J. Austral. Math. Soc. (*Series A*) **62** (1997), 259–278

LATTICE EMBEDDINGS OF ABELIAN PRIME POWER GROUPS

ROLAND SCHMIDT

(Received 10 January 1996; revised 29 July 1996)

Communicated by R. Howlett

Abstract

We solve the following problem which was posed by Barnes in 1962. For which abelian groups G and H of the same prime power order is it possible to embed the subgroup lattice of G in that of H? It follows from Barnes' results and a theorem of Herrmann and Huhn that if there exists such an embedding and G contains three independent elements of order p^2, then G and H are isomorphic. This reduces the problem to the case that G is the direct product of cyclic p-groups only two of which have order larger than p. We determine all groups H for which the desired embedding exists.

1991 *Mathematics subject classification* (*Amer. Math. Soc.*): primary 20D30; secondary 20K01.

Introduction

We want to solve the following problem. Given two abelian groups G and H of the same prime power order, when does there exist an embedding (that is, a monomorphism) of the subgroup lattice $L(G)$ of G in that of H?

This problem was studied and partly solved by Barnes [1] already in 1962. He showed that if H is elementary abelian, then $L(G)$ can be embedded in $L(H)$ if and only if G does not contain a subgroup of type (3,3,2). Recall that a finite abelian p-group G is a direct product of cyclic groups of order $p^{\lambda_1}, \ldots, p^{\lambda_r}$ where $\lambda_1 \geq \cdots \geq \lambda_r \geq 1$, and then the r-tuple $(\lambda_1, \ldots, \lambda_r)$ is called the *type* of G. In the general case, Barnes showed further that if G has a subgroup of this type and $L(G)$ is embedded in $L(H)$, then G and H are isomorphic; but he left the problem open for groups having no such subgroups.

Unfortunately, these results are not quite correct. They are inconsistent with a theorem of Herrmann and Huhn saying that a certain lattice law holds in the subgroup lattice of an elementary abelian p-group but not in that of an abelian p-group of type

(2,2,2) (see [2, Theorem 5]). As Barnes told me, this was realized in 1980 by Sheila Oates-Williams who also located and corrected his error: in the proof of Lemma 6.2 of his paper he uses an argument that a certain set of n equations modulo p^2 implies two sets of n equations modulo p which, however, is not the case.

It is not difficult to see that the theorem of Herrmann and Huhn has just the effect of replacing the group of type (3,3,2) in Barnes' results by the group of type (2,2,2). So we obtain the following theorems in which we call an embedding of $L(G)$ in $L(H)$ an *L-embedding* of G in H, for short.

THEOREM A. *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* $(2, 2, 2)$.

An easy consequence of this is

THEOREM B. *Let G and H be abelian groups of the same prime power order. Suppose G has a subgroup of type* $(2, 2, 2)$ *and that φ is an L-embedding of G in H. Then $X^\varphi \simeq X$ for every subgroup X of G; in particular, $H \simeq G$.*

This theorem reduces the general problem to groups of type $(\lambda_1, \ldots, \lambda_r)$ where $r \leq 2$ or $\lambda_3 = 1$. The subgroup lattice of a cyclic group of order p^n is a chain of length n and therefore can be embedded in $L(H)$ for any group H of order p^n. So we may assume that $r \geq 2$ and the following result completes the solution of our problem.

THEOREM C. *Let $n \geq k \geq 1$ and $r \geq 2$. Suppose that $G = A \times B \times C_3 \times \cdots \times C_r$ where A and B are cyclic of order p^n and p^k, respectively, and $|C_i| = p$ for $i = 3, \ldots, r$; it is understood that $G = A \times B$ if $r = 2$. Then G has an L-embedding in an abelian group H of the same order if and only if there exist subgroups U, V, W_i of H such that $H = U \times V \times W_3 \times \cdots \times W_r$, $|U| = p^n$, $|V| = p^k$, $|W_i| = p$ for $i = 3, \ldots, r$, and one of the following holds.*

(i) $k = 1$.

(ii) $k \geq 2$, $n = \lambda k + t$ *where* $\lambda \in \mathbb{N}$ *and* $0 \leq t < k$, *V is elementary abelian and U has type* $(\alpha_1, \ldots, \alpha_s)$ *where* $\alpha_1 \leq \lambda + 1$ *and* $\alpha_{t+1} \leq \lambda$.

(iii) $U \simeq G_{n,s}$ *and* $V \simeq G_{k,s}$ *for some integer s such that* $1 \leq s < k$.

Here, if $1 \leq s \leq m$, the group $G_{m,s}$ is defined as follows: write $m = \mu s + t$ with $\mu \in \mathbb{N}$ and $0 \leq t < s$; then μ, t are uniquely determined by m, s and we let $G_{m,s}$ be the abelian group of type $(\mu_1, \ldots, \mu_s)$ where $\mu_i = \mu$ for $i > t$ and $\mu_i = \mu + 1$ for $i \leq t$. Then $G_{m,s}$ is a group of order p^m with s generators; in particular, $G_{m,1}$ is the cyclic and $G_{m,m}$ the elementary abelian group of order p^m.

Since neither Barnes nor Oates-Williams published a corrected version of Barnes' results, we shall give short proofs of Theorems A and B in Section 1. The proof of

Theorem C will occupy Sections 2 and 3; crucial for this is the concept of a smooth group introduced in 2.1.

All groups considered are finite, the notation is standard (see [1, 4]), except that we write $A \cup B$ for the group generated by the subgroups A and B of the group X.

1. Barnes' results

In the whole paper, p is a prime and G and H are abelian p-groups of the same order. A *lattice embedding* (which we abbreviate to *L-embedding*) of G in H is an embedding of $L(G)$ in $L(H)$, and this is defined to be an injective mapping φ of $L(G)$ into $L(H)$ such that X^φ covers Y^φ for all $X, Y \in L(G)$ where X covers Y. Barnes shows [1, Corollary 1.3] that in our case (of abelian groups) this is equivalent to φ being a lattice monomorphism, that is, an injective map satisfying

$$(1) \quad (X \cup Y)^\varphi = X^\varphi \cup Y^\varphi \quad \text{and} \quad (X \cap Y)^\varphi = X^\varphi \cap Y^\varphi \quad \text{for all} \quad X, Y \in L(G).$$

We need the following lattice polynomials introduced by Herrmann and Huhn. For elements A, B, C, D of a lattice L, we define inductively

$$\begin{aligned} f_1(A, B, C, D) &= (A \cup B) \cap (C \cup D) \\ f_{n+1}(A, B, C, D) &= (((f_n(A, B, C, D) \cup f_1(A, C, B, D)) \cap (B \cup C)) \cup D) \\ &\quad \cap (A \cup B). \end{aligned}$$

LEMMA 1.1 (Herrmann and Huhn [2]). *Let $X = A \times B \times C$ with isomorphic abelian groups A, B, C. Suppose that $\mu : A \to B$ and $\nu : A \to C$ are isomorphisms and let $D = \{aa^\mu a^\nu \mid a \in A\}$. Then for all $n \in \mathbb{N}$,*

$$f_n(A, B, C, D) = \{a(a^n)^\mu \mid a \in A\}.$$

PROOF. We use induction on n. Since $A \cup B = AB = \{ab \mid a \in A,\ b \in B\}$ and $C \cup D = \{aa^\mu c \mid a \in A,\ c \in C\}$, we have $f_1(A, B, C, D) = \{aa^\mu \mid a \in A\}$ and the assertion holds for $n = 1$. If we write $F = f_n(A, B, C, D) \cup f_1(A, C, B, D)$, the induction assumption yields that

$$F = \{a(a^n)^\mu \mid a \in A\} \cdot \{bb^\nu \mid b \in A\} = \{ab(a^n)^\mu b^\nu \mid a, b \in A\}.$$

An element $ab(a^n)^\mu b^\nu$ of F lies in $B \cup C$ if and only if $b = a^{-1}$. Therefore

$$\begin{aligned} (F \cap (B \cup C)) \cup D &= \{(a^n)^\mu (a^{-1})^\nu \mid a \in A\} \cdot \{cc^\mu c^\nu \mid c \in A\} \\ &= \{c(a^n c)^\mu (a^{-1}c)^\nu \mid a, c \in A\} \end{aligned}$$

https://doi.org/10.1017/S144678870000080X Published online by Cambridge University Press

and such an element lies in $A \cup B$ if and only if $a = c$. Thus

$$f_{n+1}(A, B, C, D) = \{a(a^{n+1})^{\mu} \mid a \in A\},$$

as desired.

We can now prove Theorems A and B stated in the introduction.

PROOF OF THEOREM A. If G has no subgroup of type (2,2,2), then its type is of the form $(\lambda_1, \ldots, \lambda_r)$ with $r \leq 2$ or $\lambda_3 = 1$. By [1, Lemma 6.1], G has an L-embedding in the elementary abelian group.

Since an L-embedding of a group induces an L-embedding of every subgroup, to prove the converse, we only have to show that there is no L-embedding of a group G of type (2,2,2) in an elementary abelian group H of order p^6. So suppose, for a contradiction, that $\varphi : L(G) \to L(H)$ is such an embedding, let $G = A \times B \times C$ where A, B, C are cyclic of order p^2 and let μ, ν, and D be as in Lemma 1.1. Then D is a complement to $A \cup B$, $A \cup C$, and to $B \cup C$ in G.

By (1), $H = A^{\varphi} \times B^{\varphi} \times C^{\varphi}$ and D^{φ} is a complement to $A^{\varphi} \cup B^{\varphi}$, $A^{\varphi} \cup C^{\varphi}$, and to $B^{\varphi} \cup C^{\varphi}$ in H. It follows that the projection of D^{φ} into A^{φ} is surjective, that the maps $\sigma : A^{\varphi} \to B^{\varphi}$ and $\tau : A^{\varphi} \to C^{\varphi}$ mapping the first component of an element of D^{φ} to its second and third component, respectively, are isomorphisms and that $D^{\varphi} = \{aa^{\sigma}a^{\tau} \mid a \in A^{\varphi}\}$.

By 1.1, $f_p(A, B, C, D) = \{a(a^p)^{\mu} \mid a \in A\} \neq A$ and by (1) and 1.1,

$$f_p(A, B, C, D)^{\varphi} = f_p(A^{\varphi}, B^{\varphi}, C^{\varphi}, D^{\varphi}) = \{a(a^p)^{\sigma} \mid a \in A^{\varphi}\} = A^{\varphi}$$

since H has exponent p; but φ is injective. This contradiction shows that there is no L-embedding of G in H.

PROOF OF THEOREM B. We use induction on $|G|$. Let $X \leq G$. Then we have $X = X_1 \times \cdots \times X_r$ with cyclic subgroups X_i and by (1), $X^{\varphi} = X_1^{\varphi} \times \cdots \times X_r^{\varphi}$. So if $X_i^{\varphi} \simeq X_i$ for all i, then $X^{\varphi} \simeq X$. Thus we may assume that X is cyclic and that $|X| = p^k$ where $k \geq 2$. Since G contains a subgroup of type (2,2,2), there exist cyclic subgroups Y and Z of G such that $G_0 = X \times Y \times Z$ is a subgroup of type $(k, 2, 2)$ of G. If $k = 2$ and X^{φ} were not cyclic, then $G_0^{\varphi} = X^{\varphi} \times Y^{\varphi} \times Z^{\varphi}$ would not be of type (2,2,2) and hence, by Theorem A, would have an L-embedding in an elementary abelian group. But then also G_0 would have such an L-embedding, contradicting Theorem A. Thus $X^{\varphi} \simeq X$ in this case.

Finally, assume that $k \geq 3$ and let A be the maximal subgroup of X. Then $A \times Y \times Z$ and $G/\Omega(X)$ both contain subgroups of type (2,2,2) and hence by induction, A^{φ} and $X^{\varphi}/\Omega(X)^{\varphi}$ are cyclic. Since $k \geq 3$, $\Omega(X) < A$ and hence $\Omega(X)^{\varphi} \leq \Phi(A^{\varphi})$; furthermore $\Phi(A^{\varphi}) \leq \Phi(X^{\varphi})$ since X^{φ} is a p-group (see [3, p. 273]). Thus $X^{\varphi}/\Phi(X^{\varphi})$ is cyclic; hence X^{φ} is cyclic and $X^{\varphi} \simeq X$.

2. Smooth groups

In this section we shall prove that if G is of type $(\lambda_1, \dots, \lambda_r)$ with $r \leq 2$ or $\lambda_3 = 1$ and $L(G)$ can be embedded in $L(H)$, then H has the structure given in Theorem C. Basic for this is the following concept.

DEFINITION 2.1. Let p be a prime, $n, k \in \mathbb{N}$, let G be an abelian group of order p^n and suppose that $X_i \leq G$ are such that

$$1 = X_0 < X_1 < \cdots < X_n = G; \tag{2}$$

thus $|X_i| = p^i$ for $i = 0, \dots, n$.

(a) The chain (2) is called *k-smooth* if for every $j \in \{1, \dots, k\}$, we have $X_j \simeq X_{i+j}/X_i$ for all $i = 1, \dots, n-j$.

(b) The group G is called *k-smooth* if there exists a k-smooth chain (2) in G; in this case, the isomorphism type of the group X_k is called the *k-type* of G.

(c) The chain (2) or the group G is called *smooth* if it is n-smooth; that is, if it is k-smooth for every $k \in \mathbb{N}$.

Certainly, cyclic and elementary abelian p-groups are smooth and it is also clear that all the subgroups and factor groups appearing in a smooth chain are smooth. More precisely, we have the following inheritance property.

LEMMA 2.2. *If* (2) *is a k-smooth chain, $0 \leq s < t \leq n$ and $1 \leq j \leq k$, then the chain*

$$1 = X_s/X_s < X_{s+1}/X_s < \cdots < X_t/X_s \tag{3}$$

is j-smooth. In particular, if (2) *is smooth, then so is* (3).

The significance of the concept of smooth groups for our problem may be seen from the following result.

LEMMA 2.3. *Let $n \geq k \geq 1$ and $r \geq 2$. Let $G = A \times B \times C_3 \times \cdots \times C_r$, where A and B are cyclic of order p^n and p^k, respectively, and $|C_i| = p$ for $i = 3, \dots, r$. If φ is an L-embedding of G in the abelian group H, then $H = A^\varphi \times B^\varphi \times C_3^\varphi \times \cdots \times C_r^\varphi$ where A^φ and B^φ are k-smooth of k-type B^φ. More precisely, if A_i and B_i are the subgroups of order p^i of A and B, respectively, then $1 = A_0^\varphi < \cdots < A_n^\varphi = A^\varphi$ and $1 = B_0^\varphi < \cdots < B_k^\varphi = B^\varphi$ are k-smooth chains and $B^\varphi \simeq A_k^\varphi$.*

PROOF. By (1), $H = A^\varphi \times B^\varphi \times C_3^\varphi \times \cdots \times C_r^\varphi$ since every subgroup of H is normal. We show that the chain $1 = A_0^\varphi < \cdots < A_n^\varphi = A^\varphi$ is k-smooth. For this let $1 \leq j \leq k$

https://doi.org/10.1017/S144678870000080X Published online by Cambridge University Press

and $0 \leq i \leq n-j$ and put $R = A_{i+j} \times B_j$. Then $R/A_i = A_{i+j}/A_i \times B_j A_i/A_i$ is a direct product of two cyclic groups of order p^j. By [4, Theorem 1.6.2] there exists a diagonal S/A_i in this group; that is, $S \cap A_{i+j} = A_i = S \cap B_j A_i$ and $S \cup A_{i+j} = R = S \cup B_j A_i$. By (1), S^φ/A_i^φ is a diagonal in $R^\varphi/A_i^\varphi = A_{i+j}^\varphi/A_i^\varphi \times B_j^\varphi A_i^\varphi/A_i^\varphi$ and [4, Theorem 1.6.2] now implies that $A_{i+j}^\varphi/A_i^\varphi \simeq B_j^\varphi A_i^\varphi/A_i^\varphi \simeq B_j^\varphi$. For $i = 0$ we obtain $A_j^\varphi \simeq B_j^\varphi$ and hence $A_{i+j}^\varphi/A_i^\varphi \simeq A_j^\varphi$ for arbitrary i. Thus our chain is k-smooth and $A_k^\varphi \simeq B_k^\varphi = B^\varphi$. In the same way we show that the chain $1 = B_0^\varphi < \cdots < B_k^\varphi = B^\varphi$ is k-smooth.

The above lemma in particular says that B^φ is smooth. Therefore our next aim is to determine all smooth groups. For this we need that every smooth chain of G contains all the groups

$$\Omega_m(G) := \{x \in G \mid x^{p^m} = 1\} \quad \text{and} \quad G^{p^m} := \{x^{p^m} \mid x \in G\}.$$

LEMMA 2.4. *Let $1 = X_0 < \cdots < X_n = G$ be a smooth chain in an abelian p-group G. For every $m \in \mathbb{N}$ there exist integers i and j such that $\Omega_m(G) = X_i$ and $G^{p^m} = X_j$.*

PROOF. Since $\Omega_m(G)/\Omega_1(G) = \Omega_{m-1}(G/\Omega_1(G))$ and $G^{p^m} = (G^p)^{p^{m-1}}$, Lemma 2.2 and an obvious induction yield that we only have to show the assertion for $m = 1$. To do this we use induction on $|G|$. By 2.2 and the induction assumption there exist integers s and t such that $\Omega(G/X_1) = X_s/X_1$ and $X_{n-1}^p = X_t$.

If $X_s < G$, then again by induction, $\Omega(G) = \Omega(X_s) = X_i$ for some $i \in \mathbb{N}$. And if $X_s = G$, then $X_{n-1} \simeq G/X_1$ is elementary abelian and hence $\Omega(G) = X_{n-1}$ or $\Omega(G) = G = X_n$.

Similarly, if $X_t \neq 1$, the induction assumption implies that $G^p/X_t = (G/X_t)^p = X_j/X_t$ for some integer j and hence $G^p = X_j$. And if $X_t = 1$, then $G/X_1 \simeq X_{n-1}$ is elementary abelian and hence $G^p = X_1$ or $G^p = 1 = X_0$, as desired.

THEOREM 2.5. *The abelian p-group of type $(\lambda_1, \ldots, \lambda_r)$ is smooth if and only if $\lambda_1 - \lambda_r \leq 1$.*

PROOF. Write $G = A_1 \times \cdots \times A_r$ with cyclic groups A_i of order p^{λ_i} where $\lambda_1 \geq \cdots \geq \lambda_r \geq 1$ and put $\lambda = \lambda_1$.

First assume that G is smooth and let $1 = X_0 < \cdots < X_n = G$ be a smooth chain. If $\lambda \leq 2$, then clearly $\lambda_1 - \lambda_r \leq 1$, so assume further that $\lambda \geq 3$. For every $\mu \in \mathbb{N}$,

$$\Omega_\mu(G) = \Omega_\mu(A_1) \times \cdots \times \Omega_\mu(A_r)$$

and hence $p^j := |\Omega_{\lambda-1}(G)/\Omega_{\lambda-2}(G)| \leq p^r$ with equality if and only if $\lambda_r \geq \lambda - 1$. By Lemma 2.4, $\Omega(G) = X_r$ and there exists $i \in \mathbb{N}$ such that $\Omega_{\lambda-2}(G) = X_i$ and

$\Omega_{\lambda-1}(G) = X_{i+j}$. Then $\Omega(G/X_i) = X_{i+j}/X_i$ and hence X_{i+j+1}/X_i is not elementary abelian. Since the chain is smooth, $X_{i+j+1}/X_i \simeq X_{j+1}$ and therefore $X_{j+1} \not\leq X_r$. It follows that $j = r$ and so $\lambda_r \geq \lambda - 1$, as desired.

Now suppose that, conversely, $\lambda_r \geq \lambda - 1$. Then there exists $s \leq r$ such that $\lambda_i = \lambda$ for $1 \leq i \leq s$ and $\lambda_i = \lambda - 1$ for $s + 1 \leq i \leq r$; thus $n = r(\lambda - 1) + s$. Since cyclic groups are smooth, we may assume that $r \geq 2$.

For $1 \leq i \leq n$, write $i = rj + k$ where $0 \leq j \leq \lambda - 1$, and where $0 < k \leq r$ if $j < \lambda - 1$, $0 < k \leq s$ if $j = \lambda - 1$, and define

$$X_i = \Omega_{j+1}(A_1) \times \cdots \times \Omega_{j+1}(A_k) \times \Omega_j(A_{k+1}) \times \cdots \times \Omega_j(A_r). \tag{4}$$

We prove by induction on $|G|$ that $1 = X_0 < \cdots < X_n = G$ is a smooth chain. First of all, clearly, $X_i < X_{i+1}$ for all i and $|X_i| = p^i$. For $U \leq G$ we write $\overline{U} = UX_1/X_1$, let $\overline{A}_{r+1} := \overline{A}_1$ and define Y_i with respect to the decomposition $\overline{G} = \overline{A}_2 \times \cdots \times \overline{A}_r \times \overline{A}_{r+1}$ as we defined X_i in (4). Then for $i = rj + k \leq n - 1$ as above, we obtain that

$$Y_i = \Omega_{j+1}(\overline{A}_2) \times \cdots \times \Omega_{j+1}(\overline{A}_{k+1}) \times \Omega_j(\overline{A}_{k+2}) \times \cdots \times \Omega_j(\overline{A}_{r+1}).$$

Since $\Omega_j(\overline{A}_{r+1}) = \Omega_{j+1}(A_1)/X_1$, we have $Y_i = X_{i+1}/X_1$ for all i; this is clear if $k < r$, and for $k = r$ it follows since then $i + 1 = r(j + 1) + 1$. By the induction assumption, $1 = Y_0 < \cdots < Y_{n-1} = G/X_1$ is a smooth chain. Furthermore Y_i and X_i both are the direct product of k cyclic groups of order p^{j+1} and $r - k$ cyclic groups of order p^j. Therefore $Y_i \simeq X_i$ and hence for $i = 1, \ldots, n - 1$ and $t = 1, \ldots, n - i$, we obtain that $X_{t+i}/X_t \simeq Y_{t+i-1}/Y_{t-1} \simeq Y_i \simeq X_i$. Thus the chain $1 = X_0 < \cdots < X_n = G$ is smooth.

COROLLARY 2.6. *If $1 \leq r \leq n$, then the group $G_{n,r}$ defined in the Introduction is the unique smooth abelian group of order p^n with r generators.*

PROOF. Let G be an abelian group of order p^n with r generators, that is, of type $(\lambda_1, \ldots, \lambda_r)$. By Theorem 2.5, G is smooth if and only if there exist integers s, λ with $0 \leq s < r$ such that $\lambda_i = \lambda$ for $i > s$ and $\lambda_i = \lambda + 1$ for $i \leq s$. Since $n = \sum_{i=1}^{r} \lambda_i$, this implies that $n = r\lambda + s$. Thus G is smooth if and only if $G \simeq G_{n,r}$.

In view of Lemma 2.3 we still have to determine all k-smooth groups of order p^n for $k < n$. If $k = 1$, every group of order p^n is k-smooth. So we may assume that $k \geq 2$ and show first that we don't get any new groups if the k-type is not elementary abelian. Note that every k-type is the isomorphism type of a smooth group of order p^k and therefore of one of the groups $G_{k,r}$ ($r \leq k$) appearing in Corollary 2.6.

THEOREM 2.7. *Let $1 \leq r < k \leq n$. The abelian group G of order p^n is k-smooth of k-type $G_{k,r}$ if and only if G is the smooth group $G_{n,r}$ of order p^n with r generators.*

https://doi.org/10.1017/S144678870000080X Published online by Cambridge University Press

PROOF. If $G = G_{n,r}$ and $1 = X_0 < \cdots < X_n = G$ is a smooth chain, then by 2.2, G is k-smooth and X_k is smooth. By 2.4, $\Omega(G) = X_r \leq X_k$ and hence $|\Omega(X_k)| = p^r$. By Corollary 2.6, $X_k \simeq G_{k,r}$.

Conversely, assume that $1 = X_0 < \cdots < X_n = G$ is a k-smooth chain and $X_k \simeq G_{k,r}$. By 2.2 and 2.4, $\Omega(X_k) = X_r$ and since $r < k$, it follows from 2.6 that $X_{r+1} \simeq G_{r+1,r}$. Thus G is $(r+1)$-smooth of $(r+1)$-type $G_{r+1,r}$ and it suffices to prove the following special case of our assertion.

(5) If $1 \leq r < n$, $|G| = p^n$ and G is $(r+1)$-smooth of $(r+1)$-type $G_{r+1,r}$, then $G \simeq G_{n,r}$.

To prove this, we use induction on n. The assertion is clearly true for $n = r+1$. So assume it holds for $r+1 \leq m < n$ and let $1 = Y_0 < \cdots < Y_n = G$ be an $(r+1)$-smooth chain with $Y_{r+1} \simeq G_{r+1,r}$. Then $Y_{n-1} \simeq G_{n-1,r}$ and by 2.4, $\Omega(Y_{n-1}) = Y_r$. If $\Omega(G) > Y_r$ and $x \in \Omega(G) \setminus Y_r$, then $x \notin Y_{n-1}$ and hence $G = Y_{n-1} \times \langle x \rangle$. Since $Y_{n-1}/Y_{n-1-r} \simeq Y_r$, it would follow that G/Y_{n-1-r} is elementary abelian of order p^{r+1}; but $G/Y_{n-1-r} \simeq Y_{r+1}$ is not elementary abelian. This contradiction shows that $\Omega(G) = Y_r$; let $(\lambda_1, \ldots, \lambda_r)$ be the type of G.

Now $|G/\Omega(G)| = p^{n-r}$. If $n \leq 2r$, then $G/\Omega(G) \simeq Y_{n-r} \leq Y_r$ is elementary abelian and hence $\operatorname{Exp} G \leq p^2$; by 2.5, G is smooth. So assume that $n > 2r$. Then the induction assumption implies that $G/\Omega(G) \simeq G_{n-r,r}$. It follows that $\lambda_r \geq 2$ and $G/\Omega(G)$ is smooth of type $(\lambda_1 - 1, \ldots, \lambda_r - 1)$. By 2.5, $1 \geq (\lambda_1 - 1) - (\lambda_r - 1) = \lambda_1 - \lambda_r$ and hence G is smooth. By 2.6, $G \simeq G_{n,r}$ and this proves (5).

We finally determine the k-smooth groups of k-type $G_{k,k}$ or $(1, \ldots, 1)$, that is, with elementary abelian factors of order p^k.

THEOREM 2.8. *Let $1 < k \leq n$ and write $n = \lambda k + t$ where $\lambda \in \mathbb{N}$ and $0 \leq t < k$. The abelian p-group G of order p^n is k-smooth of k-type $(1, \ldots, 1)$ if and only if $G/\Omega_\lambda(G)$ is elementary abelian of order at most p^t, that is, G has type $(\lambda_1, \ldots, \lambda_r)$ where $\lambda_1 \leq \lambda + 1$ and $\lambda_{t+1} \leq \lambda$.*

PROOF. We use induction on $|G|$. Suppose first that $1 = X_0 < \cdots < X_n = G$ is a k-smooth chain with X_k elementary abelian. If $t > 0$, then $M := X_{\lambda k} < G$ and, by Lemma 2.2, M is k-smooth of k-type $(1, \ldots, 1)$. The induction assumption yields that $M = \Omega_\lambda(M) \leq \Omega_\lambda(G)$. Since $n = \lambda k + t$, we have $|G/M| = p^t$ and $G/M \simeq X_t \leq X_k$ is elementary abelian. Thus $G/\Omega_\lambda(G)$ is elementary abelian of order at most p^t.

Now assume that $t = 0$. Then for $\lambda = 1$ we get that $G = X_k$ is elementary abelian, and if $\lambda \geq 2$, the induction assumption implies that $X_{n-k} = X_{(\lambda-1)k}$ has exponent at most $p^{\lambda-1}$. Since $G/X_{n-k} \simeq X_k$ is elementary abelian, it follows that $G = \Omega_\lambda(G)$, as desired.

It is clear that $G/\Omega_\lambda(G)$ is elementary abelian of order at most p^t if and only if G has type $(\lambda_1, \dots, \lambda_r)$ with $\lambda_1 \le \lambda + 1$ and $\lambda_{t+1} \le \lambda$. So suppose, conversely, that $G = A_1 \times \cdots \times A_r$ with cyclic groups A_i of order p^{λ_i} where $\lambda + 1 \ge \lambda_1 \ge \lambda_2 \ge \cdots \ge \lambda_r \ge 1$ and $\lambda_{t+1} \le \lambda$. Then $n = \sum_{i=1}^{r} \lambda_i \le r\lambda + t$ and hence $k \le r$. Thus $N := \Omega(A_1) \times \cdots \times \Omega(A_k)$ is elementary abelian of order p^k and $|G/N| = p^m$ where $m = (\lambda - 1)k + t$. We write $\overline{U} = UN/N$ for every $U \le G$ and show next that there exists a k-smooth chain

$$1 = X_k/N < X_{k+1}/N < \cdots < X_n/N = \overline{G} \quad \text{of } l\text{-type } (1, \dots, 1), \tag{6}$$

where $l = \min(m, k)$. This is clear if $m < k$; for then $\lambda = 1$ and $|\overline{A}_i| = p$ for all i since $t < k$. Thus $\overline{G}$ is elementary abelian in this case and has the desired chain. So suppose that $m \ge k$. Then (6) follows from the induction assumption if $\overline{G}/\Omega_{\lambda-1}(\overline{G})$ is elementary abelian of order at most p^t. Since $t < k$, $|\overline{A}_i| \le p^\lambda$ for all i and hence $\overline{G}/\Omega_{\lambda-1}(\overline{G})$ clearly is elementary abelian. So suppose, for a contradiction, that $|\overline{G}/\Omega_{\lambda-1}(\overline{G})| \ge p^{t+1}$. Assume that d of the A_i have order $p^{\lambda+1}$. Then $i \le t$ for these A_i and hence $d \le t$. Since $|\overline{A}_i| \le p^{\lambda-1}$ for $t < i \le k$, there exist at least $t + 1 - d$ indices i for which $k < i$ and $p^\lambda = |\overline{A}_i| = |A_i|$. Thus $\lambda_{k+t+1-d} = \lambda$ and it follows that $|A_1 \times \cdots \times A_{k+t+1-d}| = p^w$ where

$$\begin{aligned} w &= d(\lambda + 1) + (k + t + 1 - 2d)\lambda \\ &= k\lambda + (t - d)\lambda + d + \lambda \\ &\ge k\lambda + t + 1 = n + 1 \end{aligned}$$

since $\lambda \ge 1$. This contradiction proves (6).

We finally put $X_0 = 1$ and inductively define subgroups X_i of N $(i = 1, \dots, k-1)$ such that $X_{i-1} < X_i$ and $|X_i| = p^i$ for all i, and X_{i+k}/X_i is elementary abelian for all i with $i + k \le n$. Then all factor groups X_u/X_v of order at most p^k in the chain $1 = X_0 < \cdots < X_n = G$ will be elementary abelian and therefore the chain will be k-smooth of k-type $(1, \dots, 1)$. So suppose that subgroups $X_0, \dots, X_i$ with these properties have been defined and that $i < k - 1$. Then if $i + k \ge n$, any subgroup X_{i+1} of order p^{i+1} of N containing X_i will do the job. If $i + k < n$, then since X_{i+k}/X_i is elementary abelian, X_{i+k+1}/X_i is of type $(2, 1, \dots, 1)$ or $(1, \dots, 1)$. In the first case we take $X_{i+1}/X_i = \Phi(X_{i+k+1}/X_i)$; in the second case we let X_{i+1}/X_i be any subgroup of order p of N/X_i. Since X_{i+k+1}/N is elementary abelian, in both cases $X_{i+1} \le N$ and X_{i+1+k}/X_{i+1} is elementary abelian.

We shall need two simple properties of smooth groups.

LEMMA 2.9. *Let $1 \le r < n$ and suppose that $1 = X_0 < \cdots < X_n = G$ is a smooth chain in $G = G_{n,r}$; let p^e be the exponent of G. Then there exist $g \in G$ and*

https://doi.org/10.1017/S144678870000080X Published online by Cambridge University Press

$K = S \times T \leq G$ such that $o(g) = p^e$, S is of type $(e, \ldots, e)$ or $S = 1$, T is of type $(e-1, \ldots, e-1)$ or $T = 1$, and satisfying $G = \langle g \rangle \times K$, $X_{n-1} = \langle g^p \rangle \times K$, $X_{n-r} = \langle g^p \rangle \times K^p$, $X_{n-r-1} = \langle g^{p^2} \rangle \times K^p$.

PROOF. Since $r < n$, we have $e > 1$ and $G = R \times T$ where R is of type $(e, \ldots, e)$ and T is of type $(e-1, \ldots, e-1)$ or $T = 1$. So $T \leq \Omega_{e-1}(G) \leq X_{n-1}$, by Lemma 2.4, and hence $X_{n-1} = (R \cap X_{n-1}) \times T$. Since $R \cap X_{n-1}$ is a maximal subgroup of R, we have $R \cap X_{n-1} = \langle u \rangle \times S$ where $o(u) = p^{e-1}$ and S is of type $(e, \ldots, e)$ or $S = 1$. Since R is homocyclic, there exists $g \in R$ such that $g^p = u$. Then $R = \langle g \rangle \times S$ and hence $G = \langle g \rangle \times K$ and $X_{n-1} = \langle g^p \rangle \times K$ where $K = S \times T$. By 2.4, $X_{n-r} = G^p = \langle g^p \rangle \times K^p$ and $X_{n-r-1} = (X_{n-1})^p = \langle g^{p^2} \rangle \times K^p$.

LEMMA 2.10. *Suppose that $G \simeq H$ and that $1 = X_0 < \cdots < X_n = G$ and $1 = Y_0 < \cdots < Y_n = H$ are smooth chains. Then every isomorphism $\alpha : X_{n-1} \to Y_{n-1}$ satisfying $X_i^\alpha = Y_i$ for $i = 1, \ldots, n-2$ can be extended to an isomorphism of G to H.*

PROOF. If G and H are elementary abelian, it is clear that every isomorphism $\alpha : X_{n-1} \to Y_{n-1}$ can be extended. So we may assume that G is not elementary abelian and by Corollary 2.6, $G \simeq G_{n,r}$ for some r satisfying $1 \leq r < n$. Let g, S, T be as in Lemma 2.9; since also $H \simeq G_{n,r}$, there exist h, U, V having the corresponding properties with respect to the chain $1 = Y_0 < \cdots < Y_n = H$.

Now $X_{n-1}^\alpha = Y_{n-1}$ implies that $(g^p)^\alpha = h^{ip}uv$ with $i \in \mathbb{Z}$, $u \in U$, $v \in V$. By Lemma 2.4 there exists $j \in \mathbb{N}$ such that $X_j = G^{p^{e-1}}$ and $Y_j = H^{p^{e-1}}$. Since $X_j^\alpha = Y_j$, it follows that $H^{p^{e-1}} = \langle h^{p^{e-1}} \rangle \times \Omega(U)$ contains $((g^p)^{p^{e-2}})^\alpha = h^{ip^{e-1}} u^{p^{e-2}} v^{p^{e-2}}$; this yields $u^{p^{e-1}} = 1 = v^{p^{e-2}}$. Since U and V are trivial or homocyclic of exponent p^e and p^{e-1}, respectively, there exist $x \in U$, $y \in V$ such that $x^p = u$ and $y^p = v$. Thus $(g^p)^\alpha = h^{ip}uv = (h^i xy)^p$ and so $o(h^i xy) = p^e$. For $K = S \times T$ we have $X_{n-1}^\alpha = \langle g^p \rangle^\alpha \times K^\alpha$ and hence $\langle h^i xy \rangle \cap K^\alpha = \langle g^p \rangle^\alpha \cap K^\alpha = 1$. It follows that $H = \langle h^i xy \rangle \times K^\alpha$ and thus there exists an isomorphism $\beta : G \to H$ satisfying $g^\beta = h^i xy$ and $w^\beta = w^\alpha$ for $w \in K$. Since $(g^p)^\beta = (g^\beta)^p = (h^i xy)^p = (g^p)^\alpha$, β is an extension of α.

3. Canonical L-embeddings and bases

In this section we shall prove that if G and H have the structure given in Theorem C, then there exists an L-embedding of G in H. For this we use Barnes' methods and therefore need some of the concepts introduced by him. For the convenience of the reader we recall them briefly.

https://doi.org/10.1017/S144678870000080X Published online by Cambridge University Press

Let G and H be abelian p-groups of the same order and let X_1, Y_1, X_2, Y_2 be subgroups of G such that $X_2 = X_1 \cup Y_2$ and $Y_1 = X_1 \cap Y_2$. Then the mappings

$$\sigma_1 : X_1/Y_1 \to X_2/Y_2; \quad xY_1 \mapsto xY_2 \qquad (x \in X_1)$$
$$\sigma_2 : X_2/Y_2 \to X_1/Y_1; \quad xY_2 \mapsto xY_2 \cap Y_1 \qquad (x \in X_2)$$

are mutually inverse isomorphisms. Such isomorphisms are called *projectivities*. If $\varphi : L(G) \to L(H)$ is an L-embedding, then by (1), $X_2^\varphi = X_1^\varphi \cup Y_2^\varphi$ and $Y_1^\varphi = X_1^\varphi \cap Y_2^\varphi$ so that there exist the corresponding projectivities

$$\overline{\sigma}_1 : X_1^\varphi/Y_1^\varphi \to X_2^\varphi/Y_2^\varphi \quad \text{and} \quad \overline{\sigma}_2 : X_2^\varphi/Y_2^\varphi \to X_1^\varphi/Y_1^\varphi$$

in the group H. For a closed chain

$$c : X/Y = X_1/Y_1 \xrightarrow{\sigma_1} X_2/Y_2 \xrightarrow{\sigma_2} \cdots \xrightarrow{\sigma_{n-1}} X_n/Y_n = X/Y$$

of projectivities in G, the composition $\alpha(c) := \sigma_1 \ldots \sigma_{n-1}$ is an automorphism of X/Y and

$$\overline{c} : X^\varphi/Y^\varphi = X_1^\varphi/Y_1^\varphi \xrightarrow{\overline{\sigma}_1} X_2^\varphi/Y_2^\varphi \xrightarrow{\overline{\sigma}_2} \cdots \xrightarrow{\overline{\sigma}_{n-1}} X_n^\varphi/Y_n^\varphi = X^\varphi/Y^\varphi$$

is a closed chain of projectivities in H. So if X/Y is cyclic of order p - we call X/Y a *prime interval* in this case - there exist integers $r(c)$ and $r(\overline{c})$ prime to p such that $x^{\alpha(c)} = x^{r(c)}$ for all $x \in X/Y$ and $y^{\alpha(\overline{c})} = y^{r(\overline{c})}$ for all $y \in X^\varphi/Y^\varphi$.

DEFINITION 3.1. The L-embedding $\varphi : L(G) \to L(H)$ is called *canonical* if $r(c) \equiv r(\overline{c}) \pmod{p}$ for all closed chains c of projectivities on prime intervals in G.

Barnes uses the term '1-*canonical*' instead of 'canonical' since he considers, more generally, L-embeddings having similar properties with respect to cyclic intervals of order p^n ($n \in \mathbb{N}$) which he then terms 'n-canonical'. He shows [1, Theorem 3.1 and 3.3] that if C and $\overline{C}$ are cyclic groups of order p and φ is a canonical L-embedding of G in H, then φ can be extended to a canonical L-embedding of $G \times C$ in $H \times \overline{C}$. Thus to prove Theorem C, it will suffice to show that $A \times B$ has a canonical L-embedding in $U \times V$; this can then be extended to $A \times B \times C_3 \times \cdots \times C_r$.

Again let $\varphi : L(G) \to L(H)$ be an L-embedding. We consider the set $\mathfrak{A}$ of all pairs (x, y) where x is a generator of a prime interval X/Y of G and y is a generator of X^φ/Y^φ. A subset $\mathfrak{B}$ of $\mathfrak{A}$ is called a *basis* of φ if for every prime interval X/Y in G there is a unique pair $(x, y) \in \mathfrak{B}$ such that $X/Y = \langle x \rangle$ and $X^\varphi/Y^\varphi = \langle y \rangle$.

DEFINITION 3.2. Let $\mathfrak{B}$ be a basis of φ.

https://doi.org/10.1017/S144678870000080X Published online by Cambridge University Press

(a) A projectivity $\sigma : X_1/Y_1 \to X_2/Y_2$ between prime intervals in G is called *regular* with respect to $\mathfrak{B}$ if there exists $r \in \mathbb{Z}$ such that $x_1^\sigma = x_2^r$ and $y_1^\sigma = y_2^r$, where $(x_i, y_i) \in \mathfrak{B}$ satisfy $X_i/Y_i = \langle x_i \rangle$ and $X_i^\varphi/Y_i^\varphi = \langle y_i \rangle$ $(i = 1, 2)$.

(b) $\mathfrak{B}$ is called *canonical* if every projectivity between prime intervals in G is regular with respect to $\mathfrak{B}$.

It was noted by Barnes [1, p. 21] that an L-embedding is canonical if and only if it has a canonical basis. We need some simple properties of canonical bases.

LEMMA 3.3. *Suppose that $\mathfrak{B}$ is a canonical basis of φ, let X/Y be a prime interval in G and let $(x, \overline{x}) \in \mathfrak{B}$ be such that $X/Y = \langle x \rangle$. If $Z, W \leq G$ are such that $X \cap Z = Y$ and $X \cup Z = W$, then there exists $i \in \mathbb{Z}$, $i \not\equiv 0 \pmod p$ such that $(x^i Z, \overline{x}^i Z^\varphi) \in \mathfrak{B}$.*

PROOF. Consider the projectivity $\sigma : X/Y \to W/Z$ and let $(w, \overline{w}) \in \mathfrak{B}$ be such that $W/Z = \langle w \rangle$. Since $\mathfrak{B}$ is canonical, there exists $r \in \mathbb{Z}$ such that $xZ = x^\sigma = w^r$ and $\overline{x}Z^\varphi = \overline{x}^{\overline{\sigma}} = \overline{w}^r$. Thus $w = (xZ)^i$ and $\overline{w} = (\overline{x}Z^\varphi)^i$ for some $i \not\equiv 0 \pmod p$.

LEMMA 3.4. *Suppose that φ is induced by an isomorphism $\varrho : G \to H$. Then φ is canonical and we obtain a canonical basis $\mathfrak{B}$ of φ if we choose for every prime interval in G a generator x and put the pair (x, x^ϱ) in $\mathfrak{B}$.*

PROOF. If $\sigma : X/Y \to W/Z$ is a projectivity between prime intervals and x, w are the chosen generators of X/Y and W/Z, respectively, then the definition of $\overline{\sigma}$ implies that $(x^\varrho)^{\overline{\sigma}} = (x^\sigma)^\varrho$. So if $x^\sigma = w^r$, it follows that $(x^\varrho)^{\overline{\sigma}} = (w^r)^\varrho = (w^\varrho)^r$. Thus σ is regular.

Conversely, we need that every canonical basis is of this type if G and H are elementary abelian (of order p^2).

LEMMA 3.5. *Let G and H be elementary abelian of order p^2 and let φ be a canonical L-embedding of G in H with canonical basis $\mathfrak{B}$. Suppose that $a, b \in G$ are such that $\langle a \rangle \neq \langle b \rangle$ and that $\mathfrak{B}$ contains the pairs (a, x) and (b, y). Then φ is induced by the isomorphism $\varrho : G \to H$; $a^i b^j \mapsto x^i y^j$, and for every pair $(c, z) \in \mathfrak{B}$ we have $z = c^\varrho$.*

PROOF. We clearly have $G = \langle a \rangle \times \langle b \rangle$, $\langle a \rangle^\varphi = \langle x \rangle$ and $\langle b \rangle^\varphi = \langle y \rangle$, so that $H = \langle x \rangle \times \langle y \rangle$. Suppose that $\langle ab^k \rangle^\varphi = \langle xy^m \rangle$ and let $((ab^k)^r, (xy^m)^s) \in \mathfrak{B}$ where $1 \leq k, m, r, s \leq p - 1$. By 3.3 there exist $i, j \in \mathbb{Z}$ such that $a^r b^{kr} \langle b \rangle = a^i \langle b \rangle$ and $x^s y^{ms} \langle y \rangle = x^i \langle y \rangle$ and also $a^r b^{kr} \langle a \rangle = b^j \langle a \rangle$ and $x^s y^{ms} \langle x \rangle = y^j \langle x \rangle$. It follows that $r \equiv i \equiv s \pmod p$ and $kr \equiv j \equiv ms \pmod p$ and hence $r = s$ and $k = m$. Thus φ is induced by ϱ and the pairs $(c, z) \in \mathfrak{B}$ belonging to prime intervals $C/1$ satisfy $z = c^\varrho$. By 3.3, this then also holds for the prime intervals G/C.

If $M \leq G$ and φ is an L-embedding of G in H, then the restriction of φ to $L(M)$ is an L-embedding of M in M^φ which we call φ_M. If $\mathfrak{B}$ is a basis of φ, we let $\mathfrak{B}_M$ be the set of pairs $(x, y) \in \mathfrak{B}$ belonging to prime intervals X/Y with $X \leq M$; clearly, $\mathfrak{B}_M$ is a basis of φ_M.

We want to construct canonical L-embeddings of groups of type (n, k). This we shall do by induction, extending L-embeddings of smaller groups in the following obvious way; of course, the lemma holds more generally.

LEMMA 3.6. *Suppose that $|G : F| = p^2$, where $F = \Phi(G)$; let $K \leq H$ and μ be an L-embedding of G/F in H/K with basis $\mathfrak{B}_\mu$.*

Let $\mathfrak{M}$ be the set of maximal subgroups of G and for every $M \in \mathfrak{M}$, let $\varphi(M)$ be an L-embedding of M in $\overline{M}$ with basis $\mathfrak{B}(M)$ where $\overline{M}/K = (M/F)^\mu$. Assume further that $\varphi(M)_F = \varphi(N)_F$ and $\mathfrak{B}(M)_F = \mathfrak{B}(N)_F$ for all $M, N \in \mathfrak{M}$.

(a) *Then $\psi : L(G) \to L(H)$, defined by $G^\psi = H$ and $X^\psi = X^{\varphi(M)}$ if $X \leq M \in \mathfrak{M}$, is an L-embedding of G in H.*

(b) *If for every $M \in \mathfrak{M}$, the bases $\mathfrak{B}_\mu$ and $\mathfrak{B}(M)$ contain the same pair belonging to M/F, then the union $\mathfrak{C}$ of $\mathfrak{B}_\mu$ and all the $\mathfrak{B}(M)$ is a basis of ψ. If, in addition, $\mathfrak{B}_\mu$ and all the $\mathfrak{B}(M)$ are canonical, then so is $\mathfrak{C}$.*

PROOF. (a) Since the L-embeddings $\varphi(M)$ and $\varphi(N)$ coincide on $F = M \cap N$ for different $M, N \in \mathfrak{M}$, the map ψ is well-defined and injective. By definition, we have to show that if X covers Y, then X^ψ covers Y^ψ. This is clear if $X \leq M \in \mathfrak{M}$, since in that case ψ coincides with $\varphi(M)$ on X and Y; and if $X = G$, then $Y^\psi = Y^{\varphi(Y)}$ is a maximal subgroup of H, since $Y^{\varphi(Y)}/K = (Y/K)^\mu$.

(b) Our assumptions imply that for a given prime interval X/Y, all the bases $\mathfrak{B}(M)$ and $\mathfrak{B}_\mu$ which contain a pair belonging to X/Y contain the same pair. Thus the union $\mathfrak{C}$ is a basis of ψ. If $\mathfrak{B}_\mu$ and all the $\mathfrak{B}(M)$ are canonical, then by [1, Lemma 4.1], so is $\mathfrak{C}$.

The main difficulty in extending a given L-embedding of a maximal subgroup to a canonical L-embedding of G in $H = U \times V$ is that this extension can be done rather arbitrarily if V is elementary abelian, has to be constructed suitably if $|V/\Omega(V)| = p$, but is uniquely determined if $|V/\Omega(V)| \geq p^2$. Fortunately, we only have to study this in the case $n = k$.

LEMMA 3.7. *Let $G = A \times B$ with cyclic groups A and B of order p^n, let φ be an L-embedding of G in H and suppose that H is not elementary abelian. Write $F = \Phi(G)$, $U = A^\varphi$, $V = B^\varphi$; for $i = 0, \ldots, n$, let $A_i \leq A$ and $B_i \leq B$ with $|A_i| = p^i = |B_i|$, $U_i = A_i^\varphi$ and $V_i = B_i^\varphi$. Finally, suppose that $\mathfrak{B}$ is a basis of φ and that $|\Omega(U)| = p^r$.*

https://doi.org/10.1017/S144678870000080X Published online by Cambridge University Press

(a) *There exist generators a of A and b of B, elements $u \in U$, $v \in V$, and integers $i, j, s, t \in \{1, \dots, p-1\}$ such that $\mathfrak{B}$ contains the pairs (aA_{n-1}, uU_{n-1}), $(a^{ip^r}A_{n-r-1}, u^{isp}U_{n-r-1})$, (bB_{n-1}, vV_{n-1}) and $(b^{jp^r}B_{n-r-1}, v^{jtp}V_{n-r-1})$.*

(b) *If $\mathfrak{B}_F$ is a canonical basis of φ_F and a, b, u, v, s, t are as in* (a), *then φ is induced on G/F by the isomorphism $\sigma : G/F \to H/F^\varphi$ given by $(aF)^\sigma = u^s F^\varphi$ and $(bF)^\sigma = v^t F^\varphi$.*

(c) *If $\mathfrak{B}$ is a canonical basis of φ, then, in addition, $s = t$.*

PROOF. (a) By 2.3, $1 = U_0 < \cdots < U_n = U$ and $1 = V_0 < \cdots < V_n = V$ are smooth chains, $H = U \times V$ and $U \simeq V$. Since H is not elementary abelian, it follows that neither U nor V is; thus $r < n$. By 2.6, $U \simeq G_{n,r}$ and by 2.9 there exist $u \in U$ and $K \leq U$ such that

$$(7)\quad U = \langle u \rangle \times K,\ U_{n-1} = \langle u^p \rangle \times K,\ U_{n-r} = \langle u^p \rangle \times K^p,\ U_{n-r-1} = \langle u^{p^2} \rangle \times K^p.$$

Thus $U/U_{n-1} = \langle uU_{n-1} \rangle$ and hence $\mathfrak{B}$ contains an element of the form $(aA_{n-1}, u^k U_{n-1})$ where $A = \langle a \rangle$ and $k \not\equiv 0 (\mathrm{mod}\, p)$. So if we replace u by u^k, we still have (7) and $(aA_{n-1}, uU_{n-1}) \in \mathfrak{B}$. Since $A_{n-r}/A_{n-r-1} = \langle a^{p^r} A_{n-r-1} \rangle$ and $U_{n-r}/U_{n-r-1} = \langle u^p U_{n-r-1} \rangle$, there exist $i, s \in \{1, \dots, p-1\}$ such that $\mathfrak{B}$ contains $(a^{ip^r}A_{n-r-1}, u^{isp}U_{n-r-1})$. In the same way we get b, v, j, t with the desired properties.

(b) Let $W = A_{n-r} \times B_{n-r}$, $R = A_{n-r} \times B_{n-r-1}$, $S = A_{n-r-1} \times B_{n-r}$, and $T = A_{n-r-1} \times B_{n-r-1}$. Then $W/T = R/T \times S/T$ is elementary abelian of order p^2. Since R/T is projective to A_{n-r}/A_{n-r-1} and $\mathfrak{B}_F$ is canonical, by 3.3 there exists $\nu \in \mathbb{Z}$ such that $\mathfrak{B}_F$ contains $(a^{ip^r\nu}T,\ u^{isp\nu}T^\varphi)$; similarly, there exists $\mu \in \mathbb{Z}$ such that $(b^{jp^r\mu}T,\ v^{jtp\mu}T^\varphi) \in \mathfrak{B}_F$ belongs to the interval S/T. By 3.5, φ is induced on W/T by the isomorphism $\varrho : W/T \to W^\varphi/T^\varphi$ satisfying $(a^{ip^r\nu}T)^\varrho = u^{isp\nu}T^\varphi$ and $(b^{jp^r\mu}T)^\varrho = v^{jtp\mu}T^\varphi$; it follows that

$$(8)\qquad (a^{p^r}T)^\varrho = u^{sp}T^\varphi \quad \text{and} \quad (b^{p^r}T)^\varrho = v^{tp}T^\varphi.$$

For $\lambda \in \{1, \dots, p-1\}$ let $D = D_\lambda = \langle ab^\lambda \rangle$. This is a diagonal in $G = A \times B$; by (1), D^φ is a diagonal in $H = U \times V$; that is, $D^\varphi = D(\alpha) = \{xx^\alpha \mid x \in U\}$ for some isomorphism $\alpha : U \to V$ (see [4, Theorem 1.6.2]). Since $D \cap F = \langle a^p b^{\lambda p} \rangle$ is a diagonal in $F = A_{n-1} \times B_{n-1}$, $(D \cap F)^\varphi = D^\varphi \cap F^\varphi$ is a diagonal in $F^\varphi = U_{n-1} \times V_{n-1}$ and hence $U_{n-1}^\alpha = V_{n-1}$. We have $U/U_{n-1} = \langle uU_{n-1} \rangle$ and $V/V_{n-1} = \langle vV_{n-1} \rangle$; thus there exists $d = d_\lambda \in \{1, \dots, p-1\}$ such that $u^\alpha = v^d w$ with $w \in V_{n-1}$. Since $(DF)^\varphi = D^\varphi F^\varphi$, it follows that

$$(9)\qquad (\langle ab^\lambda \rangle F)^\varphi = \langle uv^{d_\lambda} \rangle F^\varphi.$$

Now $(D \cap W)T/T = \langle a^{p^r} b^{\lambda p^r} \rangle T/T$ is a diagonal in W/T which, by (8), is mapped to $\langle u^{sp} v^{\lambda tp} \rangle T^\varphi/T^\varphi$ by φ. On the other hand, $(D \cap W) \cup T$ is mapped to

$$(D^\varphi \cap W^\varphi) \cup T^\varphi = \{xx^\alpha \mid x \in U_{n-r}\}T^\varphi = \langle u^p v^{dp} \rangle T^\varphi = \langle u^{sp} v^{sdp} \rangle T^\varphi$$

https://doi.org/10.1017/S144678870000080X Published online by Cambridge University Press

since $(u^p)^\alpha = v^{dp}w^p$ and $w^p \in V_{n-1}^p = V_{n-r-1} \leq T^\varphi$; see (7). It follows that $\lambda t \equiv sd (\mathrm{mod}\, p)$. Now $d = d_\lambda$ and (9) yields that for $\lambda = 1, \ldots, p-1$,

$$(\langle ab^\lambda \rangle F)^\varphi = \langle u^s v^{sd_\lambda} \rangle F^\varphi = \langle u^s v^{\lambda t} \rangle F^\varphi;$$

that is, φ is induced on G/F by the isomorphism σ satisfying $(aF)^\sigma = u^s F^\varphi$ and $(bF)^\sigma = v^t F^\varphi$.

(c) Since $\mathfrak{B}$ is a canonical basis containing (aA_{n-1}, uU_{n-1}) and AF/F is projective to A/A_{n-1}, Lemma 3.3 implies that there exists $\nu \in \mathbb{Z}$ such that $(a^\nu F, u^\nu F^\varphi) \in \mathfrak{B}$; similarly, $(b^\mu F, v^\mu F^\varphi) \in \mathfrak{B}$ for some $\mu \in \mathbb{Z}$. By 3.5, φ is induced on G/F by the isomorphism $\tau : G/F \to H/F^\varphi$ satisfying $(aF)^\tau = uF^\varphi$ and $(bF)^\tau = vF^\varphi$. Now σ and τ induce the same lattice isomorphism of G/F and hence $\sigma\tau^{-1}$ is a power automorphism. It follows that $s = t$.

LEMMA 3.8. *Let G be of type (n, n), suppose that φ is an L-embedding of G in H and that $|H/\Omega(H)| > p^2$. Let $F = \Phi(G)$ and $\mathfrak{M}$ be the set of maximal subgroups of G and assume further that for every $M \in \mathfrak{M}$, the induced L-embedding φ_M is canonical and has a canonical basis $\mathfrak{B}(M)$ such that $\mathfrak{B}(M)_F = \mathfrak{B}(N)_F$ for all $N \in \mathfrak{M}$. Then φ is canonical and has a canonical basis $\mathfrak{B}$ such that $\mathfrak{B}_M = \mathfrak{B}(M)$ for all $M \in \mathfrak{M}$.*

PROOF. We show first that the lemma is an easy consequence of the following.

(10) For every two different maximal subgroups M and N of G there exists an isomorphism $\sigma = \sigma_{MN} : G/F \to H/F^\varphi$ inducing φ there and satisfying: if $(x, \overline{x}) \in \mathfrak{B}(M)$ and $(y, \overline{y}) \in \mathfrak{B}(N)$ are such that $M/F = \langle x \rangle$ and $N/F = \langle y \rangle$, then $x^\sigma = \overline{x}$ and $y^\sigma = \overline{y}$.

So assume that (10) holds, take $M, N \in \mathfrak{M}$ such that $M \neq N$ and put $\sigma = \sigma_{MN}$. If $M \neq L \in \mathfrak{M}$ and $(z, \overline{z}) \in \mathfrak{B}(L)$ is such that $L/F = \langle z \rangle$, then $\tau = \sigma_{ML}$ induces φ on G/F and satisfies $x^\tau = \overline{x}$ and $z^\tau = \overline{z}$. Then σ and τ induce the same lattice isomorphism of G/F, so $\sigma\tau^{-1}$ is a power automorphism which is trivial since $x^\sigma = x^\tau$. Thus $\sigma = \tau$ and hence σ satisfies for all $L \in \mathfrak{M}$,

$$(11) \qquad z^\sigma = \overline{z} \quad \text{if} \quad (z, \overline{z}) \in \mathfrak{B}(L) \quad \text{is such that} \quad L/F = \langle z \rangle.$$

Let μ be the L-embedding of G/F in H/F^φ induced by φ, and hence by σ; let $\mathfrak{B}_\mu$ be the canonical basis of μ constructed in 3.4 using the pairs $(z, z^\sigma) \in \mathfrak{B}(L)$ for $L \in \mathfrak{M}$. Then $\mathfrak{B}_\mu$ and the $\mathfrak{B}(M)$ satisfy the assumptions of 3.6(b) and hence their union is a canonical basis of φ.

It remains to prove (10). Let $\mathfrak{B}$ be a basis of φ that contains every $\mathfrak{B}(L)$, $L \in \mathfrak{M}$; such a basis exists by 3.6(b).

Now let $M, N \in \mathfrak{M}$ be such that $M \neq N$. Then M and N are of type $(n, n-1)$ and hence $M = \langle c \rangle \times \langle d \rangle$ and $N = \langle x \rangle \times \langle y \rangle$ where $o(c) = o(x) = p^n$ and

https://doi.org/10.1017/S144678870000080X Published online by Cambridge University Press

$o(d) = o(y) = p^{n-1}$. Since $M \neq N$, we have $G = MN = \langle c, x\rangle F$ and hence $G = \langle c\rangle \times \langle x\rangle$; furthermore $M = \langle c\rangle \times (M \cap \langle x\rangle) = \langle c\rangle \times \langle x^p\rangle$ and, similarly, $N = \langle c^p\rangle \times \langle x\rangle$. So if we put $A = \langle c\rangle$ and $B = \langle x\rangle$, we have that $G = A \times B$ where A and B are cyclic of order p^n. Let $U = A^\varphi$, $V = B^\varphi$, and for $i = 0, \ldots, n$, let $A_i \leq A$ and $B_i \leq B$ be such that $|A_i| = p^i = |B_i|$, $U_i = A_i^\varphi$, $V_i = B_i^\varphi$. Then

$$M = A \times B_{n-1} \quad \text{and} \quad N = A_{n-1} \times B. \tag{12}$$

By 2.3, $H = U \times V$, $1 = U_0 < \cdots < U_n = U$ and $1 = V_0 < \cdots < V_n = V$ are smooth chains, and $U \simeq V$. Let $|\Omega(U)| = p^r$. Since $|H/\Omega(H)| > p^2$, U_{n-1} is not elementary abelian; thus, by 2.4,

$$\Omega(U) < U_{n-1} \quad \text{and} \quad r < n-1. \tag{13}$$

If we apply 3.7 to $G = A \times B$, we obtain generators a of A and b of B, elements $u \in U$ and $v \in V$, and integers $i, j, s, t \in \{1, \ldots, p-1\}$ such that $\mathfrak{B}$ contains the pairs (aA_{n-1}, uU_{n-1}), $(a^{ip^r}A_{n-r-1}, u^{isp}U_{n-r-1})$, (bB_{n-1}, vV_{n-1}), and $(b^{jp^r}B_{n-r-1}, v^{jtp}V_{n-r-1})$. By (b) of 3.7,

(14) φ is induced on G/F by the isomorphism $\sigma^* : G/F \to H/F^\varphi$ satisfying $(aF)^{\sigma^*} = u^s F^\varphi$ and $(bF)^{\sigma^*} = v^t F^\varphi$.

Now we apply 3.7 to $F = A_{n-1} \times B_{n-1}$. By (13), the assumptions of 3.7 hold with n replaced by $n-1$ but with the same r as before. Therefore there exist generators a_1 of A_{n-1} and b_1 of B_{n-1}, elements $u_1 \in U_{n-1}$ and $v_1 \in V_{n-1}$, and integers μ, ν, m such that $\mathfrak{B}_F$, and hence also $\mathfrak{B}$, contains the pairs (a_1A_{n-2}, u_1U_{n-2}), $(a_1^{\mu p^r}A_{n-r-2}, u_1^{\mu mp}U_{n-r-2})$, (b_1B_{n-2}, v_1V_{n-2}), and $(b_1^{\nu p^r}B_{n-r-2}, v_1^{\nu mp}V_{n-r-2})$; note that $\mathfrak{B}_F$ is canonical so that 3.7(c) yields the same power of $u_1^{\mu p}$ and $v_1^{\nu p}$ here.

Next we apply 3.7 to $M/A_1 = AF/A_1 = A/A_1 \times B_{n-1}A_1/A_1$, the canonical L-embedding induced by φ_M in M/A_1 and the induced basis $\mathfrak{B}(M)^*$; since $U/U_1 \simeq U_{n-1}$, the assumptions of 3.7 hold. For short, we write $\tilde{x}$ and $\tilde{X}$ for the images of elements x or subgroups X under the natural homomorphisms of G to G/A_1 and of H to H/U_1. By (13), $A_1 \leq A_{n-r-1}$ and hence $\mathfrak{B}(M)^*$ contains the pairs $(\tilde{a}\tilde{A}_{n-1}, \tilde{u}\tilde{U}_{n-1})$ and $(\tilde{a}^{ip^r}\tilde{A}_{n-r-1}, \tilde{u}^{isp}\tilde{U}_{n-r-1})$; by 3.3 there exist $\lambda, \varrho \in \mathbb{Z}$ such that $\mathfrak{B}(M)^*$ contains $(\tilde{b}_1^\lambda \tilde{B}_{n-2}, \tilde{v}_1^\lambda \tilde{V}_{n-2})$ and $(\tilde{b}_1^{\nu\varrho p^r}\tilde{B}_{n-r-2}, \tilde{v}_1^{\nu m\varrho p}\tilde{V}_{n-r-2})$. Since $\mathfrak{B}(M)^*$ is canonical, (c) of 3.7 implies that $m = s$.

If we finally apply 3.7 to the symmetric situation in the factor group $N/B_1 = A_{n-1}B_1/B_1 \times B/B_1$, we obtain that $m = t$. It follows that $s = t$.

Let τ be the power automorphism of H/F^φ mapping every element x to x^w where $sw \equiv 1 \pmod p$ and let $\sigma = \sigma^*\tau$. Then by (14), φ is induced by σ on G/F and $(aF)^\sigma = uF^\varphi$, $(bF)^\sigma = vF^\varphi$. Since $\mathfrak{B}(M)$ is canonical and M/F is projective to A/A_{n-1}, by 3.3 there exists $k \in \mathbb{Z}$ such that $(a^kF, u^kF^\varphi) \in \mathfrak{B}(M)$ and $M/F = \langle a^kF\rangle$; similarly, there exists $l \in \mathbb{Z}$ such that $(b^lF, v^lF^\varphi) \in \mathfrak{B}(N)$ and $\langle b^lF\rangle = N/F$. Since

$(a^k F)^\sigma = u^k F^\varphi$ and $(b^l F)^\sigma = v^l F^\varphi$, the isomorphism σ satisfies (10). This proves (10) and the lemma.

We can now construct the desired extension.

LEMMA 3.9. *Let $1 \le k \le n$ and $G = A \times B$ with cyclic groups A of order p^n and B of order p^k; for $i = 0, \dots, n$, let $A_i \le A$ be such that $|A_i| = p^i$. Let $H = U \times V$ be abelian, $|U| = p^n$, $|V| = p^k$, and let $1 = U_0 < \cdots < U_n = U$ be a k-smooth chain with $U_k \simeq V$.*

Let φ be a canonical L-embedding of $G_0 = A_{n-1} \times B$ in $H_0 = U_{n-1} \times V$ such that $A_i^\varphi = U_i$ for $i = 1, \dots, n-1$ and $B^\varphi = V$; let $\mathfrak{B}$ be a canonical basis of φ and suppose that $G/G_0 = \langle w \rangle$ and $H/H_0 = \langle \overline{w} \rangle$.

Then there exists an extension of φ to a canonical L-embedding ψ of G in H satisfying $A^\psi = U$; furthermore there exists a canonical basis $\mathfrak{C}$ of ψ containing $\mathfrak{B}$ and, if V is elementary abelian, the pair $(w, \overline{w})$.

PROOF. We use induction on $|G|$. If $n = k = 1$, then G and H are elementary abelian of order p^2 and there exists an isomorphism $\varrho : G \to H$ satisfying $A^\varrho = U$, $w^\varrho = \overline{w}$, and $b^\varrho = v$ if $\mathfrak{B} = \{(b, v)\}$; by 3.4, the L-embedding ψ induced by ρ is canonical and has a canonical basis $\mathfrak{C}$ containing (b, v) and $(w, \overline{w})$.

So suppose that $n + k \ge 3$ and that the assertion is true for groups of smaller order.

Case 1: $n > k$. Then $N := A_{n-k} \ne 1$ and $G_0 = \Omega_{n-1}(G)$; by 2.2, the assumptions of the lemma hold for the L-embedding $\tilde{\varphi}$ with canonical basis $\tilde{\mathfrak{B}}$ induced by φ and $\mathfrak{B}$, respectively, in G_0/N. The induction assumption yields an extension $\tilde{\psi}$ of $\tilde{\varphi}$ to a canonical L-embedding of G/N in H/N^φ such that $(A/N)^{\tilde{\psi}} = U/N^\varphi$ and a canonical basis $\tilde{\mathfrak{C}}$ of $\tilde{\psi}$ that contains $\tilde{\mathfrak{B}}$ and, if $VN/N \simeq V$ is elementary abelian, the pair $(w, \overline{w})$.

Let $1 \le Y < X \le G$ such that $|X : Y| = p$ and suppose that $X \not\le G_0$. Then X contains an element $x = ab$ of order p^n, where $a \in A$ and $b \in B$, and $x^{p^k} = a^{p^k}$ generates N; thus $N \le X$. Furthermore, if $N \not\le Y$, it would follow that $Y \le G_0$; but then $X = NY \le G_0$, a contradiction. We have shown:

(15) If X/Y is a prime interval in G, then $X \le G_0$ or $N \le Y$.

This shows that the map $\psi : L(G) \to L(H)$ given by $X^\psi = X^\varphi$ for $X \le G_0$ and $X^\psi/N^\varphi = (X/N)^{\tilde{\psi}}$ if $X \not\le G_0$ is well-defined and, clearly, injective. To prove that ψ is an L-embedding, by definition, we have to show that if X covers Y, then X^ψ covers Y^ψ. But (15) and the fact that $\tilde{\psi}$ is induced by φ on G_0/N yield that if X covers Y, then ψ coincides on X and Y either with φ or with the map induced by $\tilde{\psi}$. In both cases, X^ψ covers Y^ψ. Thus ψ is an L-embedding satisfying $A^\psi = U$ and we show that

$$\mathfrak{C} := \mathfrak{B} \cup \left\{ (x, \overline{x}) \in \tilde{\mathfrak{C}} \mid \langle x \rangle = X/Y,\ X \not\le G_0 \right\}$$

https://doi.org/10.1017/S144678870000080X Published online by Cambridge University Press

is a canonical basis of ψ; here, to simplify notation, we identify generators of X/Y and of $(X/N)/(Y/N)$ if $N \leq Y < X$. Indeed, by (15), $\mathfrak{C}$ is a basis of ψ. We have to show that every projectivity $\sigma : X_1/Y_1 \to X_2/Y_2$ between prime intervals of G is regular with respect to $\mathfrak{C}$ and by [1, p. 21], we may assume that X_1 is a maximal subgroup of X_2. If $X_2 \leq G_0$, then $\mathfrak{C}$ coincides with $\mathfrak{B}$ on the intervals X_i/Y_i; and if $X_2 \not\leq G_0$, then by (15), $N \leq X_1 \cap Y_2 = Y_1$ and $\mathfrak{C}$ coincides with $\tilde{\mathfrak{C}}$ on these intervals. In both cases, σ is regular and $\mathfrak{C}$ is a canonical basis having all the desired properties.

Case 2: $n = k$ and V is elementary abelian. Then H is elementary abelian; we let $F = \Phi(G)$ and choose an isomorphism $\varrho : G/F \to H/F^\varphi$ satisfying $(AF/F)^\varrho = UF^\varphi/F^\varphi$, $w^\varrho = \overline{w}$, and $z^\varrho = \overline{z}$ if $(z, \overline{z}) \in \mathfrak{B}$ is such that $G_0/F = \langle z \rangle$. Since in an elementary abelian group every maximal chain is smooth, by induction, for every maximal subgroup $M \neq G_0$ of G there exists an extension of φ_F to a canonical L-embedding $\varphi(M)$ of M in $\overline{M}$ where $\overline{M}/F^\varphi = (M/F)^\varrho$; and $A^{\varphi(M)} = U$ if $M = AF$. Furthermore there exists a canonical basis $\mathfrak{B}(M)$ of $\varphi(M)$ containing $\mathfrak{B}_F$ and the pair (x, x^ϱ) for some generator x of M/F. If μ is the L-embedding of G/F in H/F^φ induced by ϱ, then by 3.4, μ is canonical and has a canonical basis $\mathfrak{B}_\mu$ containing all these (x, x^ϱ) and $(w, \overline{w})$. Now the L-embedding ψ and its canonical basis $\mathfrak{C}$ constructed in Lemma 3.6 have the desired properties.

Case 3: $n = k$ and V is not elementary abelian. Then $A = \langle a \rangle$ and $B = \langle b \rangle$ with $o(a) = o(b) = p^n$; furthermore, by assumption, $V \simeq U_n = U$ and hence both groups are smooth. For $i = 0, \ldots, n$, let $B_i \leq B$ be such that $|B_i| = p^i$, and let $V_i = B_i^\varphi$. Again write $F = \Phi(G) = A_{n-1} \times B_{n-1}$ and let $\mathfrak{M}$ be the set of maximal subgroups of G. The induction assumption applied to $AF = A \times B_{n-1} \in \mathfrak{M}$ yields the following.

(16) There exists an extension of φ_F to a canonical L-embedding $\varphi(AF)$ of AF in UF^φ satisfying $A^{\varphi(AF)} = U$; furthermore there exists a canonical basis $\mathfrak{B}(AF)$ of $\varphi(AF)$ containing $\mathfrak{B}$ and, if V_{n-1} is elementary abelian, a given pair $(x, \overline{x})$ satisfying $AF/F = \langle x \rangle$ and $UF^\varphi/F^\varphi = \langle \overline{x} \rangle$.

We now handle the $M \in \mathfrak{M}$ with $AF \neq M \neq BF = G_0$. These have the form

$$M^{(j)} = D^{(j)}F = D^{(j)} \times B_{n-1} \quad \text{for} \quad j = 1, \ldots, p-1, \tag{17}$$

where $D^{(j)} = \langle ab^j \rangle$. Let $j \in \{1, \ldots, p-1\}$ and write $M = M^{(j)}$ and $D = D^{(j)}$. Then $D \cap F = \langle a^p b^{jp} \rangle$ is a diagonal in F and therefore by (1), $(D \cap F)^\varphi$ is a diagonal in $F^\varphi = U_{n-1} \times V_{n-1}$. By [4, Theorem 1.6.2],

$$(D \cap F)^\varphi = D(U_{n-1}, \tau) = \{uu^\tau \mid u \in U_{n-1}\}$$

https://doi.org/10.1017/S144678870000080X Published online by Cambridge University Press

where $\tau : U_{n-1} \to V_{n-1}$ is an isomorphism. For $i = 1, \dots, n-1$, let D_i be the subgroup of order p^i of D. Then $D_i = (A_i \cup B_{n-1}) \cap (D \cap F)$ and hence by (1),

$$D_i^\varphi = (U_i \cup V_{n-1}) \cap D(U_{n-1}, \tau) = \{uu^\tau \mid u \in U_i\} = U_i^{\tau^*}$$

where τ^* is the natural isomorphism $\tau^* : U_{n-1} \to D(U_{n-1}, \tau)$; $u \mapsto uu^\tau$. Furthermore, $B_i = (A_i \cup (D \cap F)) \cap B_{n-1}$ and hence

$$V_i = (U_i \cup D(U_{n-1}, \tau)) \cap V_{n-1} = U_i^\tau .$$

Thus we have shown that for all $i = 1, \dots, n-1$,

$$U_i^\tau = V_i \quad \text{and} \quad U_i^{\tau^*} = D_i^\varphi . \tag{18}$$

By 2.3, the chain $1 = V_0 < \cdots < V_n = V$ is $(n-1)$-smooth and hence smooth since $|V| = p^n$. By (18) and 2.10, there is an extension of τ to an isomorphism $\overline{\tau} : U \to V$; let $\overline{D} = D(U, \overline{\tau})$. Then $\overline{D}$ is a diagonal in $H = U \times V$ and hence $\overline{M} := \overline{D}F^\varphi = \overline{D} \times V_{n-1}$ is a maximal subgroup of H containing F^φ. By (18), the natural isomorphism $\overline{\tau}^* : U \to \overline{D}; u \mapsto uu^{\overline{\tau}}$ maps U_i to D_i^φ for $i = 1, \dots, n-1$ and therefore $1 = D_0^\varphi < \cdots < D_{n-1}^\varphi < \overline{D}$ is a smooth chain. Since $\overline{D} \simeq U$ is not elementary abelian, 2.4 yields that

$$\Omega(\overline{D}) \le D_{n-1}^\varphi = (D \cap F)^\varphi . \tag{19}$$

Furthermore we see that $M = D \times B_{n-1}$, $\overline{M} = \overline{D} \times V_{n-1}$, φ_F, $\mathfrak{B}_F$ satisfy the assumptions of the lemma in place of G, H, φ, $\mathfrak{B}$, and hence the induction assumption finally implies the following.

(20) There exist an extension of φ_F to a canonical L-embedding $\varphi(M)$ of M in $\overline{M}$ and a canonical basis $\mathfrak{B}(M)$ of $\varphi(M)$ containing $\mathfrak{B}_F$ and, if V_{n-1} is elementary abelian, a given pair $(x, \overline{x})$ satisfying $M/F = \langle x \rangle$ and $\overline{M}/F^\varphi = \langle \overline{x} \rangle$.

Now if $i, j \in \{1, \dots, p-1\}$ with $i \ne j$, then $D^{(i)} \cap D^{(j)} = \langle ab^i \rangle \cap \langle ab^j \rangle = 1$ and hence by (1), $(D^{(i)} \cap F)^\varphi \cap (D^{(j)} \cap F)^\varphi = 1$. Thus by (19), $\overline{D^{(i)}}$ and $\overline{D^{(j)}}$ are diagonals of $H = U \times V$ intersecting trivially, and therefore they generate H; it follows that $\overline{M^{(i)}} \ne \overline{M^{(j)}}$. This shows that there is an L-embedding μ of G/F in H/F^φ satisfying $(AF/F)^\mu = UF^\varphi/F^\varphi$, $(G_0/F)^\mu = H_0/F^\varphi$, and $(M^{(j)}/F)^\mu = \overline{M^{(j)}}/F^\varphi$ for $j = 1, \dots, p-1$. If we write $\varphi = \varphi(G_0)$ and $\mathfrak{B} = \mathfrak{B}(G_0)$, then by (16) and (20), μ and the L-embeddings $\varphi(M)$ and bases $\mathfrak{B}(M)$ ($M \in \mathfrak{M}$) satisfy the assumptions of Lemma 3.6. Let ψ be the L-embedding of G in H constructed there; then $\psi_M = \varphi(M)$ for every $M \in \mathfrak{M}$ and ψ induces μ on G/F.

If V_{n-1} is not elementary abelian, then by 2.4, $\Omega(V) < V_{n-1}$ and hence $|H/\Omega(H)| > p^2$. By 3.8, ψ is canonical and has a canonical basis $\mathfrak{C}$ such that $\mathfrak{C}_M = \mathfrak{B}(M)$ for all $M \in \mathfrak{M}$. In particular, $A^\psi = U$ and $\mathfrak{C}$ contains $\mathfrak{B}$, as desired.

https://doi.org/10.1017/S144678870000080X Published online by Cambridge University Press

So assume, finally, that V_{n-1} is elementary abelian. Since H is not elementary abelian, (b) of 3.7 implies that ψ, and hence also μ, is induced on G/F by an isomorphism ϱ_0. Let $(b_1, v_1) \in \mathfrak{B}$ be such that $G_0/F = \langle b_1 \rangle$ and $H_0/F^\varphi = \langle v_1 \rangle$. If we add a suitable power automorphism of H/F^φ to ϱ_0, we obtain an isomorphism $\varrho : G/F \to H/F^\varphi$ inducing μ and satisfying $b_1^\varrho = v_1$. Now we choose the pairs $(x, \overline{x})$ in (16) and (20) such that $\overline{x} = x^\varrho$. By 3.4 there exists a canonical basis $\mathfrak{B}_\mu$ of μ containing (b_1, v_1) and all these pairs (x, x^ϱ). If ψ^* is the L-embedding of G in H constructed via 3.6 using μ and these new $\varphi(M)$, then by (b) of 3.6 there exists a canonical basis $\mathfrak{C}$ of ψ^* which contains $\mathfrak{B}$. In particular, ψ^* is canonical and this proves the lemma.

PROOF OF THEOREM C. Suppose first that $G = A \times B \times C_3 \times \cdots \times C_r$ has an L-embedding in H. Then by 2.3, $H = A^\varphi \times B^\varphi \times C_3^\varphi \times \cdots \times C_r^\varphi$ where A^φ and B^φ are k-smooth of k-type B^φ and $|C_i^\varphi| = |C_i| = p$ for all i. If $k = 1$, we are done; and if $k \geq 2$, then 2.6 – 2.8 show that (ii) or (iii) of Theorem C holds accordingly as V is or is not elementary abelian.

Conversely, assume that H has the properties given in Theorem C. It suffices to show that $A \times B$ has a canonical L-embedding in $U \times V$; by [1, Theorem 3.1 and 3.3], this can be extended to $G = A \times B \times C_3 \times \cdots \times C_r$. By 2.6 – 2.8, the conditions (i) – (iii) imply that V is smooth and U is k-smooth of type V. Let $1 = U_0 < \cdots < U_n = U$ and $1 = V_0 < \cdots < V_k = V$ be k-smooth chains with $U_i \simeq V_i$ for $i = 0, \ldots, k$; let $1 = A_0 < \cdots < A_n = A$ and $1 = B_0 < \cdots < B_k = B$. Then there exists a canonical L-embedding φ of $A \times B$ in $U \times V$ satisfying $A_i^\varphi = U_i$ and $B_j^\varphi = V_j$ for all i, j; indeed, by induction, we have such an L-embedding of $A_{n-1} \times B$ in $U_{n-1} \times V$ which, by Lemma 3.9, can be extended to $A \times B$. This proves Theorem C.

References

[1] D. W. Barnes, 'Lattice embeddings of prime power groups', *J. Austral. Math. Soc.* **2** (1962), 17–34.
[2] C. Herrmann and P. Huhn, 'Zum Begriff der Charakteristik modularer Verbände', *Math. Z.* **144** (1975), 185–194.
[3] B. Huppert, *Endliche Gruppen I* (Springer, Berlin, 1967).
[4] R. Schmidt, *Subgroup lattices of groups* (De Gruyter, Berlin, 1994).

Mathematisches Seminar
Universität Kiel
D-24098 Kiel
Germany