LATTICE EMBEDDINGS OF PRIME POWER GROUPS

D. W. BARNES

(received 28 July 1960)

1. Introduction

Let G be a group of order p^n where p is some prime. Denote by $n_r(G)$ the number of subgroups of G of order p^r. If H is the elementary abelian group of order p^n, then

$$n_r(G) \leqq n_r(H).^*$$

This means that it is possible to construct a one-to-one mapping f of the set of all subgroups of G into the set of all subgroups of H such that, for all subgroups $A \subseteqq G$,

$$|fA| = |A|.$$

This raises the problem of whether f can be constructed so as to preserve the partial ordering of the subgroups of G, that is, such that $fA \subseteqq fB$ whenever $A \subseteqq B$.

An *embedding* of the lattice L in a lattice M is defined to be a one-to-one mapping f of L into M such that fX covers fY for all $X, Y \in L$ such that X covers Y. If G is a group, we denote the lattice of all subgroups of G by $L(G)$. If G and H are groups of the same prime power order, we define a *lattice embedding* (which we abbreviate to L-embedding) of G in H to be an embedding of $L(G)$ in $L(H)$.

We say that the L-embeddings f_1 and f_2 of a prime power group G in a group H of the same order are similar if there exist automorphisms α, β of G, H respectively such that

$$f_1 = \beta f_2 \alpha,$$

where we do not distinguish in notation between an automorphism of a group and the lattice automorphism it induces. By $\beta f_2 \alpha$ we mean the mapping formed by first applying the mapping α, then f_2 and then β. We say f_1 and f_2 are equivalent if for some β it is possible to take $\alpha = 1$, that is, if there exists β such that

$$f_1 = \beta f_2.$$

* G. E. Wall [5].

This paper is an investigation of the groups G and H for which there exists an L-embedding of G in H. We find necessary and sufficient conditions for an abelian p-group to have an L-embedding in the elementary abelian group of the same order.

NOTATION. Where possible, capital letters will be used for groups and lattices, while small letters will be used for elements of groups and for arbitrary integers. The group generated by $x_1, \cdots, x_r$ will be denoted by $\{x_1, \cdots, x_r\}$. We shall call a group G, a group of r generators if there exists a set of r elements of G which generates G, and no set of fewer than r elements of G generates G. The intersection of all the maximal subgroups of a group G will be denoted by $\Phi(G)$. If the group (or lattice) A is isomorphic to the group (or lattice) B, we write $A \cong B$. We shall use the signs $\cup$, $\cap$ for the lattice operations of union and intersection. By $A \supset B$, we mean that A contains B and $A \neq B$. The image of x under a mapping f will be denoted by fx. Brackets will only be used when their omission would make the notation ambiguous.

The elementary abelian group of order p^n is the additive group of a vector space of dimension n over the field $GF(p)$ of p elements. Its lattice is isomorphic to the lattice of subspaces of a projective geometry of dimension $n - 1$ over $GF(p)$. We shall often use matrix and vector notations when working with this group. In this paper, only finite groups are considered. Whenever the word "group" is used, it is to be taken to mean "finite group".

G and H are always groups of the same prime power order.

THEOREM 1.1. *Let f be an embedding of a lower semi-modular lattice L of finite dimension in a lattice M. Then for all $X, Y \in L$,*

$$f(X \cap Y) = (fX) \cap (fY).$$

PROOF. (a) Suppose $X \supseteq Y$. Consider the image of a connected chain from X to Y. This is a connected chain from fX to fY, therefore $fX \supseteq fY$ and the result holds.

(b) Suppose $X \cup Y$ covers Y. We prove the result for this case by induction over $d(X) + d(Y)$, where $d(X)$ is the dimension of X in L, assuming $X \cup Y \neq X$.

There exists $Z \in L$ such that $X \cup Y$ covers Z and $Z \supseteq X$. By the lower semi-modularity of L, Y and Z cover $Y \cap Z$. Hence

$$f(Y \cap Z) = (fY) \cap (fZ) \text{ and } X \cup (Y \cap Z) = Z.$$

Hence
$$\begin{aligned} f(X \cap Y) &= f(X \cap (Y \cap Z)) \\ &= (fX) \cap f(Y \cap Z) \text{ by induction hypothesis} \\ &= (fX) \cap (fY) \cap (fZ) \\ &= (fX) \cap (fY). \end{aligned}$$

(c) We prove the theorem by induction over $d(X) + d(Y)$. By (a) and (b), we may assume $X \cup Y \neq X$ or Y and $X \cup Y$ does not cover Y.

https://doi.org/10.1017/S1446788700026355 Published online by Cambridge University Press

There exists $Z \in L$ such that $X \cup Y$ covers Z and $Z \supseteq Y$. Then $X \cap Z \neq X$.

$$\begin{aligned} f(X \cap Y) &= f((X \cap Z) \cap Y) \\ &= f(X \cap Z) \cap (fY) && \text{by induction hypothesis} \\ &= (fX) \cap (fZ) \cap (fY) && \text{by (b) since } X \cup Z = X \cup Y \text{ covers } Z \\ &= (fX) \cap (fY) && \text{since by (a), } fZ \supseteq fY. \end{aligned}$$

COROLLARY 1.2. *If f is an L-embedding of a p-group G in a p-group H, then*

$$f(X \cap Y) = (fX) \cap (fY)$$

for all $X, Y \subseteq G$.

PROOF. $L(G)$ is lower semi-modular since G is a p-group.

COROLLARY 1.3. *If f is an L-embedding of G in H and $L(G)$ is modular, then $f(L(G))$ is a sublattice of $L(H)$.*

PROOF. Apply Theorem 1.1 to $L(G)$ and to its dual.

2. Projectivities

Suppose A_1, B_1, A_2, B_2 are subgroups of a group G, and that B_1 is a normal subgroup of A_1, $A_1 = A_2 \cup B_1$ and $B_2 = B_1 \cap A_2$. Then the correspondence between the cosets of B_1 in A_1 and their intersections with A_2 is an isomorphism $A_1/B_1 \overset{\varphi_1}{\to} A_2/B_2$. The correspondence φ_2 between the cosets of B_2 in A_2 and their products with B_1 is also an isomorphism $A_2/B_2 \overset{\varphi_2}{\to} A_1/B_1$, and $\varphi_2 = \varphi_1^{-1}$. Such isomorphisms φ_1, φ_2 are called projectivities. The projectivities φ_1, φ_2 are called prime if A_1 covers A_2. The interval A_1/B_1 is called prime if A_1 covers B_1.

We call

$$c : A_1/B_1 \overset{\varphi_1}{\to} A_2/B_2 \overset{\varphi_2}{\to} \cdots \overset{\varphi_{n-1}}{\to} A_n/B_n$$

a chain of projectivities from A_1/B_1 to A_n/B_n if all the mappings φ_i are projectivities. The chain is called closed if $A_1 = A_n$ and $B_1 = B_n$. Two intervals A/B, A'/B' are said to be projective if there exists a chain of projectivities from A/B to A'/B'. If

$$c : A/B \overset{\varphi_0}{\to} A_1/B_1 \overset{\varphi_1}{\to} \cdots \overset{\varphi_{n-1}}{\to} A_n/B_n \overset{\varphi_n}{\to} A/B$$

is a closed chain of projectivities, then $\varphi_n\varphi_{n-1}\cdots\varphi_1\varphi_0$ defines an automorphism of A/B. We call this automorphism, the automorphism induced by c, and denote it by $\alpha(c)$. If

$$c' : A/B \to A_1'/B_1' \to \cdots \to A_r'/B_r' \to A/B$$

is another closed chain of projectivities from A/B to A/B, we define cc' to be the closed chain of projectivities

$$cc' : A/B \to A_1/B_1 \to \cdots \to A_n/B_n \to A/B \to A_1'/B_1' \to \cdots \to A_r'/B_r' \to A/B,$$

and

https://doi.org/10.1017/S1446788700026355 Published online by Cambridge University Press

$$c^{-1} : A/B \to A_n/B_n \to \cdots \to A_1/B_1 \to A/B.$$

Clearly

$$\alpha(cc') = \alpha(c')\alpha(c), \qquad \alpha(c^{-1}) = \alpha(c)^{-1}.$$

The automorphisms induced in A/B by closed chains of projectivities in G form a group $\mathfrak{A}(G, A/B)$. If A/B and A'/B' are projective, then

$$\mathfrak{A}(G, A/B) \cong \mathfrak{A}(G, A'/B').$$

THEOREM 2.1. *If G is a p-group with more than one subgroup of order p, then all prime intervals of G are projective.* *

PROOF. The theorem is trivial if G is elementary abelian. We suppose that G is of order greater than p^2 and that the theorem holds for all groups of smaller order than G. Since G has at least two subgroups of order p, and one of these may be taken to be in the centre, G has an elementary abelian subgroup X of order p^2. Let M be any maximal subgroup of G which contains X. Then all prime intervals of M are projective. Since G/Φ is elementary abelian of order at least p^2, and $M \supset \Phi$, all prime intervals of G/Φ are projective to all prime intervals of M. It is sufficient to prove that any prime interval, A/B of G is projective to an interval of G/M or of M. Take any composition series from G to 1 through M. By Zassenhaus's Lemma, A/B is projective to some factor of this composition series.

3. The First Canonicity Condition

Let f be an L-embedding of a p-group G in a group H of the same order. Let

$$c : A_1/B_1 \to A_2/B_2 \to \cdots \to A_1/B_1$$

be a closed chain of projectivities in G with A_i/B_i cyclic of order p. Then fB_i is normal in fA_i, fA_i/fB_i is cyclic of order p, and

$$\bar{c} : fA_1/fB_1 \to fA_2/fB_2 \to \cdots \to fA_1/fB_1$$

is a closed chain of projectivities in H. If $x, \bar{x}$ are any elements of A_1/B_1, fA_1/fB_1 respectively, then

$$\alpha(c)x = x^{r(c)}, \qquad \bar{\alpha}(\bar{c})\bar{x} = \bar{x}^{\bar{r}(\bar{c})}$$

where $r, \bar{r}$ are integers mod p, $(r, p) = (\bar{r}, p) = 1$ and $r, \bar{r}$ are independent of $x, \bar{x}$.

We say that the L-embedding f is 1-*canonical* if, for all closed chains c of projectivities on cycles of order p in G,

$$r(c) \equiv \bar{r}(\bar{c}) \pmod{p}.$$

We shall often find it more convenient to consider individual projectivities than closed chains. So we construct a system which will enable us to

* I am indebted to Dr. O. Tamaschke for a simplification of my original proof.

https://doi.org/10.1017/S1446788700026355 Published online by Cambridge University Press

deduce from its satisfying a condition for each projectivity, that the L-embedding under consideration is 1-canonical. For each prime interval A_i/B_i of G, we choose a generator a_i of A_i/B_i and a generator $\bar{a}_i$ of fA_i/fB_i. We call the set $(a_i, \bar{a}_i)$ a basis of f. The projectivity $A_i/B_i \to A_j/B_j$ is called a *regular projectivity* of the basis $(a_i, \bar{a}_i)$ if, in the isomorphisms $a_i \to a_j^r$, $\bar{a}_i \to \bar{a}_j^s$ defined by the projectivities $A_i/B_i \to A_j/B_j$, $fA_i/fB_i \to fA_j/fB_j$ respectively, $r \equiv s \pmod{p}$.

Clearly, if $A_1 \supset A_2 \supset A_3$ and any two of the projectivities $A_1/B_1 \to A_2/B_2$, $A_1/B_1 \to A_3/B_3$ and $A_2/B_2 \to A_3/B_3$ are regular, then so is the third. We shall refer to this as *"the three intervals rule"*.

The basis $(a_i, \bar{a}_i)$ of f is called *canonical* if every projectivity is regular. To prove a basis canonical, by the three intervals rule, it is clearly sufficient to prove that all prime projectivities are regular. If the L-embedding f has a canonical basis, then clearly f is 1-canonical. Conversely, if f is a 1-canonical embedding, then there exists a canonical basis of f, although in general, not all bases of f will be canonical.

The significance of the first canonicity condition may be seen from the following theorem.

THEOREM 3.1. *An L-embedding f of a p-group G in a group H of the same order can be extended to an L-embedding F of $G \times C$ in $H \times \bar{C}$ ($FX = fX$ for $X \subseteq G$) where C, $\bar{C}$ are cyclic of order p, if and only if f is 1-canonical.*

PROOF. (1) Suppose F is an extension. Let

$$c : A_1/B_1 \to A_2/B_2 \to \cdots \to A_1/B_1$$

be any closed chain of projectivities in G on prime intervals. We have to prove that $r(c) \equiv \bar{r}(\bar{c}) \pmod{p}$.

Since if c' is the chain $A_2/B_2 \to A_3/B_3 \to \cdots \to A_1/B_1 \to A_2/B_2$, $r(c) \equiv r(c')$ and $\bar{r}(\bar{c}) \equiv \bar{r}(\bar{c}')$, we need only consider the case $A_2 \supset A_1$. Further, we may assume that A_2 covers A_1, for if not, we can insert A_2'/B_2' such that $A_2 \supset A_2'$, A_2' covers A_1 and

$$c'' : A_1/B_1 \to A_2'/B_2' \to A_2/B_2 \to \cdots \to A_1/B_1$$

is a chain of projectivities in G with $r(c) \equiv r(c'')$ and $\bar{r}(\bar{c}) \equiv \bar{r}(\bar{c}'')$.

Take generators a, b, c of A_1/B_1, B_2/B_1 and $B_1 \times C/B_1$ respectively, and choose generators $\bar{a}, \bar{b}, \bar{c}$ of FA_1/FB_1, FB_2/FB_1, $F(B_1 \times C)/FB_1$ such that in the restriction of F to $A_2 \times C/B_1$,

$$F\{abc\} = \{\bar{a}\bar{b}\bar{c}\}.$$

Since $L((A_2 \times C)/B_1)$ and $L(F(A_2 \times C)/FB_1)$ are plane projective geometries over $GF(p)$, mappings of $L((A_2 \times C)/B_1)$ onto $L(F(A_2 \times C)/FB_1)$ are linear and are determined by the images of the vertices of a triangle of reference and the image of the unit point. Therefore

$$F\{a^x b^y c^z\} = \{\bar{a}^x \bar{b}^y \bar{c}^z\}.$$

Consider the closed chain of projectivities

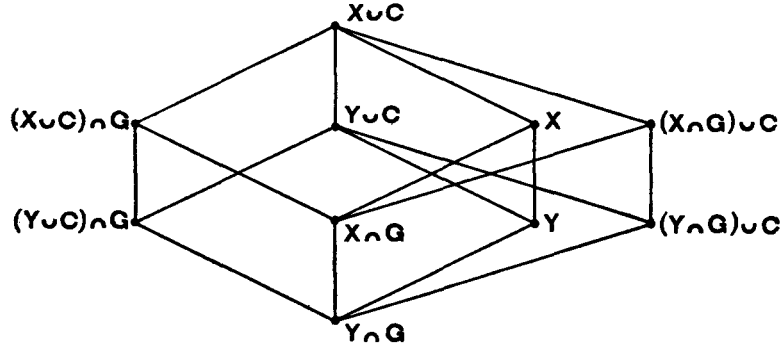
$$\gamma : A_1 \times C/B_1 \to A_2 \times C/B_2 \to \cdots \to A_1 \times C/B_1.$$

This induces in $A_1 \times C/B_1$ the automorphism $\alpha(\gamma)a^x c^z = a^{xr(c)} c^z$.
$\bar{\gamma}$ induces in $F(A_1 \times C)/FB_1$ the automorphism $\bar{\alpha}(\bar{\gamma})\bar{a}^x \bar{c}^z = \bar{a}^{x\bar{r}(\bar{c})} \bar{c}^z$. But $F\alpha(\gamma)\{a^x c^z\} = \bar{\alpha}(\bar{\gamma})F\{a^x c^z\}$. Therefore $\{\bar{a}^{xr(c)} \bar{c}^z\} = \{\bar{a}^{x\bar{r}(\bar{c})} \bar{c}^z\}$. Therefore $r(c) \equiv \bar{r}(\bar{c}) \pmod{p}$.

(2) Suppose f is 1-canonical. Take a canonical basis of f and generators $c, \bar{c}$ of $C, \bar{C}$.

For all $A \subseteq G$, define $FA = fA$, $F(A \cup C) = FA \cup \bar{C}$. Suppose X is a subgroup of $G \times C$ for which we have not yet defined FX. Then $X \cup C$ covers X covers $X \cap G$, $X \cap G$ is normal in $X \cup C$ and $(X \cup C)/(X \cap G)$ is elementary abelian of order p^2. $(X \cup C)/(X \cap G)$ is generated by the element $a \in (a_i, \bar{a}_i)$ corresponding to $((X \cup C) \cap G)/(X \cap G)$ and the coset $c' = c(X \cap G)$. Similarly $F(X \cup C)/F(X \cap G)$ is generated by the element $\bar{a} \in (a_i, \bar{a}_i)$ corresponding to $F((X \cup C) \cap G)/F(X \cap G)$ and the coset $\bar{c}' = \bar{c}F(X \cap G)$. If x is a generator of $X/(X \cap G)$, then $x = a^r c'^s$. Let $\bar{x} = \bar{a}^r \bar{c}'^s$ and define FX by $FX/F(X \cap G) = \{\bar{x}\}$.

To prove that F so defined is an L-embedding of $G \times C$ in $H \times \bar{C}$, we have only to prove that, if Y is a subgroup of $G \times C$, $G \not\equiv Y \not\equiv C$ and X covers Y, then FX covers FY.



Since $(X \cup C) \cap G$, $Y \cup C$, X are maximal subgroups of $X \cup C$, $((X \cup C) \cap G) \cap (Y \cup C) \cap X = Y \cap G$ is normal in $X \cup C$ and $(X \cup C)/(Y \cap G)$ is elementary abelian of order p^3. Take generators u, v, w of $((Y \cup C) \cap G)/(Y \cap G)$, $(X \cap G)/(Y \cap G)$, $((Y \cap G) \cup C)/(Y \cap G)$ respectively, $u, v \in (a_i, \bar{a}_i)$, $w = c(Y \cap G)$ and generators $\bar{u}, \bar{v}, \bar{w}$ of $F((Y \cup C) \cap G)/F(Y \cap G)$, $F(X \cap G)/F(Y \cap G)$, $F((Y \cap G) \cup C)/F(Y \cap G)$ respectively, with $\bar{u}, \bar{v} \in (a_i, \bar{a}_i)$ and $\bar{w} = \bar{c}F(Y \cap G)$.

In the isomorphism φ of $(X \cup C)/(Y \cap G)$ onto $F(X \cup C)/F(Y \cap G)$ defined by $\varphi u^i v^j w^k = \bar{u}^i \bar{v}^j \bar{w}^k$,

https://doi.org/10.1017/S1446788700026355 Published online by Cambridge University Press

$$\begin{aligned}\varphi X &= \varphi\{a^r c'^s, v\}\\ &= \varphi\{u^{nr} w^s, v\} \quad \text{where } n \text{ is given by } a \to u^n \text{ in the projectivity}\\ &\qquad ((X \cup C) \cap G)/(X \cap G) \to ((Y \cup C) \cap G)/(Y \cap G)\\ &= \{\bar{u}^{nr} \bar{w}^s, \bar{v}\}\\ &= \{\bar{a}^r \bar{c}'^s, \bar{v}\} \quad \text{since } ((X \cup C) \cap G)/(X \cap G) \to ((Y \cup C) \cap G)/(Y \cap G)\\ &\qquad \text{is a regular projectivity of } (a_i, \bar{a}_i)\\ &= FX.\end{aligned}$$

Trivially $\varphi Y = FY$ and therefore FX covers FY.

We call the extension constructed in the above manner, the standard extension of f. We now show that, except in some trivial exceptional cases, the standard extension is the only extension.

THEOREM 3.2. *Let G be a p-group with more than one subgroup of order p, and let f be an L-embedding of G in a group H of the same order. Let C, $\bar{C}$ be cyclic groups of order p. If F_1 and F_2 are extensions of f to L-embeddings of $G \times C$ in $H \times \bar{C}$ such that $F_1(C) = F_2(C) = \bar{C}$, then $F_1 = \alpha F_2$ where α is an automorphism of $H \times \bar{C}$ of the form $\alpha h\bar{c} = h\bar{c}^r$ for all $h \in H$, $\bar{c} \in C$ where r is an integer independent of $h, \bar{c}$ with $(r, p) = 1$.*

PROOF. (1) If for some X, $G \not\supseteq X \not\supseteq C$, $F_1 X = F_2 X$, then F_1 and F_2 coincide on $(X \cup C)/(X \cap G)$. This is true because $((X \cup C) \cap G)/(X \cap G)$ is projective in G to some other interval of G, and therefore there exist X', X'' such that $X' \supseteq X \supseteq X''$ and $(X' \cup C)/(X'' \cap G)$ is elementary abelian of order p^3. A mapping of $L((X' \cup C)/(X'' \cap G))$ onto

$$L(F_1(X' \cup C)/F_1(X'' \cap G)) = L(F_2(X' \cup C)/F_2(X'' \cap G))$$

must be linear and hence the mapping of $L((X \cup C)/(X \cap G))$ is determined by the images of the three points X, $(X \cup C) \cap G$, $(X \cap G) \cup C$.

(2) If for some $X \subseteq G \times C$, $G \not\supseteq X \not\supseteq C$, F_1 and F_2 coincide on $(X \cup C)/(X \cap G)$, then $F_1 = F_2$. This is because, by Theorem 2.1, for any $Y \subseteq G \times C$, $G \not\supseteq Y \not\supseteq C$, there exists a chain of projectivities

$$(X \cup C)/(X \cap G) \to (X_1 \cup C)/(X_1 \cap G) \to \cdots \to (Y \cup C)/(Y \cap G)$$

which determines uniquely the mapping of $L((Y \cup C)/(Y \cap G))$ from the mapping of $L((X \cup C)/(X \cap G))$.

(3) Let $g \in G$ be an element of order p and let $\bar{g}$ be a generator of $f\{g\}$. Let c, $\bar{c}$ be generators of C, $\bar{C}$ respectively. Then for some m, n, $F_1\{gc\} = \{\bar{g}\bar{c}^m\}$ and $F_2\{gc\} = \{\bar{g}\bar{c}^n\}$. If α is the automorphism of $H \times \bar{C}$: $\alpha h\bar{c}^k = h\bar{c}^{rk}$ where h is any element of H and $rn \equiv m \pmod{p}$, then $F_1\{gc\} = \alpha F_2\{gc\}$ and, by (1) and (2), $F_1 = \alpha F_2$.

When G is a group with only one subgroup of order p, this subgroup is not projective to any other prime interval of G, and consequently the mapping of the lattice of its direct product with C need not be linear and can be con-

https://doi.org/10.1017/S1446788700026355 Published online by Cambridge University Press

structed independently of the construction of the mapping of the rest of the lattice of $G \times C$. This situation arises only when G is cyclic of odd prime order as an L-embedding of an elementary abelian group of order 4 is determined by the images of two subgroups of order 2.

THEOREM 3.3. *The standard extension F of a* 1*-canonical L-embedding f of a p-group G in a group H of the same order to an L-embedding of $G \times C$ in $H \times \bar{C}$, where $C, \bar{C}$ are cyclic of order p, is* 1*-canonical.*

PROOF. We extend the canonical basis $(a_i, \bar{a}_i)$ of f used in the construction of F to a canonical basis of F. Let $c, \bar{c}$ be the generators of $C, \bar{C}$ used in the construction of F. For every $A \subsetneqq G$, take as the basis elements for $(A \cup C)/A$, the cosets cA, $\bar{c}FA$. If A covers B and $a, \bar{a}$ are the basis elements for A/B, take $a(B \cup C)$, $\bar{a}F(B \cup C)$ as the basis elements for $(A \cup C)/(B \cup C)$. For every $X \subset G \times C$, $G \not\ni X \not\ni C$, take as basis elements for $X/(X \cap G)$, x and $\bar{x}$ as defined in the construction of FX. For $(X \cup C)/X$, take as basis elements cX, $\bar{c}FX$. If X covers Y, $Y \not\subseteq G$, then take vY, $\bar{v}FY$ as the basis elements for X/Y, where $v, \bar{v}$ are elements of $(a_i, \bar{a}_i)$ for $(X \cap G)/(Y \cap G)$.

Clearly, all projectivities not involving a subgroup X, $G \not\ni X \not\ni C$ are regular. Since for every such X, there exists an isomorphism of $(X \cup C)/(X \cap G)$ onto $F(X \cup C)/F(X \cap G)$ which maps basis elements onto corresponding basis elements, all projectivities within an interval $(X \cup C)/(X \cap G)$ are regular. If X covers Y, $Y \not\subseteq G$, then there exists an isomorphism (given in the proof of the existence of F) of $(X \cup C)/(Y \cap G)$ onto $F(X \cup C)/F(Y \cap G)$ which maps basis elements onto corresponding basis elements. Hence all projectivities within $(X \cup C)/(Y \cap G)$ are regular. The only remaining prime projectivities are of the form $X/Y \to X'/Y'$, where $X' \not\ni C$, $Y' \not\subseteq G$. Suppose X covers X'. Then $X \cup C \supset X' \cup C \supset X'$ and $(X \cup C)/(Y \cup C) \to (X' \cup C)/(Y' \cup C)$ and $(X' \cup C)/(Y' \cup C) \to X'/Y'$ are regular. Therefore, by the three intervals rule, $(X \cup C)/(Y \cup C) \to X'/Y'$ is regular. But $X \cup C \supset X \supset X'$ and $(X \cup C)/(Y \cup C) \to X/Y$ is regular. By the three intervals rule, $X/Y \to X'/Y'$ is regular. Hence all prime projectivities are regular and F is therefore 1-canonical.

4. Two Generator Groups

LEMMA 4.1. *Let $(a_i, \bar{a}_i)$ be a basis of an L-embedding f of a p-group G in a group H of the same order. Suppose that, for G/Φ and for each maximal subgroup of G, $(a_i, \bar{a}_i)$ gives a canonical basis for the corresponding restriction of f. Then f is* 1*-canonical and $(a_i, \bar{a}_i)$ is a canonical basis of f.*

PROOF. Consider a prime projectivity $A_1/B_1 \to A_2/B_2$ of a prime interval A_1/B_1 of G. We may assume A_1 covers A_2. Either (1) there exists a maximal subgroup M of G with $M \supseteq A_1$ and the projectivity is regular since the

https://doi.org/10.1017/S1446788700026355 Published online by Cambridge University Press

basis is canonical for the restriction of f to M, or (2) $A_1 = G$ and A_2, B_1 are maximal subgroups of G. Then $B_2 = A_2 \cap B_1 \supseteq \Phi$ and the projectivity is regular since the basis is canonical for the restriction of f to G/Φ. Therefore all prime projectivities are regular and $(a_i, \bar{a}_i)$ is a canonical basis of f.

THEOREM 4.2. *Let G be a p-group all of whose subgroups are groups of at most two generators, and let H be an elementary abelian group of the same order as G. Let K and $\bar{K}$ be subgroups of the same order of G and H respectively, and let f be a 1-canonical L-embedding of K in $\bar{K}$. Then there exists a 1-canonical extension F of f to an L-embedding of G in H.*

PROOF. We may assume that K is a maximal subgroup of G. The theorem is trivial if G is of order p^2. We assume that, for groups of smaller order than G, an L-embedding of a maximal subgroup with a given canonical basis can be extended to an L-embedding of the group such that the given basis can be extended to a canonical basis of the extended L-embedding with prescribed basis elements for the factor group of the maximal subgroup.

Since $G/\Phi(G)$ is of order p^2, we can define F on $G/\Phi(G)$ and the elements of a canonical basis of F on $G/\Phi(G)$ having as the basis elements for $K/\Phi(G)$ the elements of the given basis, and any arbitrarily assigned basis elements for G/K. Since $\Phi(G)$ is a maximal subgroup of each of the maximal subgroups of G, and a subgroup of G not contained in $\Phi(G)$ is contained in only one maximal subgroup of G, we may apply the induction hypothesis to the maximal subgroups of G, defining F and the basis elements independently for each maximal subgroup. By Lemma 4.1, the L-embedding so constructed is 1-canonical and the basis constructed is canonical.

COROLLARY 4.3. *If G is a p-group with at most one proper subgroup of more than two generators, then G has a 1-canonical L-embedding in the elementary abelian group of the same order.*

PROOF. (1) Suppose G is a group of three generators, all of whose proper subgroups are of at most two generators. Then a subgroup of G not containing and not contained in $\Phi(G)$ is contained in exactly one subgroup of G of index p^2. Hence a 1-canonical L-embedding of a maximal subgroup M of G can be extended to the elementary abelian group $G/\Phi(G)$ with elements of canonical bases of the embeddings of M and $G/\Phi(G)$ coinciding for the common intervals, and the procedure of the proof of theorem 4.1 may be applied independently to the remaining subgroups of index p^2.

(2) Suppose G has a proper subgroup K of three generators. We may assume that this subgroup is a maximal subgroup. By (1) it has a 1-canonical L-embedding. As before, we can extend this to $G/\Phi(G)$ and apply the procedure used above to the subgroups which cover $\Phi(G)$, since every $A \subset G$, $A \not\subseteq K$, $A \not\supseteq \Phi(G)$ is contained in exactly one subgroup of G which covers $\Phi(G)$.

COROLLARY 4.4. *If G is an abelian p-group of two generators, then G has a 1-canonical L-embedding in the elementary abelian group.*

5. The nth Canonicity Condition ($n > 1$)

Let f be an L-embedding of a p-group G in the elementary abelian group $\bar{G}$ of the same order. We say that f is *n-canonical* ($n > 1$) if, for all closed chains c of projectivities in G on cyclic factors of order p^n, $\alpha(c) = 1$ if and only if $\bar{\alpha}(\bar{c}) = \bar{1}$ where 1, $\bar{1}$ are the identity automorphisms of the corresponding factors.

Throughout this section, G shall denote a p-group and $\bar{G}$ the elementary abelian group of the same order. C shall denote a cyclic group of order p^n and $\bar{C}_1, \cdots, \bar{C}_n$ cyclic groups of order p. If A is a group, we denote by A^r the group generated by the rth powers of the elements of A. We consider the problem of extending an L-embedding f of G in $\bar{G}$ to an L-embedding of $G \times C$ in $\bar{G} \times \bar{C}_1 \times \cdots \times \bar{C}_n$.

LEMMA 5.1. *If $G \times C \supset X$, $G \times C^{p} \not\supseteq X \not\supseteq C^{p^{n-1}}$, then $X \cap G$ is normal in $X \cup C$ and $(X \cup C)/(X \cap G)$ is abelian of type (n, n).*

The proof is obvious.

LEMMA 5.2. *Suppose FX is defined for all $X \subseteqq G \times C^{p}$ and for all $X \supseteqq C^{p^{n-1}}$ such that F defines an L-embedding of $G \times C^{p}$ in $\bar{G} \times \bar{C}_1 \times \cdots \times \bar{C}_{n-1}$ and of $(G \times C)/C^{p^{n-1}}$ in $(\bar{G} \times \bar{C}_1 \times \cdots \times \bar{C}_n)/\bar{C}_1$. Then F can be extended to an L-embedding of $G \times C$ in $\bar{G} \times \bar{C}_1 \times \cdots \times \bar{C}_n$ if and only if the following condition holds:*

for subgroups X such that $G \times C^{p} \not\supseteq X \not\supseteq C^{p^{n-1}}$ and for closed chains of projectivities

$\gamma : (X \cup C)/(X \cap G) \to (X_1 \cup C)/(X_1 \cap G) \to \cdots \to (X \cup C)/(X \cap G)$, *$\gamma$ induces the identity lattice automorphism in $(X \cup C^{p^{n-1}})/(X \cap (G \times C^{p}))$ if and only if $\bar{\gamma}$ induces the identity lattice automorphism in $F(X \cup C^{p^{n-1}})/F(X \cap (G \times C^{p}))$.*

PROOF. Let $\lambda(\gamma)$, $\bar{\lambda}(\bar{\gamma})$ be the lattice automorphisms induced in $(X \cup C^{p^{n-1}})/(X \cap (G \times C^{p}))$ and $F(X \cup C^{p^{n-1}})/F(X \cap (G \times C^{p}))$ by γ and $\bar{\gamma}$ respectively. If FX for any one subgroup X, $G \times C^{p} \not\supseteq X \not\supseteq C^{p^{n-1}}$, is chosen arbitrarily from the subgroups of $F(X \cup C^{p^{n-1}})/F(X \cap (G \times C^{p}))$ not already images under F, the definition of F may be extended by projectivities. F can be extended to an L-embedding of $G \times C$ if and only if this procedure does not lead to contradictory definitions of F for any subgroup. Thus F can be extended to an L-embedding of $G \times C$ if and only if the correspondence $\lambda(\gamma) \leftrightarrow \bar{\lambda}(\bar{\gamma})$ between the lattice automorphisms induced in $(X \cup C^{p^{n-1}})/(X \cap (G \times C^{p}))$ and $F(X \cup C^{p^{n-1}})/F(X \cap (G \times C^{p}))$ by closed chains of projectivities γ, $\bar{\gamma}$ of the above form is one-to-one. The condition

that the correspondence be one-to-one is that $\lambda(\gamma)$ be the identity if and only if $\bar{\lambda}(\bar{\gamma})$ is the identity.

LEMMA 5.3. *In the notation of Lemma* 5.2, γ *induces the identity lattice automorphism in* $(X \cup C^{p^{n-1}})/(X \cap (G \times C^p))$ *if and only if* γ *induces the identity automorphism in* $((X \cup C) \cap G)/(X \cap G)$.

PROOF. Let $((X \cup C) \cap G)/(X \cap G) = \{a\}$, $((X \cup G) \cup C)/(X \cap G) = \{c\}$ and $X/(X \cap G) = \{x\}$. Then a and c generate $(X \cup C)/(X \cap G)$ which is abelian of type (n, n). The generator x of $X/(X \cap G)$ may be chosen such that $x = a^k c$, $p \nmid k$. Let

$$\gamma : (X \cup C)/(X \cap G) \to (X_1 \cup C)/(X_1 \cap G) \to \cdots \to (X \cup C)/(X \cap G)$$

be any closed chain of projectivities on factors $(X_i \cup C)/(X_i \cap G)$ with $G \times C^p \not\ni X_i \not\ni C^{p^{n-1}}$ mapping $X \cup C^{p^{n-1}}$ and $X \cap (G \times C^p)$ onto themselves. Then $\alpha(\gamma)c = c$ and $\alpha(\gamma)a = a^s$, $p \nmid s$. $\alpha(\gamma)\{a^k c\} = \{a^{sk} c\}$. Therefore γ maps X onto itself if and only if $s \equiv 1 \pmod{p^n}$, which proves the lemma.

LEMMA 5.4. *In the notation of Lemma* 5.2, $\bar{\gamma}$ *induces the identity lattice automorphism in* $F(X \cup C^{p^{n-1}})/F(X \cap (G \times C^p))$ *if and only if* $\bar{\gamma}$ *induces the identity automorphism in* $F((X \cup C) \cap G)/F(X \cap G)$.

PROOF. Choose a basis $e_1, \cdots, e_{2n}$ of $F(X \cup C)/F(X \cap G)$ such that

$$F((X \cap G) \cup C^{p^{n-r}}) = \{e_1, \cdots, e_r\}$$

$$F((X \cup C^{p^{n-r}}) \cap G) = \{e_{n+1}, \cdots, e_{n+r}\}$$

and

$$F(X^{p^{n-r}} \cup (X \cap G)) = \{e_1 + e_{n+1}, \cdots, e_r + e_{n+r}\}.$$

This may be done however FX is defined. For any γ, $\bar{\alpha}(\bar{\gamma})$ is given by a matrix of the form

$$M = \left[\begin{array}{c|c} I & O \\ \hline O & N \end{array}\right]$$

where the submatrices are $n \times n$, since $\bar{\alpha}(\bar{\gamma})$ is the identity on $F((X \cap G) \cup C)/F(X \cap G)$ and maps $F((X \cup C) \cap G)/F(X \cap G)$ onto itself.

Let N_r be the submatrix of N consisting of the elements in the first r rows and columns of N. Clearly, if $N = I$, then $\bar{\gamma}$ induces the identity lattice automorphism in $F(X \cup C^{p^{n-1}})/F(X \cap (G \times C^p))$. Suppose $\bar{\gamma}$ induces the identity lattice automorphism in $F(X \cup C^{p^{n-1}})/F(X \cap (G \times C^p))$. We have to prove that $N = I$.

Since M maps $\{e_1\}$, $\{e_{n+1}\}$, $\{e_1 + e_{n+1}\}$ onto themselves, it follows that $N_1 = I$. We use induction over r. Suppose $N_r = I$.

Since $\{e_{n+1}, \cdots, e_{n+r}\}$ maps into itself,

https://doi.org/10.1017/S1446788700026355 Published online by Cambridge University Press

$$N_{r+1} = \left[\begin{array}{c|c} I & \begin{matrix} a_1 \\ \vdots \\ a_r \end{matrix} \\ \hline 0 \cdots 0 & a_{r+1} \end{array}\right].$$

$$M(e_{r+1} + e_{n+r+1}) = e_{r+1} + a_1 e_{n+1} + \cdots + a_{r+1} e_{n+r+1}$$
$$\equiv \lambda(e_{r+1} + e_{n+r+1}) \bmod \{e_1 + e_{n+1}, \cdots, e_r + e_{n+r}\}.$$

Therefore $\lambda = 1$, $a_1 = a_2 = \cdots = a_r = 0$ and $a_{r+1} = 1$ which proves the lemma.

LEMMA 5.5. *Suppose FX is defined for all $X \subseteq G \times C^{p^n}$ and for all $X \supseteq C^{p^{n-1}}$ such that F defines an L-embedding of $G \times C^{p^n}$ in $\bar{G} \times \bar{C}_1 \times \cdots \times \bar{C}_{n-1}$ and of $(G \times C)/C^{p^{n-1}}$ in $(\bar{G} \times \bar{C}_1 \times \cdots \times \bar{C}_n)/\bar{C}_1$. Let f be the restriction of F to G. Then F can be extended to an L-embedding of $G \times C$ in $\bar{G} \times \bar{C}_1 \times \cdots \times \bar{C}_n$ if and only if f is n-canonical, $n \geqq 1$.*

PROOF. The case $n = 1$ has been proved in Theorem 3.1. For $n > 1$, the result follows from Lemmas 5.2, 5.3, and 5.4.

THEOREM 5.6. *An L-embedding f of a p-group G in the elementary abelian group $\bar{G}$ of the same order can be extended to an L-embedding F of $G \times C$ in $\bar{G} \times \bar{C}_1 \times \cdots \times \bar{C}_n$, where C is cyclic of order p^n and $\bar{C}_i$ are of order p, if and only if f is 1-, 2-, $\cdots$, n-canonical.*

PROOF. If F exists, then by Lemma 5.5, f is 1-, 2-, $\cdots$, n-canonical. Suppose f is 1-, 2-, $\cdots$, n-canonical. We have to prove that there exists an extension F.

Let φ_i be the isomorphism of $G \times C^{p^{n-i+1}}$ onto $(G \times C^{p^{n-i}})/C^{p^{n-1}}$ in which the element $gc^{\alpha p^{n-i+1}}$ of $G \times C^{p^{n-i+1}}$ maps onto the coset $gc^{\alpha p^{n-i}} C^{p^{n-1}}$ where g is any element of G and c is some fixed generator of C. Clearly, the restriction of φ_{i+1} to $G \times C^{p^{n-i+1}}$ is φ_i.

Let $\bar{\varphi}_i$ be the isomorphism of $\bar{G} \times \bar{C}_1 \times \cdots \times \bar{C}_{i-1}$ onto $(\bar{G} \times \bar{C}_1 \times \cdots \times \bar{C}_i)/\bar{C}_1$ in which the element $\bar{g}\bar{c}_1^{\alpha_1}\bar{c}_2^{\alpha_2} \cdots \bar{c}_{i-1}^{\alpha_{i-1}}$ maps into the coset $\bar{g}\bar{c}_2^{\alpha_1}\bar{c}_3^{\alpha_2} \cdots \bar{c}_i^{\alpha_{i-1}} \bar{C}_1$ where $\bar{c}_1, \cdots, \bar{c}_n$ are a fixed set of generators of $\bar{C}_1, \cdots, \bar{C}_n$, and $\bar{g}$ is any element of $\bar{G}$. Clearly, the restriction of $\bar{\varphi}_{i+1}$ to $\bar{G} \times \bar{C}_1 \times \cdots \times \bar{C}_{i-1}$ is $\bar{\varphi}_i$.

By induction over n, we prove that there exist extensions $F_1, F_2, \cdots, F_n$ of $f = F_0$ to $G \times C^{p^{n-1}}, G \times C^{p^{n-2}}, \cdots, G \times C$ respectively such that

(1) F_i is an extension of F_{i-1}

(2) for all X such that $G \times C^{p^{n-i}} \supseteq X \supseteq C^{p^{n-1}}$,

$$F_i X = \bar{\varphi}_i F_i \varphi_i^{-1} X.$$

By Theorem 3.1, this holds for $n = 1$ since condition (2) is trivially satisfied by any F satisfying condition (1).

Suppose $F_1, \cdots, F_{n-1}$ exist satisfying these conditions. Define

https://doi.org/10.1017/S1446788700026355 Published online by Cambridge University Press

$F_nX = F_{n-1}X$ for all $X \subseteqq G \times C^{p}$ and $F_nX = \bar{\varphi}_n F_{n-1}\varphi_n^{-1}X$ for all $X \supseteqq C^{p^{n-1}}$. This is consistent since for $G \times C^{p} \supseteqq X \supseteqq C^{p^{n-1}}$,

$$\begin{aligned} F_{n-1}X &= \bar{\varphi}_{n-1}F_{n-1}\varphi_{n-1}^{-1}X \qquad \text{by (2)} \\ &= \bar{\varphi}_n F_{n-1}\varphi_n^{-1}X. \end{aligned}$$

By Lemma 5.5, F_nX can be defined for $G \times C^{p} \not\supseteqq X \not\subseteqq C^{p^{n-1}}$ such that F_n is an embedding of $G \times C$. F_n clearly satisfies condition (1). By the definition of F_n for $X \supseteqq C^{p^{n-1}}$

$$\begin{aligned} F_nX &= \bar{\varphi}_n F_{n-1}\varphi_n^{-1}X \\ &= \bar{\varphi}_n F_n \varphi_n^{-1}X \end{aligned}$$

and condition (2) is satisfied. This completes the proof of the theorem.

6. Abelian Groups

If G is an abelian p-group, then G has cyclic subgroups $C_1, \cdots, C_n$ such that $G = C_1 \times C_2 \times \cdots \times C_n$. Let $|C_i| = p^{\lambda_i}$. Then the λ_i are uniquely determined (up to order) by G. We may assume $\lambda_1 \geqq \lambda_2 \geqq \cdots \geqq \lambda_n$. We say that G is a group of type $(\lambda_1, \lambda_2, \cdots, \lambda_n)$.

LEMMA 6.1. *Let G be an abelian p-group of type $(\lambda_1, \lambda_2, \cdots, \lambda_n)$ with $\lambda_3 \leqq 1$. Then G has an L-embedding in the elementary abelian group.*

PROOF. G is the direct product of a group of type (λ_1, λ_2) and of cycles of order p. By Corollary 4.4, the group of type (λ_1, λ_2) has a 1-canonical L-embedding, which, by Theorems 3.1 and 3.3, can be extended to an L-embedding of G.

LEMMA 6.2. *Let G be an abelian p-group of type $(\lambda_1, \lambda_2, \cdots, \lambda_n)$ with $\lambda_2 \leqq 2$. Then G has an L-embedding in the elementary abelian group.*

PROOF. By Theorem 5.6, it is sufficient to prove the existence for the case $\lambda_1 = \lambda_2 = \cdots = \lambda_n = 2$.

There exists an integer $\alpha \pmod{p^2}$ such that $a \to a^{\alpha}$ is an automorphism of order $p-1$ of the cyclic group $\{a\}$ of order p^2. Let θ be an integer $(\bmod p)$ with $\alpha \equiv \theta \pmod{p}$. We define the symbol $*$ by $\alpha^* = 0$, $\theta^* = 0$. Then for any x, there exist r, s with $a^x = a^{\alpha^r + sp}$ where $r = *, 0, 1, \cdots, p-2$ and $s = 0, 1, \cdots, p-1$.

We construct an L-embedding of $G = \{a_1, \cdots, a_n\}$ of type $(2, 2, \cdots, 2)$ in the elementary abelian group (written additively) with basis $x_1, y_1, x_2, y_2, \cdots, x_n, y_n$. Every element $g \in G$ can be written in the form

$$g = \prod_{i=1}^{n} a_i^{\alpha^{r_i} + s_i p}.$$

Put $$f\{g\} = \left\{ \sum_{i=1}^{n} \theta^{r_i} x_i, \ \sum_{i=1}^{n} (s_i x_i + \theta^{r_i} y_i) \right\} \qquad \text{for } g = \prod_{i=1}^{n} a_i^{\alpha^{r_i} + s_i p}$$

$$f\{g_1, \cdots, g_k\} = f\{g_1\} \cup \cdots \cup f\{g_k\}.$$

https://doi.org/10.1017/S1446788700026355 Published online by Cambridge University Press

We have to prove that f so defined is one-to-one and that

$$fA \supset fB \text{ if and only if } A \supset B.$$

(a) $f\{g\} \subseteqq f\{g_1, \cdots, g_k\}$ if and only if $g \in \{g_1, \cdots, g_k\}$.

PROOF. Put

$$g_i = \prod_{j=1}^{n} a_j^{\alpha^{r_{ij}} + s_{ij}p}, \quad g = \prod_{j=1}^{n} a_j^{\alpha^{r_j} + s_j p}.$$

$g \in \{g_1, \cdots, g_k\}$ if and only if there exist u_i, v_i with

$$g = \prod_{i=1}^{k} g_1^{\alpha^{u_i} + v_i p},$$

that is, if and only if there exist u_i, v_i with

$$\begin{aligned} \alpha^{r_j} + s_j p &= \sum_{i=1}^{k} (\alpha^{r_{ij}} + s_{ij}p)(\alpha^{u_i} + v_i p) \\ &= \sum_{i=1}^{k} (\alpha^{u_i}\alpha^{r_{ij}} + p(\alpha^{u_i} s_{ij} + v_i \alpha^{r_{ij}})) \pmod{p^2} \quad j = 1, 2, \cdots, n. \end{aligned}$$

This is equivalent to

$$\theta^{r_j} = \sum_{i=1}^{k} \theta^{u_i}\theta^{r_{ij}} \pmod{p} \qquad j = 1, 2, \cdots, n$$

$$s_j = \sum_{i=1}^{k} (\theta^{u_i} s_{ij} + v_i \theta^{r_{ij}}) \pmod{p} \qquad j = 1, 2, \cdots, n.$$

This holds if and only if

$$\sum_{j=1}^{n} \theta^{r_j} x_j = \sum_{i=1}^{k} \theta^{u_i} \sum_{j=1}^{n} \theta^{r_{ij}} x_j$$

$$\sum_{j=1}^{n} (s_j x_j + \theta^{r_j} y_j) = \sum_{i=1}^{k} \theta^{u_i} \sum_{j=1}^{n} (s_{ij} x_j + \theta^{r_{ij}} y_j) + \sum_{i=1}^{k} v_i \sum_{j=1}^{n} \theta^{r_{ij}} x_j.$$

This is the condition that $f\{g\} \subseteqq f\{g_1, \cdots, g_k\}$.

(b) From (a), it follows that $f\{g\}$ is independent of the choice of the generator g of $\{g\}$.

(c) From (a), it follows that for all $A \subseteqq G$,

$$fA = \cup \{fX | X \text{ cyclic}, X \subseteqq A\}.$$

Therefore f is one-to-one and $fA \supset fB$ if and only if $A \supset B$.

THEOREM 6.3. *Let G be an abelian p-group of type $(\lambda_1, \lambda_2, \cdots, \lambda_n)$ with $\lambda_1 = \lambda_2 = \lambda_3 = 2$. Then G has a unique L-embedding in the elementary abelian group.*

PROOF. By Lemma 6.2, an L-embedding exists. Let f_1 and f_2 be L-embeddings of G in the elementary abelian group H. We have to prove that f_1

https://doi.org/10.1017/S1446788700026355 Published online by Cambridge University Press

and f_2 are equivalent. By Theorem 3.2, it is sufficient to consider the case $\lambda_1 = \lambda_2 = \cdots = \lambda_n = 2$.

Let $G = \{a_1, \cdots, a_n\}$. Since $n \geqq 3$, a basis $x_1, \cdots, x_n, y_1, \cdots, y_n$ of H can be chosen such that

$$\{x_i\} = f_1\{a_i^p\}$$
$$\{x_i, y_i\} = f_1\{a_i\}$$

and $a_i^p \to x_i$ is an isomorphism of $\{a_1^p, \cdots, a_n^p\}$ onto $\{x_1, \cdots, x_n\}$ inducing f_1 on $\{a_1^p, \cdots, a_n^p\}$, $a_i\{a_1^p, \cdots, a_n^p\} \to y_i + \{x_1, \cdots, x_n\}$ is an isomorphism of $G/\Phi(G)$ onto $H/f_1\Phi(G)$ inducing f_1 on $G/\Phi(G)$. Then $f_1\{a_1 a_2 \cdots a_n\} = \{(x_1 + x_2 + \cdots + x_n), \ (y_1 + y_2 + \cdots + y_n + \alpha_1 x_1 + \cdots + \alpha_n x_n)\}$ for some $\alpha_1, \cdots, \alpha_n$. We can choose $y_1, \cdots, y_n$ such that $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$ since we can replace y_i by $y_i + \alpha_i x_i$.

Similarly, we can choose a basis $x_1', \cdots, x_n', y_1', \cdots, y_n'$ such that

$$f_2\{a_i^p\} = \{x_i'\}$$
$$f_2\{a_i\} = \{x_i', y_i'\}$$
$$f_2\{a_1 a_2 \cdots a_n\} = \{(x_1' + x_2' + \cdots + x_n'), (y_1' + y_2' + \cdots + y_n')\}$$

and $a_i^p \to x_i'$ is an isomorphism inducing f_2 on $\{a_1^p, \cdots, a_n^p\}$, $a_i\{a_1^p, \cdots, a_n^p\} \to y_i' + \{x_1', \cdots, x_n'\}$ is an isomorphism inducing f_2 on $G/\Phi(G)$. Let β be the automorphism of H: $\beta x_i' = x_i$, $\beta y_i' = y_i$. Then $\beta f_2 X = f_1 X$ for all $X \supseteq \Phi(G)$ and for $X = \{a_i\}$, $\{a_1 a_2 \cdots a_n\}$. Let $Z \subset G$ be any subgroup such that $Z \not\supseteq \Phi(G)$, $Z \not\subseteq \Phi(G)$. Then

$$\Phi(Z \cup \Phi(G)) = (Z \cup \Phi(G))^p = Z^p \cup (\Phi(G))^p = Z^p \subset G^p = \Phi(G).$$

Therefore there exist X, Y such that $X \supset \Phi(G) \supset Y$, $X \supset Z \supset Y$ and X/Y is elementary abelian. Thus βf_2 maps $L(X/Y)$ onto $f_1 L(X/Y)$ and there exists Z' such that $\beta f_2 Z = f_1 Z'$. Therefore for all $A \subseteq G$, there exists $B \subseteq G$ such that $\beta f_2 A = f_1 B$.

Since $\beta f_2 L(G) = f_1 L(G)$, we can form the mapping $f_1^{-1}\beta f_2$ of $L(G)$ onto itself. This is a lattice automorphism of G. But by a theorem of Baer ([1] page 35 Theorem 2), there exists an automorphism α of G inducing $f_1^{-1}\beta f_2$. Therefore $\beta f_2 = f_1 \alpha$. But from the construction of β,

$$\alpha\{a_i\} = \{a_i\}$$
$$\alpha\{a_1 a_2 \cdots a_n\} = \{a_1 a_2 \cdots a_n\}.$$

Hence α has the form $\alpha g = g^r$ for all $g \in G$, where r is independent of g. Therefore α induces the identity lattice automorphism and therefore $\beta f_2 = f_1$.

LEMMA 6.4. *There exists no L-embedding of an abelian group of type* (3, 3, 2) *in the elementary abelian group.*

PROOF. Let $G = \{a, b\}$, $a^{p^3} = b^{p^2} = 1$ be an abelian group of type (3, 2). Let f be any L-embedding of G in the elementary abelian group. It is suffi-

cient to prove that f is not 1- 2-, 3-canonical. Suppose f is 1- and 2-canonical. Take a basis e_1, e_2, e_3 of $f\{a\}$ such that

$$f\{a^{p^2}\} = \{e_1\}, \qquad f\{a^p\} = \{e_1, e_2\}.$$

Consider the chain of projectivities

$$c : \{a\} \to \{a, b\}/\{b\} \to \{ab\} \to \{a, b\}/\{a^p b\} \to \{a\}.$$

In this, $a \to a\{b\} \to ab \to ab\{a^p b\} \to a^{1-p}$. If A is the matrix of $\bar{\alpha}(\bar{c})$ then from the first canonicity condition, A is of the form

$$A = \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix}.$$

(a) Case $p > 2$. The automorphism $\alpha(c)$ is of order p^2.

$$\begin{aligned} A^p - I &= (A - I)^p && \text{since the matrix is over the field of } p \text{ elements} \\ &= 0 && \text{since } p \geqq 3 \text{ and } (A - I)^3 = 0. \end{aligned}$$

Put $\gamma = c^p$. Then $\alpha(\gamma) \neq 1$ but $\bar{\alpha}(\bar{\gamma}) = 1$ and f is not 3-canonical.

(b) Case $p = 2$. $\alpha(c)a = a^{-1}$.

Consider the restrictions c', c'' of c to chains of projectivities on factors of order 4, starting at $\{a^2\}$ and $\{a\}/\{a^4\}$. Let A', A'' be the matrices of $\bar{\alpha}(\bar{c}')$, $\bar{\alpha}(\bar{c}'')$ respectively. Then

$$A' = \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad A'' = \begin{bmatrix} 1 & z \\ 0 & 1 \end{bmatrix}.$$

$\alpha(c')a^2 = (a^2)^{-1}$ and $\alpha(c') \neq 1$. Therefore $x \neq 0$ since f is 2-canonical. $\alpha(c'')a\{a^4\} = a^{-1}\{a^4\}$ and $\alpha(c'') \neq 1$. Therefore $z \neq 0$. Therefore $A^2 \neq I$. Put $\gamma = c^2$. Then $\alpha(\gamma) = 1$ but $\bar{\alpha}(\bar{\gamma})$ has matrix $A^2 \neq I$ and f is not 3-canonical.

THEOREM 6.5. *There exists an L-embedding of the abelian p-group G in the elementary abelian group if and only if G has no subgroup of type* (3, 3, 2).

PROOF. If an L-embedding of G in the elementary abelian group exists, then G has no subgroup of type (3, 3, 2) by Lemma 6.4.

Suppose G has no subgroup of type (3, 3, 2). Let G be of type $(\lambda_1, \cdots, \lambda_r)$. Either $\lambda_3 \leqq 1$ and G has an L-embedding in the elementary abelian group by Lemma 6.1, or $\lambda_2 \leqq 2$ and by Lemma 6.2 G has an L-embedding in the elementary abelian group.

For abelian p-groups with a subgroup of type (3, 3, 2), we have the stronger result:

THEOREM 6.6. *Let G and H be abelian groups of the same prime power order. Suppose G has a subgroup of type* (3, 3, 2) *and that f is an L-embedding of G in H. Then* $G \cong H$.

https://doi.org/10.1017/S1446788700026355 Published online by Cambridge University Press

PROOF. The result holds for G of type (3, 3, 2) since it cannot have an L-embedding in a group which is L-embeddable in the elementary abelian group.

Take a direct decomposition $G = X_1 \times X_2 \times \cdots \times X_n$ of G with X_i cyclic. It is sufficient to prove that fX_i is cyclic.

If X_i is of order p, then trivially fX_i is cyclic. If X_i is of order p^2 or p^3, then there exist subgroups $A \subseteqq X_j$, $B \subseteqq X_k$ (i, j, k distinct) such that $X_i \times A \times B$ is of type (3, 3, 2) and therefore fX_i is cyclic.

Suppose X_i is of order p^r, $r > 3$. We use induction over r. There exist $A \subseteqq X_j$, $B \subseteqq X_k$ (i, j, k distinct) such that $X_i \times A \times B$ is of type $(r, 3, 2)$. We assume that the theorem holds for groups of type $(r - 1, 3, 2)$, $r > 3$. $X_i^p \times A \times B$ and $(X_i \times A \times B)/X_i^{p^{r-1}}$ are of type $(r - 1, 3, 2)$ and therefore $f(X_i^p)$ and $fX_i/f(X_i^{p^{r-1}})$ are cyclic. But

$$\Phi(fX_i) \supseteqq \Phi(f(X_i^p)) \supseteqq f(X_i^{p^{r-1}}).$$

Therefore $fX_i/\Phi(fX_i)$ is cyclic. Hence fX_i is cyclic.

7. Non-Abelian Groups

Clearly, if a p-group G is lattice isomorphic to an abelian p-group A, then G has an L-embedding in the elementary abelian group if and only if A has. We use this to extend the result of Theorem 6.5 to p-groups with modular lattices of subgroups.

Iwasawa ([1], p. 15) in determining the structure of non-Hamiltonian modular p-groups, shows that such a group G has a basis $a_1, \cdots, a_k$. If a_i has order p^{λ_i}, $\lambda_1 \geqq \lambda_2 \geqq \cdots \geqq \lambda_k$, we say G is of type $(\lambda_1, \cdots, \lambda_k)$. By a theorem of Jones ([2], p. 554, Theorem 3.13), G is lattice isomorphic to an abelian p-group of the same type.

THEOREM 7.1. (a) *Let G be a non-Hamiltonian modular p-group. Then G has an L-embedding in the elementary abelian group of the same order if and only if G contains no subgroup of type* (3,3,2).

(b) *Let G be a Hamiltonian p-group. Then G has an L-embedding in the elementary abelian group of the same order.*

PROOF. (a) has already been proved. Suppose G is a Hamiltonian p-group. Then G is the direct product of a quaternion group of order 8 with an elementary abelian 2-group. By Theorems 4.2, 3.1, G has an L-embedding in the elementary abelian group of the same order.

Lazard ([3], p. 176, Theorem 4.6) has given a construction based on the Baker-Hausdorff formula which defines, for any p-group G such that all subgroups generated by three (not necessarily distinct) elements have class strictly less than p, an addition and Lie multiplication on the elements of G making G a Lie-ring $\mathscr{L}(G)$ with respect to this addition and Lie multiplication. In this construction, subgroups correspond to subrings, the element

$1 \in G$ corresponds to $0 \in \mathscr{L}(G)$ and $x^{p^r} = 1$ in G if and only if $p^r x = 0$ in $\mathscr{L}(G)$. We denote by $A(G)$ the additive group of $\mathscr{L}(G)$. Since G is regular, we can define the type invariants as done by P. Hall ([4], p. 79—81). When G is modular, these invariants coincide with those used above. Let $\Omega_\alpha(G) = \{x | x \in G, x^{p^\alpha} = 1\}$. Then $A(\Omega_\alpha(G)) = \Omega_\alpha(A(G))$. Hence G and $A(G)$ have the same invariants. If $X \subsetneqq G$, then $A(X) \subsetneqq A(G)$. Thus the mapping f defined by $fX = A(X)$ is an L-embedding of G in $A(G)$.* Hence we have

THEOREM 7.2. *Suppose G is a p-group of class less than p. Then G has an L-embedding in the abelian group with the same invariants.*

THEOREM 7.3. *Suppose G is a p-group of class less than p and with invariants $(\lambda_1, \cdots, \lambda_k)$, $\lambda_1 \geqq \lambda_2 \geqq \cdots \geqq \lambda_k$ satisfying either $\lambda_2 \leqq 2$ or $\lambda_3 \leqq 1$. Then G has an L-embedding in the elementary abelian group of the same order.*

Using these results, we can generalize Theorem 6.6.

THEOREM 7.4. *Let G be a modular p-group of order p^n, $p \geqq n$, and suppose that G has a subgroup of type (3, 3, 2). Suppose G has an L-embedding in the group H of the same order. Then $L(G) \cong L(H)$.*

PROOF. G, H have class at most $n - 1 < p$. Thus $A(G)$, $A(H)$ exist and G has an L-embedding in $A(H)$. But $L(G) \cong L(A(G))$. Therefore $A(G)$ has an L-embedding in $A(H)$. By Theorem 6.6, $A(G) \cong A(H)$. Therefore $A(H)$ has an L-embedding in H. Therefore $L(H) \cong L(A(H)) \cong L(G)$.

I should like to express my thanks to Dr. G. Higman and Dr. G. E. Wall for guiding my research, and to the C.S.I.R.O. and the University of Sydney for financial assistance.

References

[1] Suzuki, M., *Structure of a group and the structure of its lattice of subgroups.* (Springer, 1956).
[2] Jones, A. W., The lattice isomorphisms of certain finite groups, *Duke Math. J.* 12 (1945), 541—560.
[3] Lazard, M., Sur les groupes nilpotents et les anneaux de Lie, *Ann. Sc. de l'École Normale Supérieure* (1954), 101—190.
[4] Hall, P., A contribution to the theory of groups of prime-power order, *Proc. London Math. Soc.* (2) 36 (1933), 29—95.
[5] Wall, G. E., Some applications of the Eulerian functions of a finite group (submitted to this Journal).

Universität Tübingen
Germany

* For this result I am indebted to Dr. G. Higman.