THE RESTRICTED ISOMORPHISM PROBLEM
FOR METACYCLIC RESTRICTED LIE ALGEBRAS

HAMID USEFI

(Communicated by Gail R. Letzter)

Abstract. Let $L$ be a restricted Lie algebra with the restricted enveloping algebra $u(L)$ over a perfect field of positive characteristic $p$. The restricted isomorphism problem asks what invariants of $L$ are determined by $u(L)$. This problem is the analogue of the modular isomorphism problem for finite $p$-groups. Bagiński and Sandling have given a positive answer to the modular isomorphism problem for metacyclic $p$-groups. In this paper, we provide a positive answer to the restricted isomorphism problem in case $L$ is metacyclic and $p$-nilpotent.

1. Introduction

Let $L$ be a Lie algebra over a field $F$ of positive characteristic $p$ and denote by ad : $L \to L$ the adjoint representation of $L$ given by $(\text{ad}x)(y) = [y, x]$, where $x, y \in L$. Recall that $L$ is called restricted if $L$ additionally affords a $p$-map $[p] : L \to L$, satisfying

1. $(\text{ad}x)^{p} = \text{ad}(x^{[p]})$, for every $x \in L$;
2. $(\alpha x)^{[p]} = \alpha^{p}x^{[p]}$, for every $x \in L$ and $\alpha \in F$; and
3. $(x + y)^{[p]} = x^{[p]} + y^{[p]} + \sum_{i=1}^{p-1} s_{i}(x, y)$, for all $x, y \in L$, where $s_{i}(x, y)$ is the coefficient of $\lambda^{i-1}$ in $\text{ad}(\lambda x + y)^{p-1}(x)$.

Let $L$ be a restricted Lie algebra and denote by $u(L)$ the restricted enveloping algebra of $L$. The restricted isomorphism problem asks what invariants of $L$ are determined by $u(L)$; i.e., given another restricted Lie algebra $H$ with the property that $u(L) \cong u(H)$, as algebras, can we deduce that $L$ and $H$ have the same invariants? Of course, the strongest invariant of $L$ is its isomorphism type. We have considered the restricted isomorphism problem for abelian restricted Lie algebras in [10]. One main result of [10] states that if $L$ is an abelian restricted Lie algebra in the class $\mathcal{F}_{p}$, then the isomorphism type of $L$ is determined. Recall that $L$ is said to be in the class $\mathcal{F}_{p}$ if $L$ is finite-dimensional and there exists an integer $k$ such that $L^{[p]} = 0$. It is also proved in [10] that if $F$ is algebraically closed, then every finite-dimensional abelian restricted Lie algebra over $F$ is determined by its enveloping algebra.
The restricted isomorphism problem is the analogue of the modular isomorphism problem for group algebras of finite \( p \)-groups [8]. This sort of isomorphism problem also makes sense for ordinary Lie algebras and has been considered by David Riley and the present author in [6].

Bagiński [2] and Sandling [7] proved that every metacyclic \( p \)-group \( G \) is determined by its modular group algebra \( \mathbb{F}_p G \), where \( \mathbb{F}_p \) denotes the field of \( p \) elements.

Motivated by this result of Bagiński and Sandling, in this paper we consider the isomorphism problem for metacyclic restricted Lie algebras in the class \( \mathcal{F}_p \). Recall that a restricted Lie algebra \( L \) is called metacyclic if \( L \) has a cyclic restricted ideal \( I \) such that \( L/I \) is cyclic. Our main result is as follows:

**Theorem.** Let \( L \in \mathcal{F}_p \) be a metacyclic restricted Lie algebra over a perfect field of positive characteristic. Then \( L \) is determined by its enveloping algebra \( u(L) \).

Before closing this section, I would like to thank Luzius Grunenfelder for many useful discussions.

2. Preliminaries

Let \( L \) be a restricted Lie algebra with the restricted enveloping algebra \( u(L) \) over a field \( \mathbb{F} \) of characteristic \( p \). Let \( X \) be an ordered basis of \( L \) over \( \mathbb{F} \). The analogue of the Poincaré-Birkhoff-Witt (PBW) Theorem for restricted Lie algebras (see [3]) allows us to view \( L \) as a restricted Lie subalgebra of \( u(L) \) in such a way that \( u(L) \) has a basis consisting of PBW monomials, that is, monomials of the form

\[ x_1^{a_1} \cdots x_t^{a_t}, \]

where \( x_1 < \cdots < x_t \) in \( X \), \( 0 \leq a_i \leq p - 1 \), and \( t \) is a non-negative integer. Henceforth, we identify the \([p] \)-map of \( L \) by the exponentiation by \( p \) in \( u(L) \).

The augmentation ideal, \( \omega(L) \), of \( u(L) \) is the associative ideal of \( u(L) \) generated by \( L \). Let \( \gamma_1(L) := L \). We denote by \( \gamma_n(L) := [\gamma_{n-1}(L), L] \) the \( n \text{th} \) term of the lower central series of \( L \). Hence, \( L' = \gamma_2(L) \). Recall that \( L \) is said to be nilpotent if \( \gamma_n(L) = 0 \) for some \( n \); the nilpotence class of \( L \), denoted by \( cl(L) \), is the minimal integer \( c \) such that \( \gamma_{c+1}(L) = 0 \). We shall denote by \( L' \) the restricted Lie subalgebra of \( L \) generated by \( L' \). For a subset \( X \) of \( L \) we denote by \( \langle X \rangle \) and \( \langle X \rangle_p \) the Lie subalgebra and the restricted Lie subalgebra generated by \( X \), respectively. We consider left-normed commutators, that is,

\[ [x_1, \ldots, x_n] = [(x_1, x_2), x_3, \ldots, x_n]. \]

An element \( x \in L \) is called \( p \)-nilpotent if there exists some non-negative integer \( t \) such that \( x^{p^t} = 0 \); the exponent of \( x \), denoted by \( \exp(x) \), is the least integer \( s \) such that \( x^{p^s} = 0 \). A \( p \)-polynomial in \( x \) has the form \( c_0 x + c_1 x^{p} + \cdots + c_t x^{p^t} \), where each \( c_i \in \mathbb{F} \). Also, recall that \( L \) is \( p \)-nilpotent if there exists a positive integer \( k \) such that \( L^{p^k} = 0 \); the exponent of \( L \), denoted by \( \exp(L) \), is the minimal integer \( s \) such that \( L^{p^s} = 0 \). We say \( L \in \mathcal{F}_p \) if \( L \) is finite-dimensional and \( p \)-nilpotent. Note that if \( L \in \mathcal{F}_p \), then \( L \) is nilpotent by Engel’s Theorem. It is known that \( L \in \mathcal{F}_p \) if and only if \( \omega(L) \) is nilpotent as an associative ideal of \( u(L) \); see [5].

The \( n \text{th} \) dimension subalgebra of \( L \) is

\[ D_n(L) = L \cap \omega^n(L) = \sum_{p^j \geq n} \gamma_j(L)^{p^j}, \]
where $\gamma_i(L)^p$ is the restricted subalgebra of $L$ generated by all $x^{p^i}$, $x \in \gamma_i(L)$; see [5]. It follows from the defining axioms of $L$ that $(x + y)^p = x^p + y^p$ modulo $\gamma_p((x, y))$. It is not hard to see that $[D_n(L), D_m(L)] = \gamma_{m+n}(L) \subseteq D_{m+n}(L)$ and $D_n(L)^p \subseteq D_{np}(L)$, for every $m, n \geq 1$.

Throughout this paper, we assume that $L$ and $H$ are restricted Lie algebras and $\varphi : u(L) \to u(H)$ is an isomorphism. It is proved in [10] that $\varphi$ can be replaced by another isomorphism that preserves the augmentation ideals. So, without loss of generality, we assume that $\varphi(\omega(L)) = \omega(H)$. We need the following results from [10].

**Lemma 2.1.** If $u(L) \cong u(H)$, then the following statements hold.

1. If $L \in \mathcal{F}_p$, then $|cl(L) - cl(H)| \leq 1$.
2. $D_i(L)/D_{i+1}(L) \cong D_i(H)/D_{i+1}(H)$, for every $i \geq 1$.

We remark that whether or not the nilpotence class of $G$ is determined by $\mathcal{F}_p G$ has been considered in recent years. However no major result is reported up-to-date; see [1].

We note that $u(L)$ has the invariant dimension property: that is, the rank of every $u(L)$-module is uniquely defined. Now let $I$ be a restricted ideal of $L$ and denote by $I^n$ the vector space spanned by all $z_1 z_2 \ldots z_n$, where $z_i \in I$. We know that the kernel of the natural map $u(L) \to u(L/I)$ is equal to $I u(L) = u(L) I$. It follows that $\omega^n(I) u(L) = I^n u(L) \cong (I u(L))^n$, for every $n \geq 1$. Furthermore, we observe that each quotient $I^n u(L)/I^{n+1} u(L)$ has a natural right $u(L/I)$-module structure given by

$$(u + I^{n+1} u(L)) \cdot (z + I u(L)) = uz + I^{n+1} u(L),$$

for every $u \in I^n u(L)$ and $z \in u(L)$. The proofs of the following two lemmas are analogous to the corresponding lemmas in [9].

**Lemma 2.2.** Let $I$ be an ideal of $L$. Then each factor $I^n u(L)/I^{n+1} u(L)$ is a free right $u(L/I)$-module of rank $\dim \omega^I(I)/\omega^{n+1}(I)$.

**Lemma 2.3.** Suppose that $\dim \omega^I(D_2(I))$ is finite. Suppose further that $J$ is a restricted ideal of $H$ such that $\varphi(I u(L)) = J u(H)$. Then $D_n(I)/D_{n+1}(I) \cong D_n(J)/D_{n+1}(J)$, for every $n \geq 1$.

Using the identity $[a, [b, c]] = [a b, c] + [a, c] b$, which holds in any associative algebra, we can see that $L_p u(L) = \omega(L) \omega(L) u(L)$. Thus the ideal $L_p u(L)$ is preserved by $\varphi$. So we may apply the previous lemma to the case $I = L_p$ and $J = H_p$.

**Corollary 2.4.** Suppose that $L$ and $H$ are finite-dimensional restricted Lie algebras such that $u(L) \cong u(H)$. Then, for every positive integer $n$, we have

$$D_n(L_p)/D_{n+1}(L_p) \cong D_n(H_p'/p)/D_{n+1}(H_p'),$$

**Lemma 2.5.** Let $L \in \mathcal{F}_p$ such that $cl(L) = 2$. Then, $\dim L_p$ is determined, for every $t \geq 0$. In particular, the exponent of $L'$ is determined.

**Proof.** Note that, by Lemma 2.1, $H$ is nilpotent of class at most 3. So, $H'$ is abelian. Note that $D_{p^t+1}(H_p') = \cdots = D_{p^t}(H_p') = H^{p^t}$, for every $t \geq 1$. So, by Corollary 2.4 we have $L'_p / L^{p^t} \cong H_p'/H'$, for every $t \geq 1$.
for every \( t \geq 1 \). Now let \( s = \exp(L') \). It follows that

\[
H^{p^t} = H^{p^{t+1}}.
\]

But \( H \) is \( p \)-nilpotent. Hence, \( H^{p^t} = 0 \). Thus \( \exp(H') \leq \exp(L') \). It follows then by symmetry that the exponent of \( H' \) is \( s \). A reverse induction on \( t \) shows that \( \dim s L'_p \) is determined, for every \( t \geq 0 \).

\[\square\]

**Lemma 2.6.** Let \( L \in \mathcal{F}_p \) such that \( L'_p \) is cyclic. The following statements hold.

1. \( cl(L) \leq 3 \).
2. We have \( L^{p^t} u(L) = (L'_p u(L))^{p^t} \), for every \( t \geq 1 \).

**Proof.** Let \( u \in L'_p \) such that \( L'_p = \langle u \rangle_p \). Let \( z \in L \). There exist coefficients \( \alpha_0, \ldots, \alpha_t \in F \) such that \( [u,z] = \sum_{k=0}^{t} \alpha_k u^k \). So, \( [z,u^k] = 0 \), for every \( k \geq 1 \). It follows that

\[
[u,z^{p^k}] = \alpha_0^{p^k-1}[u,z],
\]

for every \( k \geq 1 \). But \( z \) is \( p \)-nilpotent. Hence, either \( \alpha_0 = 0 \) or \( [u,z] = 0 \). Thus \( [u,z] \in \langle u^p \rangle_p \). Hence, \( \gamma_3(L) \subseteq L^p \). Now let \( v \in L \). Note that \( [v,u^k] = 0 \), for every \( k \geq 1 \). Since \( [u,z] \subseteq \langle u^p \rangle_p \), we deduce that \( [u,z,v] = 0 \). It follows that \( cl(L) \leq 3 \).

To prove the second assertion note that \( L^{p^t} u(L) \subseteq (L'_p u(L))^{p^t} \). So we need to prove that \( (L'_p u(L))^{p^t} \subseteq L^{p^t} u(L) \). Note that \( [vz,u] = v[z,u] + [v,u]z \in \langle u^p \rangle_p u(L) \), for every \( v, z \in L \). It follows by the PBW Theorem that \( [u(L), L'_p] \subseteq \langle u^p \rangle_p u(L) \).

Hence, for every \( t \geq 1 \), we have

\[
(L'_p u(L))^{p^t} = (\langle u \rangle_p u(L))^{p^t} \subseteq (\langle u \rangle_p)^{p^t} u(L) = L^{p^t} u(L),
\]

as required.

\[\square\]

3. **Metacyclic restricted Lie algebras**

A restricted Lie algebra \( L \) is called metacyclic if \( L \) has a cyclic restricted ideal \( I \) such that \( L/I \) is cyclic. In other words, there exist generators \( x, y \in L \) and some \( p \)-polynomials \( g \) and \( h \) such that

\[
h(x) \in \langle y \rangle_p, \quad [y,x] = g(y).
\]

In this section \( L \) is a non-abelian metacyclic restricted Lie algebra in the class \( \mathcal{F}_p \).

Let \( g(y) = \beta_0 y + \beta_1 y^p + \beta_2 y^{p^2} + \cdots \). We claim that \( \beta_0 = 0 \). Suppose otherwise. Then

\[
y = \beta [y, x] + \beta_1 y^p + \beta_2 y^{p^2} + \cdots,
\]

where \( \beta \neq 0 \). Note that \( [x, y^p] = 0 \), for every \( t \geq 1 \). Since \( x \) is \( p \)-nilpotent, there exists an integer \( k \) such that

\[
[y, x] = \beta [y, x, x] = \cdots = \beta y^{p^{k-1}} [y, x^p] = 0,
\]

contradicting the fact that \( L \) is non-abelian.

Let \( m \) be the largest integer such that \( x, x^p, \ldots, x^{p^{m-1}} \) are linearly independent modulo \( \langle y \rangle_p \). So there exist coefficients \( c_1, \ldots, c_m \in F \) such that \( \sum_{i=1}^{m} c_i x^{p^i} \in \langle y \rangle_p \).

Let \( k \) be the smallest integer such that \( c_k \neq 0 \). Then

\[
x^{p^k} = - \sum_{i=k+1}^{m} (c_i/c_k) x^{p^i} \text{ modulo } \langle y \rangle_p.
\]
It follows from the equation above that $x^{p^k} \in \langle y, x^{p^{k+1}} \rangle_p$ and hence $x^{p^k} \in \langle y, x^p \rangle_p$, for every $j \geq k$. Since $x$ is $p$-nilpotent, we get $x^{p^k} \in \langle y \rangle_p$. So, by our choice of $m$, we should have $k = m$. We conclude that there exist another $p$-polynomial $f$ and positive integers $m, n$ such that the following relations hold in $L$:

$$
x^{pm} = f(y) = y^{pr} + \cdots,$$

$$
y^{pn} = 0,$$

$$
[y, x] = g(y) = \beta_s y^{pr} + \cdots, \beta_s \neq 0.
$$

Since $L$ is not abelian, we have $1 \leq r \leq n$ and $1 \leq s \leq n - 1$. Now it is easy to see that the commutator subalgebra $L'$ is one-dimensional and $\text{cl}(L) = 2$. So, $L' = F[x, y] \subseteq L^p$. Since $x^{p^{n+r} - r} = y^{pn} = 0$, we have $\exp(x) = m + n - r$. Also, $[y, x]^{p^{n+r} - s} = \beta_s^{-1} y^{pn} = 0$. Thus, the exponent of $L'$ is equal to $n - s$ which is determined by Lemma 2.5.

Since $L' \subseteq L^p$, we have $D_{y^k}(L) = L^{p^k} + L^{y^{p^{k-1}}} = L^{p^k}$, for every $k \geq 1$. But each quotient $D_{y^k}(L)/D_{y^{k+1}}(L)$ is determined by Lemma 2.1. We can then use a similar method as in Lemma 2.2 (a) to show that $\dim_\mathbb{F} L^{p^k}$ is determined, for every $k \geq 0$. In particular, the exponent of $L$ is determined. So we have:

**Lemma 3.1.** Let $L \in \mathcal{F}_p$ be a non-abelian metacyclic restricted Lie algebra. Then the exponent of $L$ is determined.

We need the following technical lemma in the case $p = 2$.

**Lemma 3.2.** Let $L$ and $H$ be non-abelian restricted Lie algebras over a perfect field of characteristic 2. Suppose that $L$ and $H$ are generated by $x, y$ and $u, v$, respectively, subject to the following relations:

$$
x^2 = f(y^2) = \alpha_r y^{2r} + \cdots, \quad u^2 = f(v^2) = \alpha v^{2n-1},$$

$$
y^{2n} = 0, \quad v^{2n} = 0,$$

$$
[x, y] = g(y^2) = \beta_s y^{2r} + \cdots, \beta_s \neq 0, \quad [u, v] = g(v^2) + \beta v^{2n-1},$$

where $f$ and $g$ are some 2-polynomials, $s < r \leq n$, and $\alpha, \beta \in \mathbb{F}$. If $u(L) \cong u(H)$, then $L \cong H$.

**Proof.** Note that $n \geq 2$, since $L$ is not abelian. Suppose first that $n \geq 3$ and $s < n - 1$. We first replace $v$ by $v_1 = v + \beta v^{2n-s-1}$, where $\beta' = (\beta/3s)^{2-s}$. So we get the following relations in $H$:

$$
u^2 = f(v_1^2) + \alpha' v_1^{2n-1}, \quad v_1^{2n} = 0, \quad [u, v_1] = g(v_1^2).$$

We can now replace $u$ by $u_1 = u + \alpha 1/2 v_1^{2n-2}$ and note that the map induced by $x \mapsto u_1, \ y \mapsto v_1$ is an isomorphism between $L$ and $H$. Similarly, if $n \geq 3$ and $r = s = n - 1$, we can find generators $u_1, v_1$ of $H$ such that the map induced by $x \mapsto u_1, \ y \mapsto v_1$ is an isomorphism. Now we consider the case $n = 2$. We have the following relations:

$$
x^2 = a_1 y^2, \quad u^2 = (a_1 + a_2) v^2,$$

$$
y^4 = 0, \quad v^4 = 0,$$

$$
[x, y] = b_1 y^2, \quad [u, v] = (b_1 + b_2) v^2,$$
where $a_1, a_2, b_1, b_2 \in F$. Suppose that $\varphi : u(L) \to u(H)$ is an isomorphism and let $f = \varphi(x)$ and $g = \varphi(y)$. So, $f$ and $g$ generate $u(H)$, $f^2 = a_1g^2$, $g^4 = 0$, and $[f, g] = b_1g^2$. Let $w = [u, v]$ and take $\{u, v, w\}$, $u < v < w$, as a basis for $H$. Let $E$ be the vector space spanned by PBW monomials $w, uw, vw, wv$. Observe that $E$ is in fact a two-sided ideal of $\omega(H)$ and $E \cap H = 0$. Now we express $f$ and $g$ in terms of PBW monomials in $u, v, w$. So we have $f = \alpha_1 u + \alpha_2 v + \alpha_3 w + f_1$, $g = \beta_1 u + \beta_2 v + \beta_3 w + g_1$, where $f_1, g_1 \in E$. Let $\bar{f} = \alpha_1 u + \alpha_2 v + \alpha_3 w$ and $\bar{g} = \beta_1 u + \beta_2 v + \beta_3 w$. Note that $f^2 = \bar{f}^2 + f_1^2$ modulo $\gamma_2((\bar{f}, f_1))$. Since $f^2 = a_1g^2$ we get $\bar{f}^2 = a_1\bar{g}^2 \in H \cap E = 0$.

Similarly we deduce that $\bar{g}^4 = 0$. Furthermore, $[f, g] = [\bar{f}, \bar{g}]$ modulo $E$ and $g^2 = \bar{g}^2$ modulo $E$. So $[\bar{f}, \bar{g}] - b_1\bar{g}^2 \in H \cap E$ and we get $[\bar{f}, \bar{g}] = b_1\bar{g}^2$. Since $f, g$ generate $u(H)$, it follows that $\bar{f}, \bar{g}$ generate $u(H)/\omega^2(H)$. Hence, $\bar{f}, \bar{g}$ generate $u(H)$ since $\omega(H)$ is nilpotent. Thus, the homomorphism induced by $x \mapsto \bar{f}$, $y \mapsto \bar{g}$ is an isomorphism between $L$ and $H$.

4. Proof of the theorem

Suppose that $L \in F_p$ is a non-abelian metacyclic restricted Lie algebra over a perfect field $F$. Let $\varphi : u(L) \to u(H)$ be an algebra isomorphism. Note that $H \in F_p$, since $\omega(L)$ and $\omega(H)$ are nilpotent.

Let $x, y$ be some generators of $L$. By our discussion from Section 3 there exist $p$-polynomials $f, g$ and positive integers $m, n$ such that:

\[
x^p^m = f(y) = y^{p^r} + \cdots, \quad r \geq 1,
\]

\[
y^p^n = 0,
\]

\[
[y, x] = g(y) = \beta_s y^{p^s} + \cdots, \quad s \geq 1.
\]

We fix the generators $x, y$ such that $\exp(L/\langle y \rangle_p) = m$ is minimum. Note that if $\exp(x) \leq \exp(y)$, that is, $m \leq s$, we can assume that $s \leq r$. Indeed, if $r < s$, then we replace $x$ by $x' = x - y^{p^s-m}$ and continue this process if necessary.

Let $t = n - s - 1$. Since $cl(L) = 2$, we have $\exp(L') = \exp(H') = t + 1$, by Lemma 2.5. Also, $cl(H) \leq 3$, by Lemma 2.4. In particular, $H'$ is abelian. Hence, by Corollary 2.4 we have

\[
L'_p / L'^p \cong H'_p / H'^p = (H' + H'^p) / H'^p.
\]

Since $L'_p$ is cyclic, there exists $w \in H'$ such that $H'_p = Fw + H'^p$. Hence, $H'_p = \langle w \rangle_p$ because $H \in F_p$. Since the ideal $L'_p u(L)$ is preserved by $\varphi$, we use Lemma 2.6 to see that $\varphi(L'^p u(L)) = H'^pu(H)$. So, $\varphi$ induces an isomorphism $u(L/L'^p) \to u(H/H'^p)$.

We may now assume by induction on $\dim pL$ that $L/L'^p \cong H/H'^p$. We shall find generators $u, v \in H$ and replace $x$ and $y$ by appropriate generators of $L$, if necessary, so that the map induced by $x \mapsto u$, $y \mapsto v$ is an isomorphism between $L$ and $H$.

**Step 1.** $H$ is metacyclic, too.
Let $u$ and $v$ be some fixed representatives of the images of $x$ and $y$ under the isomorphism $L/L^\beta \to H/H^\beta$. Thus we have the following relations between $u$ and $v$:

\begin{align}
(1) \quad u^p &= f(v) + \alpha_1 v^\beta, \quad v^p = \alpha_2 v^\beta, \quad [v, u] = g(v) + \alpha_3 v^\beta,
\end{align}

where $H' = \langle w \rangle$. Note that $c(H) \leq 3$, by Lemma 2.1. We observe that $w_{p+1} \in \langle v \rangle_p$, $w_{p+1} = 0$, and $[u, v] \in \langle v \rangle_p$. So, $H$ is metacyclic.

Since $\exp(H') = t + 1$, we have $v^{p-1} \neq 0$. Note that $y^{p-1} = [y, x]^p \in L^\beta$. We deduce that $v^{p-1} = 0$ modulo $H^\beta$. Hence, $v^p = 0$. So we can replace (1) by the following relations:

\begin{align}
\quad u^p &= f(v) + \alpha v^{p-1}, \\
\quad v^p &= 0, \\
\quad [v, u] &= g(v) + \beta v^{p-1}.
\end{align}

**Step 2.** Assume $(x)_p \cap (y)_p = 0$.

In other words, $f = 0$. So, we have the following relations in $L$:

\begin{align}
\quad x^p &= y^p = 0, \\
\quad [y, x] &= g(y).
\end{align}

Thus the following relations hold in $H$:

\begin{align}
\quad u^p &= \alpha v^{p-1}, \\
\quad v^p &= 0, \\
\quad [v, u] &= g(v) + \beta v^{p-1}.
\end{align}

Suppose $\beta \neq 0$. If $s < n - 1$, then we replace $v$ by $v_1 = v + \beta v^s v^{n-1}$, where $\beta' = (\beta/\beta^s)^{p-1}$. Suppose $s = n - 1$. Since $L$ and $H$ are non-abelian, we have $\beta + \beta^s \neq 0$. Now we replace $u$ by $u_1 = \beta s u/(\beta + \beta^s)$. So, without loss of generality,

we assume that the following relations hold in $H$:

\begin{align}
\quad u^p &= \alpha v^{p-1}, \\
\quad v^p &= 0, \\
\quad [v, u] &= g(v).
\end{align}

If $m \geq n$, then $\alpha = 0$. Otherwise, $\exp(H) = m + 1$ whereas $\exp(L) = m$, contradicting Lemma 3.1. If $m \leq n - 1$, then we replace $u$ by $u_1 = u - \alpha' v^{n-1-m}$, where $\alpha' = \alpha^{p-m}$. Then we have

\begin{align}
\quad u_1^p &= u^p - \alpha' v^{n-1-m} \quad \text{modulo} \quad \gamma_p((u, v^{n-1-m})),
\end{align}

So, if $m \geq 2$, then

\begin{align}
\quad u_1^p &= u^p - \alpha v^{p-1} \quad \text{modulo} \quad \gamma_p((H^p, H')).
\end{align}

Note that $\gamma_p((H^p, H')) = 0$ since $c(H) = 2$. In the case $m = 1$, note that $\gamma_p((u, v^{n-1-m})) \subseteq \gamma_2(H) = 0$ unless $p = 2$ and $m = n - 1 = 1$. So, virtually, $u_1^p = 0$ and we would be done. The remaining case $p = 2$ and $m = n - 1 = 1$ satisfies the hypothesis of Lemma 3.2 and so $L \cong H$.

**Step 3.** The general case.
Suppose that $\exp(x) \leq \exp(y)$, that is, $m \leq r$. So, as mentioned earlier, we can assume that $s \leq r$. We replace $x$ by $x_1 = x - (f(y))^{p-1}$. So, $x_1^{m} = 0$ unless $m = r = 1$ and $p = 2$. We observe that $x_1$ and $y$ generate $L$ and $(x_1)_p \cap (y)_p = 0$. So we would be done by Step 2. In the special case $m = r = 1$ and $p = 2$, we note that $L \cong H$, by Lemma 3.2. Hence we may assume that $m > r$. Now we have two cases.

Case I. $r \leq s$. Since $x_1^{m} = f(y)$, we get $y^{p^r} \in \langle x_1^{m}, y^{p^{r+1}} \rangle_p$. Thus, $y^{p^r} \in \langle x^{p^m} \rangle_p$, because $y$ is $p$-nilpotent. Since $r \leq s$, it follows that $[y, x] \in \langle x^{p^m} \rangle_p$. Thus, there exists a $p$-polynomial $h$ such that $y^{p^r} = h(x^{p^m})$. Now we replace $y$ by $y_1 = y - (h(x^{p^m}))^{p-r}$. Note that $\exp(y_1) = r < m$. So we have found new generators $x' = y_1$, $y' = x$ such that $\exp(L/(y')_p) < m$. This contradicts the minimality of $m$. So Case I is not possible and we have to consider the case $r > s$.

Case II. $r > s$.

If $r = n - 1$, then $x_1^{m} = y_1^{p^{n-1}}$. We replace $y$ by $y_1 = y - x_1^{p^{m-n+1}}$. Observe that $(x_1)_p \cap (y_1)_p = 0$ and so we are done by Step 2. It remains to consider the case $r < n - 1$. In this case we replace $x$ by $x_1 = x + \alpha x_1^{p^{n-r-1}}$, where $\alpha = \alpha^{p^{-m}}$. We get the following relations in $L$:

$$x_1^{m} = f(y) + \alpha y_1^{p^{n-1}}, \quad y_1^{p^n} = 0, \quad [y, x_1] = g(y).$$

Note that $s < n - 1$. Now we replace $y$ by $y_1 = y - \beta y_1^{p^{n-s-1}}$, where $\beta = (\beta_1/\beta_2)^{p^{-s}}$. Note that $[x_1, y_1] = [x_1, y_1]$. Also, we observe that $g(y_1) = g(y) - \beta y_1^{p^{n-1}}$. Thus,

$$[y_1, x_1] = [y, x_1] = g(y) = g(y_1) + \beta y_1^{p^{n-1}}.$$

Furthermore, $x_1^{m} = f(y_1) + \alpha y_1^{p^{n-1}}$, since $r > s$. So, we get the following relations in $L$:

$$x_1^{m} = f(y_1) + \alpha y_1^{p^{n-1}}, \quad y_1^{p^n} = 0, \quad [y_1, x_1] = g(y_1) + \beta y_1^{p^{n-1}}.$$

We deduce that the map induced by $x_1 \mapsto u$, $y_1 \mapsto v$ is an isomorphism between $L$ and $H$. \hfill $\Box$

REFERENCES


**Department of Mathematics, University of British Columbia, 1984 Mathematics Road, Vancouver, BC, Canada, V6T 1Z2**

**E-mail address:** usefi@math.ubc.ca

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use