The GAP Package LiePRing

Bettina Eick[1(✉)] and Michael Vaughan-Lee[2]

[1] TU Braunschweig, Braunschweig, Germany
beick@tu-bs.de
[2] Christ Church, Oxford, England
michael.vaughan-lee@chch.ox.ac.uk
http://www.iaa.tu-bs.de/beick/, http://users.ox.ac.uk/~vlee

Abstract. A symbolic Lie p-ring defines a family of Lie rings with p^n elements for infinitely many different primes p and a fixed positive integer n. Symbolic Lie p-rings are used to describe the classification of isomorphism types of nilpotent Lie rings of order p^n for all primes p and all $n \leq 7$. This classification is available as the LiePRing package of the computer algebra system GAP. We give a brief description of this package, including an approach towards computing the automorphism group of a symbolic Lie p-ring.

Keywords: Lie ring · Automorphism group · Finite p-group

1 Introduction

A Lie ring is an additive abelian group with a multiplication, denoted by $[.,.]$, that is bilinear, alternating and satisfies the Jacobi identity. A Lie p-ring is a nilpotent Lie ring with p^n elements for some prime power p^n. Such a Lie p-ring of order p^n can be described by a presentation $P(A)$ on n generators $b_1, \ldots, b_n$ with coefficients $A = (a_{ijk}, a_{ik} \mid 1 \leq i < j < k \leq n)$, so that a_{ijk} and a_{ik} are integers in the range $\{0, \ldots, p-1\}$ and the following relations hold:

$$[b_j, b_i] = \sum_{k=j+1}^{n} a_{ijk} b_k \quad \text{for} \quad 1 \leq i < j \leq n, \quad \text{and}$$

$$p b_i = \sum_{k=i+1}^{n} a_{ik} b_k \quad \text{for} \quad 1 \leq i \leq n.$$

We generalize this type of presentation so that it defines a family of Lie p-rings for various different primes. For this purpose let p be an indeterminate, let $R = \mathbb{Z}[w, x_1, \ldots, x_m]$ be a polynomial ring in $m+1$ commuting variables and let a_{ijk} and a_{ik} in R. In some (rare) cases it is convenient to allow some of the coefficients a_{ijk} and a_{ik} to be rational functions over R; note that we use this only for coefficients a_{ijk} or a_{ik} if $pb_k = 0$ so that b_k is an element of order p.

If a fixed prime P and integers $X_1, \ldots, X_m$ are given, then we *specify* the a polynomial $a \in R$ at these values by choosing W to be the smallest primitive

A. M. Bigatti et al. (Eds.): ICMS 2020, LNCS 12097, pp. 131–140, 2020.
https://doi.org/10.1007/978-3-030-52200-1_13

root mod P and evaluating $\overline{a} = a(W, X_1, \ldots, X_m)$ in $\mathbb{Z}$. We *specify* a rational function a/b with $a, b \in R$ by specifying the polynomials a and b to $\overline{a}$ and $\overline{b}$ in $\mathbb{Z}$, and then we determine $\overline{a}\,\overline{c}$ where $\overline{c} \in \{1, \ldots P-1\}$ satisfies $\overline{c}\overline{b} \equiv 1 \bmod P$. Note that only choices of $W, X_1, \ldots, X_m$ with $P \nmid \overline{b}$ are valid.

Let $\mathbb{P}$ be an infinite set of primes, let $m \in \mathbb{N}_0$ and for $P \in \mathbb{P}$ let

$$\Sigma_P \subseteq \{(X_1, \ldots, X_m) \in \mathbb{Z}^m \mid 0 \leq X_i < P\}.$$

Then the presentation $P(A)$ defines a *symbolic* Lie p-ring with respect to $\mathbb{P}$ and Σ_P if for each $P \in \mathbb{P}$ and each $(X_1, \ldots, X_m) \in \Sigma_P$ the presentation $P(A)$ specified at these points is a finite Lie p-ring of order P^n.

A symbolic Lie p-ring describes a family of finite Lie p-rings: for each $P \in \mathbb{P}$ this contains $|\Sigma_P| \leq P^m$ members. Symbolic Lie p-rings are used to describe the complete classification up to isomorphism of all Lie p-rings of order dividing p^7 for $p > 3$ as obtained by Newman, O'Brien and Vaughan-Lee [6,7]. This is available in computational form in the LiePRing package [4] of the computer algebra system GAP [9]. The following exhibits an example.

Example 1. We consider the symbolic Lie p-ring $\mathcal{L}$ with generators $b_1, \ldots, b_7$ and the (non-trivial) relations

$$\begin{aligned} [b_2, b_1] &= b_4, & pb_1 &= b_4 + b_6 + x_2 b_7, \\ [b_3, b_1] &= b_5, & pb_3 &= x_1 b_6. \\ [b_3, b_2] &= b_6, \\ [b_5, b_1] &= b_6, \\ [b_5, b_3] &= b_7, \end{aligned}$$

Let $\mathbb{P}$ be the set of all primes and let

$$\Sigma_P = \{(X_1, X_2) \mid 0 < X_1 < P, 0 \leq X_2 < P\}.$$

Then $\mathcal{L}$ defines a family of $P(P-1)$ Lie p-rings of order P^7 for each $P \in \mathbb{P}$.

The LiePRing package allows symbolic computations with symbolic Lie p-rings $\mathcal{L}$. "Symbolic computations" means that it computes with $\mathcal{L}$ as if computing with all Lie p-rings L in the family defined by $\mathcal{L}$ simultaneously. For example, it allows us

- to compute series of ideals such as the lower central series of L,
- to describe the automorphism group of L, and
- to determine the Schur multiplier of L, see [3].

Let P be a prime and let $n \in \mathbb{N}$ with $n \leq P$. The Lazard correspondence [5] associates to each Lie p-ring L of order P^n a group $G(L)$ of order P^n. This correspondence translates Lie ring isomorphisms to group isomorphisms and vice versa. Cicalo, de Graaf and Vaughan-Lee [2] determined an effective version of the Lazard correspondence and implemented this in the LieRing package [1] of GAP.

The following sections give a brief overview of some of the algorithms in the LiePRing package and they exhibit how the Lazard correspondence can be evaluated in GAP in this setting.

2 Elementary Computations

In this section we investigate computations with elements, subrings and ideals. Throughout, let $\mathcal{L}$ be a symbolic Lie p-ring with respect to Σ_P, let L be a finite Lie p-ring in the family defined by $\mathcal{L}$ and let P be the prime of L. We write $P(A)$ for the defining presentation in the finite and in the symbolic case. Thus depending on the context A is an integer matrix or a matrix over the ring $Quot(R)$ of rational functions over the polynomial ring R.

2.1 Ring Invariants

The definition of Σ_P can often be used for computations with $\mathcal{L}$. For example, if $\Sigma_P = \{(x_1, x_2, x_3) \in \mathbb{Z}_P^3 \mid x_1 \neq 1, x_3 = \pm 1\}$, then $(x_1 - 1)$ specifies to an invertible element in L and $(x_3 - 1)(x_3 + 1) = (x_3^2 - 1)$ specifies to 0. Hence we can treat $(x_1 - 1)$ as a unit and $(x_3^2 - 1)$ as zero. The following example illustrates this for $\Sigma_P = \{(x, y) \mid x \neq 0, y \in \{1, w\}\}$.

```
gap> L := LiePRingsByLibrary(7)[3195];
<LiePRing of dimension 7 over prime p with parameters [ x, y ]>
gap> ViewPCPresentation(L);
p*l2 = x*l7, p*l3 = l5 + y*l7, p*l4 = l6,
[l2,l1] = l5, [l3,l1] = l6, [l4,l1] = l7
gap> RingInvariants(L);
rec( units := [ x, y ], zeros := [ w*y-y^2-w+y ] )
```

2.2 The Word Problem

Consider the case of a finite Lie p-ring L and let a be an arbitrary word in the generators of $P(A)$. Then the relations in $P(A)$ readily allow us to rewrite a to a *unique* equivalent *normal form*

$$c_1 b_1 + \ldots + c_n b_n \quad \text{with} \quad c_i \in \{0, \ldots, P-1\} \text{ for } 1 \leq i \leq n.$$

Now consider the case of a symbolic Lie p-ring $\mathcal{L}$ and let a be a word in the generators of $P(A)$. Then the relations and the zeros of $\mathcal{L}$ allow us to translate this to an equivalent *reduced form*; that is, a linear combination of the form

$$c_1 b_1 + \ldots + c_n b_n \quad \text{with} \quad c_i \in R \quad \text{for } 1 \leq i \leq n,$$

where $c_1, \ldots, c_n \in R$ are reduced modulo the polynomials in *zeros*; that is, the polynomial division algorithm dividing c_i by the polynomials in zeros yields only trivial quotients. If $c_1 = \ldots = c_k = 0$ and $c_{k+1} \neq 0$, then $k+1$ is the *depth* of this reduced form and c_{k+1} is its *leading coefficient*. We say that $(c_1, \ldots, c_n)$ *represents* the element a.

Example 2. We continue Example 1.

(1) Consider the element $a = pb_1 - [b_2, b_1] - [b_3, b_2] - [[b_3, b_1], b_3]$. Using the relations of $\mathcal{L}$ this reduces to $a = b_4 + b_6 + x_2 b_7 - b_4 - b_6 - [b_5, b_3] = x_2 b_7 - b_7 = (x_2 - 1) b_7$. Note that a can be zero and non-zero in the Lie p-rings in the family defined by $\mathcal{L}$, depending on the choice of x_2.
(2) Consider the element $a = pb_3$. Then $a = x_1 b_6$ and hence, since $x_1 \neq 0$ in $\mathcal{L}$, it follows that a is a non-zero element in each Lie p-ring in the family defined by $\mathcal{L}$.

2.3 Subrings, Ideals and Series

Let $\mathcal{L}$ be a symbolic Lie p-ring, let $w_1, \ldots, w_k$ be words in the generators $b_1, \ldots, b_n$ of $P(A)$ and let U be the subring of $\mathcal{L}$ generated by these words. Our aim is to determine an *echelon generating set* for U; that is, a generating set $v_1, \ldots, v_l$ so that each v_i is a reduced form in the generators with leading coefficient 1, the depths satisfy $d(v_1) < \ldots < d(v_l)$ and each element in U is a linear combination in $v_1, \ldots, v_l$ with coefficients in $Quot(R)$. This may require the distinction of finitely many cases, as the following example indicates.

Example 3. We continue Example 1.

(1) Let $U = \langle [b_3, b_1], pb_3 \rangle$. As $[b_3, b_1] = b_5$ and $pb_3 = x_1 b_6$ with $x_1 \neq 0$, it follows that $U = \langle b_5, b_6 \rangle$ in each Lie ring in the family defined by $\mathcal{L}$.
(2) Let $U = \langle pb_1 - b_4 - b_6, [b_3, b_2] \rangle$. Then using the relations of $\mathcal{L}$ it follows that $U = \langle x_2 b_7, b_6 \rangle$. Hence $U = \langle b_6, b_7 \rangle$ if $x_2 \neq 0$ and $U = \langle b_6 \rangle$ otherwise. Thus a case distinction is necessary to determine an echelon generating set for U.

Ideals are subrings that are closed under multiplication and hence they can also be described via echelon generating sets (subject to a case distinction). In turn, this then allows us to determine series such as the lower central series and the derived series of $\mathcal{L}$. The following example illustrates the handling of case distinctions in GAP.

```
gap> L := LiePRingsByLibrary(6)[267];
<LiePRing of dimension 6 over prime p with parameters [x,y,z,t]>
gap> ViewPCPresentation(L);
p*l1 = t*l5 + x*l6, p*l2 = y*l5 + z*l6,
[l2,l1] = l4, [l3,l1] = l6, [l4,l1] = l5,
[l3,l2] = w*l5, [l4,l2] = l6
gap> RingInvariants(L);
rec( units := [ -x*y+z*t ], zeros := [  ] )
gap> S := LiePRecSubring(L, [p*b[1]]);
[<LiePRing of dimension 1 over prime p with parameters [x,y,z,t]>,
 <LiePRing of dimension 1 over prime p with parameters [x,y,z,t]>]
```

Here the LiePRing package returns two new symbolic Lie p-rings $S[1]$ and $S[2]$. These have different ring invariants and different bases:

```
gap> RingInvariants(S[1]);
rec( units := [ y, x ], zeros := [ t ] )
gap> BasisOfLiePRing(S[1]);
[ l6 ]
gap> RingInvariants(S[2]);
rec( units := [ -x*y+z*t, t ], zeros := [  ] )
gap> BasisOfLiePRing(S[2]);
[ l5 + x/t*l6 ]
```

In particular, in $S[2]$ the polynomial t is a unit and the rational function x/t turns up as coefficient for the basis element l_6.

3 Automorphism Groups

Given a symbolic Lie p-ring $\mathcal{L}$, we show how to determine a generic description for $Aut(L)$ for each finite Lie p-ring L in the family defined by $\mathcal{L}$. The following gives a first illustration.

Example 4. We continue Example 1.

We note that $\mathcal{L}$ is generated by b_1, b_2, b_3. This allows us to describe each automorphism of $\mathcal{L}$ via its images of b_1, b_2, b_3 and the same holds for each finite Lie p-ring in the family defined by $\mathcal{L}$. Write g_r for the image of b_r. Then $g_r = g_{r1}b_1 + \ldots + g_{r7}b_7$ for certain integers g_{rs}. We say that the automorphism is represented by the 3×7 matrix (g_{rs}). Note that different matrices may represent the same automorphism for a finite Lie p-ring L; for example, if P is the prime of L, then b_7 has order P and g_{37} and $g_{37} + P$ give the same automorphism. We expand on this below.

Our algorithm determines that each automorphism of $\mathcal{L}$ corresponds to a matrix of the form

$$\begin{pmatrix} g_{11} & g_{12} & 0 & g_{14} & g_{15} & g_{16} & g_{17} \\ 0 & 1 & 0 & g_{24} & 0 & g_{26} & g_{27} \\ 0 & g_{32} & g_{11} & g_{34} & g_{35} & g_{36} & g_{37} \end{pmatrix}$$

with $g_{11} = \pm 1$ and g_{rs} arbitrary otherwise. If P is prime and L is a finite Lie p-ring over P, then we can choose $g_{rs} \in \{0, \ldots, P-1\}$ for $(r,s) \neq (1,1)$ and thus $Aut(L)$ has order $2P^{13}$.

Given a finite Lie p-ring L with prime P, we define its radical $R(L)$ as the ideal of L generated by $\{[b_j, b_i], Pb_k \mid 1 \leq i < j \leq n, 1 \leq k \leq n\}$. The additive group of $L/R(L)$ is an elementary abelian group of order P^d, say, and the Lie ring multiplication of $L/R(L)$ is trivial. Burnside's Basis theorem (for example, see [8, page 140]) for finite p-groups translates readily to the following.

Lemma 1. *Let L be a finite Lie p-ring and let $\varphi : L \to L/R(L)$ the natural ring homomorphism.*

(a) $R(L)$ is the intersection of all maximal Lie subrings of L.

(b) Each minimal generating set of L has d elements and maps under φ onto a minimal generating set of $L/R(L)$.
(c) Each list of preimages under φ of a minimal generating set of $L/R(L)$ is a minimal generating set of L.

Next, let $P(A)$ be the presentation for the finite Lie p-ring L with generators $b_1, \ldots, b_n$ so that $R(L) = \langle b_{d+1}, \ldots, b_n \rangle$. Then $b_1, \ldots, b_d$ is a minimal generating set of L. Thus each automorphism α of L is defined by its images on $b_1, \ldots, b_d$. These have the general form

$$\alpha(b_r) = g_{r1}b_1 + \ldots + g_{rn}b_n \quad \text{for} \quad 1 \leq r \leq d,$$

with integer coefficients g_{rs}. For $k > d$ we note that $b_k \in R(L)$. This allows us to write b_k as a word in the ideal generators $[b_j, b_i]$ and Pb_i of $R(L)$ and that, in turn, allows us to determine the image $\alpha(b_k)$ in the form

$$\alpha(b_k) = w_{k1}b_1 + \ldots + w_{kn}b_n,$$

where w_{kj} is a word in $\{g_{rs}\}$.

Theorem 1. *The matrix $(g_{rs})_{1 \leq r \leq d, 1 \leq s \leq n}$ defines an automorphism α of L if and only if*

(a) $det(G) \not\equiv 0 \bmod P$, where $G = (g_{rs})_{1 \leq r,s \leq d}$, and
(b) the images $\alpha(b_1), \ldots, \alpha(b_n)$ satisfy the relations of L.

Proof. First recall that a map $b_i \mapsto v_i$ for $1 \leq i \leq n$ with $v_1, \ldots, v_n \in L$ extends to a Lie ring homomorphism $L \to L$ if and only if $v_1, \ldots, v_n$ satisfy the defining relations of L. This is von Dyck's theorem (for example, see [8, page 51]) in the case of finitely presented groups and it translates readily to other algebraic objects such as Lie rings.

$\Rightarrow$: Suppose that the coefficients g_{rs} define an automorphism α. Then α induces an automorphism $\beta : L/R(L) \to L/R(L)$. As $L/R(L) \cong \mathbb{Z}_P^d$ with trivial multiplication, it follows that $Aut(L/R(L)) \cong GL(d, \mathbb{Z}_P)$. Hence $det(G) \not\equiv 0 \bmod P$ so (a) follows. (b) follows from von Dyck's theorem.

$\Leftarrow$: Suppose that (a) and (b) hold. As (b) holds, von Dyck's theorem asserts that α is a Lie ring homomorphism. As $P \nmid det(G)$. it follows that the images of $b_1, \ldots, b_d$ generate L as Lie ring. Hence α is surjective. Since L is finite, it follows that α is also injective and hence an automorphism.

This allows us to determine a generic description for $Aut(L)$. Suppose that we have an automorphism given by indeterminates $\{g_{rs} \mid 1 \leq r \leq d, 1 \leq s \leq n\}$ and write $g_i = g_{i1}b_1 + \ldots + g_{in}b_n$ for $1 \leq i \leq d$. For $k > d$ write b_k as a word w_k in the generators $b_1, \ldots, b_d$ and use this to determine $g_k = w_k(g_1, \ldots, g_d)$. Evaluate the defining relations $R_1, \ldots, R_m$ of L in $g_1, \ldots, g_n$. For each relation R_i this leads to an expression

$$\overline{R}_i = R_i(g_1, \ldots, g_n) = w_{i\,d+1}b_{d+1} + \ldots + w_{in}b_n,$$

with w_{ij} a polynomial in the indeterminates $\{g_{rs} \mid 1 \leq r \leq d, 1 \leq s \leq n\}$.

Lemma 2. *Let P be a prime and k minimal with $P^k b_i = 0$ for $d < i \leq n$. If $w_{ij} \equiv 0 \bmod P^k$ for all i, j and if $det(G) \not\equiv 0 \bmod P$, then the matrix $(g_{rs})_{1 \leq r \leq d, 1 \leq s \leq n}$ defines an automorphism.*

Proof. The generators that appear in the relations $\overline{R}_i = 0$ all lie in the radical, and so $w_{ij} \equiv 0 \bmod P^k$ ensures that $w_{ij} b_j = 0$ for all i, j. Hence the conditions of Theorem 1 are satisfied and the matrix $(g_{rs})_{1 \leq r \leq d, 1 \leq s \leq n}$ defines an automorphism.

The integer P^k in Lemma 2 is called the characteristic of $R(L)$. If $k = 1$, then the conditions in Lemma 2 clearly determine all automorphisms of L. If $k > 1$, then the conditions in Lemma 2 may miss some automorphisms and there are examples where

$$\overline{R}_i = w_{i\,d+1} b_{d+1} + \ldots + w_{in} b_n = 0,$$

but some of the summands $w_{ij} b_j$ are non-zero. So it seems possible that restricting our search to integer matrices (g_{rs}) which satisfy the equations $w_{ij} = 0 \bmod P^k$ could miss some automorphisms in some cases. In practice, we have not found a case where this happens.

Example 5. We continue Example 1 for a specific prime P.

Since the radical has characteristic P our method shows that the matrix

$$\begin{pmatrix} g_{11} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & g_{11} & 0 & 0 & 0 & 0 \end{pmatrix}$$

gives an automorphism if and only if $g_{11}^2 = 1 \bmod P$. Let $P = 5$. Then

$$B = \begin{pmatrix} 4 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 4 & 0 & 0 & 0 & 0 \end{pmatrix}$$

gives an automorphism. There was no need in this case to look for solutions to $g_{11}^2 = 1 \bmod P^2$, but it is easy to "lift" B to a matrix $C = (h_{rs})$ which gives the same automorphism as B, but where $h_{11}^2 = 1 \bmod 25$. The first row of the matrix B represents the element $4b_1$. Now $5b_1 = b_4 + b_6 + x_2 b_7$ and so the vector $(-1, 0, 0, 1, 0, 1, x_2)$ also represents $4b_1$. Similarly the vector $(0, 0, -1, 0, 0, x_1, 0)$ represents the same element of L as the third row of B. So

$$C = \begin{pmatrix} -1 & 0 & 0 & 1 & 0 & 1 & x_2 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & x_1 & 0 \end{pmatrix}$$

gives the same automorphism as B, but the $(1, 1)$ entry in C satisfies the equation $x^2 = 1 \bmod 25$. Note that B gives an automorphism, but does not have the form specified in Example 4, whereas C gives the same automorphism as B, but does have the form specified.

More generally, in every case of Lie p-rings from our database that we have examined, we can show that if B is an integer matrix which gives an automorphism of L for some prime P, and if k is any positive integer, then B can be "lifted" to an integer matrix $C = (h_{rs})$ which gives the same automorphism as B but where the entries h_{rs} satisfy all the equations $w_{ij} = 0 \bmod P^k$. So in every case that we have examined our method finds the full automorphism group.

We do not have a proof that our method always finds the full automorphism group. But there are several general criteria (such as the radical having characteristic P) which imply that our method does not miss any automorphisms. So in most cases our program is able to issue a "certificate of correctness". In some cases it may be necessary to examine the output from our program to prove that it has found the full automorphism group.

Example 6. We consider the symbolic Lie p-ring $\mathcal{L}$ on 7 generators with the non-trivial relations

$$\begin{aligned}
[b_2, b_1] &= b_3, & pb_1 &= b_5 + xb_7,\\
[b_3, b_1] &= b_4, & pb_2 &= w^2 b_6 + yb_7,\\
[b_3, b_2] &= b_5, & pb_3 &= w^2 b_7.\\
[b_4, b_1] &= b_6, & &\\
[b_5, b_2] &= -w^2 b_7, & &\\
[b_6, b_1] &= b_7, & &
\end{aligned}$$

Then $R(\mathcal{L}) = \langle b_3, \ldots, b_7 \rangle$ and each Lie p-ring L in the family of $\mathcal{L}$ is generated by $\{b_1, b_2\}$. We define

$$g_1 = g_{11}b_1 + \ldots + g_{17}b_7 \quad \text{and} \quad g_2 = g_{21}b_1 + \ldots + g_{27}b_7.$$

Next, we write $b_3, \ldots, b_7$ as words in $\{b_1, b_2\}$. It can be read off from the defining relations that $b_3 = [b_2, b_1], b_4 = [b_3, b_1], b_5 = [b_3, b_2], b_6 = [b_4, b_1], b_7 = [b_6, b_1]$. Using this, we expand the mapping defined by $\{g_{rs}\}$ to the remaining generators $b_3, \ldots, b_7$. For example, for b_3 this yields

$$\begin{aligned}
&g_3 = [g_2, g_1]\\
&= (g_{11}g_{22} - g_{12}g_{21})b_3 + (g_{11}g_{23} - g_{13}g_{21})b_4 + (g_{12}g_{23} - g_{13}g_{22})b_5\\
&+ (g_{11}g_{24} - g_{14}g_{21})b_6 + (-g_{12}g_{25}w^2 + g_{15}g_{22}w^2 + g_{11}g_{26} - g_{16}g_{21})b_7.
\end{aligned}$$

We now evaluate the defining relations of $\mathcal{L}$ in $g_1, \ldots, g_n$. For example $pb_1 = b_5 + xb_7$ evaluates to

$$\begin{aligned}
pg_1 - g_5 - xg_7 = {}& 0b_1 + 0b_2 + 0b_3\\
&+ (-g_{11}g_{21}g_{22} + g_{12}g_{21}^2)b_4\\
&+ (-g_{11}g_{22}^2 + g_{12}g_{21}g_{22} + g_{11})b_5\\
&+ (-g_{11}g_{21}g_{23} + g_{12}w^2 + g_{13}g_{21}^2)b_6\\
&+ (-g_{11}^4 g_{22}x + g_{11}^3 g_{12}g_{21}x + g_{12}g_{22}g_{23}w^2 - g_{13}g_{22}^2 w^2 - g_{11}g_{21}g_{24}\\
&\quad + g_{13}w^2 + g_{14}g_{21}^2 + g_{11}x + g_{12}y)b_7
\end{aligned}$$

Note that the coefficient of b_3 in this relation is zero. More generally, if R_i is any of the relations then

$$\overline{R}_i = w_{i4}b_4 + \ldots + w_{i7}b_7 = 0,$$

and b_4, b_5, b_6, b_7 all have order p. So we obtain an automorphism at the prime P if and only if $w_{ij} = 0 \bmod P$ ($j = 4, 5, 6, 7$) for all relations R_i.

Now let L be a finite Lie p-ring in the family defined by $\mathcal{L}$ and let P be its prime. If the integer coefficients g_{rs} define an automorphism of L, then $det(G)$ is coprime to P. Hence, examining the coefficient of b_4 in the relation above we see that

$$-g_{11}g_{21}g_{22} + g_{12}g_{21}^2 = -g_{21}det(G) \equiv 0 \bmod P$$

is equivalent to $g_{21} \equiv 0 \bmod P$. In turn, this can now be used to simplify the remaining coefficients. Using $g_{21} \equiv 0 \bmod P$ now yields

$$-g_{11}g_{22}^2 + g_{12}g_{21}g_{22} + g_{11} = -g_{11}g_{22}^2 + g_{11} = -g_{11}(g_{22}^2 - 1)$$

As $det(G) \equiv g_{11}g_{22} \bmod P$ via $g_{21} \equiv 0 \bmod P$, it follows that g_{11} is coprime to P and $g_{22}^2 = 1 \bmod P$. We now iterate this approach. Introducing another indeterminate D with $Ddet(G) \equiv 1 \bmod P$ we finally obtain that

$$\begin{aligned}&g_{21}, g_{12}, x(g_{22} - 1), g_{22}^2 - 1, y(g_{11} - 1), y(D - g_{22}), Dg_{22} - g_{11}^2,\\ &Dg_{11} - g_{22}, D^2 - g_{11}, x(g_{11}^2 - D), g_{11}^2 g_{22} - D, g_{11}^3 - 1\end{aligned}$$

evaluate to 0 modulo P. We use this to eliminate indeterminates in the descriptions of g_1, g_2; for example, we can replace g_{21} by 0. We obtain

$$\begin{array}{l} g_1 = (D^2 \;\; 0 \;\; g_{13}\; g_{14}\; g_{15}\; g_{16}\; g_{17}) \\ g_2 = \;\, (0 \;\; D^3\; g_{23}\; g_{24}\; g_{25}\; g_{26}\; g_{27}) \end{array},$$

subject to the additional condition that the polynomials

$$(D-1)xy, (D^2-1)y, (D^3-1)x, D^6 - 1$$

must evaluate to $0 \bmod P$. This is the resulting description of the automorphism groups of the Lie p-rings L in the family defined by $\mathcal{L}$. It implies that $|Aut(L)| = kP^{10}$, where $k \in \{1, 2, 3, 6\}$. The precise value of k depends on the two parameters x, y. When $P \equiv 1 \bmod 3$, if $x = y = 0$ then $k = 6$; if $x = 0$ and $y \neq 0$ then $k = 2$; if $x \neq 0$ and $y = 0$ then $k = 3$; finally if $x, y \neq 0$ then $k = 1$. When $P \equiv 2 \bmod 3$ then $k = 1$ or 2.

4 The Lazard Correspondence

The final example of this abstract illustrates how the Lazard correspondent $G(L)$ to a finite Lie p-ring L can be determined using the LieRing package [1].

```
gap> L := LiePRingsByLibrary(7)[300];
<LiePRing of dimension 7 over prime p with parameters [ x ]>
gap> NumberOfLiePRingsInFamily(L);
p
gap> LiePRingsInFamily(L, 7);
[ <LiePRing of dimension 7 over prime 7>,
...
gap> List(last, x -> PGroupByLiePRing(x));
[ <pc group of size 823543 with 7 generators>,
...
gap> List(last, x -> Size(AutomorphismGroup(x)));
[80707214,80707214,80707214,80707214,80707214,80707214,80707214]
gap> a := AutGroupDescription(L);
rec( auto := [ [ A11, A12, A13, A14, A15, A16, A17 ],
               [   0,   1, A23,   0, A25, A26, A27 ] ],
     eqns := [ A11^2-1, A12*w*x-A11*A26 ] )
gap> 2*7^9;
80707214
```

References

1. Cicalò, S., de Graaf, W.A.: Liering, a GAP 4 package, see [9] (2010)
2. Cicalò, S., de Graaf, W.A., Vaughan-Lee, M.R.: An effective version of the lazard correspondence. J. Algebra **352**, 430–450 (2012)
3. Eick, B., Jalaleean, T.: Computing the Schur multiplier of a symbolic lie ring (2020, submitted)
4. Eick, B., Vaughan-Lee, M.: LiePRing version 2.5, : a GAP 4 package, see [9]. Version **2**, 5 (2020). http://www.iaa.tu-bs.de/beick/soft/liepring
5. Lazard, M.: Sur les groupes nilpotents et les anneaux de Lie. Ann. Sci. Ecole Norm. Sup. **3**(71), 101–190 (1954)
6. Newman, M.F., O'Brien, E.A., Vaughan-Lee, M.R.: Groups and nilpotent Lie rings whose order is the sixth power of a prime. J. Alg. **278**, 383–401 (2003)
7. O'Brien, E.A., Vaughan-Lee, M.R.: The groups with order p^7 for odd prime p. J. Algebra **292**(1), 243–258 (2005)
8. Robinson, D.J.S.: A Course in the Theory of Groups. Graduate Texts in Math, vol. 80. Springer, New York (1982)
9. The GAP Group: GAP - Groups, Algorithms and Programming, Version 4.10 (2019). http://www.gap-system.org