PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 136, Number 12, December 2008, Pages 4125–4133
S 0002-9939(08)09632-9
Article electronically published on July 23, 2008

# 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 $\mathbb{F}$ of positive characteristic $p$ and denote by $\mathrm{ad} : L \to L$ the adjoint representation of $L$ given by $(\mathrm{ad}x)(y) = [y, x]$, where $x, y \in L$. Recall that $L$ is called *restricted* if $L$ additionally affords a $p$-map $^{[p]} : L \to L$, satisfying

(1) $(\mathrm{ad}x)^p = \mathrm{ad}(x^{[p]})$, for every $x \in L$;
(2) $(\alpha x)^{[p]} = \alpha^p x^{[p]}$, for every $x \in L$ and $\alpha \in \mathbb{F}$; 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 $is_i(x, y)$ is the coefficient of $\lambda^{i-1}$ in $\mathrm{ad}(\lambda x + y)^{p-1}(x)$.

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 $L^{[p]^k} = 0$. It is also proved in [10] that if $\mathbb{F}$ is algebraically closed, then every finite-dimensional abelian restricted Lie algebra over $\mathbb{F}$ is determined by its enveloping algebra.

Received by the editors September 28, 2007.
2000 *Mathematics Subject Classification.* Primary 17B35, 17B50; Secondary 20C05.
*Key words and phrases.* Restricted Lie algebras, metacylic, enveloping algebras, isomorphism problem, modular group algebras.

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 $\mathbb{F}_pG$, 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

$$x_1^{a_1} \dots x_t^{a_t},$$

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 $L'_p$ 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,

$$[x_1, \dots, x_n] = [[x_1, x_2], x_3, \dots, x_n].$$

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 $c_0x + c_1x^p + \cdots + c_tx^{p^t}$, 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

$$D_n(L) = L \cap \omega^n(L) = \sum_{ip^j \geq n} \gamma_i(L)^{p^j},$$

where $\gamma_i(L)^{p^j}$ is the restricted subalgebra of $L$ generated by all $x^{p^j}$, $x \in \gamma_i(L)$; see [4]. It follows from the defining axioms of $L$ that $(x+y)^p = x^p + y^p$ modulo $\gamma_p(\langle x, y\rangle)$. 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 $\mid cl(L) - cl(H) \mid \leq 1$.*
(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 $\mathbb{F}_pG$ 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 $z_1 z_2 \dots z_n$, where $z_i \in I$. We know that the kernel of the natural map $u(L) \to u(L/I)$ is equal to $Iu(L) = u(L)I$. It follows that $\omega^n(I)u(L) = I^n u(L) = (Iu(L))^n$, for every $n \geq 1$. Furthermore, we observe that each quotient $I^n u(L)/I^{n+1}u(L)$ has a natural right $u(L/I) \cong u(L)/Iu(L)$-module structure given by

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

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 [6].

**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 $\dim_{\mathbb{F}} \omega^n(I)/\omega^{n+1}(I)$.*

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

Using the identity $[ab, c] = a[b, c] + [a, c]b$, 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*

$$D_n(L'_p)/D_{n+1}(L'_p) \cong D_n(H'_p)/D_{n+1}(H'_p).$$

**Lemma 2.5.** *Let $L \in \mathcal{F}_p$ such that $cl(L) = 2$. Then, $\dim_{\mathbb{F}} {L'_p}^{p^t}$ 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 $D_{p^{t-1}+1}(H'_p) = \cdots = D_{p^t}(H'_p) = H'^{p^t}$, for every $t \geq 1$. So, by Corollary 2.4, we have $L'_p/L'^p \cong H'_p/H'^p$ and

$$L'^{p^t}/L'^{p^{t+1}} \cong H'^{p^t}/H'^{p^{t+1}},$$

for every $t \geq 1$. Now let $s = \exp(L')$. It follows that

$$H'^{p^s} = H'^{p^{s+1}}.$$

But $H$ is $p$-nilpotent. Hence, $H'^{p^s} = 0$. 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 $\dim_{\mathbb{F}} {L'_p}^{p^t}$ is determined, for every $t \geq 0$. □

**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 $\alpha_0, \ldots, \alpha_t \in \mathbb{F}$ such that $[u, z] = \sum_{k=0}^{t} \alpha_k u^{p^k}$. So, $[z, u^{p^k}] = 0$, 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 $[v, u^{p^k}] = 0$, 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. □

## 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 $[x, y^{p^t}] = 0$, for every $t \geq 1$. Since $x$ is $p$-nilpotent, there exists an integer $k$ such that

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

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 $c_1, \ldots, c_m \in \mathbb{F}$ 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 $x^{p^k} \in \langle y, x^{p^j} \rangle_p$, 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 $L$:

$$\begin{aligned} x^{p^m} &= f(y) = y^{p^r} + \cdots, \\ y^{p^n} &= 0, \\ [y, x] &= g(y) = \beta_s y^{p^s} + \cdots, \beta_s \neq 0. \end{aligned}$$

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 $cl(L) = 2$. So, $L' = \mathbb{F}[x, y] \subseteq L^p$. Since $x^{p^{m+n-r}} = y^{p^n} = 0$, we have $\exp(x) = m + n - r$. Also, $[y, x]^{p^{n-s}} = \beta_s^{n-s} y^{p^n} = 0$. Thus, the exponent of $L'$ is equal to $n - s$ which is determined by Lemma 2.5.

Since $L' \subseteq L^p$, we have $D_{p^k}(L) = L^{p^k} + L'^{p^{k-1}} = L^{p^k}$, for every $k \geq 1$. But each quotient $D_{p^k}(L)/D_{p^{k+1}}(L)$ is determined by Lemma 2.1. We can then use a similar method as in Lemma 2.5 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:*

$$\begin{aligned} x^2 = f(y^{2^r}) = \alpha_r y^{2^r} + \cdots, \qquad & u^2 = f(v^{2^r}) + \alpha v^{2^{n-1}}, \\ y^{2^n} = 0, \qquad & v^{2^n} = 0, \\ [x, y] = g(y^{2^s}) = \beta_s y^{2^s} + \cdots, \quad \beta_s \neq 0, \qquad & [u, v] = g(v^{2^s}) + \beta v^{2^{n-1}}, \end{aligned}$$

*where $f$ and $g$ are some 2-polynomials, $s \leq r \leq n$, 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 $v_1 = v + \beta' v^{2^{n-s-1}}$, where $\beta' = (\beta/\beta_s)^{2^{-s}}$. So we get the following relations in $H$:

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

We can now replace $u$ by $u_1 = u + \alpha'^{1/2} v_1^{2^{n-2}}$ 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:

$$\begin{aligned} x^2 &= a_1 y^2, & u^2 &= (a_1 + a_2) v^2, \\ y^4 &= 0, & v^4 &= 0, \\ [x, y] &= b_1 y^2, & [u, v] &= (b_1 + b_2) v^2, \end{aligned}$$

where $a_1, a_2, b_1, b_2 \in \mathbb{F}$. 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 $u(H)$, $f^2 = a_1 g^2$, $g^4 = 0$, and $[f, g] = b_1 g^2$. 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 $uv, uw, vw, uvw$. 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 $\gamma_2(\langle \bar{f}, f_1 \rangle)$. Since $f^2 = a_1 g^2$ 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 $L \in \mathcal{F}_p$ is a non-abelian metacyclic restricted Lie algebra over a perfect field $\mathbb{F}$. Let $\varphi : u(L) \to u(H)$ be an algebra isomorphism. Note that $H \in \mathcal{F}_p$, 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:

$$\begin{aligned} x^{p^m} &= f(y) = y^{p^r} + \cdots, r \geq 1, \\ y^{p^n} &= 0, \\ [y, x] &= g(y) = \beta_s y^{p^s} + \cdots, s \geq 1. \end{aligned}$$

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, $m \leq r$, we can assume that $s \leq r$. Indeed, if $r < s$, then we replace $x$ by $x' = x - y^{p^{r-m}}$ 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 2.1. 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 $H'_p = \mathbb{F}w + H'^p$. Hence, $H'_p = \langle w \rangle_p$ because $H \in \mathcal{F}_p$. Since the ideal $L'_p u(L)$ is preserved by $\varphi$, we use Lemma 2.6 to see that $\varphi(L'^{p^t} u(L)) = H'^{p^t} u(H)$. So, $\varphi$ induces an isomorphism

$$u(L/L'^{p^t}) \to u(H/H'^{p^t}).$$

We may now assume by induction on $\dim_{\mathbb{F}} L$ that $L/L'^{p^t} \cong H/H'^{p^t}$. 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 $L/L'^{p^t} \to H/H'^{p^t}$. Thus we have the following relations between $u$ and $v$:

$$u^{p^m} = f(v) + \alpha_1 w^{p^t}, \quad v^{p^n} = \alpha_2 w^{p^t}, \quad [v,u] = g(v) + \alpha_3 w^{p^t}, \tag{1}$$

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

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

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

**Step 2.** Assume $\langle x \rangle_p \cap \langle y \rangle_p = 0$.

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

$$\begin{aligned} x^{p^m} &= y^{p^n} = 0, \\ [y,x] &= g(y). \end{aligned}$$

Thus the following relations hold in $H$:

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

Suppose $\beta \neq 0$. If $s < n-1$, then we replace $v$ by $v_1 = v + \beta' v^{p^{n-s-1}}$, where $\beta' = (\beta/\beta_s)^{p^{-s}}$. 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 $H$:

$$u^{p^m} = \alpha v^{p^{n-1}}, \ v^{p^n} = 0, \ [v,u] = g(v).$$

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 $u_1 = u - \alpha' v^{p^{n-1-m}}$, where $\alpha' = \alpha^{p^{-m}}$. Then we have

$$u_1^p = u^p - \alpha'^p v^{p^{n-m}} \text{ modulo } \gamma_p(\langle u, v^{p^{n-1-m}} \rangle).$$

So, if $m \geq 2$, then

$$u_1^{p^m} = u^{p^m} - \alpha v^{p^{n-1}} \text{ modulo } \gamma_p(\langle H^p, H' \rangle).$$

Note that $\gamma_p(\langle H^p, H' \rangle) = 0$ since $cl(H) = 2$. In the case $m = 1$, note that $\gamma_p(\langle u, v^{p^{n-1-m}} \rangle) \subseteq \gamma_3(H) = 0$ unless $p = 2$ and $m = n-1 = 1$. So, virtually, $u_1^{p^m} = 0$ 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 $x_1 = x - (f(y))^{p^{-m}}$. So, $x_1^{p^m} = 0$ unless $m = r = 1$ and $p = 2$. We observe that $x_1$ and $y$ generate $L$ and $\langle x_1 \rangle_p \cap \langle y \rangle_p = 0$. 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 $x^{p^m} = f(y)$, we get $y^{p^r} \in \langle x^{p^m}, y^{p^{r+1}} \rangle_p$. 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 $\exp(L/\langle y' \rangle_p) < m$. 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 $x^{p^m} = y^{p^{n-1}}$. We replace $y$ by $y_1 = y - x^{p^{m-n+1}}$. Observe that $\langle x \rangle_p \cap \langle y_1 \rangle_p = 0$ and so we are done by Step 2. It remains to consider the case $r < n - 1$. In this case we replace $x$ by $x_1 = x + \alpha' x^{p^{n-r-1}}$, where $\alpha' = \alpha^{p^{-m}}$. We get the following relations in $L$:

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

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

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

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

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

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

## References


[1] C. Bagiński, A. Konovalov, The modular isomorphism problem for finite $p$-groups with a cyclic subgroup of index $p^2$, *Groups St. Andrews 2005. Vol. 1*, 186–193, London Math. Soc. Lecture Note Ser., **339** (Cambridge Univ. Press, 2007). MR2327323 (2008f:20009)

[2] C. Bagiński, The isomorphism question for modular group algebras of metacyclic $p$-groups, *Proc. Amer. Math. Soc.* **104** (1988), no. 1, 39–42. MR958039 (89i:20016)

[3] N. Jacobson, *Lie Algebras* (Interscience, New York, 1962). MR0143793 (26:1345)

[4] D.M. Riley, A. Shalev, Restricted Lie algebras and their envelopes, *Canad. J. Math.*, **47** (1995), 146–164. MR1319694 (96e:16031)

[5] D.M. Riley, A. Shalev, The Lie structure of enveloping algebras, *J. Algebra*, **162** (1993), no. 1, 46–61. MR1250526 (94k:17019)

[6] D.M. Riley, H. Usefi, The isomorphism problem for universal enveloping algebras of Lie algebras, *Algebras and Representation Theory*, **10** (2007), no. 6, 517–532. MR2350224

[7] R. Sandling, The modular group algebra problem for metacyclic $p$-groups, *Proc. Amer. Math. Soc.*, **124** (1996), no. 5, 1347–1350. MR1343723 (96g:20003)

[8] R. Sandling, The isomorphism problem for group rings: a survey, *Orders and Their Applications* (Oberwolfach, 1984), Lecture Notes in Math., **1142** (Springer, Berlin, 1985), 256–288. MR812504 (87b:20007)

[9] H. Strade, R. Farnsteiner, *Modular Lie Algebras and Their Representations*, Monographs and Textbooks in Pure and Applied Mathematics, **116** (Marcel Dekker, New York, 1988). MR929682 (89h:17021)

[10] H. Usefi, Isomorphism invariants of restricted enveloping algebras, preprint is available on `arXiv:0804.2281`.

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

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