lemmas 2.3 and 2.4 that $B^\pi C_0 = B_0C_0$. Hence

$$B^\pi \leqslant \Psi^\pi \leqslant \Psi_0 = B_0C_0 = B^\pi C_0,$$

so

$$\Psi^\pi = B^\pi(\Psi^\pi \cap C_0).$$

Also there is a nonsingular symplectic form $f_0(u, v)$ on W which is preserved by Ψ^π. Put $W_1 = \mathbb{F}_{r^k} \otimes_{\mathbb{F}_r} W$, and let f_1 be the induced symplectic form on W_1, determined by taking

$$f_1(\lambda \otimes u, \mu \otimes v) = \lambda\mu f_0(u, v) \quad (\lambda, \mu \in \mathbb{F}_{r^k},\ u, v \in W).$$

By Lemma 1.1(c) there exist an $\mathbb{F}_{r^k}$-basis $\{\xi_0, \xi_1, \ldots, \xi_{k-1}\}$ of W_1, and a generator γ_0 of $\mathbb{F}_{r^k}^\times$, such that $\xi_i c_0 = \gamma_0^{r^i}\xi_i$ $(i \in \mathbb{Z}_k)$. Then $\xi_i c = \gamma^{r^i}\xi_i$ where $\gamma = \gamma_0^{(r^k-1)/q}$ is a primitive q-th root of 1, and hence

$$f_1(\xi_0, \xi_i) = f_1(\xi_0 c, \xi_i c) = f_1(\gamma\xi_0, \gamma^{r^i}\xi_i) = \gamma^{r^i+1} f_1(\xi_0, \xi_i).$$

If $0 < i < k/2$ then $q \nmid r^{2i} - 1 = (r^i - 1)(r^i + 1)$, so $\gamma^{r^i+1} \neq 1$, and similarly if $k/2 < i < k$ then $q \nmid r^{2(k-i)} - 1 = (r^{k-i} - 1)(r^{k-i} + 1)$, so $\gamma^{r^i+1} = \gamma^{r^i(1+r^{k-i})} \neq 1$. It follows that $f_1(\xi_0, \xi_i) = 0$ when $i \neq k/2$, and therefore $f_1(\xi_0, \xi_{k/2}) \neq 0$ (because f_1 is nonsingular). Now suppose $c_0^i \in \Psi^\pi \cap C_0$, and note that

$$\begin{aligned} f_1(\xi_0, \xi_{k/2}) &= f_1(\xi_0 c_0^i, \xi_{k/2} c_0^i) = f_1(\gamma_0^i \xi_0, \gamma_0^{ir^{k/2}} \xi_{k/2}) \\ &= \gamma_0^{i(r^{k/2}+1)} f_1(\xi_0, \xi_{k/2}), \end{aligned}$$

and therefore $r^{k/2} - 1 \mid i$. Using the definition of C_1 in the proof of Lemmas 2.3 and 2.4, we deduce that $c_0^i \in C_0^{r^{k/2}-1} = C_1^\pi$. This shows that $\Psi^\pi \cap C_0 = C_1^\pi$, so

$$\Psi^\pi = B^\pi(\Psi^\pi \cap C_0) = (BC_1)^\pi.$$

But π is monomorphic by Lemma 4.1(c), so it follows that $\Psi = BC_1$. This completes the proof in case (b), while in case (a) we get $\Psi = BC_1 = B_\infty$. □

5 Fixed points and regular submodules

In this section we prove results corresponding to Lemma 1.2 (d), when the elementary abelian group W is replaced by an extraspecial group R. These results can be used in proving the permutability of the injectors for certain Fitting classes in a finite solvable group [3].

Lemma 5.1 *Suppose* r *is a prime number, and* k *is a natural number. Let* B_0C_0W *be the group described in Lemma 1.2*(a)*, and choose a generator* γ_0 *of* $\mathbb{F}_{r^k}^\times$.

(a) *Suppose* $h \mid k$*, and let* $\Pi = \{\mathbb{F}_{r^h}\gamma_0^i : i \in \mathbb{Z}_{r^k-1}\}$ *be the set of* 1*-dimensional* $\mathbb{F}_{r^h}$*-subspaces of* $\mathbb{F}_{r^k}$*. Then* Π *induces a partition of* $\mathbb{F}_{r^k}^\times$*, with*

$$\mathbb{F}_{r^h}\gamma \cap \mathbb{F}_{r^h}\delta = \begin{cases} \mathbb{F}_{r^h}\gamma & \textit{when } \gamma \in \mathbb{F}_{r^h}\delta \\ 0 & \textit{when } \gamma \notin \mathbb{F}_{r^h}\delta \end{cases}$$

and Π *is permuted by* B_0C_0.

(b) *Suppose* $r \neq 2$ *and* $2 \mid k$*, and take* $\Pi = \{\mathbb{F}_{r^{k/2}}\gamma_0^i : i \in \mathbb{Z}_{r^k-1}\}$*,* $\Pi_0 = \{\mathbb{F}_{r^{k/2}}\gamma_0^i : 2 \mid i\}$*,* $\Pi_1 = \{\mathbb{F}_{r^{k/2}}\gamma_0^i : 2 \nmid i\}$ *and* $c_1 = c_0^{r^{k/2}-1}$*,* $C_1 = \langle c_1 \rangle \simeq \mathbb{C}_{r^{k/2}+1}$*. Then* Π_0 *and* Π_1 *are the* C_1*-orbits in* Π*, with* $\Pi_0 \cup \Pi_1 = \Pi$ *and* $\Pi_0 \cap \Pi_1 = \emptyset$*.*

(c) *Suppose* $r = 2$ *and* $2 \mid k$*, and take* $\Pi = \{\mathbb{F}_{2^{k/2}}\gamma_0^i : i \in \mathbb{Z}_{2^k-1}\}$ *and* $c_1 = c_0^{2^{k/2}-1}$*,* $C_1 = \langle c_1 \rangle \simeq \mathbb{C}_{2^{k/2}+1}$*. Then* C_1 *permutes* Π *regularly.*

Proof — (a) This follows from Lemma 1.2(a).

(b) Note that $\mathbb{F}_{r^{k/2}}\gamma_0^i c_1 = \mathbb{F}_{r^{k/2}}\gamma_0^{i+(r^{k/2}-1)}$ with $2 \mid r^{k/2}-1$, so C_1 stabilizes Π_0 and Π_1, and it remains to show that C_1 permutes Π_0 and Π_1 transitively. Now the stabilizer in C_0 of each $\mathbb{F}_{r^{k/2}}$-subspace $\mathbb{F}_{r^{k/2}}\gamma_0^i$ is $C_2 = C_0^{r^{k/2}+1} \simeq \mathbb{C}_{r^{k/2}-1}$, and the highest common factor of $|C_1|$ and $|C_2|$ is $(r^{k/2}+1, r^{k/2}-1) = 2$. Hence the stabilizer in C_1 of $\mathbb{F}_{r^{k/2}}\gamma_0^i$ is $C_1 \cap C_2 = \langle \gamma_0^{(r^k-1)/2} \rangle \simeq \mathbb{C}_2$ $(i \in \mathbb{Z}_{r^k-1})$, so the C_1-orbits in Π are of size $(r^{k/2}+1)/2$. Since $|\Pi| = r^{k/2}+1$ and $|\Pi_0| = |\Pi_1| = (r^{k/2}+1)/2$, this proves the result.
(c) As before the stabilizer in C_0 of $\mathbb{F}_{2^{k/2}}$ is

$$C_2 = C_0^{2^{k/2}+1} \simeq \mathbb{C}_{2^{k/2}-1},$$

but in this case the highest common factor of $|C_1|$ and $|C_2|$ is $(2^{k/2}+1, 2^{k/2}-1) = 1$. Hence the stabilizer in C_1 of $\mathbb{F}_{2^{k/2}}$ is $C_1 \cap C_2 = 1$, while $|C_1| = |\Pi| = 2^{k/2}+1$, so this proves the result. □

Theorem 5.2 *Suppose* r *is a prime number, and* k *is a natural number, and let* $BC_\infty R$ *be the group described in Lemma 2.1, with* $R = D_1D_2$ *and* $X_i = D_i/R'$ $(i = 1, 2)$.

(a) *If* $L \leqslant BC_\infty$ *and* $C_{X_1}(L) \neq 0$, *then there is an element* $c \in C_1$ *such that* $L \leqslant B^c$.

(b) *There are* $d_0, d_1, \ldots, d_{k-1} \in D_1$ *and* $e_0, e_1, \ldots, e_{k-1} \in D_2$ *such that* R *can be written as a central product*

$$R = E_0 \circ E_1 \circ \ldots \circ E_{k-1},$$

with $|E_i| = r^3$, $E_i^r = 1$, $E_i' = Z$, *and* $[E_i, E_j] = 1$ *when* $i \neq j$, *where* $E_i = \langle d_i, e_i \rangle$ *and* $d_i^b = d_{i+1}$, $e_i^b = e_{i+1}$ $(i \in \mathbb{Z}_k)$.

Proof — With the notation of Lemma 2.1, take $W = X_1 \oplus X_2$ with $X_1 = X_2 = \mathbb{F}_{r^k}^+$, and $Z = \mathbb{F}_r^+$, and define $f_0 : W \times W \to Z$ by taking $f_0(\xi_1 \oplus \xi_2, \eta_1 \oplus \eta_2) = \rho(\xi_2\eta_1)$ $(\xi_i, \eta_i \in X_i)$. If also $\alpha, \beta \in Z$, then as in Lemma 1.4, $R = W \times Z$ with

$$(\xi_1 \oplus \xi_2, \alpha)(\eta_1 \oplus \eta_2, \beta) = ((\xi_1+\eta_1) \oplus (\xi_2+\eta_2), \alpha+\beta+\rho(\xi_2\eta_1)),$$
$$(\xi_1 \oplus \xi_2, \alpha)^r = (0, 0),$$
$$[(\xi_1 \oplus \xi_2, \alpha), (\eta_1 \oplus \eta_2, \beta)] = (0, \rho(\xi_2\eta_1 - \xi_1\eta_2)).$$

(a) Note that L stabilizes X_1, so $L \leqslant N_{BC_\infty}(X_1) = BC_1$. But BC_1X_1 is the affine semilinear group described in Lemma 1.2(a), so the result follows from Lemma 1.2(d).
(b) Given $\xi \in X_1$ and $\eta \in X_2$, define an $\mathbb{F}_r$-bilinear map

$$f_1 : X_1 \times X_2 \to Z$$

by taking $f_1(\xi,\eta) = -\rho(\xi\eta)$. Then

$$[(\xi \oplus 0, 0),\ (0 \oplus \eta, 0)] = (0, f_1(\xi,\eta)),$$

and f_1 is nonsingular, so $X_1 \simeq X_2^*$. Now let $\{\lambda_0, \lambda_1, \ldots, \lambda_{k-1}\}$ be a normal $\mathbb{F}_r$-basis of X_1, with $\lambda_i = \lambda_0^{r^i} = \lambda_0^{b^i}$. Then there is a vector $\mu_0 \in X_2$ such that

$$f_1(\lambda_i, \mu_0) = \begin{cases} 1 & \text{when } i = 0 \\ 0 & \text{when } i \neq 0 \end{cases}$$

Taking $\mu_i = \mu_0^{r^i}$ and $d_i = (\lambda_i \oplus 0, 0)$, $e_i = (0 \oplus \mu_i, 0)$ $(i \in \mathbb{Z}_k)$, we get

$$f_1(\lambda_i, \mu_j) = \begin{cases} 1 & \text{when } i = j \\ 0 & \text{when } i \neq j \end{cases} \qquad [d_i, e_j] = \begin{cases} (0,1) & \text{when } i = j \\ (0,0) & \text{when } i \neq j \end{cases}$$

and $d_i^b = d_{i+1}$, $e_i^b = e_{i+1}$ $(i \in \mathbb{Z}_k)$. □

Notation — Write $\mathbb{D}_8$ for the dihedral group of order 8.

Theorem 5.3 *Suppose* k *is a natural number, and let* $BC_\infty R$ *be the group described in Lemma 2.2, with* $R = D_1D_2$ *and* $X_i = D_i/R'$ $(i = 1, 2)$.

(a) *If* $L \leqslant BC_\infty$ *and* $C_{X_1}(L) \neq 0$, *then there is an element* $c \in C_1$ *such that* $L \leqslant B^c$.

(b) *There are* $d_0, d_1, \ldots, d_{k-1} \in D_1$ *and* $e_0, e_1, \ldots, e_{k-1} \in D_2$ *such that* R *can be written as a central product*

$$R = E_0 \circ E_1 \circ \ldots \circ E_{k-1},$$

where $E_i = \langle d_i, e_i \rangle \simeq \mathbb{D}_8$, $[E_i, E_j] = 1$ *when* $i \neq j$, *and* $d_i^b = d_{i+1}$, $e_i^b = e_{i+1}$ $(i \in \mathbb{Z}_k)$.

Proof — We can copy the proof of Theorem 5.2 as follows. With the notation of Lemma 2.2, put $X_1 = X_2 = \mathbb{F}_{2^k}^+$, $W = X_1 \oplus X_2$, $Z = \mathbb{F}_2^+$, and define $f_0 : W \times W \to Z$ by taking

$$f_0(\xi_1 \oplus \xi_2, \eta_1 \oplus \eta_2) = \rho(\xi_2\eta_1) \quad (\xi_i, \eta_i \in X_i).$$

If also $\alpha, \beta \in Z$, then as in Lemma 1.4, $R = W \times Z$ with

$$\begin{gathered}(\xi_1 \oplus \xi_2, \alpha)(\eta_1 \oplus \eta_2, \beta) = ((\xi_1 + \eta_1) \oplus (\xi_2 + \eta_2), \alpha + \beta + \rho(\xi_2\eta_1)),\\ (\xi_1 \oplus \xi_2, \alpha)^2 = (0, \rho(\xi_1\xi_2)),\\ [(\xi_1 \oplus \xi_2, \alpha),\ (\eta_1 \oplus \eta_2, \beta)] = (0, \rho(\xi_2\eta_1 + \xi_1\eta_2)).\end{gathered}$$

(a) Note that $L \leqslant N_{BC_\infty}(X_0) = BC_1$. But BC_1X_1 is the affine semilinear group described in Lemma 1.2(a), so the result follows from Lemma 1.2(d).
(b) Given $\xi \in X_1$ and $\eta \in X_2$, define an $\mathbb{F}_2$-bilinear map

$$f_1 : X_1 \times X_2 \to Z$$

by taking $f_1(\xi, \eta) = \rho(\xi\eta)$. Then

$$[(\xi \oplus 0, 0),\ (0 \oplus \eta, 0)] = (0, f_1(\xi, \eta)),$$

and f_1 is nonsingular, so $X_1 \simeq X_2^*$. Now let $\{\lambda_0, \lambda_1, \ldots, \lambda_{k-1}\}$ be a normal $\mathbb{F}_2$-basis of X_1, with $\lambda_i = \lambda_0^{2^i} = \lambda_0^{b^i}$. Then there is a vector $\mu_0 \in X_2$ such that

$$f_1(\lambda_i, \mu_0) = \begin{cases} 1 & \text{when } i = 0 \\ 0 & \text{when } i \neq 0 \end{cases}$$

Taking $\mu_i = \mu_0^{2^i}$, $d_i = (\lambda_i \oplus 0, 0)$ and $e_i = (0 \oplus \mu_i, 0)$ $(i \in \mathbb{Z}_k)$, we get

$$f_1(\lambda_i, \mu_j) = \begin{cases} 1 & \text{when } i = j \\ 0 & \text{when } i \neq j \end{cases} \qquad [d_i, e_j] = \begin{cases} (0, 1) & \text{when } i = j \\ (0, 0) & \text{when } i \neq j \end{cases}$$

and $d_i^b = d_{i+1}$, $e_i^b = e_{i+1}$ $(i \in \mathbb{Z}_k)$. □

Theorem 5.4 *Suppose* r *is an odd prime number, and* $k = k_0k_1$ *is an even number, where* k_0 *is a power of* 2 *and* $2 \nmid k_1$. *Let* $B_\infty R$ *be the group described in Lemma 2.3 and its proof.*

(a) *There are subgroups* $D_1, D_2 \leqslant R$ *with* $D_1D_2 = R$, $D_1 \cap D_2 = Z$, $D_i' = 1$ *and* $|D_i| = r^{(k/2)+1}$. *Moreover if* $W = R/Z$ *and* $X_i = D_i/Z$

are regarded as additive abelian groups, then $W = X_1 \oplus X_2$ *and* $X_i b_1^{2k_0} = X_i$ $(i = 1, 2)$.

(b) *If* $L \leqslant B_\infty$ *and* $C_W(L) \neq 0$, *then there is an element* $c \in C_1$ *such that* $L \leqslant (B^{2k_0})^c$.

(c) *There are* $d_0, d_1, \ldots, d_{(k/2)-1} \in D_1$ *and* $e_0, e_1, \ldots, e_{(k/2)-1} \in D_2$ *such that* $R = E_0 \circ E_1 \circ \ldots \circ E_{(k/2)-1}$ *can be written as a central product, with* $|E_i| = r^3$, $E_i^r = 1$, $E_i' = Z$, *and* $[E_i, E_j] = 1$ *when* $i \neq j$, *where* $E_i = \langle d_i, e_i \rangle$ *and*

$$d_i^{b_1^{2k_0}} = d_{i+2k_0}, e_i^{b_1^{2k_0}} = e_{i+2k_0} \quad (i \in \mathbb{Z}_{k/2}).$$

PROOF — (a) With the notation of Lemma 2.3, put $W = \mathbb{F}_{r^k}^+$, $Z = \mathbb{F}_r^+$, and define $f_0 : W \times W \to Z$ by taking

$$f_0(\omega, \zeta) = \tfrac{1}{2}\rho(\omega\zeta^{r^{k/2}} - \omega^{r^{k/2}}\zeta) \quad (\omega, \zeta \in W).$$

If also $\alpha, \beta \in Z$, then as in Lemma 1.4, $R = W \times Z$ with

$$(\omega, \alpha)(\zeta, \beta) = (\omega + \zeta, \alpha + \beta + f_0(\omega, \zeta)),$$
$$(\zeta, \alpha)^r = (0, 0),$$
$$[(\omega, \alpha), (\zeta, \beta)] = (0, \rho(\omega\zeta^{r^{k/2}} - \omega^{r^{k/2}}\zeta)).$$

Now take

$$\begin{aligned} X_1 &= \operatorname{Img}\tau = \operatorname{Ker}\sigma = \{\omega + \omega^{r^{k/2}} : \omega \in \mathbb{F}_{r^k}\} \\ &= \{\zeta \in \mathbb{F}_{r^k} : \zeta^{r^{k/2}} = \zeta\} = \mathbb{F}_{r^{k/2}}, \\ X_2 &= \operatorname{Img}\sigma = \operatorname{Ker}\tau = \{\omega - \omega^{r^{k/2}} : \omega \in \mathbb{F}_{r^k}\} \\ &= \{\zeta \in \mathbb{F}_{r^k} : \zeta^{r^{k/2}} = -\zeta\}, \\ D_i &= \{(\xi, \alpha) : \xi \in X_i,\ \alpha \in Z\} \quad (i = 1, 2), \\ r_1 &= \frac{r^k - 1}{r^{k_0} - 1} = 1 + r^{k_0} + r^{2k_0} + \ldots + r^{(k_1 - 1)k_0}. \end{aligned}$$

Then $W = X_1 \oplus X_2$, where X_1 and X_2 are 1-dimensional $\mathbb{F}_{r^{k/2}}$-subspaces of $\mathbb{F}_{r^k}$, with $X_i b = X_i$, and hence $D_1 D_2 = R$,

$$D_1 \cap D_2 = Z, \quad D_i' = 1 \quad \text{and} \quad |D_i| = r^{(k/2)+1} \quad (i = 1, 2).$$

Also $2 \nmid r_1$ and

$$\begin{aligned} b_1^{2k_0} &= b^{2k_0} c_0^{r_1(r^{2k_0}-1)/2} = b^{2k_0} c_0^{r_1(r^{k_0}-1)(r^{k_0}+1)/2} \\ &= b^{2k_0} c_0^{(r^k-1)(r^{k_0}+1)/2} = b^{2k_0}, \end{aligned}$$

so $X_i b_1^{2k_0} = X_i$ $(i = 1, 2)$.

(b) Note that the element $y = b_1^k = c_1^{(r^{k/2}+1)/2}$ is the unique involution in B_∞, with $\omega y = -\omega$ $(\omega \in W)$. It follows that if $2 \mid |L|$, then $y \in L$ and $C_W(L) \leqslant C_W(y) = 0$. This proves that $2 \nmid |L|$, while $|B_\infty / B^{k_0} C_1| = k_0$ is a power of 2, so

$$L \leqslant B^{k_0} C_1 = (B^{2k_0} \times B^k) C_1 = B^{2k_0} C_1.$$

Let γ_0 be a generator of $\mathbb{F}_{r^k}^\times$, and put $\delta = \gamma_0^{r_1}$.

Take $\Pi_0 = \{\mathbb{F}_{r^{k/2}} \gamma_0^i : 2 \mid i\}$ and $\Pi_1 = \{\mathbb{F}_{r^{k/2}} \gamma_0^i : 2 \nmid i\}$, and choose a vector $\gamma \in C_W(L) - 0$. Then $\mathbb{F}_{r^{k/2}} \in \Pi_0$ and $\mathbb{F}_{r^{k/2}} \delta \in \Pi_1$, and it follows from Lemma 5.1(b) that there exist elements $\lambda \in \mathbb{F}_{r^{k/2}} \cup \mathbb{F}_{r^{k/2}} \delta$ and $c \in C_1$ such that $\lambda c = \gamma$. Now b stabilizes $\mathbb{F}_{r^{k/2}}$, and moreover

$$\delta b^{k_0} = \gamma_0^{r_1 r^{k_0}} = \gamma_0^{r_1(r^{k_0}-1)+r_1} = \gamma_0^{r^k-1} \gamma_0^{r_1} = \delta,$$

so b^{k_0} also stabilizes $\mathbb{F}_{r^{k/2}} \delta$. On the other hand, the stabilizers in C_1 of $\mathbb{F}_{r^{k/2}}$ and $\mathbb{F}_{r^{k/2}} \delta$ are both equal to $C_1^{(r^{k/2}+1)/2}$. It follows that if $\frac{1}{2}(r^{k/2}+1) \nmid j$, then

$$\begin{aligned} \mathbb{F}_{r^{k/2}} b_1^{2ik_0} c_1^j &= \mathbb{F}_{r^{k/2}} b^{2ik_0} c_1^j = \mathbb{F}_{r^{k/2}} c_1^j \neq \mathbb{F}_{r^{k/2}}, \\ (\mathbb{F}_{r^{k/2}} \delta) b_1^{2ik_0} c_1^j &= (\mathbb{F}_{r^{k/2}} \delta) b^{2ik_0} c_1^j = (\mathbb{F}_{r^{k/2}} \delta) c_1^j \neq \mathbb{F}_{r^{k/2}} \delta, \end{aligned}$$

and in particular $b_1^{2ik_0} c_1^j \notin C_{B^{2k_0} C_1}(\lambda)$. Thus

$$C_{B^{2k_0} C_1}(\lambda) \leqslant B^{2k_0} C_1^{(r^{k/2}+1)/2} = B^{2k_0} \times C_1^{(r^{k/2}+1)/2},$$

and hence

$$L \leqslant C_{B^{2k_0} C_1}(\gamma) = C_{B^{2k_0} C_1}(\lambda)^c \leqslant (B^{2k_0})^c \times C_1^{(r^{k/2}+1)/2}.$$

But $2 \nmid |L|$, while $C_1^{(r^{k/2}+1)/2} \simeq \mathbb{C}_2$, and therefore $L \leqslant (B^{2k_0})^c$.
(c) If $\xi \in X_1$, $\eta \in X_2$, define an $\mathbb{F}_r$-bilinear map $f_1 : X_1 \times X_2 \to Z$ by taking $f_1(\xi,\eta) = -2\rho(\xi\eta)$. Then $[(\xi,0),(\eta,0)] = (0, f_1(\xi,\eta))$, and f_1 is nonsingular, so $X_1 \simeq X_2^*$. Now let $\{\lambda_0, \lambda_1, \dots, \lambda_{(k/2)-1}\}$ be a normal $\mathbb{F}_r$-basis of $X_1 = \mathbb{F}_{r^{k/2}}$, with $\lambda_i = \lambda_0^{r^i}$. Then there is a vector $\mu_0 \in X_2$ such that

$$f_1(\lambda_i, \mu_0) = \begin{cases} 1 & \text{when } i = 0 \\ 0 & \text{when } i \neq 0 \end{cases}$$

Taking $\mu_i = \mu_0^{r^i}$ and $d_i = (\lambda_i, 0)$, $e_i = (\mu_i, 0)$ $(i \in \mathbb{Z}_{k/2})$, we get

$$f_1(\lambda_i, \mu_j) = \begin{cases} 1 & \text{when } i = j \\ 0 & \text{when } i \neq j \end{cases} \qquad [d_i, e_j] = \begin{cases} (0,1) & \text{when } i = j \\ (0,0) & \text{when } i \neq j \end{cases}$$

Also $d_i^b = d_{i+1}$ and $e_i^b = e_{i+1}$, so

$$d_i^{b_1^{2k_0}} = d_{i+2k_0} \text{ and } e_i^{b_1^{2k_0}} = e_{i+2k_0}$$

for all $i \in \mathbb{Z}_{k/2}$. □

Lemma 5.5 *Suppose* $k = k_0 k_1$ *is an even number, where* k_0 *is a power of* 2 *and* $2 \nmid k_1$. *Let* BC_1R *be the group described in Lemma 2.4.*

(a) *There are subgroups* $D_1, D_2 \leqslant R$ *with*

$$D_1 D_2 = R, D_1 \cap D_2 = Z, D_i' = 1 \quad \textit{and} \quad |D_i| = 2^{(k/2)+1}.$$

Moreover if $W = R/Z$ *and* $X_i = D_i/Z$ *are regarded as additive abelian groups, then* $W = X_1 \oplus X_2$ *and* $X_i b^{k_0} = X_i$ $(i = 1, 2)$.

(b) *If* $P \leqslant L \leqslant BC_1$ *with* $2 \nmid |P|$ *and* $C_W(P) = C_W(L) \neq 0$, *then there is an element* $c \in C_1$ *such that* $L \leqslant (B^{k_0})^c$.

(c) *There are* $d_0, d_1, \dots, d_{(k/2)-1} \in D_1$ *and* $e_0, e_1, \dots, e_{(k/2)-1} \in D_2$ *such that* $R = E_0 \circ E_1 \circ \dots \circ E_{(k/2)-1}$, *can be written as a central product, with* $|E_i| = 2^3$, $E_i^2 \leqslant E_i' = Z$, *and* $[T_i, E_j] = 1$ *when* $i \neq j$, *where* $E_i = \langle d_i, e_i \rangle$ *and* $d_i^{b^{k_0}} = d_{i+k_0}$,

$$e_i^{b^{k_0}} = e_{i+k_0} \quad (i \in \mathbb{Z}_{k/2}).$$

Proof — (a) With the notation of Lemma 2.4, put $W = \mathbb{F}_{2^k}^+$, $Z = \mathbb{F}_2^+$, and define $f_0 : W \times W \to Z$ by taking

$$f_0(\omega, \zeta) = \rho(\epsilon\omega\zeta^{2^{k/2}} + \epsilon^{2^{k/2}}\omega^{2^{k/2}}\zeta) \quad (\omega, \zeta \in W).$$

If also $\alpha, \beta \in Z$, then as in Lemma 1.4, $R = W \times Z$ with

$$\begin{gathered}(\omega, \alpha)(\zeta, \beta) = (\omega + \zeta, \alpha + \beta + f_0(\omega, \zeta)),\\ (\omega, \alpha)^2 = (0, \rho(\omega^{2^{k/2}+1})),\\ [(\omega, \alpha), (\zeta, \beta)] = (0, \rho(\omega\zeta^{2^{k/2}} + \omega^{2^{k/2}}\zeta)).\end{gathered}$$

Note that $\mathbb{F}_{2^{k_0}} \leqslant \mathbb{F}_{2^k}$ but $\mathbb{F}_{2^{k_0}} \nleqslant \mathbb{F}_{2^{k/2}}$ [10, (2.3)], and choose an element $\delta \in \mathbb{F}_{2^{k_0}} - \mathbb{F}_{2^{k/2}}$. Take

$$\begin{gathered}X_1 = \operatorname{Img}\tau = \operatorname{Ker}\tau = \mathbb{F}_{2^{k/2}}, \quad X_2 = \mathbb{F}_{2^{k/2}}\delta,\\ D_i = \{(\xi, \alpha) : \xi \in X_i,\ \alpha \in Z\} \quad (i = 1, 2).\end{gathered}$$

Then $W = X_1 \oplus X_2$, where X_1 and X_2 are 1-dimensional $\mathbb{F}_{2^{k/2}}$-subspaces of $\mathbb{F}_{2^k}$, with $X_1 b = X_1$, $X_2 b^{k_0} = X_2$ (because $\delta \in \mathbb{F}_{2^{k_0}}$). Hence $D_1 D_2 = R$, $D_1 \cap D_2 = Z$, $D_i' = 1$ and $|D_i| = 2^{(k/2)+1}$ for $i = 1, 2$.
(b) Take $\Pi = \{\mathbb{F}_{2^{k/2}}\gamma_0^i : i \in \mathbb{Z}_{2^k-1}\}$ (where γ_0 is a generator of $\mathbb{F}_{2^k}^\times$), and choose a vector $\gamma \in C_W(L) - 0$. By Lemma 5.1(c), there are elements $\lambda \in \mathbb{F}_{2^{k/2}}$ and $c \in C_1$ such that $\lambda c = \gamma$. Now B stabilizes $\mathbb{F}_{2^{k/2}}$, and C_1 permutes Π regularly, so if $2^{k/2} + 1 \nmid j$, then

$$\mathbb{F}_{2^{k/2}} b^i c_1^j = \mathbb{F}_{2^{k/2}} c_1^j \neq \mathbb{F}_{2^{k/2}},$$

and in particular $b^i c_1^j \notin C_{BC_1}(\lambda)$. Thus

$$P \leqslant C_{BC_1}(\lambda c) = C_{BC_1}(\lambda)^c \leqslant B^c = (B^{k_0})^c \times (B^{k_1})^c,$$

so $P \leqslant (B^{k_0})^c$ (because $2 \nmid |P|$). Hence

$$C_W(L^{c^{-1}}) = C_W(P^{c^{-1}}) \geqslant C_W(B^{k_0}) = \mathbb{F}_{2^{k_0}},$$

and therefore $L \leqslant C_{BC_1}(\mathbb{F}_{2^{k_0}})^c = (B^{k_0})^c$.
(c) If $\xi \in X_1$, $\eta \in X_2$, define an $\mathbb{F}_2$-bilinear map $f_1 : X_1 \times X_2 \to Z$ by taking

$$f_1(\xi, \eta) = \rho(\xi\eta^{2^{k/2}} + \xi^{2^{k/2}}\eta).$$

Then $[(\xi, 0), (\eta, 0)] = (0, f_1(\xi, \eta))$, and f_1 is nonsingular, so $X_2 \simeq X_1^*$. Now let $\{\lambda_0, \lambda_1, \ldots, \lambda_{(k/2)-1}\}$ be a normal $\mathbb{F}_2$-basis of $X_1 = \mathbb{F}_{2^{k/2}}$, with $\lambda_i = \lambda_0^{2^i}$. Since $X_2 \simeq X_1^*$, there is a unique dual $\mathbb{F}_2$-basis $\{\mu_0, \mu_1, \ldots, \mu_{(k/2)-1}\}$ of X_2, such that

$$f_1(\lambda_i, \mu_j) = \begin{cases} 1 & \text{when } i = j \\ 0 & \text{when } i \neq j \end{cases}$$

Moreover $b \in \operatorname{Aut} R$, and so

$$\begin{aligned} f_1(\lambda_i, \mu_j b^{k_0}) &= f_1(\lambda_{i-k_0} b^{k_0}, \mu_j b^{k_0}) = f_1(\lambda_{i-k_0}, \mu_j) \\ &= \begin{cases} 1 & \text{when } i = j + k_0 \\ 0 & \text{when } i \neq j + k_0 \end{cases} \end{aligned}$$

with $\mu_j b^{k_0} \in X_2$, and hence $\mu_j b^{k_0} = \mu_{j+k_0}$ $(j \in \mathbb{Z}_{k/2})$. Now put $d_i = (\lambda_i, 0)$, $e_i = (\mu_i, 0)$ $(0 \leqslant i < k_0/2)$, and define the elements

$$d_{k_0/2}, d_{(k_0/2)+1}, \ldots, d_{(k/2)-1} \text{ and } e_{k_0/2}, e_{(k_0/2)+1}, \ldots, e_{(k/2)-1}$$

by taking

$$d_{i+jk_0} = d_i^{b^{jk_0}} = \Big(\lambda_{i+jk_0}, \rho\big(\textstyle\sum_{l=0}^{jk_0-1} \epsilon_1^{2^l} \lambda_{i+jk_0}^{2^{k/2}+1}\big)\Big),$$

$$e_{i+jk_0} = e_i^{b^{jk_0}} = \Big(\mu_{i+jk_0}, \rho\big(\textstyle\sum_{l=0}^{jk_0-1} \epsilon_1^{2^l} \mu_{i+jk_0}^{2^{k/2}+1}\big)\Big),$$

where $0 \leqslant i < k_0/2$, $1 \leqslant j < k_1$ and $i + jk_0 \in \mathbb{Z}_{k/2}$. Note that if $0 \leqslant j < (k_1+1)/2$ then $(2j)k_0/2 \leqslant i + jk_0 < (2j+1)k_0/2$, while if $(k_1+1)/2 \leqslant j < k_1$, then taking $j' = j - (k_1+1)/2$, we get

$$i + jk_0 \equiv i + (2j'+1)k_0/2 \pmod{k/2}$$

and

$$(2j'+1)k_0/2 \leqslant i + (2j'+1)k_0/2 < 2(j'+1)k_0/2.$$

Also

$$[d_i, e_j] = \begin{cases} (0,1) & \text{when } i = j \\ (0,0) & \text{when } i \neq j \end{cases}$$

and $d_i^{b^{k_0}} = d_{i+k_0}$ and $e_i^{b^{k_0}} = e_{i+k_0}$ $\quad (i \in \mathbb{Z}_{k/2})$. □

REFERENCES

[1] M. Aschbacher: "Sporadic Groups", *Cambridge University Press*, Cambridge (1994).

[2] R. Dark – A. Feldman – M.D. Pérez-Ramos: "Persistent characterizations of injectors in finite solvable groups", *J. Group Theory* 12 (2009), 511–538.

[3] R. Dark – A. Feldman – M.D. Pérez-Ramos: "The permutability of injectors with a central socle in a finite solvable group", *submitted*.

[4] R. Dark – C.M. Scoppola: "On Camina groups of prime power order", *J. Algebra* 181 (1996), 787–802.

[5] K. Doerk – T. Hawkes: "Finite Soluble Groups", *de Gruyter*, Berlin (1992).

[6] B. Huppert: "Endliche Gruppen I", *Springer*, Berlin (1967).

[7] B. Huppert: "Singer-Zyklen in klassischen Gruppen", *Math. Z.* 117 (1970), 141–150.

[8] B. Huppert – N. Blackburn: "Finite Groups II", *Springer*, Berlin (1982).

[9] D. Jonah – M. Konvisser: "Abelian subgroups of p-groups, an algebraic approach", *J. Algebra* 34 (1975), 386–402.

[10] R. Lidl – H. Niederreiter: "Finite Fields", *Cambridge University Press*, Cambridge (1984).

[11] O. Manz – T.R. Wolf: "Representations of Solvable Groups", *Cambridge University Press*, Cambridge (1993).

[12] D.L. Winter: "The automorphism group of an extraspecial p-group", *Rocky Mountain J. Math.* 2 (1972), 159–168.

Rex Dark
School of Mathematics, Statistics and Applied Mathematics
National University of Ireland
University Road
Galway (Ireland)
e-mail: rex.dark@nuigalway.ie

Arnold D. Feldman
Mathematics Department
Franklin and Marshall College
Lancaster
PA 17604-3003 (U.S.A.)
e-mail: afeldman@fandm.edu

María Dolores Pérez-Ramos
Departament de Matemàtiques
Universitat de València
C/ Doctor Moliner 50
46100 Burjassot (València) (Spain)
e-mail: Dolores.Perez@uv.es