A LATTICE OF NORMAL SUBGROUPS
THAT IS NOT EMBEDDABLE INTO THE
SUBGROUP LATTICE OF AN ABELIAN GROUP

E. W. KISS and P. P. PÁLFY

1. Introduction.

In this paper we give a negative solution to the following problem of Bjarni Jónsson:

PROBLEM. Is the lattice of normal subgroups of every group embeddable into
the subgroup lattice of an abelian group?

The problem goes back to the famous 1953 paper of Jónsson [J] (see the
last sentence of the text there), and it is also mentioned in the third edition of
Birkhoff’s Lattice Theory [B] (Problem 63, p. 179).

We give a group of order $2^9$ whose lattice of normal subgroups does not
have the desired embedding.

THEOREM. The lattice of normal subgroups of the three generator free
group $G$ in the group variety defined by the laws $x^4 = 1$ and $x^2 y = y x^2$ cannot
be embedded into the subgroup lattice of an abelian group.

We obtained this negative solution in 1988 (see the account given by
McKenzie [M], p. 42), but the publication of the result has been delayed.
Meanwhile the second author and Csaba Szabó [PSz1], [PSz2] have obtained
a stronger result by exhibiting a lattice identity valid in subgroup lattices of
all abelian groups that fails in the lattice of normal subgroups of a certain
group of order $2^{20}$. For the lattice of normal subgroups $\mathcal{N}(G)$ of our group $G$
this identity, however, does hold. We do not know, whether $\mathcal{N}(G)$ belongs
to the lattice variety generated by the subgroup lattices of abelian groups or
not. Our result shows only that it does not belong to the quasivariety
generated by them.

* Research of both authors was partially supported by the Hungarian National Science Founda-
tion, grant nos. 7442 and 16432.

Received July 24, 1996.
Our notation is mostly standard. For basic results from group theory used here the reader may consult [A]. The lattice of normal subgroups of a group \( G \) will be denoted by \( \mathcal{N}(G) \). If \( G \) is abelian, then \( \mathcal{N}(G) \) is simply the subgroup lattice of \( G \). For normal subgroups \( A \subseteq B \subseteq G \) we shall denote the interval in \( \mathcal{N}(G) \) consisting of the normal subgroups \( N \) with \( A \subseteq N \subseteq B \) by \( I[A, B] \). Sometimes we shall treat abelian groups of exponent \( k \) as \( \mathbb{Z}_k \)-modules. For a group \( G \) and a natural number \( m \) we use \( G^m \) to denote the subgroup generated by all \( m \)-th powers in \( G \). If \( G \) is an additively written abelian group then we write \( mG = \{mg \mid g \in G\} \) instead. (Notice that these elements already form a subgroup.)

2. The group \( G \).

As it was mentioned in the Introduction we consider the (relatively) free group \( G \) on three generators in the group variety defined by the laws

\[
\begin{align*}
x^4 &= 1, \\
x^2 y &= xy^2.
\end{align*}
\]

So the square of every element belongs to the center \( Z(G) \) of \( G \). Notice that the commutators \( [x, y] = x^{-1}y^{-1}xy = (x^{-1})^2(xy^{-1})^2y^2 \) also belong to the center and have order at most two. From these observations it follows that \( [xy, z] = [x, z][y, z] \), \( (xy)^2 = x^2y^2[x, y] \), and \( [y, x] = [x, y] \) (see [A], p. 26). Notice that our variety contains both the 8-element dihedral group and the quaternion group (in fact each of these groups generates the variety). Let the generators of \( G \) be \( a, b, \) and \( c \). It is easy to verify that every element of \( G \) can be written in the form

\[
da^\alpha b^\beta c^\gamma [a, b]^\rho[a, c]^\sigma [b, c]^\tau,
\]

where \( 0 \leq \alpha, \beta, \gamma < 4 \), \( 0 \leq \rho, \sigma, \tau < 2 \). By constructing appropriate homomorphisms into the quaternion group it is also straightforward to see that the above form of the elements of \( G \) is unique. Thus, the order of \( G \) is \( 2^9 \). We have that the center \( Z(G) \) is elementary abelian of order \( 2^6 \) with basis \( a^2, b^2, c^2, [a, b], [a, c], [b, c] \). The commutator subgroup \( G' \) has order \( 2^3 \), the factor group \( G/G' \) is the direct product of three cyclic groups of order four. Furthermore, we have \( 2(G/G') = Z(G)/G' \).

3. The lattice of normal subgroups.

To shorten notation let \( Z = Z(G) \) denote the center. Now the factor group \( G/Z \) is elementary abelian of order \( 2^3 \), so it contains seven minimal subgroups \( U_i/Z \) \((i = 1, \ldots, 7)\). Each \( U_i \) is abelian. Let \( V_i = U_i^2[U_i, G] \).
Let us list all $U_i$’s and the corresponding $V_i$’s by giving their generators.

\[
\begin{align*}
U_1 &= \langle Z, a \rangle & V_1 &= \langle a^2, [a, b], [a, c] \rangle \\
U_2 &= \langle Z, b \rangle & V_2 &= \langle b^2, [a, b], [b, c] \rangle \\
U_3 &= \langle Z, c \rangle & V_3 &= \langle c^2, [a, c], [b, c] \rangle \\
U_4 &= \langle Z, ab \rangle & V_4 &= \langle a^2 b^2 [a, b], [a, b], [a, c] [b, c] \rangle \\
U_5 &= \langle Z, ac \rangle & V_5 &= \langle a^2 c^2 [a, c], [a, c], [a, b] [b, c] \rangle \\
U_6 &= \langle Z, bc \rangle & V_6 &= \langle b^2 c^2 [b, c], [a, b] [a, c], [b, c] \rangle \\
U_7 &= \langle Z, abc \rangle & V_7 &= \langle a^2 b^2 c^2 [a, b] [a, c], [a, b] [a, c], [a, b] [b, c] \rangle
\end{align*}
\]

**Lemma 3.1.** For each $1 \leq i \leq 7$ every subgroup between $V_i$ and $U_i$ is normal in $G$. Moreover, $U_i / V_i$ is elementary abelian of order $2^4$.

**Proof.** Let $V_i \subseteq H \subseteq U_i$. Since $[H, G] \subseteq [U_i, G] \subseteq V_i \subseteq H$, we see that $H$ is normal indeed. As $U_i^0 \subseteq V_i$, it follows that $U_i / V_i$ has exponent 2. For the orders we have $|U_i| = 2^7$ and $|V_i| = 2^3$, hence $|U_i / V_i| = 2^4$.

Though we do not need it for the proof of our main result, we describe the lattice of normal subgroups of $G$. We shall use the following simple

**Lemma 3.2.** If $P$ is a finite $p$-group and $M$ is a maximal subgroup of $P$, then $[M, P] = P'$.

**Proof.** Notice that $|P : M| = p$ and $M$ is normal in $P$. Now $M / [M, P] \leq Z(P / [M, P])$ and $(P / [M, P]) / (M / [M, P])$ is cyclic (of order $p$), hence $P / [M, P]$ is abelian. Therefore we have $[M, P] \supseteq P'$. The converse inclusion is obvious.

**Proposition 3.3.** The lattice of normal subgroups of $G$ is the union of the following nine intervals:

\[I[G', G], \ I[V_i, U_i] \ (i = 1, \ldots, 7), \ I[\{1\}, Z(G)].\]

**Proof.** Let $N$ be an arbitrary normal subgroup of $G$. We consider the product $NZ$. If $NZ = Z$, then $N$ is contained in $Z$. If $NZ = U_i$ for some $i$, $1 \leq i \leq 7$, then we have $N \supseteq N^2 [N, G] = (NZ)^2 [NZ, G] = U_i^2 [U_i, G] = V_i$, so $N$ belongs to the interval $I[V_i, U_i]$. Finally, if $|G : NZ| \leq 2$, then $N \supseteq [N, G] = [NZ, G] = G'$.

4. **Embeddings of $\mathcal{N}(Z^n_p)$.**

The following lemma about embeddings of the subgroup lattice of $Z^n_p$ ($n \geq 3$) will play a central role in our proof. Parts of its statement are well-known, but the freeness of $X$ may not have been observed before.
Lemma 4.1. Let \( \varphi : \mathcal{N}(\mathbb{Z}_p^n) \to \mathcal{N}(A) \) be a lattice embedding, where \( p \) is a prime, \( k \geq 1 \), \( A \) is an abelian group, and assume that \( \varphi(\{0\}) = \{0\} \) and \( \varphi(\mathbb{Z}_p^n) = A \). If \( n \geq 3 \), then \( A \) is isomorphic to a direct power \( X^n \) of a free \( \mathbb{Z}_p \)-module \( X \). Moreover, having identified \( A \) and \( X^n \),

\[(1) \quad \varphi((z_1, \ldots, z_n)) = \{(z_1x, \ldots, z_nx) \mid x \in X\} \]

holds for all \((z_1, \ldots, z_n) \in \mathbb{Z}_p^n\).

Proof. For notational simplicity we deal with the case \( n = 3 \), the proof for \( n > 3 \) is similar. Let \( E_1 = \langle (1, 0, 0) \rangle \), \( E_2 = \langle (0, 1, 0) \rangle \), \( E_3 = \langle (0, 0, 1) \rangle \), and \( E_0 = \langle (1, 1, 1) \rangle \). These subgroups form a spanning 3-frame in \( \mathcal{N}(\mathbb{Z}_p^3) \), hence so do their images in \( \mathcal{N}(A) \). So by Lemma 1 of [HH2] we may assume that \( A = X^3 \) for some abelian group \( X \), and we have \( \varphi(E_1) = \{(x, 0, 0) \mid x \in X\} \), \( \varphi(E_2) = \{(0, x, 0) \mid x \in X\} \), \( \varphi(E_3) = \{(0, 0, x) \mid x \in X\} \), and \( \varphi(E_0) = \{(x, x, x) \mid x \in X\} \). We introduce the notation \( E_i^* = \varphi(E_i) \), \( i = 0, 1, 2, 3 \).

In [HH2] lattice terms \( f_j \) \((j = 1, 2, \ldots)\) are constructed such that \( f_j(E_0^*, E_1^*, E_2^*, E_3^*) = \{(0, jx, x) \mid x \in X\} \) (and also \( f_j(E_0, E_1, E_2, E_3) = \{(0, j, t) \mid t \in \mathbb{Z}_p\} \)). Since in \( \mathbb{Z}_p^3 \) we have \( f_p(E_0, E_1, E_2, E_3) = E_3 \), using the homomorphism \( \varphi \) we obtain \( f_p(E_0^*, E_1^*, E_2^*, E_3^*) = E_3^* \), i.e. \( p^kX = 0 \), so \( X \) can be considered as a \( \mathbb{Z}_p \)-module. Our goal is to prove that \( X \) is in fact a free \( \mathbb{Z}_p \)-module.

We have in \( \mathcal{N}(\mathbb{Z}_p^n) \):

\[
\langle (p, 0, 0) \rangle = \langle (1, 0, 0) \rangle \cap \langle (1, p^{k-1}, 0) \rangle = E_1 \cap f_{p^{k-1}}(E_0, E_3, E_2, E_1)
\]

and

\[
\langle (p, 0, 0) \rangle = \langle (1, 0, 0) \rangle \cap (\langle (p, 1, 0) \rangle + \langle (0, 1, 0) \rangle)
\]

\[
= E_1 \cap (f_p(E_0, E_3, E_1, E_2) + E_2).
\]

Using the lattice homomorphism \( \varphi \) we obtain

\[
E_1^* \cap f_{p^{k-1}}(E_0^*, E_3^*, E_2^*, E_1^*) = E_1^* \cap (f_p(E_0^*, E_3^*, E_1^*, E_2^*) + E_2^*),
\]

that is

\[
\{(x, 0, 0) \mid x \in X\} \cap \{(y, p^{k-1}y, 0) \mid y \in X\}
\]

\[
= \{(u, 0, 0) \mid u \in X\} \cap (\{(pv, v, 0) \mid v \in X\} + \{(0, w, 0) \mid w \in X\}),
\]

so

\[
\{(x, 0, 0) \mid x \in X, p^{k-1}x = 0\} = \{(pv, 0, 0) \mid v \in X\},
\]
from which it follows that $X$ is a free $\mathbb{Z}_{p^k}$-module. Thus we can assume that $X$ is equal to a direct sum of some, say $\kappa$, copies of $\mathbb{Z}_{p^k}$'s.

It remains to show (1). For every element

$$u = (\ldots, u_i, \ldots) \in \bigoplus_{\kappa} \mathbb{Z}_{p^k}$$

with

$$u_i = (u_i^1, u_i^2, u_i^3) \in \mathbb{Z}_{p^k}^3$$

define

$$\rho(u) = ((\ldots, u_i^1, \ldots), (\ldots, u_i^2, \ldots), (\ldots, u_i^3, \ldots)) \in X^3.$$ 

Clearly, $\rho : \bigoplus_{\kappa} \mathbb{Z}_{p^k}^3 \to X^3$ is a group-isomorphism. For a subgroup $U \subseteq \mathbb{Z}_{p^k}^3$ let $\psi(U) \subseteq X^3$ be the image of $\bigoplus_{\kappa} U$ under $\rho$. Then $\psi$ is a lattice embedding of $\mathcal{N}(\mathbb{Z}_{p^k}^3)$ into $\mathcal{N}(X^3)$. An easy calculation shows that (1) holds, when $\varphi$ is replaced by $\psi$. In particular, $\psi(E_i) = \varphi(E_i)$ for $i = 0, 1, 2, 3$. It is shown in [HH1] (see Section 3.2) that the 3-frame $E_0, E_1, E_2, E_3$ generates $\mathcal{N}(\mathbb{Z}_{p^k}^3)$. Therefore $\psi = \varphi$, proving (1).

**Corollary 4.2.** For every subgroup $U$ of $\mathbb{Z}_{p^k}^n$ and for every positive integer $m$ we have $\varphi(mU) = m\varphi(U)$.

**Proof.** By (1) the claim is obvious for cyclic subgroups $U$. If $U$ is arbitrary, then write it as a sum of cyclic subgroups $U = \sum C_i$. Then it follows easily that $\varphi(mU) = \varphi(m \sum C_i) = \varphi(\sum mC_i) = \sum \varphi(mC_i) = m \sum \varphi(C_i) = m \varphi(\sum C_i) = m\varphi(U)$.

5. **Proof of the Theorem.**

Let us assume, by way of contradiction, that there exists an embedding of $\mathcal{N}(G)$ into $\mathcal{N}(A)$ for some abelian group $A$. Let us denote the image of a normal subgroup $N$ of $G$ under this embedding by $N^\ast$. Without loss of generality we may suppose that $\{1\}^\ast = \{0\}$ and $G^\ast = A$.

The interval between $\{1\}$ and $Z = Z(G)$ in $\mathcal{N}(G)$ is isomorphic to $\mathcal{N}(\mathbb{Z}_2^k)$ and the interval between $Z$ and $G$ is isomorphic to $\mathcal{N}(\mathbb{Z}_3^2)$. Hence by Lemma 4.1 both $Z^\ast$ and $A/Z^\ast$ have exponent 2, hence the exponent of $A$ divides 4, so in other words $A$ is a $\mathbb{Z}_4$-module. Moreover, the interval between $D = G^\ast$ and $G$ is isomorphic to $\mathcal{N}(\mathbb{Z}_4^2)$, hence – again by Lemma 4.1 – it follows that $A/D^\ast$ is a free $\mathbb{Z}_4$-module. Since free modules are projective, we have that $A = D^\ast \oplus B$ for some subgroup $B$. Note that $2D^\ast = 0$, hence $2A = 2B$. 
Now take the normal subgroups $U_i$, $V_i$ defined in Section 3. Since $U_i/V_i$ is elementary abelian of order $2^4$, another application of Lemma 4.1 yields that $U_i^*/V_i^*$ has exponent 2, i.e. $2U_i^* \subseteq V_i^*$. We also have $2U_i^* \subseteq 2A = 2B$.

Consider the embedding $\psi$ of $\mathcal{N}(G/D) \cong \mathcal{N}(Z_4^2)$ into $\mathcal{N}(A/D^*)$ induced by $\iota$. Applying Corollary 4.2 we get that $2\psi(U_iD/D) = \psi(2(U_iD/D))$. But we have $V_iD = U_i^2D$ in $G$, so $2(U_iD/D) = V_iD/D$. Thus, $(D^* + V_i^*)/D^* = \psi(V_iD/D) = 2((D^* + U_i^*)/D^*)$, hence

$$D^* + V_i^* = D^* + 2U_i^*.$$ From $A = D^* \oplus B$ we get for every $C \supseteq D^*$ that $C = D^* \oplus (B \cap C)$. The mapping $\iota: (B \cap C)$ is a lattice isomorphism $\mathcal{N}(A/D^*) \rightarrow \mathcal{N}(B)$. Denote by $\psi: \mathcal{N}(G/D) \rightarrow \mathcal{N}(B)$ the embedding obtained from $\psi$ by composing it with this isomorphism. Applying Corollary 4.2 again we get that $\psi'(2(G/D)) = 2\psi'(G/D)$. We have seen that $2(G/D) = Z/D$, so from $\psi'(G/D) = B$ we obtain that $\psi'(Z/D) = 2B$. On the other hand, $\psi'(Z/D) = Z^* \cap B$. Therefore we get that

$$Z^* = D^* \oplus 2B.$$ Notice that we do not claim that $2B$ or $2U_i^*$ corresponds to any normal subgroup of $G$.

We will show that

$$V_i^* = (D^* \cap V_i^*) \oplus (2B \cap V_i^*)$$

holds for each $1 \leq i \leq 7$. Let us denote the right-hand side of the equation by $W_i$. We obviously have $V_i^* \supseteq W_i$. We take intersection and sum of both $V_i^*$ and $W_i$ with $D^*$. The equation

$$D^* \cap W_i = D^* \cap V_i^*$$

is trivial. On the other hand, we have

$$D^* + W_i = D^* \oplus (2B \cap V_i^*) \supseteq D^* \oplus 2U_i^* = D^* + V_i^*.$$ By modularity, we infer that $V_i^* = W_i$, indeed.

We will reach the contradiction by showing that no such subgroup $K$ exists for which $Z^* = D^* \oplus K$ and $V_i^* = (D^* \cap V_i^*) \oplus (K \cap V_i^*)$ for all $1 \leq i \leq 7$ hold. Using the basis $[a, b], [a, c], [b, c], a^2, b^2, c^2$ of $Z$, Lemma 4.1 provides a decomposition $Z^* \cong X^6$ such that we have
From the direct decomposition that $2$ proves our theorem. The latter condition means $t \neq 0$.

Now $D^* \cap V_1^* = \{(x, y, 0, 0, 0) \mid x, y \in X\}$, hence $V_1^* = (D^* \cap V_1^*) \oplus (K \cap V_1^*)$ implies that

$$V_1^* \cap K = \{(\alpha_1 t, \alpha_2 t, 0, 0, 0) \mid t \in X\}$$

for suitable maps $\alpha_1, \alpha_2$ from $X$ to $X$. It is easy to check that in fact $\alpha_1$ and $\alpha_2$ are endomorphisms of $X$. Similarly,

$$V_2^* \cap K = \{(\alpha_2 t, 0, 0, 0, 0) \mid t \in X\},$$

$$V_3^* \cap K = \{(0, \alpha_3 t, 0, 0, 0) \mid t \in X\}.$$

Hence we have

$$K \supseteq \{ (\alpha_1 r + \alpha_2 s, \alpha_1 r + \alpha_3 s, \alpha_2 r + \alpha_3 s, r, s, t) \mid r, s, t \in X \}.$$

From $Z^* = D^* \oplus K$ it follows that we have equality here. Then

$$V_4^* \cap K = \{((\alpha_1 + \alpha_2) r, \alpha_1 r, \alpha_2 r, r, 0) \mid r \in X, \alpha_1 r = \alpha_2 r\}.$$

From the direct decomposition $V_4^* = (D^* \cap V_4^*) \oplus (K \cap V_4^*)$ we infer that $\alpha_1 r = \alpha_2 r$ holds for every $r \in X$, i.e. $\alpha_1 = \alpha_2$. Similarly, calculating $V_5^* \cap K$ and $V_6^* \cap K$ we obtain $\alpha_1 = \alpha_3$ and $\alpha_2 = \alpha_3$. Finally, using that $2X = 0$ we get

$$V_7^* \cap K = \{((\alpha_1 + \alpha_2) t, (\alpha_1 + \alpha_2) t, (\alpha_2 + \alpha_3) t, t, t) \mid t \in X, \alpha_1 + \alpha_2 + \alpha_3 = 0\}.$$

The latter condition means $t = 0$, so $V_7^* \cap K = \{0\}$, a contradiction. This proves our theorem.

REFERENCES


EÖTVÖS UNIVERSITY
DEPARTMENT OF ALGEBRA AND NUMBER THEORY
BUDAPEST
HUNGARY
*Email:* ewkiss@cs.elte.hu

MATHEMATICAL INSTITUTE OF THE HUNGARIAN ACADEMY OF SCIENCES
BUDAPEST
HUNGARY
*Email:* ppp@math-inst.hu