Algebra and Logic, Vol. 36, No. 4, 1997

NORMAL AUTOMORPHISMS OF FREE SOLVABLE PRO-p-GROUPS

N. S. Romanovskii*

UDC 512.5

An automorphism of a profinite group is called normal if it leaves invariant all (closed) normal subgroups. An automorphism of an abstract group is called p-normal if it leaves invariant each normal subgroup of p-power, where p is prime. An inner automorphism satisfies both of these conditions. Earlier, Romanovskii and Boluts [2] gave a description of normal automorphisms of a free solvable pro-p-group of derived length 2. That description implied, in particular, that the number of normal automorphisms in that group exceeds the number of inner ones. Here we prove that each normal automorphism of a free solvable pro-p-group of derived length ≥ 3 and a p-normal automorphism of an abstract free solvable group of derived length ≥ 2 are inner.

An automorphism of a profinite group is said to be *normal* if all (closed) normal subgroups are left invariant by it. For abstract groups, distinction is made among *normal automorphisms* — keeping normal subgroups, *f-normal* automorphisms — keeping normal subgroups of finite index, and *p-normal* automorphisms — keeping normal subgroups of p-power, where p is prime. Obviously, an inner automorphism satisfies all the conditions mentioned. In [1], f-normal automorphisms of a free solvable group of derived length ≥ 2 were proved inner. In [2], normal automorphisms of a free solvable pro-p-group of derived length 2 were described. That description implied, in particular, that the number of normal automorphisms in the group in question exceeds the number of inner ones. In [3], it was proved that, for $p \neq 2$, each normal automorphism of a free rank ≥ 2 pro-p-group in the variety $\mathcal{N}_2\mathcal{A}$ is inner. This supposition served as a basis for asserting that a p-normal automorphism ($p \neq 2$) of an abstract free $\mathcal{N}_2\mathcal{A}$-group of rank ≥ 2 is inner. Here $\mathcal{N}_2$ denotes the variety of nilpotent groups of class ≤ 2 and $\mathcal{A}$ denotes the variety of Abelian groups. In the present article, we prove the following two statements.

THEOREM 1. Every normal automorphism of a free solvable pro-p-group of derived length ≥ 3 is inner.

THEOREM 2. Every p-normal automorphism of an abstract free solvable group of derived length ≥ 2 is inner.

Obviously, Theorem 2 makes stronger the result by Roman'kov [1] of which we have mentioned above.

1. PRELIMINARY INFORMATION AND STATEMENTS

1.1. All necessary definitions and facts concerning varieties of profinite groups can be found in [3]. We adopt the following notation. Let G be a (profinite) group; then a (closed) subgroup generated by the

*Supported by RFFR grant No. 96-01-01948.

Translated from *Algebra i Logika*, Vol. 36, No. 4, pp. 441-453, July-August, 1997. Original article submitted February 21, 1996.

0002-5232/97/3604-0257 $18.00

subset A will be denoted by $\langle A\rangle$; if $x, y \in G$, put $x^y = y^{-1}xy$, $[x,y] = x^{-1}y^{-1}xy$. If A and B are subsets of G, denote by $[A, B]$ a subgroup generated by all commutators $[a, b]$, where $a \in A$ and $b \in B$. Write G' for a commutator subgroup of G, $G^{(n)} = [G^{(n-1)}, G^{(n-1)}]$, $n \geq 2$. If $g \in G$, $\hat{g}$ stands for a conjugation by an element g, which is an inner automorphism of G.

LEMMA 1. A normal automorphism of a free solvable pro-p-group F of derived length ≥ 3 induces an inner automorphism on the factor group F/F''.

Proof. Let φ be a normal automorphism of the group F. The factor group $\bar{F} = F/[F', F', F']$ is free in the variety $\mathcal{N}_2\mathcal{A}$ of pro-p-groups. The automorphism φ induces a normal automorphism on that group. By Lemma 2 in [3], every normal automorphism of $\bar{F}$ induces an inner automorphism on $\bar{F}/\bar{F}'' \cong F/F''$, whence the lemma.

Let G be a pro-p-group represented as a projective limit $\varprojlim G_i$ of finite p-groups G_i and let Z_p be the ring of p-adic integers. Recall that a *group algebra* of G over Z_p is a (topological) algebra Z_pG equal to the projective limit $\varprojlim Z_p[G_i]$. Denote by $\Delta(G)$ the augmentation ideal of the ring Z_pG, that is, the kernel of the canonical homomorphism $Z_pG \to Z_p$.

LEMMA 2. Let F be a free rank ≥ 2 pro-p-group which is solvable of derived length 2, and $A = F/F'$. Conjugation by elements in F equips F' with the structure of a Z_pA-module. Let φ be an automorphism of F which induces an identity map on A and assume that there exists an element $w \in Z_pA$ such that $t\varphi = tw$ for all $t \in F'$. Then $w \equiv 1 \bmod \Delta(A)$.

The proof imitates that of Lemma 4 in [3].

LEMMA 3. Let F be a free rank ≥ 2 pro-p-group which is solvable of derived length 2. Then any automorphism of F that induces an identity map on the factor group F/F' and on the subgroup F' is a conjugation by an element in F'.

This fact was established in proving the main theorem in [2].

LEMMA 4. Let F be a free solvable pro-p-group of derived length k, $k \geq 3$, and let the automorphism φ of F induce an identity map on the factor group $F/F^{(k-1)}$ and on the subgroup $F^{(k-2)}$. Then φ is an identity automorphism.

Proof. We follow the derivational route of an appropriate statement for abstract groups in Shmel'kin [4].

1.2. Let F be a free solvable pro-p-group of derived length $k \geq 2$, with basis $\{x_1, \ldots, x_n\}$. Below we use the Magnus embedding, which now we are going to describe for the group given. Let A be a free solvable pro-p-group of derived length $k-1$, with basis $\{a_1, \ldots, a_n\}$, and let $Y = y_1 \cdot Z_pA \oplus \cdots \oplus y_n \cdot Z_pA$ be a right free (topological) module over the ring Z_pA, with basis $\{y_1, \ldots, y_n\}$. Consider a pro-p-group G, which is a natural extension of an additive group of the module Y by A. That group can be treated as the matrix group $\begin{pmatrix} A & 0 \\ Y & 1 \end{pmatrix}$, that is, the group of matrices of the form $\begin{pmatrix} a & 0 \\ y & 1 \end{pmatrix}$, where $a \in A$, $y \in Y$. The group F is then identified with a subgroup in G, if we put $x_1 = \begin{pmatrix} a_1 & 0 \\ y_1 & 1 \end{pmatrix}, \ldots, x_n = \begin{pmatrix} a_n & 0 \\ y_n & 1 \end{pmatrix}$. (For more information, consult [5, 6].)

In [6], we showed that there exists a central series (finite for $k = 2$ and infinite for $k > 2$)$\cdot$ $A = A_1 > A_2 > \ldots$ such that $A_i/A_{i+1} \cong Z_p$, $A_i = \langle a_i\rangle \cdot A_{i+1}$ (here $a_1, \ldots, a_n$ coincide with generators of the group A), $\bigcap A_i = 1$, and every neighborhood of unity of A contains a certain subgroup A_i. The group algebra Z_pA, as a topological Z_p-module, is a free module with a basis Ω_A consisting of elements of the form $M = (a_1 - 1)^{\alpha_1} \ldots (a_m - 1)^{\alpha_m}$, where $0 \leq \alpha_i \in Z$. In particular, every element in Z_pA has a unique presentation in the form of a series $\sum\limits_{M \in \Omega_A} \gamma_M \cdot M$, where $\gamma_M \in Z_p$. The weight of an element M is defined thus: $\omega(M)=\alpha_1+2\alpha_2+\cdots+2^{m-1}\alpha_m$. Order elements in Ω_A w.r.t. their weights; elements of equal weight are ordered by successively comparing $\alpha_m,\alpha_{m-1},\ldots,\alpha_1$. The *weight* $\omega(u)$ of a nonzero element $u\in Z_pA$ is the minimum of weights of elements $M\in\Omega_A$, which do really occur in the expansion of u. Put $\omega(0)=\infty$. If $u=\lambda\cdot M+\cdots$, $0\neq\lambda\in Z_p$, and M is a minimal element in Ω_A occurring in the expansion of u, then $\lambda\cdot M$ is called a *lowest* term of u in the expansion w.r.t. Ω_A. Note that if $M=(a_1-1)^{\alpha_1}\ldots(a_m-1)^{\alpha_m}$ and $L=(a_1-1)^{\beta_1}\ldots(a_m-1)^{\beta_m}$ are two elements in Ω_A, then $ML=(a_1-1)^{\alpha_1+\beta_1}\ldots(a_m-1)^{\alpha_m+\beta_m}+v$, where $\omega(v)>\omega(M)+\omega(L)$. This follows immediately from the following:

$$(x-1)(y-1)=(y-1)(x-1)+([x,y]-1)+(y-1)([x,y]-1)+(x-1)([x,y]-1)+(y-1)(x-1)([x,y]-1). \quad (1)$$

Throughout this section, elements of an additive group of the module Y are written multiplicatively, that is, instead of $y_1u_1+\cdots+y_nu_n$, where $u_i\in Z_pA$, we write $y_1^{u_1}\ldots y_n^{u_n}$. A group algebra Z_pY, if treated as a Z_p-module, is a free module with a basis Ω_Y consisting of elements of the form $P=(y_1^{M_1}-1)^{\beta_1}\ldots(y_1^{M_r}-1)^{\beta_r}\ldots(y_n^{L_1}-1)^{\gamma_1}\ldots(y_n^{L_s}-1)^{\gamma_s}$, where $M_i,L_i\in\Omega_A$, $0\le\beta_i,\ \gamma_i\in Z$. Order elements in Ω_Y by successively comparing the following parameters: $\omega_1(P)=\beta_1+\cdots+\beta_r+\cdots+\gamma_1+\cdots+\gamma_s$, $\omega_2(P)=\beta_1\omega(M_1)+\cdots+\beta_r\omega(M_r)+\cdots+\gamma_1\omega(L_1)+\cdots+\gamma_s\omega(L_s)$, $L_s,\gamma_s,\ldots,L_1,\gamma_1,\ldots,M_r,\beta_r,\ldots,M_1,\beta_1$. As a Z_p-basis Ω of the algebra Z_pG, we choose the products MP, where $M\in\Omega_A$ and $P\in\Omega_Y$. An arbitrary element $t\in Z_pG$ has a unique presentation in the form of a series $\sum u_iP_i$, where $u_i\in Z_pA$ and $P_i\in\Omega_Y$. If P_0 is a minimal element in Ω_Y, which does indeed occur in that representation, then u_0P_0 is called a *lowest* term of the element t in the expansion w.r.t. the basis Ω_Y. In turn, if αM is a lowest term of u_0 in its expansion w.r.t. the basis Ω_A, then αMP_0 is called a *lowest* term of t in the expansion w.r.t. Ω. A multiplication rule for the elements in Z_pG expanded in terms of Ω can be underpinned by formula (1) and the following:

$$\begin{gathered}(y_i^M-1)(a_j-1)=\\ (a_j-1)(y_i^M-1)+a_j(y_i^{M(a_j-1)}-1)+a_j(y_i^M-1)(y_i^{M(a_j-1)}-1)=\\ (a_j-1)((y_i^M-1)+(y_i^{M(a_j-1)}-1)+(y_i^M-1)(y_i^{M(a_j-1)}-1))+\\ (y_i^{M(a_j-1)}-1)+(y_i^M-1)(y_i^{M(a_j-1)}-1).\end{gathered} \quad (2)$$

Denote by V_m (resp., by W_l) the collection of elements of Z_pG in the expansion of which w.r.t. the basis Ω_Y only those elements occur for which $\omega_1(P)\ge m$ (resp., $\omega_2(P)\ge l$). Formula (2) implies that the sets V_m and W_l are two-sided ideals of the ring Z_pG, and $V_mV_r\subseteq V_{m+r}$ and $W_lW_s\subseteq W_{l+s}$ hold. Let $l=\omega(M)=\omega_2(y_i^M-1)$. Again from (2), we have $(y_i^M-1)(a_1-1)\equiv(a_1-1)(y_i^M-1)\bmod W_{l+1}$ and $(y_i^M-1)(a_1-1)\equiv(a_1-1)(y_i^M-1)+a_1(y_i^{M(a_1-1)}-1)\bmod V_2$. Moreover, $y_i^{M(a_1-1)}-1\equiv y_i^{(a_1-1)M}-1\bmod W_{l+2}$. This yields the following:

LEMMA 5. Let $1\neq P=(y_{i_1}^{M_1}-1)^{\alpha_1}\ldots(y_{i_s}^{M_s}-1)^{\alpha_s}\in\Omega_Y$ and $\omega_1(P)=m$, $\omega_2(P)=l$. Then $P(a_1-1)\equiv(a_1-1)P\bmod W_{l+1}$ and $P(a_1-1)\equiv(a_1-1)P+a_1(\alpha_1(y_{i_1}^{M_1}-1)^{\alpha_1-1}(y_{i_1}^{(a_1-1)M_1}-1)(y_{i_2}^{M_2}-1)^{\alpha_2}\ldots(y_{i_s}^{M_s}-1)^{\alpha_s}+\cdots+\alpha_s(y_{i_1}^{M_1}-1)^{\alpha_1}\ldots(y_{i_{s-1}}^{M_{s-1}}-1)^{\alpha_{s-1}}(y_{i_s}^{M_s}-1)^{\alpha_s-1}(y_{i_s}^{(a_1-1)M_s}-1))\bmod V_{m+1}+(V_m\cap W_{l+2})$.

LEMMA 6. If $w\in\Delta(G)$ and the element $w(x_1-1)$ is divided in Z_pG on the left by x_1-1, then w is also divided on the left by x_1-1.

Proof. Since $x_1-1=a_1y_1-1=(a_1-1)+(y_1-1)+(a_1-1)(y_1-1)$, this and Lemma 5 imply that if $0\neq t\in Z_pG$ and $t=\sum_{i=1}^{r}u_iP_i+t_1$, where $\omega_1(P_1)=\ldots=\omega_1(P_r)=m$, $\omega_2(P_1)=\ldots=\omega_2(P_r)=l$, and

$t_1 \in V_{m+1} + (V_m \cap W_{l+1})$, then

$$
\begin{aligned}
t(x_1 - 1) &\equiv \sum_{i=1}^{r} u_i(a_1 - 1)P_i, \\
(x_1 - 1)t &\equiv \sum_{i=1}^{r} (a_1 - 1)u_i P_i \bmod V_{m+1} + (V_m \cap W_{l+1}).
\end{aligned} \tag{3}
$$

Assume that the conclusion of the lemma is untrue, that is, w is not divided on the left by $x_1 - 1$. Substituting $a_1 - 1 = (x_1 - 1)y_1^{-1} + (y_1^{-1} - 1)$ produces a representation $w = (x_1 - 1)w_1 + w_2$, where w_2 is expressed only in terms of those elements of the basis Ω in the expansion of which the factor $a_1 - 1$ does not occur. According to (3), the element w_2 cannot be divided either on the left or on the right by $x_1 - 1$. Without loss of generality, we may assume that $w = w_2$. Let uP be a lowest term in the expansion of w w.r.t. the basis Ω_Y. Let $\omega_1(P) = m$ and $\omega_2(P) = l$. If $P \neq 1$, choose all elements $P = P_1, P_2, \ldots, P_r \in \Omega_Y$ which do really occur in the expansion of w w.r.t. Ω_Y, for which $\omega_1(P_i) = m$ and $\omega_2(P_i) = l$. We have $w = \sum_{i=1}^{r} u_i P_i + w'$, where $0 \neq u_i \in Z_pA$, $w' \in V_{m+1} + (V_m \cap W_{l+1})$. To be specific, let $P_1 < P_2 < \ldots < P_r$. Below, we consider three cases.

(1) First assume that $k \geq 3$ and some element u_{i_0} $(1 \leq i_0 \leq r)$ does not lie in Z_p. Let $u_{i_0} = u' + u''$, where $u' \in Z_p$ and $u'' \in \Delta(A)$. By (3), then, the element $u''(a_1 - 1)$ is divided on the left by $a_1 - 1$. The group A has derived length $k-1$, and by induction on k, we can state that the element u'' is divided in Z_pA on the left by $a_1 - 1$. This contradicts the above-envisaged condition that the element w can be expressed only in terms of those elements of Ω in the expansion of which the factor $a_1 - 1$ does not occur.

(2) Next assume that $P \neq 1$ and either $k \geq 3$, $u_1, \ldots, u_r \in Z_p$, or $k = 2$, that is, A is Abelian. Let $P_r = P'(y_s^L - 1)^\beta$, where P' can have only those factors $y_i^M - 1$ which are less than $y_s^L - 1$. It follows from Lemma 5 that the maximal element $Q \in \Omega_Y$, which occurs in the expansion of $(\sum_{i=1}^{r} u_i P_i)(x_1 - 1)$ w.r.t. the basis Ω_Y and satisfies $\omega_1(Q) = m$ and $\omega_2(Q) = l + 1$, is equal to $P'(y_s^L - 1)^{\beta-1}(y_s^{(a_1-1)L} - 1)$. In the expansion mentioned, that element occurs with coefficient $\beta u_r a_1$. If Q occurs in the expansion of w' with coefficient $v \in Z_pA$, then, in the expansion of $w(x_1 - 1)$, it will occur with coefficient $\beta u_r a_1 + v(a_1 - 1)$, by Lemma 5 again. Let $w(x_1 - 1) = (x_1 - 1)h$. Then $h \in V_m$. Since $x_1 - 1 \equiv a_1 - 1 \bmod V_1$, we have $(x_1 - 1)h \equiv (a_1 - 1)h \bmod V_{m+1}$. This means that the element $\beta u_r a_1 + v(a_1 - 1)$ is divided in Z_pA on the left by $a_1 - 1$, which contradicts the assumptions.

(3) Consider the last case where $P = 1$, $k = 2$, and $0 \neq u \in \Delta(A)$. Distinguish in w a component of degree 1, that is, that part of v which is expressed in terms of elements of Ω_Y of the form $y_i^M - 1$. Let $w(x_1-1) = (x_1-1)h$. Then $h \equiv u+z \bmod W_2$, where z is a degree 1 component of the element h. The ensuing congruences will be taken modulo $V_2 + (a_1 - 1)Z_pG$. We have $w(x_1 - 1) \equiv (u + v)((a_1 - 1) + a_1(y_1 - 1)) \equiv v(a_1 - 1) + u(y_1 - 1)$; $(x_1 - 1)h \equiv (y_1 - 1)u$. If $v = v_1(y_{i_1}^{M_1} - 1) + \ldots$, then $v(a_1 - 1) \equiv v_1(y_{i_1}^{(a_1-1)M_1} - 1) + \ldots$ by (2). In this case $v_1(y_{i_1}^{(a_1-1)M_1} - 1) + \ldots + u(y_1 - 1) \equiv (y_1 - 1)u$. The left-hand side of the latter has a canonical expansion w.r.t. Ω_Y. If we want to expand the right-hand side via (2), then no elements of the form $y_i^{(a_1-1)M} - 1$ in Ω_Y are likely to appear, since $u \in Z_p\langle a_2, \ldots, a_n\rangle$. Therefore, $v = 0$, and we are led to the congruence $u(y_1 - 1) \equiv (y_1 - 1)u$. Reduce the right-hand side to the canonical form. Let αM be a lowest term of u in its expansion w.r.t. Ω_A and $M = (a_2 - 1)^{\alpha_2} \ldots (a_n - 1)^{\alpha_n}$. From (2), we have

$$
\begin{gathered}
(y_1 - 1)M - M(y_1 - 1) \equiv \alpha_2 a_2 (a_2 - 1)^{\alpha_2 - 1}(a_3 - 1)^{\alpha_3} \ldots (a_n - 1)^{\alpha_n}(y_1^{a_2 - 1} - 1) + \cdots \\
\alpha_n a_n (a_2 - 1)^{\alpha_2} \ldots (a_{n-1} - 1)^{\alpha_{n-1}}(a_n - 1)^{\alpha_n - 1}(y_1^{a_n - 1} - 1) \equiv \\
\alpha_2 (a_2 - 1)^{\alpha_2 - 1}(a_3 - 1)^{\alpha_3} \ldots (a_n - 1)^{\alpha_n}(y_1^{a_2 - 1} - 1) + \cdots
\end{gathered}
$$

$$\alpha_n(a_2-1)^{\alpha_2}\dots(a_{n-1}-1)^{\alpha_{n-1}}(a_n-1)^{\alpha_n-1}(y_1^{a_n-1}-1)+$$
$$M(\alpha_2(y_1^{a_2-1}-1)+\dots+\alpha_n(y_1^{a_n-1}-1)).$$

It follows that, in the expansion of $(y_1-1)u-u(y_1-1)$ w.r.t. Ω, the coefficients at elements of the basis $(a_1-1)^{\alpha_2-1}(a_3-1)^{\alpha_3}\dots(a_n-1)^{\alpha_n}(y_1^{a_2-1}-1),\dots,(a_2-1)^{\alpha_2}\dots(a_{n-1}-1)^{\alpha_{n-1}}(a_n-1)^{\alpha_n-1}(y_1^{a_n-1})$ are $\alpha\alpha_2,\dots,\alpha\alpha_n$, respectively. In particular, $(y_1-1)u-u(y_1-1)\not\equiv 0$. The lemma is proved.

COROLLARY. Suppose $w\in Z_pG$, and for any natural m, the element $w(x_1-1)^m$ is divided on the left by $(x_1-1)^m$. Then $w\in Z_p\langle x_1\rangle$.

Proof. If an element w is not in $Z_p\langle x_1\rangle$, then it has a presentation in the form $w=\alpha_0+\alpha_1(x_1-1)+\dots+\alpha_m(x_1-1)^m+(x_1-1)^m u$, where $\alpha_i\in Z_p$, $u\in\Delta(G)$, and u is not divided on the left by x_1-1. Let $w(x_1-1)^{m+1}=(x_1-1)^{m+1}v$. Then $(x_1-1)^m u(x_1-1)^{m+1}=(x_1-1)^{m+1}v'$, where $v'=v-\alpha_0-\alpha_1(x_1-1)-\dots-\alpha_m(x_1-1)^m$. We have $u(x_1-1)^{m+1}=(x_1-1)v'$. If $m+1\geq 2$, then $v'\in\Delta(G)$, since otherwise $v_0(x_1-1)\in\Delta(G)^2$, where $v=v_0+v_1$, $0\neq v_0\in Z_p$, $v_1\in\Delta(G)$. By Lemma 6, then, v' is divided on the right by x_1-1. If we continue the argument we come to the equality $u(x_1-1)=(x_1-1)v''$ for some element v''. By Lemma 6, u is divided on the left by x_1-1, which contradicts the condition imposed on u. The corollary is proved.

2. PROOF OF THEOREM 1

2.1. It suffices to prove the theorem for the case where a free solvable pro-p-group has finite rank. Indeed, let F be a free solvable pro-p-group of derived length ≥ 3, with an arbitrary basis X. Let $\{X_j\,/\,j\in J\}$ be the collection of all finite subsets of X, consisting of at least two elements. Consider the canonical homomorphisms $\tau_j: F\to F_j=\langle X_j\rangle$. By definition, $x\tau_j=x$, if $x\in X_j$, and $x\tau_j=1$ if $x\in X\setminus X_j$. Let φ be a normal automorphism of F. Then the restriction of $\varphi\tau_j$ to F_j will be a normal automorphism of the group F_j. Assume that, for each j, that automorphism is inner and equals $\hat{f}_j$, where $f_j\in F_j$. Therefore, if f is a saturation point of the set $\{f_j\,/\,j\in J\}$, then $\varphi=\hat{f}$.

2.2. Assume that a free solvable pro-p-group F of derived length $k\geq 3$ has finite basis $X=\{x_1,\dots,x_n\}$. Let $A=F/F^{(k-1)}$ and $a_1,\dots,a_n$ be canonical images in A of the elements $x_1,\dots,x_n$, respectively. Then A is a free solvable pro-p-group of derived length $k-1$, with basis $\{a_1,\dots,a_n\}$. Let φ be a normal automorphism of F. For $k=3$ by Lemma 1 and for $k\geq 4$ by the inductive hypothesis, then, that automorphism induces an inner automorphism on the group A. The φ modified to an inner automorphism induces an identity map on A. Conjugation by elements in F equips $F^{(k-1)}$ with the structure of a Z_pA-module. The automorphism φ preserves submodules of that module. Therefore, if t is a nontrivial element of $F^{(k-1)}$, then $t\varphi=tw$, where $w\in Z_pA$. Let m be a natural number and $(t(a_1-1)^m)\varphi=t(a_1-1)^m v$, $v\in Z_pA$. Since $(t(a_1-1)^m)\varphi=t\varphi\cdot(a_1-1)^m=tw(a_1-1)^m$ and the Z_pA-submodule generated by t is free, we have $w(a_1-1)^m=(a_1-1)^m v$. For any natural m, therefore, the element $w(a_1-1)^m$ is divided in Z_pA on the left by $(a_1-1)^m$. By the corollary to Lemma 6, we have $w\in Z_p\langle a_1\rangle$. Likewise we can assert that $w\in Z_p\langle a_2\rangle$, whence $w\in Z_p$. If we apply Lemma 2 to a free solvable pro-p-group $F^{(k-2)}$ of derived length 2 we obtain $w=1$. By Lemma 3, the restriction of φ to $F^{(k-2)}$ is a conjugation by some element in $F^{(k-1)}$. Modifying the φ again makes it act identically on $F^{(k-2)}$. By Lemma 4, then, the automorphism φ is an identity map. Theorem 1 is proved.

3. PROOF OF THEOREM 2

Let $\tilde{F}$ be an abstract free solvable group of derived length $k \geq 2$, with basis X, and let φ be a p-normal automorphism of $\tilde{F}$. We break up the proof into a number of stages.

3.1. Theorem 2 reduces to the case of a group of finite rank. Indeed, if $x_1, \dots, x_m$ are distinct elements in X, $m \geq 2$, then there exist $x_{m+1}, \dots, x_n \in X$ such that $\langle x_1, \dots, x_m \rangle \varphi \leq \langle x_1, \dots, x_n \rangle$. Represent the group $\langle x_1, \dots, x_n \rangle$ as the factor group $\tilde{F}/H$, where H is a normal subgroup of $\tilde{F}$, generated by all elements $x \in X \setminus \{x_1, \dots, x_n\}$. In view of that representation, φ induces a p-normal automorphism on the group $\langle x_1, \dots, x_n \rangle$. Assume that this automorphism is a conjugation by some element in $\tilde{F}/H$, letting f $(f \in \langle x_1, \dots, x_n \rangle)$ be a representative of the corresponding coset w.r.t. H. Put $\psi = \varphi \hat{f}^{-1}$. We claim that ψ is an identity automorphism. By construction, ψ acts identically on the elements $x_1, \dots, x_m$. Let $x \in X$. By the above argument, for some element f_1 $(f_1 \in \tilde{F})$, the restriction of ψ to $\langle x_1, \dots, x_n, x \rangle$ coincides with $\hat{f}_1$. The element f_1 then centralizes a subgroup $\langle x_1, \dots, x_m \rangle$. It is trivial to mention that the centralizer of that subgroup is equal to 1 for $m \geq 2$. Consequently, $x\psi = 1$ and $\varphi = \hat{f}$.

Thus, let $X = \{x_1, \dots, x_n\}$ be a finite set and F be a completion of the group $\tilde{F}$ in the pro-p-topology. Then F is a free solvable pro-p-group of derived length k, with basis X, and $\tilde{F}$ is embedded in F. The automorphism φ is uniquely extended to a normal automorphism of the pro-p-group F, which we denote by $\bar{\varphi}$.

3.2. Let $k = 2$. The group $A = F/F'$ is a free Abelian pro-p-group with basis $\{a_1, \dots, a_n\}$, where a_i denotes the canonical image of an element x_i in A. The group $\tilde{A} = \tilde{F}/\tilde{F}'$ is an abstract subgroup of A, generated by elements $a_1, \dots, a_n$. Recall that F' can be treated as a topological Z_pA-module, and $\tilde{F}'$ — as an abstract $Z\tilde{A}$-module. Let t be a nontrivial element of $\tilde{F}'$. Then $t\varphi = tw$, where $w \in Z\tilde{A}$. The description of normal automorphisms of a free solvable pro-p-group of derived length 2 (see [2]) implies that $w \equiv 1 \bmod \Delta(A)$, and if $w \in A$, then $\bar{\varphi}$ is an inner automorphism of F. In our case, the element w is invertible in the ring $Z\tilde{A}$, whence $w = \pm a$, where $a \in \tilde{A}$. The congruence $w \equiv 1 \bmod \Delta(A)$ yields the equality $w = a$. If $\bar{\varphi} = \hat{f}$, where $f \in F$, then $f \equiv a \bmod F'$.

3.3. Let $k \geq 2$. From the preceding subsection (for $k = 2$) and Theorem 1 (for $k \geq 3$), it follows that $\bar{\varphi}$ is an inner automorphism of F. Let $\bar{\varphi} = \hat{f}$, where $f \in F$. By 3.2, an element f modulo F' is comparable with some element of $\tilde{F}$. We prove that $f \in \tilde{F}$. By induction, assume that f modulo $F^{(k-1)}$ is comparable with some element in $\tilde{F}$. This allows us to reduce our problem to the case where $f \in F^{(k-1)}$.

Further, with the notation used in 1.2, consider the Magnus embedding for a group F, introduced therein. Recall that the group $F^{(k-1)}$ is identified with an additive subgroup of the Z_pA-module Y. Let $\tilde{Y}$ be an abstract $Z\tilde{A}$-module (with $\tilde{A} = \tilde{F}/\tilde{F}^{(k-1)}$), generated by $y_1, \dots, y_n$. By [5], the element $y_1u_1 + \dots + y_nu_n$ of Y (resp., of $\tilde{Y}$) lies in F^{k-1} (resp., in $\tilde{F}^{(k-1)}$) if and only if $(a_1 - 1)u_1 + \dots + (a_n - 1)u_n = 0$. Let $f = y_1u_1 + \dots + y_nu_n$. If a is an arbitrary element of $\tilde{A}$ and h an element of $\tilde{F}$ whose projection onto $\tilde{A}$ is equal to a, then $h^{-1}(h\varphi^{-1}) = h^{-1}fhf^{-1} = f(a-1)$. Since $h^{-1}(h\varphi^{-1}) \in \tilde{F}^{(k-1)}$, we have $u_1(a-1), \dots, u_n(a-1) \in Z\tilde{A}$. If we succeed in proving that this implies $u_1, \dots, u_n \in Z\tilde{A}$, it will follow that $f \in \tilde{F}^{(k-1)}$ and φ is an inner automorphism of the group $\tilde{F}$. For the proof of the theorem to be completed, we are thus left to validate the following:

LEMMA 7. Let $\tilde{F}$ be an abstract free solvable group of derived length $k \geq 1$, with basis $\{x_1, \dots, x_n\}$, and let F be its pro-p-completion. If $0 \neq u \in Z_pF$, and for any $\tilde{f} \in \tilde{F}$, $u(\tilde{f} - 1) \in Z\tilde{F}$, then $u \in Z\tilde{F}$.

Proof. Let $k = 1$, that is, $\tilde{F}$ and F are Abelian. The map $x_1 \to 1$, $x_2 \to x_2, \dots, x_n \to x_n$ yields endomorphisms of the rings $Z\tilde{F}$ and Z_pF, whose kernels are the ideals $Z\tilde{F} \cdot (x_1 - 1)$ and $Z_pF \cdot (x_1 - 1)$, respectively. It follows that $Z\tilde{F} \cap Z_pF \cdot (x_1 - 1) = Z\tilde{F} \cdot (x_1 - 1)$. Since $u(x_1 - 1) \in Z\tilde{F}$, there exists an element $u' \in Z\bar{F}$ such that $u(x_1 - 1) = u'(x_1 - 1)$. Then $u = u' \in Z\bar{F}$. Note that in the argument above, use has not been made of $\bar{F}$ being of finite rank.

Let $k \geq 2$ and $1 \neq b \in \bar{F}^{(k-1)}$. The element $u(b-1)$ lies in $Z\bar{F}$, and so it has a representation $u(b-1) = f_1 v_1 + \cdots + f_m v_m$, where f_i are elements of $\bar{F}$, representatives of distinct cosets w.r.t. the subgroup $\bar{F}^{(k-1)}$, $0 \neq v_i \in Z\bar{F}^{(k-1)}$. We prove that $u = f_1 u_1 + \cdots + f_m u_m$ for some $u_i \in Z_p F^{(k-1)}$. To do this, again we consider the Magnus embedding of the group F in $G = \begin{pmatrix} A & 0 \\ Y & 1 \end{pmatrix}$. Let $\{U_j \,/\, j \in J\}$ be the collection of open normal subgroups of A, forming the base of neighborhoods of unity. Put $A_j = A/U_j$ and $G_j = \begin{pmatrix} A_j & 0 \\ Y_j & 1 \end{pmatrix}$, where Y_j is a free $Z_p A_j$-module with basis $\{y_1^{(j)}, \ldots, y_n^{(j)}\}$. The canonical homomorphism $A \to A_j$ and the map $y_1 \to y_1^{(j)}, \ldots, y_n \to y_n^{(j)}$ determine a homomorphism $\tau_j : G \to G_j$. Let $F_j = F\tau_j$. Then $F_j / F_j^{(k-1)}$ is a finite p-group. The homomorphism τ_j induces a homomorphism of group algebras $Z_p F \to Z_p F_j$, which we denote by the same symbol τ_j. If the element u does not have the required representation, then, for some index $j \in J$, we have $u\tau_j = h_1 w_1 + \cdots + h_l w_l$, where h_i are elements of F_j, representatives of distinct cosets w.r.t. the subgroup $F_j^{(k-1)}$, $0 \neq w_i \in Z_p F_j^{(k-1)}$, and, for instance, the coset $h_1 F_j^{(k-1)}$ is distinct from the cosets $f_1\tau_j \cdot F_j^{(k-1)}, \ldots, f_m\tau_j \cdot F_j^{(k-1)}$. We also assume that $c = b\tau_j \neq 1$. The group algebra $Z_p F_j^{(k-1)}$ has no zero divisors, and so $w_i(c-1) \neq 1$. Then $h_1 w_1(c-1) + \cdots + h_l w_l(c-1) \neq (f_1 v_1)\tau_j + \cdots + (f_m v_m)\tau_j = (u(b-1))\tau_j$. We are led to a contradiction.

Thus, there exist elements $u_i \in Z_p F^{(k-1)}$ such that $u = f_1 u_1 + \cdots + f_m u_m$. For any nontrivial element $b \in \bar{F}^{(k-1)}$, we have $u(b-1) \in Z\bar{F}^{(k-1)}$, whence $u_i(b-1) \in Z\bar{F}^{(k-1)}$. Since $\bar{F}^{(k-1)}$ is Abelian, $u_i \in Z\bar{F}$. This proves the lemma, which completes the proof of Theorem 2.

REFERENCES

1. V. A.Roman'kov, "Normal automorphisms of discrete groups," *Sib. Mat. Zh.*, 24, No. 4, 138-149 (1983).
2. N. S. Romanovskii and V. Yu. Boluts, "Normal automorphisms of free solvable pro-p-groups of derived length 2," *Algebra Logika*, 32, No. 4, 441-449 (1993).
3. Ch. Gupta and N. S. Romanovskii, "Normal automorphisms of a free pro-p-group in the variety $\mathcal{N}_2\mathcal{A}$," *Algebra Logika*, 35, No. 3, 249-267 (1996).
4. A. L. Shmel'kin, "Two remarks on free solvable groups," *Algebra Logika*, 6, No. 2, 95-109 (1967).
5. V. N. Remeslennikov, "Embedding theorems for profinite groups," *Izv. Akad. Nauk SSSR, Ser. Mat.*, 43, No. 2, 399-417 (1979).
6. N. S. Romanovskii, "A generalized theorem on freeness for pro-p-groups," *Sib. Mat. Zh.*, 27, No. 2, 154-170 (1986).