S0021-8693(03)00777-4/FLA AID:9967 Vol.●●●(●●●) yjabr9967 P.1(1-19)
ELSGMLTM(YJABR):m1 2004/01/13 Prn:5/02/2004; 11:39 by:V.Cer p. 1

Available online at www.sciencedirect.com
SCIENCE DIRECT®

ELSEVIER

Journal of Algebra ●●● (●●●●) ●●●–●●●

JOURNAL OF Algebra

www.elsevier.com/locate/jalgebra

Groups and nilpotent Lie rings whose order is the sixth power of a prime ☆

M.F. Newman,[a,*] E.A. O'Brien,[b] and M.R. Vaughan-Lee [c]

[a] *Mathematical Sciences Institute, Australian National University, ACT 0200, Australia*
[b] *Department of Mathematics, University of Auckland, Auckland, New Zealand*
[c] *Christ Church, University of Oxford, OX1 1DP, United Kingdom*

Received 20 August 2003

Communicated by Efim Zelmanov

Abstract

We prove that there are $3p^2 + 39p + 344 + 24\gcd(p-1,3) + 11\gcd(p-1,4) + 2\gcd(p-1,5)$ isomorphism types of groups and nilpotent Lie rings with order p^6 for every prime $p \geqslant 5$. We establish the result, and power-commutator presentations for the groups, in various ways. The most novel method constructs product presentations for nilpotent Lie rings with order p^6 and then uses the Baker–Campbell–Hausdorff formula to construct power-commutator presentations for the corresponding groups. Public access to the group presentations is provided via a database distributed with computer algebra systems.

1. Introduction

The determination of the groups with a given order has a long history; for a detailed account see Besche, Eick, and O'Brien [6]. The central task is to provide a *complete* and *irredundant* list of the groups with a given order. The primary difficulty is the reduction to isomorphism types; it is comparatively easy to give a complete list.

The 5 groups with order p^3 are well-known, so are the 14 groups with order 16 and the 15 groups with order p^4 for p odd (see, for example, Burnside [10]). There are

☆ This work was supported by the Marsden Fund of New Zealand via grant UOA 124.
* Corresponding author.
E-mail addresses: newman@maths.anu.edu.au (M.F. Newman), obrien@math.auckland.ac.nz (E.A. O'Brien), michael.vaughan-lee@christ-church.oxford.ac.uk (M.R. Vaughan-Lee).

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2003.11.012

S0021-8693(03)00777-4/FLA AID:9967 Vol.●●●(●●●) yjabr9967 P.2(1-19)
ELSGMLTM(YJABR):m1 2004/01/13 Prn:5/02/2004; 11:39 by:V.Cer p. 2

51 groups with order 2^5 (Miller [23]). The groups with order p^5 for $p \geqslant 5$, of which there are $61 + 2p + 2\gcd(p-1,3) + \gcd(p-1,4)$, were first determined and tabulated by Bagnera [2]. The 67 groups with order 3^5 were finally listed by James in 1980 [20].

Here we report on a new and independent determination of the groups with order p^6 for primes $p \geqslant 5$. Our primary result is the following.

Theorem 1. *There are*

$$3p^2 + 39p + 344 + 24\gcd(p-1,3) + 11\gcd(p-1,4) + 2\gcd(p-1,5)$$

groups with order p^6 for $p \geqslant 5$.

Previous attempts to obtain such a result, and to list the groups, have been flawed. There is a description of some of this work in Section 2.

The 267 groups with order 2^6 were first determined by P. Hall and Senior in the late 1930s and their descriptions were published by M. Hall and Senior [16]; the 504 groups with order 3^6 were first described in James [20].

Recall the Baker–Campbell–Hausdorff formula [18] and the Lazard correspondence [8] establish an isomorphism between the category of nilpotent Lie rings with order p^n and nilpotency class at most $p-1$ and the category of finite p-groups with order p^n and class at most $p-1$; in particular, this applies where $p \geqslant n$. As a novel approach to proving Theorem 1, we first determine the nilpotent Lie rings with order p^6 and then exploit this equivalence to obtain all of the p-groups with order p^6 for $p \geqslant 5$, excluding the 5-groups of maximal class. The 5-groups with order 5^6 and maximal class are well-known; see, for example, Blackburn [5].

In Section 5, we present an algorithm to determine the nilpotent Lie rings with order p^n. It is an analogue of the p-group generation algorithm, which we now briefly recall; for a detailed description see O'Brien [27]. Let P be a p-group. The algorithm uses the lower p-central series, defined recursively by $\mathcal{P}_1(P) = P$ and $\mathcal{P}_{i+1}(P) = [\mathcal{P}_i(P), P]\mathcal{P}_i(P)^p$ for $i \geqslant 1$. The p-class of P is the length of this series. Each p-group P, apart from the elementary abelian ones, is an *immediate descendant* of the quotient P/R where R is the last non-trivial term of the lower p-central series of P. Thus all the groups with order p^6, except the elementary abelian one, are immediate descendants of groups with order p^k for $k < 6$. All of the immediate descendants of a p-group Q are quotients of a certain extension of Q; the isomorphism problem for these descendants is equivalent to the problem of determining orbits of certain subgroups of this extension under an action of the automorphism group of Q. Not all p-groups have immediate descendants, those that do are called *capable*. We observe that Lie ring calculations are usually significantly easier for an arbitrary prime than those for the corresponding groups.

We used the *Lie ring generation algorithm* to determine all of the nilpotent Lie rings with order p^6 for all $p > 2$, and to obtain *product presentations* (see [17]) for them. We then applied the Baker–Campbell–Hausdorff formula to "translate" these presentations into group presentations; this is discussed in Section 4. In this way our Lie ring generation algorithm leads to a list of presentations for the groups with order p^6 for $p > 5$.

S0021-8693(03)00777-4/FLA AID:9967 Vol.●●●(●●●) yjabr9967 P.3(1-19)
ELSGMLTM(YJABR):m1 2004/01/13 Prn:5/02/2004; 11:39 by:V.Cer p. 3

In summary, for $p \geqslant 3$, there are 42 nilpotent Lie rings which have immediate descendants with order p^6. For $p \geqslant 5$ presentations for the corresponding groups are given in Theorem 2. Table 1 gives the number of immediate descendants with order p^6 for these 42 groups. Theorem 1 is now an immediate consequence.

An alternative proof of Theorem 1 uses P. Hall's notion of isoclinism [15]; this is the basis of the 1940 work of Easterfield [12] and the work of James [19,20]. Recall that two groups G and H are called *isoclinic* if there are isomorphisms $\varphi : G/Z(G) \mapsto H/Z(H)$ and $\psi : G' \mapsto H'$, such that for all $g_1, g_2 \in G$,

$$g_1 Z(G)\varphi = h_1 Z(H), \qquad g_2 Z(G)\varphi = h_2 Z(H), \qquad [g_1, g_2]\psi = [h_1, h_2].$$

For $p \geqslant 5$ the groups with order p^6 are classified into 43 isoclinism families [12]. All of the groups in a family are quotients of certain "generating groups". The isomorphism problem for these quotients is equivalent to the problem of determining orbits of certain subgroups under (a quotient of) the automorphism group of each generating group. For a discussion of this approach, see Section 7.

Easterfield [12] tabulated parametrised presentations for the groups with order p^6 for $p \geqslant 5$. We have, with the help of Robert McKibbin, checked this tabulation. It was chosen initially because it seemed reasonably accurate and gave lots of detail about the groups to help with checking. Easterfield's tables are not completely error-free. There are $p - 1$ groups missing from isoclinism family Φ_{13} and the presentations for one isoclinism family (Φ_{19}) had sufficient problems that we replaced them by the corresponding presentations of James [20]. There were also a small number of typographical errors.

That the two proofs, via Lie ring generation and isoclinism, reach the same conclusion significantly increases our confidence in Theorem 1.

We have created a database of parametrised presentations for the groups with order p^6 for $p \geqslant 5$, based on the corrected Easterfield list. The database is currently designed for use with MAGMA [7]; the data can readily be incorporated into other computer algebra systems. The construction from the database of the list for a given prime is extremely fast. For example, on an 800 MHz processor, MAGMA constructs power-commutator presentations [34] for the 860 groups with order 7^6 in about 1 second, and for the 181 076 groups with order 239^6 in about 500 seconds.

We describe the construction, the content, and the organisation of the database in Section 8 and in Section 9 discuss steps taken to verify the results.

2. Background

The first attempt to list the groups with order p^6 was made by Potron [32] in his Paris thesis of 1904. He followed Burnside [10] and de Séguier [11] in using the structure of the upper central factors as the basis for his classification. Miller [24] and Easterfield [12] have drawn attention to substantial problems with Potron's list. However, in retrospect, his list exhibits some significant aspects of the situation. The list is partitioned into several hundred cases each of which is described by a (usually parametrised) power-commutator presentation. This can be done so that at most 2 parameters are used in addition to a prime

S0021-8693(03)00777-4/FLA AID:9967 Vol.●●●(●●●) yjabr9967 P.4(1-19)
ELSGMLTM(YJABR):m1 2004/01/13 Prn:5/02/2004; 11:39 by:V.Cer p. 4

parameter. The primes can be partitioned into 11 parts; with 2, 3, 5 separate and the others classified according to whether their remainders modulo 3, 4, and 5 are 1 or not.

Miller [24] used maximal abelian normal subgroups as the basis of an attempt to determine the groups with order 64. This led to the work by Senior and his collaboration with Hall. From 1935 Brahana determined certain groups with class 2 and exponent p mainly using projective geometric methods, see [9].

Easterfield in his 1939/1940 Cambridge dissertation [12] used isoclinism (which he called isologism) as a basis for listing the regular (in the sense of Hall) groups. This handles all primes greater than 5 and the prime 5 for nilpotency class less than 5. He also handled the 5-groups with class 5 and determined the isoclinism families for the prime 3. James used a similar method in his PhD thesis [19], published (in amended form) in 1980 [20]. That paper has a number of inaccuracies. Some of these were pointed out by Pilyavskaya [29].

Pilyavskaya (also transcribed Pylyavska) made a determination using maximal abelian normal subgroups. Her approach is described in a document deposited in the VINITI archive [30] and in her Candidate's thesis [31]. Some errors were corrected in an English version of her thesis which was circulated privately. Recently an exchange of emails has resulted in other errors being corrected. This further supports the enumeration stated in Theorem 1. There is agreement at the level of presentations in the small number of isoclinism families that have been compared in detail.

Other contributions to the problem include work by Tordella [35], Küpper [22], and Baldwin [3].

3. The main result

For $p \geqslant 5$, there are 42 groups with order p^k for $k < 6$ which have immediate descendants with order p^6. These groups were determined directly using the Lie ring generation algorithm. Of course, the result can also be deduced from the published tabulations: Bagnera [2], de Séguier [11], Schreier [33], Bender [4], and James [20].

In Theorem 2 we record a finite presentation for each such capable group (or *parent*), and the number of its immediate descendants with order p^6. The finite presentation and the listed p-class can be used to construct a power-commutator presentation. (For example, it can be supplied with a specific prime p to the p-quotient algorithm [26].)

Theorem 2. *For $p \geqslant 5$, the groups with order dividing p^5 which have immediate descendants with order p^6 are the following where ω is a primitive root of unity* mod p:

(1) $\langle a \mid \text{class } 5\rangle$;
(2) $\langle a, b \mid [b, a],\ \text{class } 2\rangle$;
(3) $\langle a, b \mid b^p,\ \text{class } 2\rangle$;
(4) $\langle a, b \mid\ b^p[b, a]^{-1},\ \text{class } 2\rangle$;
(5) $\langle a, b \mid \text{class } 2\rangle$;
(6) $\langle a, b \mid\ a^p,\ b^p,\ \text{class } 3\rangle$;
(7) $\langle a, b \mid\ a^p[b, a, a]^{-1},\ b^p,\ \text{class } 3\rangle$;

S0021-8693(03)00777-4/FLA AID:9967 Vol.●●●(●●●) yjabr9967 P.5(1-19)
ELSGMLTM(YJABR):m1 2004/01/13 Prn:5/02/2004; 11:39 by:V.Cer p. 5

(8) $\langle a, b \mid a^p[b,a,b]^{-1},\ b^p,\ \text{class } 3\rangle$;
(9) $\langle a, b \mid a^p[b,a,b]^{-\omega},\ b^p,\ \text{class } 3\rangle$;
(10) $\langle a, b \mid a^p[b,a,a]^{-1},\ b^p[b,a,b],\ \text{class } 3\rangle$;
(11) $\langle a, b \mid a^p[b,a,b],\ b^p[b,a,a]^{\omega},\ \text{class } 3\rangle$;
(12) $\langle a, b \mid [b,a],\ b^{p^2},\ \text{class } 3\rangle$;
(13) $\langle a, b \mid [b,a]a^{-p^2},\ b^{p^2},\ \text{class } 3\rangle$;
(14) $\langle a, b \mid [b,a,a],\ [b,a,b],\ b^p,\ \text{class } 3\rangle$;
(15) $\langle a, b \mid [b,a,b],\ a^{p^2},\ b^p,\ \text{class } 3\rangle$;
(16) $\langle a, b \mid [b,a,b],\ a^{p^2},\ b^p[b,a,a]^{-1},\ \text{class } 3\rangle$;
(17) $\langle a, b \mid [b,a,b],\ a^{p^2},\ b^p[b,a,a]^{-\omega},\ \text{class } 3\rangle$;
(18) $\langle a, b \mid [b,a,a],\ a^{p^2},\ b^p,\ \text{class } 3\rangle$;
(19) $\langle a, b \mid [b,a,a],\ b^p[b,a]^{-1},\ \text{class } 3\rangle$;
(20) $\langle a, b \mid [b,a],\ b^p,\ \text{class } 4\rangle$;
(21) $\langle a, b \mid [b,a,b],\ a^p,\ b^p,\ \text{class } 4\rangle$;
(22) $\langle a, b \mid [b,a,b][b,a,a,a]^{-1},\ a^p,\ b^p,\ \text{class } 4\rangle$;
(23) $\langle a, b, c \mid \ \text{class } 1\rangle$;
(24) $\langle a, b, c \mid [c,a],\ [c,b], a^p,\ b^p,\ c^p,\ \text{class } 2\rangle$;
(25) $\langle a, b, c \mid [b,a],\ [c,a],\ [c,b],\ c^p,\ \text{class } 2\rangle$;
(26) $\langle a, b, c \mid [c,a],\ [c,b],\ b^p,\ c^p,\ \text{class } 2\rangle$;
(27) $\langle a, b, c \mid [c,a],\ [c,b],\ b^p[b,a]^{-1},\ c^p,\ \text{class } 2\rangle$;
(28) $\langle a, b, c \mid [c,a],\ [c,b],\ b^p,\ c^p[b,a]^{-1},\ \text{class } 2\rangle$;
(29) $\langle a, b, c \mid [c,a],\ [c,b],\ a^p,\ b^p,\ \text{class } 2\rangle$;
(30) $\langle a, b, c \mid [c,a],\ [c,b],\ a^p[b,a]^{-1},\ b^p,\ \text{class } 2\rangle$;
(31) $\langle a, b, c \mid [c,b],\ a^p,\ b^p,\ c^p,\ \text{class } 2\rangle$;
(32) $\langle a, b, c \mid [c,b],\ a^p[b,a]^{-1},\ b^p,\ c^p,\ \text{class } 2\rangle$;
(33) $\langle a, b, c \mid [c,b],\ a^p,\ b^p[b,a]^{-1},\ c^p,\ \text{class } 2\rangle$;
(34) $\langle a, b, c \mid [c,b],\ a^p,\ b^p[c,a]^{-1},\ c^p,\ \text{class } 2\rangle$;
(35) $\langle a, b, c \mid [c,b],\ a^p[b,a]^{-1},\ b^p[c,a]^{-1},\ c^p,\ \text{class } 2\rangle$;
(36) $\langle a, b, c \mid [b,a],\ [c,a],\ [c,b],\ b^p,\ c^p,\ \text{class } 3\rangle$;
(37) $\langle a, b, c \mid [b,a,b],\ [c,a],\ [c,b],\ a^p,\ b^p,\ c^p,\ \text{class } 3\rangle$;
(38) $\langle a, b, c \mid [b,a,b],\ [c,a],\ [c,b][b,a,a]^{-1},\ a^p,\ b^p,\ c^p,\ \text{class } 3\rangle$;
(39) $\langle a, b, c, d \mid \text{class } 1\rangle$;
(40) $\langle a, b, c, d \mid [b,a],\ [c,a],\ [d,a],\ [c,b],\ [d,b],\ [d,c],\ b^p,\ c^p,\ d^p,\ \text{class } 2\rangle$;
(41) $\langle a, b, c, d \mid [c,a],\ [c,b],\ [d,a],\ [d,b],\ [d,c],\ a^p,\ b^p,\ c^p,\ d^p,\ \text{class } 2\rangle$;
(42) $\langle a, b, c, d, e \mid \text{class } 1\rangle$.

The number of immediate descendants of each group is summarised in Table 1.

As presented, Theorem 2 concerns p-groups. We proved the theorem by using Lie ring generation to construct the immediate descendants of each of the corresponding 42 nilpotent Lie rings; in Section 6 we illustrate some of the relevant calculations. The theorem was also established using the corrected Easterfield list.

S0021-8693(03)00777-4/FLA AID:9967 Vol.●●●(●●●) yjabr9967 P.6(1-19)
ELSGMLTM(YJABR):m1 2004/01/13 Prn:5/02/2004; 11:39 by:V.Cer p. 6

Table 1
Number of immediate descendants with order p^6 of the 42 parents

Parent	Number of immediate descendants
1	1
2	2
3	$p+15$
4	1
5	$p+8$
6	$5+3\gcd(p-1,3)$
7	$p+\gcd(p-1,3)+1$
8	$1+\gcd(p-1,3)+\gcd(p-1,4)/2$
9	$1+\gcd(p-1,3)+\gcd(p-1,4)/2$
10	$p+1$
11	p
12	2
13	1
14	4
15	$2\gcd(p-1,3)+\gcd(p-1,4)+3$
16	$3(p+1)/2$
17	$3(p+1)/2$
18	$2\gcd(p-1,3)+\gcd(p-1,4)+3$
19	2
20	2
21	$3\gcd(p-1,4)+2\gcd(p-1,3)+7$
22	$2p+2\gcd(p-1,3)+\gcd(p-1,4)+2\gcd(p-1,5)$
23	$3p+27$
24	$3p^2+13p+37+\gcd(p-1,3)+\gcd(p-1,4)$
25	4
26	23
27	5
28	4
29	12
30	$p+1$
31	35
32	$2p+13$
33	$4p+8$
34	$2p+3\gcd(p-1,3)+\gcd(p-1,4)+13$
35	3
36	3
37	$4\gcd(p-1,3)+2\gcd(p-1,4)+11$
38	$2\gcd(p-1,3)+4$
39	$4p+48$
40	4
41	18
42	7

4. Baker–Campbell–Hausdorff

It has been known since the 1950s that the Baker–Campbell–Hausdorff formula gives an isomorphism between the category of nilpotent Lie rings with order p^n and the category of finite p-groups with order p^n provided $p \geqslant n$. However, we are not aware that this connection has been systematically exploited to classify finite p-groups until now.

S0021-8693(03)00777-4/FLA AID:9967 Vol.●●●(●●●) yjabr9967 P.7(1-19)
ELSGMLTM(YJABR):m1 2004/01/13 Prn:5/02/2004; 11:39 by:V.Cer p. 7

Let A be the free associative algebra with unity over the rationals $\mathbb{Q}$ which is freely generated by non-commuting indeterminates x, y. We extend A to the ring $\widehat{A}$ of formal power series consisting of the formal sums

$$\sum_{n=0}^{\infty} u_n,$$

where u_n is a homogeneous element of weight n in A. If $a \in \widehat{A}$, and if the homogeneous component of a of weight 0 is 0, then we define

$$\mathrm{e}^a = 1 + a + \frac{a^2}{2!} + \frac{a^3}{3!} + \cdots$$

in the usual way. The product $\mathrm{e}^x \mathrm{e}^y \in \widehat{A}$ can be expressed in the form $1 + u$ for some $u \in \widehat{A}$ with 0 as its homogeneous component of weight 0, and

$$\mathrm{e}^x \mathrm{e}^y = \mathrm{e}^v, \quad \text{where } v = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{u^n}{n}.$$

The Baker–Campbell–Hausdorff formula (see, for example, Jacobson [18]) enables us to compute the homogeneous components of v. The first few components are given by

$$v = x + y - \frac{1}{2}[y,x] + \frac{1}{12}[y,x,x] - \frac{1}{12}[y,x,y] + \frac{1}{24}[y,x,x,y] - \frac{1}{720}[y,x,x,x,x] + \cdots.$$

It turns out that all the homogeneous components of v are Lie elements of A (that is, elements in the Lie subalgebra of A generated by x and y with respect to the Lie product $[a,b] = ab - ba$). A proof of this may be found in Vaughan-Lee [36]. A similar formula holds for commutators

$$\left[\mathrm{e}^y, \mathrm{e}^x\right] = \mathrm{e}^w,$$

where

$$w = [y,x] + \frac{1}{2}[y,x,x] + \frac{1}{2}[y,x,y] + \frac{1}{6}[y,x,x,x] + \frac{1}{4}[y,x,x,y] + \frac{1}{6}[y,x,y,y] + \cdots.$$

(Here $[\mathrm{e}^y, \mathrm{e}^x]$ is the group commutator $\mathrm{e}^{-y}\mathrm{e}^{-x}\mathrm{e}^y\mathrm{e}^x$, and w is an infinite sum of Lie elements in A.)

These formulae sometimes enable us to define a group structure on a Lie algebra. Perhaps the simplest situation where this applies is when L is a nilpotent Lie algebra

S0021-8693(03)00777-4/FLA AID:9967 Vol.●●●(●●●) yjabr9967 P.8(1-19)
ELSGMLTM(YJABR):m1 2004/01/13 Prn:5/02/2004; 11:39 by:V.Cer p. 8

over $\mathbb{Q}$. As described in [1], the Baker–Campbell–Hausdorff formula provides an isomorphism (the Mal'cev correspondence) between the category of nilpotent Lie algebras over $\mathbb{Q}$ and the category of torsion-free divisible nilpotent groups.

The Baker–Campbell–Hausdorff formula also provides a connection between finite p-groups and nilpotent Lie rings (over $\mathbb{Z}$) with prime-power order, in the case when the groups and Lie rings are nilpotent of class at most $p-1$. We write the element v above as

$$v = v_1 + v_2 + \cdots,$$

where v_i is a homogeneous Lie element of weight i, for $i = 1, 2, \ldots$, and we consider the truncated expression

$$\tilde{v}(x, y) = v_1 + v_2 + \cdots + v_{p-1}.$$

Observe that the denominators of the coefficients that occur in $\tilde{v}(x, y)$ are coprime to p. If L is a Lie ring with order p^n (so that L has characteristic p^k for some k), and if L is nilpotent of class at most $p-1$, then we can define a group operation "$\circ$" on L by setting

$$a \circ b = \tilde{v}(a, b) \quad \text{for } a, b \in L.$$

This turns L into a group with order p^n, and every finite p-group of nilpotency class at most $p-1$ arises in this way from a finite Lie ring. This *Lazard correspondence* appears as Exercise §7.4 in Bourbaki [8, Chapter 2].

5. The Lie ring generation algorithm

Our method of classifying nilpotent Lie rings with order p^n closely follows the p-group generation algorithm (see Newman [25] and O'Brien [27]). A Lie ring L is an abelian group under $+$ (addition) together with a bilinear product which satisfies

$$aa = 0 \quad \text{for all } a \in L,$$
$$(ab)c + (bc)a + (ca)b = 0 \quad \text{for all } a, b, c \in L.$$

(We use ab to denote the Lie product of a and b, rather than the more familiar $[a, b]$.) Note that the axiom $aa = 0$ together with bilinearity implies that $ba = -ab$. The identity $(ab)c + (bc)a + (ca)b = 0$ is the Jacobi identity.

Since the Lie product is not associative the bracketing of a product is significant. We adopt the left-normed convention whereby

$$a_1 a_2 \ldots a_n = \big(\ldots\big((a_1 a_2)a_3\big)\ldots a_{n-1}\big)a_n.$$

For a Lie ring L we define the *lower central series*

$$L \geqslant L^2 \geqslant L^3 \geqslant \cdots \geqslant L^c \geqslant \cdots$$

S0021-8693(03)00777-4/FLA AID:9967 Vol.●●●(●●●) yjabr9967 P.9(1-19)
ELSGMLTM(YJABR):m1 2004/01/13 Prn:5/02/2004; 11:39 by:V.Cer p. 9

by setting $L^2 = \langle ab \mid a, b \in L \rangle$, and $L^{c+1} = \langle ab \mid a \in L^c,\ b \in L \rangle$ for $c > 1$. It is easy to show that a product of c elements of L (with any choice of bracketing) lies in L^c. Further, L^c consists of the set of all linear combinations of left-normed products $a_1 a_2 \dots a_c$ of elements of L. We say that L is nilpotent of class c if $L^{c+1} = \{0\}$, $L^c \neq \{0\}$.

When calculating in finite nilpotent Lie rings with prime-power order, the *lower p-central series*

$$L = L_1 \geqslant L_2 \geqslant L_3 \geqslant \cdots \geqslant L_c \geqslant \cdots$$

is often more useful than the lower central series. This is defined for Lie rings in an analogous way to groups. We set $L_1 = L$, $L_2 = L^2 + pL$, and for $c > 1$ we set $L_{c+1} = L_c L + pL_c$. (Here $L_c L$ is $\langle ab \mid a \in L_c,\ b \in L \rangle$.) Note that we use superscripts to denote terms of the lower central series, and subscripts to denote terms of the lower p-central series. The ideal L_c consists of all linear combinations of terms of the form

$$a_1 a_2 \dots a_c, \quad p a_1 a_2 \dots a_{c-1}, \quad p^2 a_1 a_2 \dots a_{c-2}, \quad \dots, \quad p^{c-1} a_1.$$

We say that L has p-class c if $L_{c+1} = \{0\}$, $L_c \neq \{0\}$.

If L is a nilpotent Lie ring with finite order p^n for some prime p, then L_{c+1} will equal $\{0\}$ for some c. In fact if L is nilpotent of class k and if the exponent of L as a finite abelian group is p^m then L has p-class c for some c with $k \leqslant c < k + m$.

If L and M are two finite nilpotent Lie rings with prime-power order, then L is a *descendant* of M if $L/L_c \cong M$ for some $c \geqslant 2$. If $L/L_c \cong M$ and L has p-class c (so that $L_c \neq \{0\}$, $L_{c+1} = \{0\}$) then L is an *immediate descendant* of M. Note that if L is a descendant of M then $L/L_2 \cong M/M_2$, so that L and M have the same generator number.

The key idea for calculating nilpotent Lie rings L with order p^n is as follows. If L has p-class 1 then L is the direct sum of n copies of $\mathbb{Z}_p$; call L *elementary abelian*. If L has p-class greater than 1, then L is an immediate descendant of a nilpotent Lie ring with order p^m for some $m < n$. The starting point for calculating the nilpotent Lie rings with order p^6 is to calculate the nilpotent Lie rings with order p^k for $1 \leqslant k < 6$. For each of these Lie rings we calculate the immediate descendants with order p^6 as follows. Given a d-generator Lie ring M we construct its p-covering ring $\widehat{M}$. This is a d-generator Lie ring $\widehat{M}$ having a central elementary abelian ideal Z such that $\widehat{M}/Z \cong M$ and every immediate descendant of M is isomorphic to $\widehat{M}/T$ for some $T \leqslant Z$. However $\widehat{M}/T$ is not an immediate descendant of M for every subring $T \leqslant Z$. If M has p-class c (so that $M_{c+1} = \{0\}$) then we define the *nucleus* of M to be $\widehat{M}_{c+1}$. Then $\widehat{M}/T$ is an immediate descendant of M if and only if T is a proper subring of Z such that T supplements the nucleus $\widehat{M}_{c+1}$. It can happen that $\widehat{M}_{c+1} = \{0\}$, in which case M has no immediate descendants and is *terminal*.

Hence we obtain a complete list of the immediate descendants of M by calculating its p-covering ring $\widehat{M}$, and listing the proper subrings $T < Z$ such that $T + \widehat{M}_{c+1} = Z$. (These are the *allowable subrings* of Z.) If M is a d-generator Lie ring with order p^n then Z is elementary abelian of rank at most $d(d-1)/2 + d(n-d+1)$. The elementary abelian Lie

S0021-8693(03)00777-4/FLA AID:9967 Vol.●●●(●●●) yjabr9967 P.10 (1-19)
ELSGMLTM(YJABR):m1 2004/01/13 Prn:5/02/2004; 11:39 by:V.Cer p. 10

ring with order p^5 has p-covering ring with order p^{20}; this is the largest ring we construct in studying the nilpotent Lie rings with order dividing p^6.

We now have a list of the immediate descendants of M, and we can easily restrict to those with a specified order. This list will usually contain redundancies, and we need to solve the isomorphism problem. This is done as follows. We compute the automorphism group of M and we extend each automorphism α of M to an automorphism α^* of $\widehat{M}$. (If M is generated by $a_1, a_2, \ldots, a_d$ then we choose preimages $x_1, x_2, \ldots, x_d$ in $\widehat{M}$ for $a_1, a_2, \ldots, a_d$, and preimages $y_1, y_2, \ldots, y_d$ in $\widehat{M}$ for $a_1\alpha, a_2\alpha, \ldots, a_d\alpha$. Then $x_1, x_2, \ldots, x_d$ generate $\widehat{M}$, and we define α^* by setting $x_i\alpha^* = y_i$ for $i = 1, 2, \ldots, d$.) Then $Z\alpha^* = Z$, and the action of α^* on Z is uniquely determined by α. Two allowable subrings T_1, T_2 define isomorphic descendants $\widehat{M}/T_1, \widehat{M}/T_2$ if and only if $T_2\alpha^* = T_1$ for some automorphism α of M. We obtain a complete irredundant set of immediate descendants of M by choosing a set of representatives for the orbits of the allowable subrings of Z under this action of the automorphism group of M.

The p-covering ring is completely analogous to the p-covering group. We refer the reader to the proofs of the corresponding results in O'Brien [27, Section 2].

6. Lie ring examples

As an illustration of the Lie ring generation algorithm, we compute the descendants with order p^6 of

$$A = \langle a, b \mid baa,\ p^2a,\ pb,\ \text{class } 3 \rangle$$

A is a 2-generator Lie ring with order p^5 and p-class 3. If we apply the Baker–Campbell–Hausdorff formula to its presentation then we obtain the following group presentation:

$$\{a, b \mid [b, a, a],\ a^{p^2},\ b^p,\ \text{class } 3\}.$$

This group presentation has the same form as that of the Lie ring, although this is not always the case. (This is group 18 from Theorem 2.)

It is easy to show that A/A_2 has order p^2 and is generated by $a + A_2$, $b + A_2$; further A_2/A_3 has order p^2 and is generated by $ba + A_3$, $pa + A_3$; the last term A_3 has order p and is generated by bab. It is also easy to show that if a', b' are the images of a, b under an automorphism of A then $a' = \alpha a + \gamma ba + \delta pa + \varepsilon bab$ and $b' = \beta b + \zeta ba + \eta pa + \theta bab$ with α, β coprime to p. Further, if a', b' are of this form then there is an automorphism of A mapping a, b to a', b'. Hence the automorphism group of A has order $(p-1)^2p^6$.

Let L be a 2-generator Lie ring of p-class 4 such that $L/L_4 \cong A$. Then L is generated by a, b; further L_2 is generated by ba, pa modulo L_3 and L_3 is generated by bab modulo L_4. Recall that L_4 is defined to be $L_3L + pL_3$. Since L_3 is generated modulo L_4 by bab we see that L_4 is generated by $baba$, $babb$ and $p(bab)$. However baa, p^2a and pb are in L_4, and so $baba = baab = 0$ and $p(bab) = (pb)ab = 0$. Hence L_4 is generated by $babb$ and $baa = \lambda babb$, $p^2a = \mu babb$, $pb = \nu babb$ for some λ, μ, ν. Since L_4 has order p, we can think of λ, μ, ν as elements of $\mathbb{Z}_p$. It is easy to show that all p^3 values of the

S0021-8693(03)00777-4/FLA AID:9967 Vol.●●●(●●●) yjabr9967 P.11(1-19)
ELSGMLTM(YJABR):m1 2004/01/13 Prn:5/02/2004; 11:39 by:V.Cer p. 11

triple λ, μ, ν define a Lie ring L with order p^6 and p-class 4 which is a descendant of A. It remains to solve the isomorphism problem: when do two triples λ, μ, ν and λ', μ', ν' define isomorphic Lie rings?

We solve this problem by letting the automorphism group of A act on the set of possible presentations for L. In other words we consider a presentation

$$L = \{a, b \mid baa - \lambda babb,\ p^2a - \mu babb,\ pb - \nu babb,\ \text{class } 4\}$$

for a descendant of A with order p^6 and p-class 4, and we let

$$a' = \alpha a + \gamma ba + \delta pa + \varepsilon bab, \qquad b' = \beta b + \zeta ba + \eta pa + \theta bab.$$

It is now easy to compute that

$$\begin{aligned} b'a'a' &= \alpha^2\beta baa = \alpha^2\beta\lambda babb = \alpha\beta^{-2}\lambda b'a'b'b', \\ p^2a' &= \alpha p^2a = \alpha\mu babb = \beta^{-3}\mu b'a'b'b', \\ pb' &= \beta pb + \eta p^2a = (\beta\nu + \eta\mu)babb = \alpha^{-1}\beta^{-3}(\beta\nu + \eta\mu)b'a'b'b'. \end{aligned}$$

Hence the triples λ, μ, ν and $\alpha\beta^{-2}\lambda,\ \beta^{-3}\mu, \alpha^{-1}\beta^{-3}(\beta\nu + \eta\mu)$ determine isomorphic algebras.

It follows easily that we get a complete set of pairwise non-isomorphic descendants of A with order p^6 by taking triples λ, μ, ν satisfying the following properties:

- $\lambda = 0$ or 1,
- $\mu = 0$ or 1, or (when $p = 1 \bmod 3$) ω or ω^2 where ω is a primitive element in $\mathbb{Z}_p$,
- $\nu = 0$ when $\mu \neq 0$, $\nu = 0$ or 1 when $\lambda = \mu = 0$, and when $\lambda = 1$, $\mu = 0$ then $\nu = 0, 1$ or ω, or (when $p = 1 \bmod 4$) ω^2 or ω^3 where ω is a primitive element in $\mathbb{Z}_p$.

Hence the number of descendants of $\langle a, b \mid\ baa, p^2a,\ pb,\ \text{class } 3\rangle$ with order p^6 depends on the value of p mod 12, and is $2\gcd(p-1, 3) + \gcd(p-1, 4) + 3$.

We now apply the Baker–Campbell–Hausdorff formula to the Lie ring presentations described above to obtain a complete and irredundant list of (group) presentations for the immediate descendants of the group having presentation

$$\{a, b \mid [b, a, a],\ a^{p^2},\ b^p,\ \text{class } 3\}.$$

The Baker–Campbell–Hausdorff formula applied to the Lie ring presentation

$$\{a, b \mid baa - \lambda babb,\ p^2a - \mu babb,\ pb - \nu babb,\ \text{class } 4\}$$

gives the group presentation

$$\{a, b \mid [b, a, a][b, a, b, b]^{-\lambda},\ a^{p^2}[b, a, b, b]^{-\mu},\ b^p[b, a, b, b]^{-\nu},\ \text{class } 4\}.$$

S0021-8693(03)00777-4/FLA AID:9967 Vol.●●●(●●●) yjabr9967 P.12(1-19)
ELSGMLTM(YJABR):m1 2004/01/13 Prn:5/02/2004; 11:39 by:V.Cer p. 12

Again, the group presentations have the same form as the Lie ring presentations, with the same ranges for the parameters.

We sometimes obtain group presentations which differ significantly from the corresponding Lie ring presentations. For example, when computing the immediate descendants with order p^6 of

$$\langle a, b \mid bab,\ p^2a,\ pb - baa,\ \text{class } 3\rangle,$$

we obtain presentations

$$\{a, b \mid bab,\ p^2a,\ pb - baa - \lambda baaa,\ \text{class } 4\}$$

with $0 \leqslant \lambda < p$. (There are other descendants.) If we replace a by $-a$ in this presentation then we obtain

$$\{a, b \mid bab,\ p^2a,\ pb - baa + \lambda baaa,\ \text{class } 4\},$$

and so it is clear that the parameters λ and $-\lambda$ give isomorphic Lie rings. If we let λ take the values $0, 1, \ldots, (p-1)/2$ then we get $(p+1)/2$ pairwise non-isomorphic descendants. Applying the Baker–Campbell–Hausdorff formula to these presentations, we obtain the group presentations

$$\{a, b \mid [b, a, b],\ a^{p^2},\ b^p[b, a, a]^{-1}[b, a, a, a]^{1-\lambda},\ \text{class } 4\}.$$

Note that λ and $-\lambda$ must give isomorphic groups since the corresponding Lie rings are isomorphic, and the groups obtained by letting $\lambda = 0, 1, \ldots, (p-1)/2$ are pairwise non-isomorphic. In the group context it might seem more natural to parametrise these groups with a parameter μ replacing the exponent $1 - \lambda$. In these terms the isomorphism question is less transparent: μ and μ' give isomorphic groups if $\mu - 1 = \pm(\mu' - 1)$.

As another example, we consider the 4-generator Lie rings with order p^6 and p-class 2. Let $L = \langle a, b, c, d\rangle$ be a Lie ring of this form. As a first step we divide the problem up into three cases: L is abelian, L^2 has order p, and L^2 has order p^2. (Recall that L^2 is the derived ring $\langle xy \mid x, y \in L\rangle$.)

Just as for groups, there is only one abelian 4-generator Lie ring with order p^6 and p-class 2. It has additive structure $\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2}$.

If L^2 has order p then the map

$$(x + L_2, y + L_2) \mapsto xy$$

defines an alternating bilinear map from $L/L_2 \times L/L_2 \to L^2$. (Here we are viewing L/L_2 as a 4-dimensional vector space over $\mathbb{Z}_p$, and we are viewing L^2 as a 1-dimensional vector space over $\mathbb{Z}_p$.) We may assume that L^2 is generated by ba. Hence

$$ca = da = cb = db = dc = 0 \quad \text{or} \quad ca = da = cb = db = 0, \quad dc = ba.$$

S0021-8693(03)00777-4/FLA AID:9967 Vol.●●●(●●●) yjabr9967 P.13(1-19)
ELSGMLTM(YJABR):m1 2004/01/13 Prn:5/02/2004; 11:39 by:V.Cer p. 13

In other words, if L^2 has order p then we may assume that L satisfies one of these two sets of commutator relations. A Lie ring satisfying the first set of relations cannot be isomorphic to a Lie ring satisfying the second set. If L^2 has order p^2 then (up to isomorphism) L has 4 possible commutator structures.

We examine in detail the situation when L^2 has order p and is generated by ba, and when $ca = da = cb = db = dc = 0$. The centre of L has order p^4 and equals $\langle c, d\rangle + L_2$, so $\langle c, d\rangle + L_2$ is a characteristic subring. Hence it is easy to see that if a', b', c', d' generate L, and if

$$c'a' = d'a' = c'b' = d'b' = d'c' = 0,$$

then (modulo L_2)

$$a' = \alpha a + \beta b + \varepsilon c + \zeta d, \qquad b' = \gamma a + \delta b + \eta c + \theta d,$$
$$c' = \lambda c + \mu d, \qquad d' = \nu c + \xi d$$

for some $\alpha, \beta, \ldots, \xi \in \mathbb{Z}_p$ with $\alpha\delta - \beta\gamma$ and $\lambda\xi - \mu\nu$ coprime to p. (Further, if a', b', c', d' are elements of this form, then they generate L and satisfy the same commutator relations as a, b, c, d.) It is convenient to think of L_2 as a vector space of dimension 2 over $\mathbb{Z}_p$. Since $\langle c, d\rangle + L_2$ is a characteristic subring, we can now divide the current situation into three subcases: pc, pd are linearly independent; pc, pd span a space of dimension 1; and $pc = pd = 0$.

If pc, pd are linearly independent then we can choose

$$a' = a + \varepsilon c + \zeta d, \qquad b' = b + \eta c + \theta d$$

so that $pa' = pb' = 0$. Then we can choose c', d' so that $pc' = b'a'$, and so L_2 is generated by $b'a'$, pd'. Hence we have the presentation

$$\{a, b, c, d \mid ca,\ da,\ cb,\ db,\ dc,\ pa,\ pb,\ pc - ba,\ \text{class } 2\}.$$

Next suppose that pc, pd span a space of dimension at most 1. Then we may assume that $pd = 0$, so that

$$L = \langle a, b, c\rangle \oplus \langle d\rangle.$$

The subring $\langle a, b, c\rangle$ must have order p^5 and derived ring with order p, and from the list of nilpotent Lie rings with order p^5 we see that $\langle a, b, c\rangle$ is isomorphic to one of the following:

$$\langle a, b, c \mid ca,\ cb,\ pb,\ pc,\ \text{class } 2\rangle, \qquad \langle a, b, c \mid ca,\ cb,\ pb - ba,\ pc,\ \text{class } 2\rangle,$$
$$\langle a, b, c \mid ca,\ cb,\ pb,\ pc - ba,\ \text{class } 2\rangle, \qquad \langle a, b, c \mid ca,\ cb,\ pa,\ pb,\ \text{class } 2\rangle,$$
$$\langle a, b, c \mid ca,\ cb,\ pa - ba,\ pb,\ \text{class } 2\rangle.$$

S0021-8693(03)00777-4/FLA AID:9967 Vol.●●●(●●●) yjabr9967 P.14 (1-19)
ELSGMLTM(YJABR):m1 2004/01/13 Prn:5/02/2004; 11:39 by:V.Cer p. 14

These examples are fairly simple, but they illustrate the main ideas used. Sometimes the relevant automorphism groups are hard to compute. Once an automorphism group has been computed, then we calculate its action on the set of presentations under consideration. In these cases it was easy to compute a set of representatives for the orbits of the presentations under the action of the automorphism group, but this is sometimes a much harder problem. The methods used here parallel one possible group theoretic approach. In the p-class two example the group calculation is identical to the Lie ring calculation. But in the p-class 4 example the linearity of Lie rings means that it is much easier to compute the action of the automorphism group of A on the set of presentations for L than it would be in groups.

7. Isoclinism families

We use the determination (and linear ordering) of the isoclinism families provided by Easterfield [12]. While it would technically be possible to verify his division into isoclinism families using the algorithm of James, Newman, and O'Brien [21], we see little merit in doing this: the completeness of the list is established using Theorem 2, and hence its organization into isoclinism families does not impact on its overall accuracy. In Table 2 we record the corrected number of groups in each family.

As one example of the computations involved, we consider Φ_{15}; our results agree with Easterfield [12] and Pilyavskaya [29], but differ from James [20].

Each group in this family is a 4-generator group with p-class 2. Its central quotient is the elementary abelian group with order p^4 which has p-covering group $\widehat{P}$ with order p^{14}. The defining generators of $\widehat{P}$ are labelled $a_1, \ldots, a_4$. We choose the defining commutator relations for the family to be $a_5 = [a_2, a_1] = [a_4, a_3]$, $a_6 = [a_3, a_1]$, $a_6^\omega = [a_4, a_2]$ with all other commutators trivial; ω is a primitive root mod p. Each member of this family is a quotient of

$$\langle a_1, \ldots, a_{10} \mid a_5 = [a_2, a_1] = [a_4, a_3],\ a_6 = [a_3, a_1],\ a_6^\omega = [a_4, a_2],$$
$$a_7 = a_1^p,\ a_8 = a_2^p,\ a_9 = a_3^p,\ a_{10} = a_4^p \rangle.$$

For this group the relevant quotient of its automorphism group has order $2(p^4 - 1) \times (p^4 - p^2)$.

If G is a group in this family, then G^p has rank 0, 1, or 2 and we use the rank of this subgroup to help classify the individual groups in the family. For each group, $a_i^p = a_5^{\alpha_i} a_6^{\beta_i}$, $i = 1, \ldots, 4$, and we refer to the 2×4 matrix of these values as the *exponent matrix*. The individual groups in this family are determined by the orbits of A on the exponent matrices.

S0021-8693(03)00777-4/FLA AID:9967 Vol.●●●(●●●) yjabr9967 P.15(1-19)
ELSGMLTM(YJABR):m1 2004/01/13 Prn:5/02/2004; 11:39 by:V.Cer p. 15

Table 2
Numbers for isoclinism families

Family	Number of groups
1	11
2	31
3	32
4	$3p + 32$
5	7
6	$2p + 21$
7	21
8	$p + 5$
9	$3\gcd(p-1,3) + 7$
10	$3\gcd(p-1,4) + 3\gcd(p-1,3) + 4$
11	$2p + 10$
12	$p + 13$
13	$p + 10$
14	3
15	$p + 3$
16	$p + \gcd(p-1,3) + 12$
17	$\gcd(p-1,3) + 4p + 30$
18	$3p + \gcd(p-1,3) + \gcd(p-1,4) + 9$
19	$(3p^2 + 10p + 21)/2$
20	$5p + \gcd(p-1,3) + \gcd(p-1,4) + 13$
21	$(3p^2 + 4p + 5)/2$
22	7
23	$p + 4\gcd(p-1,3) + \gcd(p-1,4) + 5$
24	$\gcd(p-1,3) + 3$
25	$(p+3)/2$
26	$(p+3)/2$
27	$\gcd(p-1,3) + \gcd(p-1,4) + 3$
28	p
29	p
30	$2\gcd(p-1,3) + 4$
31	7
32	5
33	6
34	3
35	$\gcd(p-1,4) + 2$
36	$\gcd(p-1,4) + \gcd(p-1,6) + 1$
37	$\gcd(p-1,4) + 4$
38	$\gcd(p-1,4) + \gcd(p-1,5) + p$
39	$p + \gcd(p-1,5) + \gcd(p-1,6)$
40	$\gcd(p-1,3) + 2$
41	$\gcd(p-1,3) + 1$
42	$p + 1$
43	p

Power relations for the $p + 3$ groups together with other relevant information is summarised in Table 3. The column 'Stabiliser order' records the order of the subgroup of GL(4, p) which stabilises the subgroup factored from $\widehat{P}$.

S0021-8693(03)00777-4/FLA AID:9967 Vol.●●●(●●●) yjabr9967 P.16(1-19)
ELSGMLTM(YJABR):m1 2004/01/13 Prn:5/02/2004; 11:39 by:V.Cer p. 16

Table 3
Presentations and other information for Φ_{15}

Group	Defining relations				Stabiliser order	Rank of G^p
	a_1^p	a_2^p	a_3^p	a_4^p		
1	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$2(p^4-1)(p^4-p^2)$	0
2	a_5	$\emptyset$	$\emptyset$	$\emptyset$	$2p^2(p-1)$	1
3	a_5	a_6	$\emptyset$	$\emptyset$	2	2
4	a_5	$\emptyset$	$\emptyset$	a_6^{ω}	$2(p^4-p^2)$	2
5	a_5	$\emptyset$	$\emptyset$	$a_6^{-\omega}$	$2(p^4-p^2)$	2
$6\ldots p+3$	$a_5a_6^{\alpha}$	$\emptyset$	$\emptyset$	a_6^{β}	$2p^2(p-1)$	2

In the last row α and β are solutions of the equations

$$\omega\alpha^2-\omega^2-\beta^2=k\beta \quad \text{for } k=0,\ldots,p-1,\ k\neq\pm 2\omega.$$

8. The database

The groups with order 64 and 729 are already available in electronic form in the SMALLGROUPS library described in Besche et al. [6]. They can be accessed through the computer algebra systems GAP [14] and MAGMA [7].

Recently a database for the groups with order dividing p^5 for $p\geqslant 5$ has been prepared by Eick and Girnat.

Both proofs of Theorem 1 provide parameterised presentations for the groups with order p^6, for $p\geqslant 7$. However, the presentations obtained by applying the Baker–Campbell–Hausdorff to the product presentations are sometimes more complicated. Further, in some families certain congruences have been solved explicitly by Easterfield [12].

Hence, the database is based on a corrected version of Easterfield's list, and the linear ordering employed is very close to his. It differs only in the addition of groups in Φ_{13}, in using the James presentations for the groups in Φ_{19}, and a small number of typographical amendments.

Each group with order p^6 is described by a power-commutator presentation on 6 generators and 21 relations: 15 are commutator relations and 6 are power relations. Each presentation has the prime p as a parameter. The additional (at most two) parameters run though a small number of subsets of $[0,\ldots,p-1]$; the number can be made independent of p. Examples include $[1,\omega]$ where ω is a (fixed) primitive root and transversals of cubes in the multiplicative group of $[1,\ldots,p-1]$ mod p. There are also some more subtle invariants corresponding to ovals in the affine plane over the field of p elements. Sometimes the parameter range depends on the residue of the prime modulo 4.

For example, the parameterized presentation

$$\big\{a_1,\ldots,a_6 \mid [a_2,a_1]=a_4,\ [a_3,a_1]=a_6^{\omega},\ [a_3,a_2]=a_5,\ [a_4,a_1]=a_5,$$
$$[a_4,a_2]=a_6,\ a_1^p=a_5^{\eta},\ a_3^p=a_5^{\xi}a_6\big\},$$

S0021-8693(03)00777-4/FLA AID:9967 Vol.●●●(●●●) yjabr9967 P.17 (1-19)
ELSGMLTM(YJABR):m1 2004/01/13 Prn:5/02/2004; 11:39 by:V.Cer p. 17

where ξ is arbitrary and $\eta \in \{1, \ldots, (p-1)/2\}$ describes $p(p-1)/2$ different groups with order p^6. A more complex example is the following:

$$\{a_1, \ldots, a_6 \mid [a_2, a_1] = a_3,\ [a_3, a_1] = a_4,\ [a_3, a_2] = a_5,\ [a_4, a_1] = a_6,$$
$$[a_5, a_2] = a_6^{-1/\omega},\ a_1^p = a_5^{\omega} a_6^{-\eta+1},\ a_2^p = a_4 a_6^{-\xi+1}\},$$

where $\xi^2 - \omega^{-1}\eta^2 = i$ for $i = 1, \ldots, p-1$. (All relations whose right-hand sides are trivial are not shown.)

The database contains about 500 parametrised presentations, most of these have p as the only parameter. The precise number is not significant as it depends on decisions about the fine structure of the underlying classification. The database also has functions for accessing subsets of the corresponding groups. In particular, we provide a function which given a prime $p \geqslant 5$ produces a complete and irredundant list of presentations for the groups with order p^6. Further, the groups in a particular isoclinism family or having a particular parent can be listed.

9. Accuracy of results

We now comment on some of the steps taken to ensure that the enumeration and the resulting database are accurate.

Observe that the primes can be partitioned according to the values of the residues which occur in the formula of Theorem 1. The $\gcd(p-1, 5)$ factor enters only from the count of maximal class groups with order p^6; these groups were independently classified by Blackburn [5]. Hence, for the remaining groups with order p^6, the primes can be classified according to the residue classes of $p-1$ modulo 3 and 4: representative primes are $5, 7, 11, 13$.

The p-group generation algorithm is implemented both as a stand-alone program and in GAP and MAGMA. This allowed us to determine presentations for all the groups with order p^6 explicitly for primes p up to 13. We used it in conjunction with the enumeration algorithm of Eick and O'Brien [13] to verify Theorem 1 for all primes up to 23.

We also computed invariants, such as the structure of lower central series, for each group. With a moderate set of invariants, the groups can be divided into a large number of bins; the groups in each bin are very similar in structure and we now decide isomorphism among the remaining groups. Influenced by our observation on representative primes, we used invariant calculations and the isomorphism algorithm of O'Brien [28] to demonstrate that the database list is complete and irredundant for $p \leqslant 13$.

A useful check is to compare different determinations. Easterfield compared many of his results against those of Potron; the one serious error occurs in an isoclinism family (Φ_{13}) which Potron missed. Pilyavskaya compared her work with that of James. We have compared our results with those of earlier workers and those from our different approaches. In particular, we established a correspondence for primes at most 13 between the corrected version of Easterfield's list and the list obtained from the application of the Baker–Campbell–Hausdorff technique to the product presentations for nilpotent Lie rings.

S0021-8693(03)00777-4/FLA AID:9967 Vol.●●●(●●●) yjabr9967 P.18 (1-19)
ELSGMLTM(YJABR):m1 2004/01/13 Prn:5/02/2004; 11:39 by:V.Cer p. 18

References

[1] Yu.A. Bahturin, Identical Relations in Lie Algebras, VNU Science Press, 1987.
[2] G. Bagnera, La composizione dei Gruppi finiti il cui grado è la quinta potenza di un numero primo, Ann. Mat. Pura Appl. (3) 1 (1898) 137–228.
[3] D. Baldwin, The groups of order 3^n, for $n \leqslant 6$, BSc thesis, Australian National University, 1987.
[4] H.A. Bender, A determination of the groups of order p^5, Ann. of Math. (2) 29 (1927) 61–72.
[5] N. Blackburn, On a special class of p-groups, Acta Math. 100 (1958) 45–92.
[6] H.U. Besche, B. Eick, E.A. O'Brien, A millennium project: constructing small groups, Internat. J. Algebra Comput. 12 (2002) 623–644.
[7] W. Bosma, J. Cannon, C. Playoust, The MAGMA algebra system I: The user language, J. Symbolic Comput. 24 (1997) 235–265.
[8] N. Bourbaki, Groupes et Algèbres de Lie. Chapitre II: Algèbres de Lie libres. Chapitre III: Groupes de Lie, in: Éléments de mathématique, Fasc. XXXVII, Hermann, Paris, 1972, Actualités Sci. Industr. No. 1349.
[9] H.R. Brahana, Metabelian p-groups with five generators and orders p^{12} and p^{11}, Illinois J. Math. 2 (1958) 641–717.
[10] W. Burnside, Theory of Groups of Finite Order, 2nd ed., Cambridge Univ. Press, 1911; reprinted by Dover, New York, 1955.
[11] J.-A. de Séguier, Théorie des groupes finis. Éléments de la théorie des groupes abstraits, Gauthier–Villars, Paris, 1904.
[12] T.E. Easterfield, A classification of groups of order p^6, PhD thesis, Cambridge University, 1940.
[13] B. Eick, E.A. O'Brien, Enumerating p-groups, J. Austral. Math. Soc. Ser. A 67 (1999) 191–205.
[14] The GAP Group, GAP—Groups, Algorithms, and Programming, Version 4.3, 2002, http://www.gap-system.org.
[15] P. Hall, The classification of prime-power groups, J. Reine Angew. Math. 182 (1940) 130–141.
[16] M. Hall Jr., J.K. Senior, The Groups of Order 2^n $(n \leqslant 6)$, Macmillan, New York, 1964.
[17] G. Havas, M.F. Newman, M.R. Vaughan-Lee, A nilpotent quotient algorithm for graded Lie rings, J. Symbolic Comput. 9 (1990) 653–664.
[18] N. Jacobson, Lie Algebras, Wiley–Interscience, New York, 1962.
[19] R.K. James, The groups of order p^6 $(p \geqslant 3)$, PhD thesis, University of Sydney, 1968.
[20] R. James, The groups of order p^6 (p an odd prime), Math. Comp. 34 (1980) 613–637.
[21] R. James, M.F. Newman, E.A. O'Brien, The groups of order 128, J. Algebra 129 (1) (1990) 136–158.
[22] A.M. Küpper, Enumeration of some two-generator groups of prime power order, Master's thesis, Australian National University, 1979.
[23] G.A. Miller, The regular substitution groups whose orders are less than 48, Quart. J. Math. 28 (1896) 232–284.
[24] G.A. Miller, Determination of all the groups of order 64, Amer. J. Math. 52 (1930) 617–634.
[25] M.F. Newman, Determination of groups of prime-power order, in: Group Theory, Canberra, 1975, in: Lecture Notes in Math., vol. 573, Springer-Verlag, Berlin, 1977, pp. 78–84.
[26] M.F. Newman, E.A. O'Brien, Application of computers to questions like those of Burnside, II, Internat. J. Algebra Comput. 6 (1996) 593–605.
[27] E.A. O'Brien, The p-group generation algorithm, J. Symbolic Comput. 9 (1990) 677–698.
[28] E.A. O'Brien, Isomorphism testing for p-groups, J. Symbolic Comput. 17 (1994) 133–147.
[29] O.S. Pilyavskaya, Application of matrix problems to the classification of groups of order p^6, $p > 3$, in: Linear Algebra and the Theory of Representations, Akad. Nauk Ukrain. SSR, Inst. Mat., Kiev, 1983, pp. 86–89.
[30] O.S. Pilyavskaya, Classification of groups with order p^6 $(p > 3)$, Vseross. Inst. Nauchn. i Tekhn. Inform. (VINITI), Moscow, 1983, Deposit No. 1877-83 (in Russian).
[31] O.S. Pilyavskaya, Application of the theory of matrix problems to some questions in the theory of finite p-groups, Candidate's dissertation in physical–mathematical sciences, Kiev, 1989 (in Russian).
[32] M. Potron, Sur quelques groupes d'ordre p^6, PhD thesis, Gauthier–Villars, Paris, 1904.
[33] O. Schreier, Über die Erweiterung von Gruppen. II, Abh. Math. Sem. Univ. Hamburg 4 (1926) 321–346.
[34] C.C. Sims, Computation with finitely presented groups, Cambridge Univ. Press, 1994.

S0021-8693(03)00777-4/FLA AID:9967 Vol.●●●(●●●) yjabr9967 P.19(1-19)
ELSGMLTM(YJABR):m1 2004/01/13 Prn:5/02/2004; 11:39 by:V.Cer p. 19

[35] L.W. Tordella, A classification of groups of order p^6, p an odd prime, PhD thesis, University of Illinois (Urbana), 1939.
[36] M.R. Vaughan-Lee, The Restricted Burnside Problem, 2nd ed., in: London Math. Soc. Monogr. (N.S.), vol. 5, Oxford Univ. Press, Oxford, 1993.