Journal of Algebra 361 (2012) 287–312

Contents lists available at SciVerse ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Non-PORC behaviour of a class of descendant p-groups

Marcus du Sautoy, Michael Vaughan-Lee *,1

Mathematical Institute, 24-29 St Giles, Oxford OX1 3LB, United Kingdom

ARTICLE INFO

Article history:
Received 29 November 2011
Available online 20 April 2012
Communicated by Eamonn O'Brien

MSC:
20D15
11G20

Keywords:
Group theory
Finite p-groups
Higman's PORC conjecture

ABSTRACT

We prove that the function $f(p)$ enumerating the number of immediate descendants of order p^{10} of G_p is not PORC (Polynomial On Residue Classes), where G_p is the p-group of order p^9 defined by du Sautoy's nilpotent group encoding the elliptic curve $y^2 = x^3 - x$. This has important implications for Higman's PORC conjecture.

1. Introduction

In [5] the first author introduced the following nilpotent group G given by the presentation:

$$G = \left\langle \begin{matrix} x_1, x_2, x_3, x_4, x_5, x_6, y_1, y_2, y_3 : [x_1, x_4] = y_3, [x_1, x_5] = y_1, [x_1, x_6] = y_2 \\ [x_2, x_4] = y_1, [x_2, x_5] = y_3, [x_3, x_4] = y_2, [x_3, x_6] = y_1 \end{matrix} \right\rangle$$

where all other commutators are defined to be 1.

The group G is a Hirsch length 9, class two nilpotent group. This group turned out to have some fascinating properties especially in its local behaviour with respect to varying the prime p. In particular it was key to revealing that zeta functions that can be associated with nilpotent groups have a behaviour that mimics the arithmetic geometry of elliptic curves.

* Corresponding author.
E-mail addresses: dusautoy@maths.ox.ac.uk (M. du Sautoy), michael.vaughan-lee@chch.ox.ac.uk (M. Vaughan-Lee).

[1] The second author was partially supported by CIRM-FBK, Trento.

0021-8693/$ – see front matter
http://dx.doi.org/10.1016/j.jalgebra.2012.03.038

Given that this group has the arithmetic of the elliptic curve

$$E = Y^2 - X^3 + X$$

embedded into its structure it is interesting to explore other group theoretic features which reflect this arithmetic. The presentation can be refined to define a group G_p which is a finite p-group of exponent p and order p^9. It turns out that the automorphism group of G_p depends very irregularly on p, again reflecting the arithmetic of the underlying elliptic curve. This impacts very interestingly on the number of immediate descendants of G_p. (These are the class 3 groups K such that $K/\gamma_3(K)$ is isomorphic to G_p.) Immediate descendants of G_p are either of order p^{10} or p^{11}. For $p > 3$ the number of descendants of exponent p with order p^{10} is described by the following:

Theorem 1. *Let D_p be the number of descendants of G_p of order p^{10} and exponent p. Let V_p be the number of solutions (x, y) in $\mathbb{F}_p$ that satisfy $x^4 + 6x^2 - 3 = 0$ and $y^2 = x^3 - x$.*

1. *If* $p = 5 \bmod 12$ *then* $D_p = (p+1)^2/4 + 3$.
2. *If* $p = 7 \bmod 12$ *then* $D_p = (p+1)^2/2 + 2$.
3. *If* $p = 11 \bmod 12$ *then* $D_p = (p+1)^2/6 + (p+1)/3 + 2$.
4. *If* $p = 1 \bmod 12$ *and* $V_p = 0$ *then* $D_p = (p+1)^2/4 + 3$.
5. *If* $p = 1 \bmod 12$ *and* $V_p \neq 0$ *then* $D_p = (p-1)^2/36 + (p-1)/3 + 4$.

Theorem 2. *There are infinitely many primes* $p = 1 \bmod 12$ *for which* $V_p > 0$. *However there is no sub-congruence of* $p = 1 \bmod 12$ *for which* $V_p > 0$ *for all p in that sub-congruence class.*

This theorem has an impact on Higman's PORC conjecture, which relates to the form of the function $f(p,n)$ giving the number of non-isomorphic p-groups of order p^n. (We will give a full statement of the conjecture and some of its history in Section 2.)

Corollary 1. *The function D_p enumerating the number of immediate descendants of G_p of order p^{10} and exponent p is not PORC.*

Corollary 2. *The function enumerating the number of immediate descendants of G_p of order p^{10} is not PORC.*

Proof. Let E_p be the number of descendants of G_p of order p^{10} which do not have exponent p. Then the total number of descendants of order p^{10} is $D_p + E_p$. When $p = 1 \bmod 12$ and $V_p \neq 0$ then D_p has a lower value than when $p = 1 \bmod 12$ and $V_p = 0$. Similarly, the value of E_p is either the same when $V_p \neq 0$ as it is when $V_p = 0$, or (more likely) it is also lower. So, either way, the total number of descendants of G_p of order p^{10} is lower when $p = 1 \bmod 12$ and $V_p \neq 0$ than it is when $p = 1 \bmod 12$ and $V_p = 0$. □

The authors are very grateful to Jan Denef, Noam Elkies, Roger Heath-Brown and Hans Opolka for a number of helpful conversations about number theory.

2. Impact on Higman's PORC conjecture

Higman's PORC conjecture [10] asserts that for fixed n, the number $f(p,n)$ of finite p-groups of order p^n is given by a polynomial in p whose coefficients depend on the residue class of p modulo some fixed integer N, (**P**olynomial **O**n **R**esidue **C**lasses). Another way of putting this is to say that for fixed n there is a finite set of polynomials in p, $g_1(p), g_2(p), \ldots, g_k(p)$, and a fixed integer N, such that for each prime p $f(p,n) = g_i(p)$ for some i $(1 \leqslant i \leqslant k)$, with the choice of i depending on the residue class of p mod N.

Higman [10] proves that for each n the function enumerating the number of groups of order p^n which have Frattini subgroups which are central and elementary abelian is PORC. A. Evseev [8] has extended Higman's result to groups where the Frattini subgroup is central (and not necessarily elementary abelian). For $n \leqslant 7$ Higman's conjecture is known to hold true (see [13] and [15]). For $n \geqslant 8$ the conjecture is open.

The classifications of the groups of order p^6 and p^7 in [13] and [15] make use of the p-group generation algorithm [14]. If G is any group then the lower exponent-p-central series of G,

$$G = G_1 \geqslant G_2 \geqslant \cdots \geqslant G_i \geqslant \cdots,$$

is defined by setting $G_1 = G$, $G_2 = G'G^p$, and in general setting $G_{i+1} = [G_i, G]G_i^p$. If G is a finite p-group then $G_{c+1} = \{1\}$ for some c, and we say that G has p-class c if $G_c \neq \{1\}$, $G_{c+1} = \{1\}$. If G is a finite p-group of p-class $c > 1$ then we say that G is an *immediate descendant* of G/G_c. Apart from the elementary abelian group of order p^n, every group of order p^n is an immediate descendant of a group of order p^k for some $k < n$. To list the groups of order p^n, first list the groups of order p^k for all $k < n$. Then for each group G of order p^k for $k < n$, find all the immediate descendants of G which have order p^n.

So (for example) the formula

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

given in [13] for the number of p-groups of order p^6 ($p \geqslant 5$) can be obtained as follows. It turns out that for $p \geqslant 5$ there are 42 groups of order at most p^5 which have immediate descendants of order p^6. Each of these 42 groups is given by a presentation involving the prime p symbolically – for example one of the 42 groups has presentation

$$\langle a, b \mid a^p = [b, a, a],\ b^p = 1,\ \text{class } 3\rangle.$$

For each of these 42 groups we compute the number of immediate descendants of order p^6, and the formula given above is obtained by adding together each of these individual contributions. For example, the group above has $p + \gcd(p-1,3) + 1$ descendants of order p^6. Finally, we have to add one to this total to account for the elementary abelian group of order p^6. Each of the individual contributions is PORC, and as a consequence the formula above is PORC.

Higman does not use the term *immediate descendant*, and does not explicitly mention the lower exponent-p-central series. But nevertheless his theorem can be expressed in these terms. Higman's theorem is that the function enumerating the number of groups of p-class 2 and order p^n is PORC. (Higman uses the term Φ-class 2.) Every group of order p^n and p-class 2 is an immediate descendant of the elementary abelian group of order p^r for some $r < n$. If G has order p^{r+s}, and if G is an immediate descendant of the elementary abelian group of order p^r then in Higman's terminology we say that G has Φ-complexion (r, s). Higman defines $g(r, s; p)$ to be the number of groups with Φ-complexion (r, s). So the number of p-class 2 groups of order p^n is

$$\sum_{r+s=n} g(r, s; p).$$

Higman shows that $g(r, s; p)$ is PORC for all r and s, and it follows that the total number of p-class 2 groups of order p^n is PORC.

If we were to follow the same scheme for computing the number of groups of order p^{10} then we would compute the number of immediate descendants of order p^{10} of each group of order less than p^{10}. By adding up all these individual contributions, and finally adding one to account for the elementary abelian group of order p^{10}, we would obtain $f(p, 10)$. The group G_p shows that at least one of the individual summands is not PORC. It seems likely that there are other groups of order p^9 with a non-PORC number of immediate descendants of order p^{10}, and so it is possible that the grand total is PORC, even though not all of the summands are PORC. The authors' own view is that this is extremely unlikely. But we see no way to settle this question without a complete classification of the groups of order p^{10}, and there is no immediate prospect of achieving this. Certainly our example shows that it is not possible to extend Higman's methods directly to show that the function enumerating the number of p-class 3 groups of order p^n is PORC. His proof that the function enumerating the number of p-class 2 groups of order p^n is PORC relies on the fact that the grand total is made up of a sum of functions each of which is PORC.

An excellent history of work on enumerating finite p-groups, and a discussion of Higman's PORC conjecture can be found in [1].

3. Further background

In [9] Grunewald, Segal and Smith introduced the notion of the zeta function of a group G:

$$\zeta_G^{\leqslant}(s) = \sum_{H \leqslant G} |G : H|^{-s} = \sum_{n=1}^{\infty} a_n^{\leqslant}(G) n^{-s}$$

where $a_n^{\leqslant}(G)$ denotes the number of subgroups of index n in G. The definition of this zeta function as a sum over subgroups makes it look like a non-commutative version of the Dedekind zeta function of a number field. They proved that for finitely generated, torsion-free nilpotent groups the global zeta function can be written as an Euler product of local factors which are rational functions in p^{-s}:

$$\begin{aligned}\zeta_G^{\leqslant}(s) &= \prod_{p \text{ prime}} \zeta_{G,p}^{\leqslant}(s) \\ &= \prod_{p \text{ prime}} Z_p^{\leqslant}\left(p, p^{-s}\right)\end{aligned}$$

where for each prime p, $\zeta_{G,p}^{\leqslant}(s) = \sum_{n=0}^{\infty} a_{p^n}^{\leqslant}(G) p^{-ns}$ and $Z_p^{\leqslant}(X, Y) \in \mathbb{Q}(X, Y)$.

Similar definitions and results were also obtained for the zeta function $\zeta_G^{\triangleleft}(s)$ counting normal subgroups.

One of the major questions raised in the paper [9] is the variation with p of these local factors $Z_p^{\leqslant}(X, Y)$. Many of the examples showed a uniform behaviour as the prime varied. For example, if G is the discrete Heisenberg group

$$G = \begin{pmatrix} 1 & \mathbb{Z} & \mathbb{Z} \\ 0 & 1 & \mathbb{Z} \\ 0 & 0 & 1 \end{pmatrix}$$

then for all primes p

$$\zeta_{G,p}^{\leqslant} = \frac{(1 - p^{3-3s})}{(1 - p^{-s})(1 - p^{1-s})(1 - p^{2-2s})(1 - p^{3-2s})}.$$

However, if one takes the Heisenberg group with entries now from some quadratic number field then it was shown in [9] that the local factors $Z_p^{\triangleleft}(X, Y)$ counting normal subgroups depend on how the prime p behaves in the quadratic number field. The authors of [9] were led by such examples and the analogy with the Dedekind zeta function of a number field to ask whether the local factors always demonstrated a Chebotarev density type behaviour, depending on the behaviour of primes in number fields. In particular they speculated in [9] that it was 'plausible' that the following question has a positive answer:

Question. Let G be a finitely generated nilpotent group and $* \in \{\leqslant, \lhd\}$. Do there exist finitely many rational functions $W_1(X,Y), \ldots, W_r(X,Y) \in \mathbb{Q}(X,Y)$ such that for each prime p there is an i for which

$$\zeta^*_{G,p}(s) = W_i\big(p, p^{-s}\big)?$$

If the answer is 'yes' we say that the local zeta functions $\zeta^*_{G,p}(s)$ of G are *finitely uniform*. If there is one rational function $W(X,Y)$ such that $\zeta^*_{G,p}(s) = W(p, p^{-s})$ for almost all primes then we say that the local zeta functions $\zeta^*_{G,p}(s)$ of G are *uniform*.

Grunewald, Segal and Smith elevated this question to a conjecture in the case that G is a free nilpotent group. In [9] they confirmed the conjecture in the case that G is a free nilpotent group of class 2.

The question of the behaviour of these local factors has gained extra significance in the light of recent work of the first author on counting the number $f(p,n)$ of non-isomorphic finite p-groups that exist of order p^n. In [3] and [4] it is explained how Higman's PORC conjecture is directly related to whether certain local zeta functions attached to free nilpotent groups are finitely uniform.

The examples of Grunewald, Segal and Smith hinted that the behaviour of the local factors as one varied the prime would be related to the behaviour of primes in number fields. However the work of the first author with Grunewald [6] and [7] shows that this first impression is misplaced. The behaviour is rather governed by a different question, namely how the number of points $\bmod p$ on a variety varies with p.

In [6] and [7], the first author and Grunewald show that for each finitely generated nilpotent group G there exists an explicit system of subvarieties E_i ($i \in T$, T finite) of a variety Y defined over $\mathbb{Z}$ and, for each subset I of T, a rational function $W_I(X,Y) \in \mathbb{Q}(X,Y)$ such that for almost all primes p

$$\zeta^*_{G,p}(s) = \sum_{I \subset T} c_I(p) W_I\big(p, p^{-s}\big)$$

where

$$c_I(p) = \operatorname{card}\big\{a \in Y(\mathbb{F}_p)\colon\ a \in E_i(\mathbb{F}_p) \text{ if and only if } i \in I\big\}.$$

So the analogy with the Dedekind zeta function of a number field is too simplistic, rather it is the Weil zeta function of an algebraic variety over $\mathbb{Z}$ that offers a better analogy.

In contrast to the behaviour of primes in number fields, the number of points $\bmod p$ on a variety can vary wildly with the prime p and certainly does not have a finitely uniform description.

Example 1. (See [11, 18.4].) Let E be the elliptic curve $E = Y^2 - X^3 + X$. Put

$$\big|E(\mathbb{F}_p)\big| = \big|\big\{(x,y) \in \mathbb{F}_p^2\colon\ y^2 - x^3 + x = 0\big\}\big|.$$

If $p = 3 \bmod 4$ then $|E(\mathbb{F}_p)| = p$. However if $p = 1 \bmod 4$ then

$$\big|E(\mathbb{F}_p)\big| = p - 2e,$$

where $p = e^2 + f^2$ and $e + if = 1 \bmod (2 + 2i)$.

(Note that $|E(\mathbb{F}_p)|$ is one less than the value N_p given in [11, 18.4] since N_p counts the number of points on the projective version of E. This includes one extra point at infinity not counted in the affine coordinates.)

However, despite this theoretical advance which moves the problem into the behaviour of varieties mod p, it was not clear still whether exotic varieties like elliptic curves could arise in the setting of zeta functions of groups. It might be that the question of Grunewald, Segal and Smith would still have a positive answer since the varieties that arise out of the analysis of the first author and Grunewald were always rational where the number of points $\bmod p$ is uniform in p.

The group defined at the beginning of this paper turned out to be the first example of a nilpotent group G whose zeta function depends on the behaviour $\bmod p$ of the number of points on the elliptic curve $E = Y^2 - X^3 + X$. To see where the elliptic curve is hiding in this presentation, take the determinant of the 3×3 matrix (a_{ij}) with entries $a_{ij} = [x_i, x_{j+3}]$. In [5] the group is shown to provide a negative answer to the question of Grunewald, Segal and Smith:

Theorem 3. *The local zeta functions $\zeta^{\leqslant}_{G,p}(s)$ and $\zeta^{\triangleleft}_{G,p}(s)$ are not finitely uniform.*

4. Number theory

In this section we prove Theorem 2. For the whole of this section we assume p is a prime with $p = 1 \bmod 12$.

Lemma 1. *There exists x, y in $\mathbb{F}_p$ such that $x^4 + 6x^2 - 3 = 0$ and $y^2 = x^3 - x$ if and only if there exists $y \in \mathbb{F}_p$ satisfying $y^8 + 360y^4 - 48 = 0$.*

Proof. Let $x, y \in \mathbb{F}_p$ satisfy $x^4 + 6x^2 - 3 = 0$ and $y^2 = x^3 - x$. Substitute $x^3 - x$ for y^2 in $y^8 + 360y^4 - 48$ and use the identity $x^4 + 6x^2 - 3 = 0$ to see that $y^8 + 360y^4 - 48 = 0$. Conversely, let y be a root of $y^8 + 360y^4 - 48$ in $\mathbb{F}_p$ and let $x = -\frac{1}{208}(y^6 + 388y^2)$. Substituting this value for x in $x^4 + 6x^2 - 3$ we see that $x^4 + 6x^2 - 3 = 0$, and substituting this value for x in $y^2 - x^3 + x$ we see that $y^2 = x^3 - x$.

Note that although the prime 13 divides 208, this does not affect the proof of Lemma 1, since neither $x^4 + 6x^2 - 3$ nor $y^8 + 360y^4 - 48$ have roots in $\mathbb{F}_{13}$. $\square$

So we are interested in for which p does $y^8 + 360y^4 - 48 = 0$ have a solution in $\mathbb{F}_p$. The splitting field of $y^8 + 360y^4 - 48$ over $\mathbb{Q}$ has degree 16, so adjoining one root of $y^8 + 360y^4 - 48$ to $\mathbb{Q}$ gives a field which is not even Galois let alone abelian. But if we adjoin a root of $y^8 + 360y^4 - 48$ to $\mathbb{Q}(i, \sqrt{3})$ then we obtain the full splitting field. This splitting field has degree 4 over $\mathbb{Q}(i, \sqrt{3})$, with Galois group isomorphic to C_4. This will be helpful in our analysis.

Since $p = 1 \bmod 12$, 3 is a quadratic residue of p. Also p can be written as $p = a^2 - 12b^2$ with $a, b > 0$. We can now establish the following:

Theorem 4. *$z^4 + 360z^2 - 48 = 0$ has a solution in $\mathbb{F}_p$ if and only if $a = 1 \bmod 3$.*

Proof. We use quadratic reciprocity in the number field $\mathbb{Q}(\sqrt{3})$. We have $p = \pi \cdot \pi'$ in $\mathbb{Q}(\sqrt{3})$ with $\pi = a + 2b\sqrt{3}$ (where π' denotes the conjugate of π).

$$z^4 + 360z^2 - 48 = \left(z^2 - r\right)\left(z^2 - s\right)$$

where $r = 4\sqrt{3}(2 - \sqrt{3})^3$ and $s = r'$. So the question is whether r or s can be a square mod π. Since $p = 1 \bmod 12$, -48 is a square mod p, and hence rs is a square mod p. So r is a square mod π if and only if s is a square mod π.

The condition for r to be a square mod π is given by the Law of Quadratic Reciprocity for quadratic fields (see [12]). If α and β are coprime elements of $\mathbb{Z}[\sqrt{3}]$ with odd norm, and if β is irreducible, then the quadratic Legendre symbol $[\frac{\alpha}{\beta}]$ is defined to be $+1$ or -1 depending on whether or not α is a square mod β. Eisenstein's quadratic reciprocity law states that if α, β, γ, δ are irreducible elements with odd norm and if they satisfy $(\alpha, \beta) = (\gamma, \delta) = (1)$ and $\alpha \equiv \gamma$, $\beta \equiv \delta \bmod 4\infty$, then

$$\left[\frac{\alpha}{\beta}\right]\left[\frac{\beta}{\alpha}\right] = \left[\frac{\gamma}{\delta}\right]\left[\frac{\delta}{\gamma}\right].$$

The notation $\alpha \equiv \gamma \bmod 4\infty$ means that $\alpha = \gamma \bmod 4$ and that α and γ have the same signature, i.e. $(\operatorname{sign}\alpha, \operatorname{sign}\alpha') = (\operatorname{sign}\gamma, \operatorname{sign}\gamma')$. We want to know when $4\sqrt{3}(2-\sqrt{3})^3$, or equivalently $\sqrt{3}(2-\sqrt{3})$, is a square mod π. So we take $\alpha = \pi$ and $\beta = \sqrt{3}(2-\sqrt{3})$. Note that α and β are irreducible elements of $\mathbb{Z}[\sqrt{3}]$ with norms p and -3. It follows that $\mathbb{Z}[\sqrt{3}]/(\beta) \cong \mathbb{F}_3$ and that $[\frac{\alpha}{\beta}] = 1$ if and only if $a = 1 \bmod 3$. We establish Theorem 4 by showing that $[\frac{\alpha}{\beta}] = [\frac{\beta}{\alpha}]$.

If b is even, then $\alpha = \xi^2 \bmod 4$, where $\xi = 1$ or $\sqrt{3}$. So (by definition) α is primary with signature $(+1,+1)$ and $[\frac{\alpha}{\beta}] = [\frac{\beta}{\alpha}]$ by Corollary 12.9 of [12].

So suppose that b is odd. Then, depending on whether $a = 1$ or $3 \bmod 4$, we have $\alpha = 5+2\sqrt{3} \bmod 4$ or $\alpha = 11+2\sqrt{3} \bmod 4$. Accordingly, we take $\gamma = 5+2\sqrt{3}$ or $\gamma = 11+2\sqrt{3}$ and take $\delta = \beta$. Note that $5+2\sqrt{3}$ and $11+2\sqrt{3}$ are irreducible elements with norms 13 and 109, and that both have signature $(+1,+1)$. It is straightforward to check that in both cases $[\frac{\gamma}{\delta}] = [\frac{\delta}{\gamma}] = -1$, and so Eisenstein's quadratic reciprocity law implies that $[\frac{\alpha}{\beta}] = [\frac{\beta}{\alpha}]$. □

We can now use the previous theorem to prove the following:

Theorem 5. *There is no congruence class $p = c \bmod 12d$ with $c = 1 \bmod 12$ and $(c,d) = 1$ for which $y^8 + 360y^4 - 48$ always has a root.*

Proof. This follows provided we can show that there are primes $p = a^2 - 12b^2 = c \bmod 12d$ with $a > 0$ and $a = 2 \bmod 3$. By Dirichlet's Theorem, the arithmetic progression $c + 12nd$ $(n = 1,2,\ldots)$ contains infinitely many primes. Let p be one of these primes, and write $p = a^2 - 12b^2$ with $a > 0$. If $a = 2 \bmod 3$ we are done. If not, consider the "arithmetic progression" $-a + 2b\sqrt{3} + 12d(m + n\sqrt{3})$ with $m, n \in \mathbb{Z}$. From the $\mathbb{Q}(\sqrt{3})$ version of Dirichlet's theorem (see Rademacher [16]), there is an irreducible element

$$\pi = -a + 2b\sqrt{3} + 12d(m + n\sqrt{3})$$

for some $m, n \in \mathbb{Z}$, with $\pi > 0$ and $\pi' > 0$. Then

$$\pi\pi' = \bigl(-a + 12dm + (2b + 12dn)\sqrt{3}\bigr)\bigl(-a + 12dm - (2b + 12dn)\sqrt{3}\bigr)$$

is a rational prime

$$p = (-a + 12dm)^2 - 12(b + 6dn)^2 = c \bmod 12d,$$

with $-a + 12dm > 0$ and $(-a + 12dm) = 2 \bmod 3$. □

The final piece of the jigsaw is the following:

Theorem 6. *There are infinitely primes $p = 1 \bmod 12$ for which the equation $y^8 + 360y^4 - 48 = 0$ has a solution in $\mathbb{F}_p$.*

Proof. The splitting field of this polynomial has degree 16 over $\mathbb{Q}$, and so by Chebotarev's density theorem the set of primes p for which the polynomial splits over $\mathbb{F}_p$ has Dirichlet density $\frac{1}{16}$. In particular, there are infinitely many such primes and they must all be equal to 1 mod 12. □

5. Counting the descendants of G_p

We use the Lazard correspondence [2] to count the immediate descendants of G_p of exponent p. This method was used in the enumeration of groups of order p^6 [13] and p^7 [15], and is explained in [13]. The Lazard correspondence provides an isomorphism between the category of nilpotent Lie rings of order p^n and nilpotency class at most $p-1$ and the category of p-groups of order p^n and class at most $p-1$. In particular, it gives an isomorphism between the category of nilpotent Lie algebras of dimension n over the field $\mathbb{F}_p$ and class at most $p-1$ and the category of groups of exponent p of order p^n and class at most $p-1$. The Lie algebra L_p over $\mathbb{F}_p$ corresponding to the group G_p has a presentation on generators $x_1, x_2, \ldots, x_6, y_1, y_2, y_3$ with relations

$$[x_1, x_4] = y_3, \quad [x_1, x_5] = y_1, \quad [x_1, x_6] = y_2,$$

$$[x_2, x_4] = y_1, \quad [x_2, x_5] = y_3, \quad [x_3, x_4] = y_2, \quad [x_3, x_6] = y_1,$$

and with all other Lie commutators trivial. Note that in this particular case the presentation for the Lie algebra corresponding to G_p is identical to the presentation for G_p, though of course the commutators have to be read as Lie commutators rather than as group commutators. This Lie algebra is nilpotent of class 2 and of dimension 9, with $[L_p, L_p]$ having dimension 3 and vector space basis $[x_1, x_4]$, $[x_1, x_5]$, $[x_1, x_6]$. (Note that these basis elements for $[L_p, L_p]$ are equal to the defining generators y_3, y_1, y_2, but to avoid notational conflict we will not use these three defining generators in the following discussion.) For $p > 3$ the immediate descendants of L_p correspond under the Lazard correspondence to the immediate descendants of G_p of exponent p.

It turns out that L_p has immediate descendants of dimension 10 and 11, and Theorem 1 is obtained by counting the immediate descendants of L_p of dimension 10. A Lie algebra A over $\mathbb{F}_p$ is (by definition) an immediate descendant of L_p if A is nilpotent of class 3 and if $A/[A, A, A] \cong L_p$. We compute the immediate descendants as follows. First we find the covering algebra for L_p. This is the largest Lie algebra M which is nilpotent of class 3 and contains an ideal I satisfying the following properties:

1. $M/I \cong L_p$,
2. $I \leqslant [M, M]$,
3. I is contained in the centre of M.

The immediate descendants of L_p are the Lie algebras M/J, where J is an ideal of M with $J < I$ and $J + [M, M, M] = I$. The trickiest part of classifying the immediate descendants of L_p is determining when two immediate descendants M/J and M/K are isomorphic, and to solve this problem we need to know the automorphism group of L_p.

6. The automorphism group of L_p

Let V be the vector subspace of L_p spanned by $x_1, x_2, x_3, x_4, x_5, x_6$. It is sufficient to compute the subgroup G of the automorphism group of L_p which maps V onto V. We claim that if $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in \mathrm{GL}(2, p)$ then there is an automorphism in G defined as follows:

$$x_1 \to \alpha x_1 + \beta x_4,$$

$$x_2 \to \alpha x_2 + \beta x_5,$$

$$x_3 \to \alpha x_3 + \beta x_6,$$

$$x_4 \to \gamma x_1 + \delta x_4,$$

$$x_5 \to \gamma x_2 + \delta x_5,$$

$$x_6 \to \gamma x_3 + \delta x_6.$$

Let y_i be the image of x_i under this map, for $i = 1, 2, 3, 4, 5, 6$. We show that $y_1, y_2, \ldots, y_6$ satisfy the defining relations of L_p. An important and useful property of L_p is the following: if $1 \leqslant i, j \leqslant 3$ then

$$[x_{3+i}, x_j] = [x_{3+j}, x_i].$$

We will regularly make use of this property without comment.

First consider $[y_2, y_1]$.

$$[y_2, y_1] = [\alpha x_2 + \beta x_5, \alpha x_1 + \beta x_4] = \alpha\beta[x_2, x_4] + \alpha\beta[x_5, x_1] = 0.$$

The proofs that $[y_3, y_1] = [y_3, y_2] = 0$ and that $[y_i, y_j] = 0$ for $i, j \in \{4, 5, 6\}$, are similar.

Now let $1 \leqslant i, j \leqslant 3$. Then

$$[y_{3+i}, y_j] = [\gamma x_i + \delta x_{3+i}, \alpha x_j + \beta x_{3+j}] = (\alpha\delta - \beta\gamma)[x_{3+i}, x_j].$$

It follows immediately from this that

$$[y_4, y_1] = [y_5, y_2],$$
$$[y_4, y_3] = [y_6, y_1],$$
$$[y_5, y_1] = [y_4, y_2] = [y_6, y_3],$$
$$[y_5, y_3] = [y_6, y_2] = 0.$$

So this map does define an automorphism of L_p.

The subspace of V spanned by x_1, x_2, x_3 generates an abelian subalgebra of L_p of dimension 3, and it is fairly easy to check that every 3-dimensional subspace of V which generates an abelian subalgebra of L_p is the image of $\mathrm{Sp}\langle x_1, x_2, x_3\rangle$ under one of the automorphisms described above. (See Section 7 below.) So, modulo these automorphisms, it is sufficient to consider the subgroup $H \leqslant G$ consisting of automorphisms which map $\mathrm{Sp}\langle x_1, x_2, x_3\rangle$ to itself, and also map $\mathrm{Sp}\langle x_4, x_5, x_6\rangle$ to itself. So from now on we will look for automorphisms in H.

The action of $\mathrm{GL}(2, p)$ described above gives automorphisms in H of the form

$$x_1 \to \alpha x_1,$$
$$x_2 \to \alpha x_2,$$
$$x_3 \to \alpha x_3,$$
$$x_4 \to \delta x_4,$$
$$x_5 \to \delta x_5,$$
$$x_6 \to \delta x_6.$$

In addition there are automorphisms in H defined by

$$x_1 \to -x_1,$$
$$x_2 \to -x_2,$$
$$x_3 \to x_3,$$
$$x_4 \to -x_4,$$

$$x_5 \to -x_5,$$
$$x_6 \to x_6,$$

and

$$x_1 \to ux_1,$$
$$x_2 \to -ux_2,$$
$$x_3 \to x_3,$$
$$x_4 \to ux_4,$$
$$x_5 \to -ux_5,$$
$$x_6 \to x_6,$$

where $u^2 = -1$. (Of course the last of these can only occur when $p = 1 \bmod 4$.)

In addition, for some primes p there are automorphisms of the form

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \longmapsto \begin{bmatrix} a & ab & ac \\ df & -f & -def \\ 1 & d & e \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$$

and

$$\begin{bmatrix} x_4 \\ x_5 \\ x_6 \end{bmatrix} \longmapsto \begin{bmatrix} a & ab & ac \\ df & -f & -def \\ 1 & d & e \end{bmatrix} \begin{bmatrix} x_4 \\ x_5 \\ x_6 \end{bmatrix}.$$

These automorphisms occur when we can solve the two equations

$$d^4 + 6d^2 - 3 = 0,$$
$$1 - d^2 + de^2 = 0$$

over $\mathbb{F}_p$. Then we let a be a solution of $a^2 = \pm\frac{(d^2-1)^2}{4d}$, and we set $b = \frac{3d+d^3}{1-d^2}$, $c = \frac{e(d^2+3)}{d^2-1}$, $f = \frac{d^2-1}{2da}$.

The equation $x^2 + 6x - 3$ has roots $-3 \pm \sqrt{12}$, and so there is no solution to the equations unless 3 is a quadratic residue modulo p. Using quadratic reciprocity we see that 3 is a quadratic residue modulo p if $p = \pm 1 \bmod 12$.

The case $p = -1 \bmod 12$ is straightforward. We need to find solutions to

$$d^2 = -3 \pm \sqrt{12}.$$

Since

$$(-3 + \sqrt{12})(-3 - \sqrt{12}) = -3,$$

which is *not* a quadratic residue modulo p, we see that one of these two equations has a solution and the other does not. So we have two solutions $\pm d$ to the quartic equation. We now need to solve the equation

$$e^2 = \frac{d^2 - 1}{\pm d},$$

and again, one of these equations has two solutions and the other has none. So the two equations have exactly two solutions $d, \pm e$. For each of these two solutions we obtain two possibilities for a, and then the given values for d, e, a determine b, c, f. So there are four automorphisms of this form.

The case $p = 1 \bmod 12$ is much more complicated. In this case

$$(-3+\sqrt{12})(-3-\sqrt{12})$$

is a quadratic residue modulo p, and so either both the equations $d^2 = -3 \pm \sqrt{12}$ have solutions, or neither equation has a solution. So there are either 0 or 4 solutions to $d^4 + 6d^2 - 3 = 0$. Suppose that we have four solutions $\pm d_1$, $\pm d_2$. Then we need to solve the equations

$$e^2 = \frac{d_1^2 - 1}{\pm d_1}, \qquad e^2 = \frac{d_2^2 - 1}{\pm d_2}.$$

Since -1 is a quadratic residue modulo p it is clear that $e^2 = \frac{d_1^2-1}{\pm d_1}$ either has 4 solutions or none, and similarly $e^2 = \frac{d_2^2-1}{\pm d_2}$ either has 4 solutions or none. Now

$$\frac{d_1^2 - 1}{d_1} \cdot \frac{d_2^2 - 1}{d_2} = \frac{(-4+\sqrt{12})(-4-\sqrt{12})}{\sqrt{-3}} = \frac{4}{\sqrt{-3}},$$

and it turns out that $\sqrt{-3}$ is a square. This is because if $u^2 = -1$ then

$$\left(\frac{1}{4}(1+u)\bigl(d^3 + 5d\bigr)\right)^4 = -3.$$

So the equation $d^4 + 6d^2 - 3 = 0$ either has no solutions or four solutions, and in the case when there are solutions then we either obtain no solutions to the equations $1 - d^2 + de^2 = 0$, or we obtain a total of 8 solutions. The experimental evidence from looking at primes less than a million indicates that the equation $d^4 + 6d^2 - 3 = 0$ has solutions for approximately half the primes $p = 1 \bmod 12$, and that approximately half of the primes $p = 1 \bmod 12$ which have solutions to $d^4 + 6d^2 - 3 = 0$ also have solutions to the equations $1 - d^2 + de^2 = 0$. (Of course, from the proof of Theorem 2 we see that this is as predicted by Chebotarev's density theorem.) Note that d, e is a solution to these two equations in $\mathbb{F}_p$ if and only if $(x, y) = (d, de)$ is a solution to the two equations $x^4 + 6x^2 - 3 = 0$ and $y^2 = x^3 - x$. So, from Theorem 2 we see that there are infinitely many primes $p = 1 \bmod 12$ for which the two equations have solutions, but that there is no sub-congruence of $p = 1 \bmod 12$ such that there are solutions to the two equations for all p in that sub-congruence class.

For each solution d, e there are 4 solutions for a with $a^2 = \pm\frac{(d^2-1)^2}{4d}$. To see this note that to find 4 solutions for a it is sufficient that $-d$ be a square. Since $-d = \frac{1-d^2}{e^2}$ we need $1 - d^2$ to be a square, and this is indeed the case since

$$4\bigl(1-d^2\bigr) = 4\bigl(1-d^2\bigr) + \bigl(d^4 + 6d^2 - 3\bigr) = d^4 + 2d^2 + 1 = \bigl(d^2+1\bigr)^2.$$

So the four solutions for a are $u\frac{(d^2+1)e}{4}$ where $u^4 = 1$. The values of b, c, f are determined by d, e, a. So there are 0 or 32 automorphisms of this form.

We give proofs that these are the only automorphisms in H in Section 8.

7. Abelian subalgebras of dimension 3

As above we let V be the vector subspace of L_p spanned by $x_1, x_2, x_3, x_4, x_5, x_6$. In this section we justify our claim made above that any 3-dimensional subspace of V which generates an abelian subalgebra of L_p has the form $\mathrm{Sp}\langle \alpha x_1 + \beta x_4, \alpha x_2 + \beta x_5, \alpha x_3 + \beta x_6\rangle$ for some α, β. So let W be such a subspace of V. Let $U = \mathrm{Sp}\langle x_1, x_2, x_3\rangle$.

First assume that $U \cap W \neq \{0\}$, and let $u \in U \cap W \setminus \{0\}$. Then W must be a subspace of the centralizer of u in V, $C_V(u)$. We consider the possibilities for $C_V(u)$. First note that

$$C_V(x_2) = \mathrm{Sp}\langle x_1, x_2, x_3, x_6\rangle,$$

$$C_V(x_3) = \mathrm{Sp}\langle x_1, x_2, x_3, x_5\rangle,$$

and that if $\lambda \neq 0$ then

$$C_V(x_2 + \lambda x_3) = U.$$

Next consider $C_V(x_1 + dx_2 + ex_3)$. We have

$$[x_4, x_1 + dx_2 + ex_3] = [x_4, x_1] + d[x_5, x_1] + e[x_6, x_1],$$

$$[x_5, x_1 + dx_2 + ex_3] = d[x_4, x_1] + [x_5, x_1],$$

$$[x_6, x_1 + dx_2 + ex_3] = e[x_5, x_1] + [x_6, x_1].$$

It follows that $C_V(x_1 + dx_2 + ex_3) = U$ unless

$$\det\begin{bmatrix} 1 & d & e \\ d & 1 & 0 \\ 0 & e & 1 \end{bmatrix} = 1 - d^2 + de^2 = 0,$$

in which case $C_V(x_1 + dx_2 + ex_3) = \mathrm{Sp}\langle x_1, x_2, x_3, dx_4 - x_5 - dex_6\rangle$. Since $W \leqslant C_V(u)$ we see that either $W = U$, or W is a subspace of one of $\mathrm{Sp}\langle x_1, x_2, x_3, x_6\rangle$, $\mathrm{Sp}\langle x_1, x_2, x_3, x_5\rangle$, $\mathrm{Sp}\langle x_1, x_2, x_3, dx_4 - x_5 - dex_6\rangle$. It follows that W has non-trivial intersection with $\mathrm{Sp}\langle x_1, x_3\rangle$. Now $C_V(x_1 + \lambda x_3) = U$ (for any λ), and so if $W \neq U$ we must have $x_3 \in W$. Similarly, using the fact that W has non-trivial intersection with $\mathrm{Sp}\langle x_1, x_2\rangle$, we see that if $W \neq U$ then one of $x_1 + x_2$, $x_1 - x_2$, x_2 lies in W. But this implies that one of $x_1 + x_2 + x_3$, $x_1 - x_2 + x_3$, $x_2 + x_3$ lies in W. These three elements all have centralizers equal to U, and so $W = U$.

Now assume the $U \cap W = \{0\}$. Then $W = \mathrm{Sp}\langle u_1 + x_4, u_2 + x_5, u_3 + x_6\rangle$ for some $u_1, u_2, u_3 \in U$. Since W is abelian we have

$$[x_4, u_2] = [x_5, u_1],$$

$$[x_4, u_3] = [x_6, u_1],$$

$$[x_5, u_3] = [x_6, u_2],$$

and it is straightforward to show that this implies that for some λ we have $u_1 = \lambda x_1$, $u_2 = \lambda x_2$, $u_3 = \lambda x_3$.

This establishes our claim.

8. Automorphisms in *H*

We consider automorphisms of L_p which map $\mathrm{Sp}\langle x_1, x_2, x_3\rangle$ to itself, and also map $\mathrm{Sp}\langle x_4, x_5, x_6\rangle$ to itself. These automorphisms take the form

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \to A \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}, \qquad \begin{bmatrix} x_4 \\ x_5 \\ x_6 \end{bmatrix} \to B \begin{bmatrix} x_4 \\ x_5 \\ x_6 \end{bmatrix}$$

where A and B are non-singular 3×3 matrices over $\mathbb{F}_p$.

We show that for automorphisms of this form we must have $A = \lambda B$ for some scalar λ.

So let θ be an automorphism of this form. Recall that

$$C_V(x_2) = \mathrm{Sp}\langle x_1, x_2, x_3, x_6\rangle,$$

and so θx_2 must also be an element with centralizer of dimension 4. As we saw in Section 7, the elements in $\mathrm{Sp}\langle x_1, x_2, x_3\rangle$ with centralizers of dimension 4 are scalar multiples of x_2 and x_3, and scalar multiples of elements of the form $x_1 + dx_2 + ex_3$ where $1 - d^2 + de^2 = 0$. So θx_2 must be a scalar multiple of one of x_2, x_3 or $x_1 + dx_2 + ex_3$. This implies that $[\theta x_2, L_p]$ is one of the following:

$$\begin{aligned} [x_2, L_p] &= \mathrm{Sp}\big\langle [x_4, x_1], [x_5, x_1]\big\rangle, \\ [x_3, L_p] &= \mathrm{Sp}\big\langle [x_5, x_1], [x_6, x_1]\big\rangle, \\ [x_1 + dx_2 + ex_3, L_p] &= \mathrm{Sp}\big\langle [x_4, x_1] + d[x_5, x_1] + e[x_6, x_1], e[x_5, x_1] + [x_6, x_1]\big\rangle. \end{aligned}$$

Note that these 2-dimensional subspaces are all different. In particular, different solutions to the equation $1 - d^2 + de^2$ give different subspaces. Similarly θx_5 must be a scalar multiple of one of x_5, x_6 or $x_4 + dx_5 + ex_6$, and so $[\theta x_5, L_p]$ is one of the following:

$$\begin{aligned} [x_5, L_p] &= \mathrm{Sp}\big\langle [x_4, x_1], [x_5, x_1]\big\rangle, \\ [x_6, L_p] &= \mathrm{Sp}\big\langle [x_5, x_1], [x_6, x_1]\big\rangle, \\ [x_4 + dx_5 + ex_6, L_p] &= \mathrm{Sp}\big\langle [x_4, x_1] + d[x_5, x_1] + e[x_6, x_1], e[x_5, x_1] + [x_6, x_1]\big\rangle. \end{aligned}$$

Now $[x_2, L_p] = [x_5, L_p]$, and so $[\theta x_2, L_p] = [\theta x_5, L_p]$. This implies that one of three possibilities must arise:

1. θx_2 is a scalar multiple of x_2 and θx_5 is a scalar multiple of x_5,
2. θx_2 is a scalar multiple of x_3 and θx_5 is a scalar multiple of x_6,
3. θx_2 is a scalar multiple of $x_1 + dx_2 + ex_3$ and θx_5 is a scalar multiple of $x_4 + dx_4 + ex_6$ (with the same d, e).

In other words, the second row of the matrix A is a scalar multiple of the second row of B. Similarly, the third row of A is a scalar multiple of the third row of B.

Now let

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}, \qquad B = \begin{bmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{bmatrix}.$$

The second and third rows of B are scalar multiples of the second and third rows of A, and so we can express $[b_{11}, b_{12}, b_{13}]$ in the form

$$\lambda[a_{11}, a_{12}, a_{13}] + \mu[b_{21}, b_{22}, b_{23}] + \nu[b_{31}, b_{32}, b_{33}]$$

for some λ, μ, ν. It is a property of the algebra L_p that for any scalars a, b, c, d, e, f,

$$[ax_4 + bx_5 + cx_6, dx_1 + ex_2 + fx_3] = [dx_4 + ex_5 + fx_6, ax_1 + bx_2 + cx_3].$$

It follows that

$$\begin{aligned}[\theta x_4, \theta x_2] &= \lambda[a_{11}x_4 + a_{12}x_5 + a_{13}x_6, \theta x_2] + \mu[\theta x_5, \theta x_2] + \nu[\theta x_6, \theta x_2] \\ &= \lambda[a_{11}x_4 + a_{12}x_5 + a_{13}x_6, a_{21}x_1 + a_{22}x_2 + a_{23}x_3] + \mu[\theta x_5, \theta x_2] \quad \text{since } [x_6, x_2] = 0 \\ &= \lambda[a_{21}x_4 + a_{22}x_5 + a_{23}x_6, a_{11}x_1 + a_{12}x_2 + a_{13}x_3] + \mu[\theta x_5, \theta x_2].\end{aligned}$$

Now $a_{21}x_4 + a_{22}x_5 + a_{23}x_6$ is a scalar multiple of θx_5, and so

$$\lambda[a_{21}x_4 + a_{22}x_5 + a_{23}x_6, a_{11}x_1 + a_{12}x_2 + a_{13}x_3]$$

is a non-trivial scalar multiple of $[\theta x_5, \theta x_1] = [\theta x_4, \theta x_2]$. On the other hand, $[\theta x_5, \theta x_2]$ and $[\theta x_4, \theta x_2]$ are linearly independent, and so we must have $\mu = 0$. Similarly considering $[\theta x_4, \theta x_3]$ we see that $\nu = 0$. So the rows of B are all scalar multiples of the rows of A.

We may now assume that

$$\begin{aligned}[b_{11}, b_{12}, b_{13}] &= \lambda[a_{11}, a_{12}, a_{13}], \\ [b_{21}, b_{22}, b_{23}] &= \mu[a_{21}, a_{22}, a_{23}], \\ [b_{31}, b_{32}, b_{33}] &= \nu[a_{31}, a_{32}, a_{33}]\end{aligned}$$

for some λ, μ, ν. But then the relation $[x_5, x_1] = [x_4, x_2]$ implies that $\lambda = \mu$, and the relation $[x_6, x_1] = [x_4, x_3]$ implies that $\lambda = \nu$. So $B = \lambda A$, as claimed.

Composing θ with an automorphism of the form

$$\begin{aligned} x_1 &\to \alpha x_1, \\ x_2 &\to \alpha x_2, \\ x_3 &\to \alpha x_3, \\ x_4 &\to \delta x_4, \\ x_5 &\to \delta x_5, \\ x_6 &\to \delta x_6,\end{aligned}$$

we may assume that $A = B$, and that θx_3 equals x_2 or x_3 or $x_1 + dx_2 + ex_3$ for some solution of $1 - d^2 + de^2 = 0$.

We now show that the possibility $\theta x_3 = x_2$ never arises. Suppose, to the contrary, that $\theta x_3 = x_2$. The relation $[x_5, x_3] = 0$ implies that $\theta x_5 = \lambda x_6$ for some λ. The condition $A = B$ implies that $\theta x_2 = \lambda x_3$, $\theta x_6 = x_5$. Let $\theta x_1 = ax_1 + bx_2 + cx_3$. Then

$$[\theta x_5, \theta x_1] = \lambda c[x_5, x_1] + \lambda a[x_6, x_1]$$

and

$$[\theta x_6, \theta x_3] = [x_5, x_2] = [x_4, x_1].$$

However this conflicts with the relation $[x_5, x_1] = [x_6, x_3]$, and so $\theta x_3 = x_2$ cannot arise.

Next consider the possibility that $\theta x_3 = x_3$. Then we must have $\theta x_2 = \lambda x_2$ for some λ. This gives $\theta x_5 = \lambda x_5$, $\theta x_6 = x_6$. Let $\theta x_1 = ax_1 + bx_2 + cx_3$. Then

$$[\theta x_5, \theta x_1] = \lambda b[x_4, x_1] + \lambda a[x_5, x_1]$$

and

$$[\theta x_6, \theta x_3] = [x_6, x_3] = [x_5, x_1].$$

So the relation $[x_5, x_1] = [x_6, x_3]$ implies that $a = \lambda^{-1}$, $b = 0$. This gives

$$[\theta x_4, \theta x_1] = \lambda^{-2}[x_4, x_1] + c^2[x_5, x_1] + 2\lambda^{-1}c[x_6, x_1]$$

and

$$[\theta x_5, \theta x_2] = \lambda^2[x_5, x_2] = \lambda^2[x_4, x_1].$$

So the relation $[x_4, x_1] = [x_5, x_2]$ gives $\lambda^4 = 1$ and $c = 0$. So we have

$$A = B = \begin{bmatrix} \lambda^{-1} & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

where $\lambda^4 = 1$.

Finally consider the possibility that $\theta x_3 = x_1 + dx_2 + ex_3$ for some d, e satisfying $1 - d^2 + de^2 = 0$. The relation $[x_5, x_3] = 0$ implies that $\theta x_5 = dfx_4 - fx_5 - defx_6$ for some non-zero f. The assumption that $A = B$ implies that $\theta x_2 = dfx_1 - fx_2 - defx_3$, $\theta x_6 = x_4 + dx_5 + ex_6$. Let $\theta x_1 = ax_1 + bx_2 + cx_3$.

We claim that $a \neq 0$. Suppose to the contrary that $a = 0$, so that $\theta x_1 = bx_2 + cx_3$ and $\theta x_4 = bx_5 + cx_6$. Then computing $[\theta x_4, \theta x_1]$ and $[\theta x_5, \theta x_2]$ we see that the relation $[x_4, x_1] = [x_5, x_2]$ gives $d^2ef = 0$. Since $f \neq 0$ and d cannot equal 0, this implies that $e = 0$, and hence that $d = \pm 1$. But now computing $[\theta x_5, \theta x_1]$ and $[\theta x_6, \theta x_3]$ we see that the relation $[x_5, x_1] = [x_6, x_3]$ gives $-fb = 1 + d^2 = 2$, $dfb = 2d$, $dfc = 0$. However the first two of these three relations are incompatible, and so $a = 0$ is impossible.

This means that we can take $\theta x_1 = ax_1 + abx_2 + acx_3$, $\theta x_4 = ax_4 + abx_5 + acx_6$ for some a, b, c with $a \neq 0$. Thus

$$A = B = \begin{bmatrix} a & ab & ac \\ df & -f & -def \\ 1 & d & e \end{bmatrix}.$$

The relations $[x_4, x_1] = [x_5, x_2]$ and $[x_5, x_1] = [x_6, x_3]$ now give six equations which a, b, c, d, e must satisfy:

$$a^2(1 + b^2) = f^2(1 + d^2),$$

$$a^2(2b + c^2) = f^2(d^2e^2 - 2d),$$

$$a^2c = -d^2ef^2,$$

$$af(d - b) = 1 + d^2,$$

$$af(bd - cde - 1) = 2d + e^2,$$
$$adf(c - e) = 2e. \tag{1}$$

Since $af \neq 0$, the last three equations above give

$$\left(1 + d^2\right)(bd - cde - 1) - (d - b)\left(2d + e^2\right) = 0,$$
$$\left(1 + d^2\right)d(c - e) - (d - b)2e = 0.$$

Multiplying the second of these two equations by e, and then adding to the first, we obtain

$$\left(1 + d^2\right)\left(bd - 1 - de^2\right) - (d - b)\left(2d + 3e^2\right) = 0.$$

Multiplying this equation by d, and then using the relation $1 - d^2 + de^2 = 0$ to eliminate de^2 we obtain

$$(b - d)\left(d^4 + 6d^2 - 3\right) = 0.$$

Now $b = d$ is impossible, because if $b = d$ then the equation $af(d - b) = 1 + d^2$ gives $d^2 = -1$, which would imply that A is singular. So we must have

$$d^4 + 6d^2 - 3 = 0.$$

The equation $(1 + d^2)d(c - e) - (d - b)2e = 0$ gives $c = \frac{d^3e - 2be + 3de}{d(1+d^2)}$. Since a and f are both non-zero, the first and third equations from (1) give

$$\left(1 + d^2\right)c + \left(1 + b^2\right)d^2e = 0.$$

Substituting $\frac{d^3e - 2be + 3de}{d(1+d^2)}$ for c in this equation we obtain

$$e\left(b^2d^3 - 2b + 2d^3 + 3d\right) = 0.$$

Now $e \neq 0$, for if $e = 0$ then the equation $1 - d^2 + de^2 = 0$ implies that $d = \pm 1$, which is incompatible with the equation $d^4 + 6d^2 - 3 = 0$. So

$$b^2d^3 - 2b + 2d^3 + 3d = 0. \tag{2}$$

The second and third equations from (1) give

$$\left(d^2e^2 - 2d\right)c + \left(2b + c^2\right)d^2e = 0$$

Substituting $\frac{d^3e - 2be + 3de}{d(1+d^2)}$ for c, and then substituting $\frac{d^2-1}{d}$ for e^2 we obtain

$$\left(-b + 3d + bd^2 + d^3\right)\left(2b - 3d + d^5\right) = 0.$$

This gives $b = \frac{3d - d^5}{2}$ or $b = \frac{d^3 + 3d}{1 - d^2}$. However, if we substitute $\frac{3d - d^5}{2}$ for b in (2) we obtain

$$d^3\left(d^2 + 1\right)^2\left(-d^6 + 2d^4 + 3d^2 - 8\right) = 0.$$

Now we know that $d \neq 0$, $d^2+1 \neq 0$, $d^4+6d^2-3=0$. The greatest common divisor of d^4+6d^2-3 and $-d^6+2d^4+3d^2-8$ is 1, and so this is impossible. So $b=\frac{d^3+3d}{1-d^2}$.

Substituting this value for b into our expression for c we obtain $c=\frac{e(d^2+3)}{d^2-1}$. Also, substituting this value of b into the fourth equation from (1), we obtain $f=\frac{d^2-1}{2da}$. Substituting these values for b and f into the first equation from (1) we obtain

$$a^4=\frac{(d^2-1)^4}{4d^2(d^4+6d^2+1)}=\frac{(d^2-1)^4}{16d^2}.$$

So, as we showed in Section 6, the solutions for a are $a=u\frac{(d^2+1)e}{4}$ for any u with $u^4=1$.

It is straightforward to verify that with these values of a, b, c, d, e, f then $\theta x_1, \theta x_2, \dots, \theta x_6$, satisfy the defining relations of L_p provided $1-d^2+de^2=0$ and $d^4+6d^2-3=0$. To see this note that the property that

$$[\alpha x_4+\beta x_5+\gamma x_6, \delta x_1+\varepsilon x_2+\zeta x_3]=[\delta x_4+\varepsilon x_5+\zeta x_6, \alpha x_1+\beta x_2+\gamma x_3]$$

for all $\alpha, \beta, \gamma, \delta, \varepsilon, \zeta$ implies that

$$[\theta x_4, \theta x_1]=[\theta x_5, \theta x_2],$$
$$[\theta x_4, \theta x_3]=[\theta x_6, \theta x_1],$$
$$[\theta x_5, \theta x_1]=[\theta x_4, \theta x_2].$$

Also, θx_2 and θx_5 were chosen so that

$$[\theta x_5, \theta x_3]=[\theta x_6, \theta x_2]=0,$$

and the relations

$$[\theta x_i, \theta x_j]=0 \quad \text{for } i, j \in \{1,2,3\},$$
$$[\theta x_i, \theta x_j]=0 \quad \text{for } i, j \in \{4,5,6\}$$

follow from the fact that $\theta x_1, \theta x_2, \theta x_3 \in \mathrm{Sp}\langle x_1, x_2, x_3\rangle$ and $\theta x_4, \theta x_5, \theta x_6 \in \mathrm{Sp}\langle x_4, x_5, x_6\rangle$. So we only need to check the relations $[\theta x_4, \theta x_1]=[\theta x_5, \theta x_2]$ and $[\theta x_5, \theta x_1]=[\theta x_6, \theta x_3]$, and the six equations (1) ensure that these are satisfied. So we only need to check that a, b, c, d, e, f satisfy the equations (1), and this is straightforward.

9. The covering algebra

To obtain the covering algebra for L_p we need the following defining relations for L_p as a 9-dimensional Lie algebra with vector space basis $x_1, x_2, \dots, x_9$.

$$[x_2, x_1]=0,$$
$$[x_3, x_1]=0, \quad [x_3, x_2]=0, \quad [x_4, x_1]=x_7, \quad [x_4, x_2]=x_8, \quad [x_4, x_3]=x_9,$$
$$[x_5, x_1]=x_8, \quad [x_5, x_2]=x_7, \quad [x_5, x_3]=0, \quad [x_5, x_4]=0,$$
$$[x_6, x_1]=x_9, \quad [x_6, x_2]=0, \quad [x_6, x_3]=x_8, \quad [x_6, x_4]=0, \quad [x_6, x_5]=0,$$
$$[x_7, x_1]=0, \quad [x_7, x_2]=0, \quad [x_7, x_3]=0, \quad [x_7, x_4]=0, \quad [x_7, x_5]=0, \quad [x_7, x_6]=0,$$

$$[x_8, x_1] = 0, \quad [x_8, x_2] = 0, \quad [x_8, x_3] = 0, \quad [x_8, x_4] = 0, \quad [x_8, x_5] = 0, \quad [x_8, x_6] = 0,$$
$$[x_9, x_1] = 0, \quad [x_9, x_2] = 0, \quad [x_9, x_3] = 0, \quad [x_9, x_4] = 0, \quad [x_9, x_5] = 0, \quad [x_9, x_6] = 0.$$

This presentation has 33 relations, but the relations $[x_4, x_1] = x_7$, $[x_4, x_2] = x_8$, $[x_4, x_3] = x_9$ are taken to be the definitions of x_7, x_8, x_9. We introduce 30 additional generators $x_{10}, x_{11}, \ldots, x_{39}$ corresponding to the 30 relations which are *not* definitions, and add them as "tails" to these relations. This gives a presentation for the covering algebra on 39 generators with the following 33 relations giving the definitions of $x_7, x_8, \ldots, x_{39}$, together with 180 relations implying that the generators $x_{10}, x_{11}, \ldots, x_{39}$ are all central:

$$[x_2, x_1] = x_{28},$$
$$[x_3, x_1] = x_{29}, \quad [x_3, x_2] = x_{30},$$
$$[x_4, x_1] = x_7, \quad [x_4, x_2] = x_8, \quad [x_4, x_3] = x_9,$$
$$[x_5, x_1] = x_8 + x_{31}, \quad [x_5, x_2] = x_7 + x_{32}, \quad [x_5, x_3] = x_{33}, \quad [x_5, x_4] = x_{34},$$
$$[x_6, x_1] = x_9 + x_{35}, \quad [x_6, x_2] = x_{36}, \quad [x_6, x_3] = x_8 + x_{37}, \quad [x_6, x_4] = x_{38}, \quad [x_6, x_5] = x_{39},$$
$$[x_7, x_1] = x_{10}, \quad [x_7, x_2] = x_{11}, \quad [x_7, x_3] = x_{12}, \quad [x_7, x_4] = x_{13}, \quad [x_7, x_5] = x_{14}, \quad [x_7, x_6] = x_{15},$$
$$[x_8, x_1] = x_{16}, \quad [x_8, x_2] = x_{17}, \quad [x_8, x_3] = x_{18}, \quad [x_8, x_4] = x_{19}, \quad [x_8, x_5] = x_{20}, \quad [x_8, x_6] = x_{21},$$
$$[x_9, x_1] = x_{22}, \quad [x_9, x_2] = x_{23}, \quad [x_9, x_3] = x_{24}, \quad [x_9, x_4] = x_{25}, \quad [x_9, x_5] = x_{26}, \quad [x_9, x_6] = x_{27}.$$

We now need to enforce the Jacobi identity

$$[x_i, x_j, x_k] + [x_j, x_k, x_i] + [x_k, x_i, x_j] = 0$$

for all i, j, k with $1 \leqslant k < j < i \leqslant 6$. This gives 20 Jacobi relations, and we evaluate $[x_i, x_j, x_k] + [x_j, x_k, x_i] + [x_k, x_i, x_j]$ in each case.

$$[x_3, x_2, x_1] + [x_2, x_1, x_3] + [x_1, x_3, x_2] = 0,$$
$$[x_4, x_2, x_1] + [x_2, x_1, x_4] + [x_1, x_4, x_2] = x_{16} - x_{11},$$
$$[x_4, x_3, x_1] + [x_3, x_1, x_4] + [x_1, x_4, x_3] = x_{22} - x_{12},$$
$$[x_4, x_3, x_2] + [x_3, x_2, x_4] + [x_2, x_4, x_3] = x_{23} - x_{18},$$
$$[x_5, x_2, x_1] + [x_2, x_1, x_5] + [x_1, x_5, x_2] = x_{10} - x_{17},$$
$$[x_5, x_3, x_1] + [x_3, x_1, x_5] + [x_1, x_5, x_3] = -x_{18},$$
$$[x_5, x_3, x_2] + [x_3, x_2, x_5] + [x_2, x_5, x_3] = -x_{12},$$
$$[x_5, x_4, x_1] + [x_4, x_1, x_5] + [x_1, x_5, x_4] = x_{14} - x_{19},$$
$$[x_5, x_4, x_2] + [x_4, x_2, x_5] + [x_2, x_5, x_4] = x_{20} - x_{13},$$
$$[x_5, x_4, x_3] + [x_4, x_3, x_5] + [x_3, x_5, x_4] = x_{26},$$
$$[x_6, x_2, x_1] + [x_2, x_1, x_6] + [x_1, x_6, x_2] = -x_{23},$$
$$[x_6, x_3, x_1] + [x_3, x_1, x_6] + [x_1, x_6, x_3] = x_{16} - x_{24},$$

$$[x_6, x_3, x_2] + [x_3, x_2, x_6] + [x_2, x_6, x_3] = x_{17},$$

$$[x_6, x_4, x_1] + [x_4, x_1, x_6] + [x_1, x_6, x_4] = x_{15} - x_{25},$$

$$[x_6, x_4, x_2] + [x_4, x_2, x_6] + [x_2, x_6, x_4] = x_{21},$$

$$[x_6, x_4, x_3] + [x_4, x_3, x_6] + [x_3, x_6, x_4] = x_{27} - x_{19},$$

$$[x_6, x_5, x_1] + [x_5, x_1, x_6] + [x_1, x_6, x_5] = x_{21} - x_{26},$$

$$[x_6, x_5, x_2] + [x_5, x_2, x_6] + [x_2, x_6, x_5] = x_{15},$$

$$[x_6, x_5, x_3] + [x_5, x_3, x_6] + [x_3, x_6, x_5] = -x_{20},$$

$$[x_6, x_5, x_4] + [x_5, x_4, x_6] + [x_4, x_6, x_5] = 0.$$

So the Jacobi relations give the following 16 independent relations:

$$x_{10} = x_{12} = x_{13} = x_{15} = x_{17} = x_{18} = x_{20} = x_{21} = x_{22} = x_{23} = x_{25} = x_{26} = 0,$$

$$x_{11} = x_{16} = x_{24},$$

$$x_{14} = x_{19} = x_{27}.$$

If we enforce these relations, and relabel the generators, then we obtain a presentation for the covering algebra on 23 generators, with the following 33 relations together with 84 relations which imply that $x_{10}, x_{11}, \ldots, x_{23}$ are central:

$$[x_2, x_1] = x_{12},$$

$$[x_3, x_1] = x_{13}, \quad [x_3, x_2] = x_{14},$$

$$[x_4, x_1] = x_7, \quad [x_4, x_2] = x_8, \quad [x_4, x_3] = x_9,$$

$$[x_5, x_1] = x_8 + x_{15}, \quad [x_5, x_2] = x_7 + x_{16}, \quad [x_5, x_3] = x_{17}, \quad [x_5, x_4] = x_{18},$$

$$[x_6, x_1] = x_9 + x_{19}, \quad [x_6, x_2] = x_{20}, \quad [x_6, x_3] = x_8 + x_{21}, \quad [x_6, x_4] = x_{22}, \quad [x_6, x_5] = x_{23},$$

$$[x_7, x_1] = 0, \quad [x_7, x_2] = x_{10}, \quad [x_7, x_3] = 0, \quad [x_7, x_4] = 0, \quad [x_7, x_5] = x_{11}, \quad [x_7, x_6] = 0,$$

$$[x_8, x_1] = x_{10}, \quad [x_8, x_2] = 0, \quad [x_8, x_3] = 0, \quad [x_8, x_4] = x_{11}, \quad [x_8, x_5] = 0, \quad [x_8, x_6] = 0,$$

$$[x_9, x_1] = 0, \quad [x_9, x_2] = 0, \quad [x_9, x_3] = x_{10}, \quad [x_9, x_4] = 0, \quad [x_9, x_5] = 0, \quad [x_9, x_6] = x_{11}.$$

Call this covering algebra M. Then M has dimension 23, and the nucleus of M is $[M, M, M]$ which has dimension 2 and is spanned by x_{10} and x_{11} (with $x_{10} = [x_4, x_1, x_2]$ and $x_{11} = [x_4, x_1, x_5]$). The immediate descendants of L_p are the algebras M/I, where I is a proper subspace of $\mathrm{Sp}\langle x_{10}, x_{11}, \ldots, x_{23}\rangle$ such that

$$I + \mathrm{Sp}\langle x_{10}, x_{11}\rangle = \mathrm{Sp}\langle x_{10}, x_{11}, \ldots, x_{23}\rangle.$$

Thus L_p has immediate descendants of dimension 10 and 11.

10. Descendants of L_p of dimension 10

Let $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in \mathrm{GL}(2, p)$, and let

$$\begin{aligned} y_1 &= \alpha x_1 + \beta x_4, \\ y_2 &= \alpha x_2 + \beta x_5, \\ y_3 &= \alpha x_3 + \beta x_6, \\ y_4 &= \gamma x_1 + \delta x_4, \\ y_5 &= \gamma x_2 + \delta x_5, \\ y_6 &= \gamma x_3 + \delta x_6. \end{aligned}$$

Then, $[y_4, y_1] = (\alpha\delta - \beta\gamma)[x_4, x_1]$, and

$$\begin{aligned} [y_4, y_1, y_2] &= \alpha(\alpha\delta - \beta\gamma)x_{10} + \beta(\alpha\delta - \beta\gamma)x_{11}, \\ [y_4, y_1, y_5] &= \gamma(\alpha\delta - \beta\gamma)x_{10} + \delta(\alpha\delta - \beta\gamma)x_{11}. \end{aligned}$$

This means that if M/I is an immediate descendant of L_p of dimension 10, then we can choose $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$ so that $[y_4, y_1, y_2] + I$ generates $\mathrm{Sp}\langle x_{10}, x_{11}, \dots, x_{23}\rangle/I$, and so that $[y_4, y_1, y_5] \in I$. Note that if we let $J = \mathrm{Sp}\langle x_{10}, x_{11}, \dots, x_{23}\rangle$ then M/J is isomorphic to L_p and the map $x_i + J \mapsto y_i + J$ for $i = 1, 2, \dots, 6$ extends to an automorphism of L_p. So every immediate descendant of L_p of dimension 10 has a presentation on generators $x_1, x_2, \dots, x_{10}$ with relations

$$\begin{gathered} [x_2, x_1] = \varepsilon x_{10}, \qquad (3) \\ [x_3, x_1] = \zeta x_{10}, \quad [x_3, x_2] = \eta x_{10}, \\ [x_4, x_1] = x_7, \quad [x_4, x_2] = x_8, \quad [x_4, x_3] = x_9, \\ [x_5, x_1] = x_8 + \theta x_{10}, \quad [x_5, x_2] = x_7 + \kappa x_{10}, \quad [x_5, x_3] = \lambda x_{10}, \quad [x_5, x_4] = \mu x_{10}, \\ [x_6, x_1] = x_9 + \nu x_{10}, \quad [x_6, x_2] = \xi x_{10}, \quad [x_6, x_3] = x_8 + \pi x_{10}, \quad [x_6, x_4] = \rho x_{10}, \quad [x_6, x_5] = \sigma x_{10}, \\ [x_7, x_1] = 0, \quad [x_7, x_2] = x_{10}, \quad [x_7, x_3] = 0, \quad [x_7, x_4] = 0, \quad [x_7, x_5] = 0, \quad [x_7, x_6] = 0, \\ [x_8, x_1] = x_{10}, \quad [x_8, x_2] = 0, \quad [x_8, x_3] = 0, \quad [x_8, x_4] = 0, \quad [x_8, x_5] = 0, \quad [x_8, x_6] = 0, \\ [x_9, x_1] = 0, \quad [x_9, x_2] = 0, \quad [x_9, x_3] = x_{10}, \quad [x_9, x_4] = 0, \quad [x_9, x_5] = 0, \quad [x_9, x_6] = 0, \\ [x_{10}, x_1] = 0, \quad [x_{10}, x_2] = 0, \quad [x_{10}, x_3] = 0, \quad [x_{10}, x_4] = 0, \quad [x_{10}, x_5] = 0, \quad [x_{10}, x_6] = 0, \end{gathered}$$

for some scalars $\varepsilon, \zeta, \dots, \sigma$.

If we take this presentation, and let

$$\begin{aligned} y_1 &= x_1, \\ y_2 &= x_2 - \varepsilon x_8, \\ y_3 &= x_3 - \eta x_7 - \zeta x_8, \\ y_4 &= x_4, \end{aligned}$$

$$y_5 = x_5 - \kappa x_7 - \theta x_8 - \lambda x_9,$$
$$y_6 = x_6 - \xi x_7 - \nu x_8 - \pi x_9,$$

then

$$[y_2, y_1] = [x_2, x_1] - \varepsilon[x_8, x_1] = 0,$$
$$[y_3, y_1] = [x_3, x_1] - \eta[x_7, x_1] - \zeta[x_8, x_1] = 0,$$
$$[y_3, y_2] = [x_3, x_2] - \eta[x_7, x_2] - \zeta[x_8, x_2] + \varepsilon[x_8, x_3] = 0,$$
$$[y_4, y_1] = [x_4, x_1] = x_7,$$
$$[y_4, y_2] = [x_4, x_2] + \varepsilon[x_8, x_4] = x_8,$$
$$[y_4, y_3] = [x_4, x_3] + \eta[x_7, x_4] + \zeta[x_8, x_4] = x_9,$$
$$[y_5, y_1] = [x_5, x_1] - \kappa[x_7, x_1] - \theta[x_8, x_1] - \lambda[x_9, x_1] = x_8,$$
$$[y_5, y_2] = [x_5, x_2] - \kappa[x_7, x_2] - \theta[x_8, x_2] - \lambda[x_9, x_2] + \varepsilon[x_8, x_5] = x_7,$$
$$[y_5, y_3] = [x_5, x_3] - \kappa[x_7, x_3] - \theta[x_8, x_3] - \lambda[x_9, x_3] + \eta[x_7, x_5] + \zeta[x_8, x_5] = 0,$$
$$[y_5, y_4] = [x_5, x_4] - \kappa[x_7, x_4] - \theta[x_8, x_4] - \lambda[x_9, x_4] = \mu x_{10},$$
$$[y_6, y_1] = [x_6, x_1] - \xi[x_7, x_1] - \nu[x_8, x_1] - \pi[x_9, x_1] = x_9,$$
$$[y_6, y_2] = [x_6, x_2] - \xi[x_7, x_2] - \nu[x_8, x_2] - \pi[x_9, x_2] + \varepsilon[x_8, x_6] = 0,$$
$$[y_6, y_3] = [x_6, x_3] - \xi[x_7, x_3] - \nu[x_8, x_3] - \pi[x_9, x_3] + \kappa[x_7, x_6] + \theta[x_8, x_6] + \lambda[x_9, x_6] = x_8,$$
$$[y_6, y_4] = [x_6, x_4] - \xi[x_7, x_4] - \nu[x_8, x_4] - \pi[x_9, x_4] = \rho x_{10},$$
$$[y_6, y_5] = [x_6, x_5] - \xi[x_7, x_5] - \nu[x_8, x_5] - \pi[x_9, x_5] + \kappa[x_7, x_6] + \theta[x_8, x_6] + \lambda[x_9, x_6] = \sigma x_{10}.$$

And if we define $y_7 = x_7$, $y_8 = x_8$, $y_9 = x_9$, $y_{10} = x_{10}$ then we obtain the relations

$$[y_7, y_1] = 0, \quad [y_7, y_2] = y_{10}, \quad [y_7, y_3] = 0, \quad [y_7, y_4] = 0, \quad [y_7, y_5] = 0, \quad [y_7, y_6] = 0,$$
$$[y_8, y_1] = y_{10}, \quad [y_8, y_2] = 0, \quad [y_8, y_3] = 0, \quad [y_8, y_4] = 0, \quad [y_8, y_5] = 0, \quad [y_8, y_6] = 0,$$
$$[y_9, y_1] = 0, \quad [y_9, y_2] = 0, \quad [y_9, y_3] = y_{10}, \quad [y_9, y_4] = 0, \quad [y_9, y_5] = 0, \quad [y_9, y_6] = 0,$$
$$[y_{10}, y_1] = 0, \quad [y_{10}, y_2] = 0, \quad [y_{10}, y_3] = 0, \quad [y_{10}, y_4] = 0, \quad [y_{10}, y_5] = 0, \quad [y_{10}, y_6] = 0.$$

It follows that every immediate descendant of L_p of dimension 10 has a presentation on generators $x_1, x_2, \ldots, x_{10}$ with relations

$$[x_4, x_1] = x_7, \quad [x_4, x_2] = x_8, \quad [x_4, x_3] = x_9,$$
$$[x_5, x_1] = x_8, \quad [x_5, x_2] = x_7, \quad [x_5, x_4] = \mu x_{10},$$
$$[x_6, x_1] = x_9, \quad [x_6, x_3] = x_8, \quad [x_6, x_4] = \rho x_{10}, \quad [x_6, x_5] = \sigma x_{10},$$
$$[x_7, x_2] = x_{10},$$
$$[x_8, x_1] = x_{10},$$

$$[x_9, x_3] = x_{10},$$

for some scalars μ, ρ, σ, and with all other commutators $[x_i, x_j]$ with $i > j$ trivial.

11. Counting the descendants of dimension 10

As we showed above, every immediate descendant of L_p of dimension 10 has a presentation on generators $x_1, x_2, \ldots, x_{10}$ with relations

$$[x_4, x_1] = x_7, \quad [x_4, x_2] = x_8, \quad [x_4, x_3] = x_9,$$

$$[x_5, x_1] = x_8, \quad [x_5, x_2] = x_7, \quad [x_5, x_4] = \lambda x_{10},$$

$$[x_6, x_1] = x_9, \quad [x_6, x_3] = x_8, \quad [x_6, x_4] = \mu x_{10}, \quad [x_6, x_5] = \nu x_{10},$$

$$[x_7, x_2] = x_{10},$$

$$[x_8, x_1] = x_{10},$$

$$[x_9, x_3] = x_{10},$$

for some scalars λ, μ, ν, and with all other commutators $[x_i, x_j]$ with $i > j$ trivial. Denote this algebra by $A_{(\lambda,\mu,\nu)}$. The isomorphism type of $A_{(\lambda,\mu,\nu)}$ is determined by the triple (λ, μ, ν), but we still need to solve the problem of when two different triples give isomorphic algebras. Suppose that $A_{(\lambda,\mu,\nu)}$ is isomorphic to $A_{(\lambda',\mu',\nu')}$, and let $\theta : A_{(\lambda',\mu',\nu')} \to A_{(\lambda,\mu,\nu)}$ be an isomorphism. Let $y_1, y_2, \ldots, y_6$ be the images in $A_{(\lambda,\mu,\nu)}$ under θ of the defining generators of $A_{(\lambda',\mu',\nu')}$. Note that $A_{(\lambda,\mu,\nu)}/\langle x_{10}\rangle$ is isomorphic to L_p, and that the map $x_i + \langle x_{10}\rangle \mapsto y_i + \langle x_{10}\rangle$ $(i = 1, 2, \ldots, 6)$ extends to an automorphism of L_p. Note also that

$$\begin{aligned} C_{A_{(\lambda,\mu,\nu)}}\big([A_{(\lambda,\mu,\nu)}, A_{(\lambda,\mu,\nu)}]\big) &= [A_{(\lambda,\mu,\nu)}, A_{(\lambda,\mu,\nu)}] + \mathrm{Sp}\langle x_4, x_5, x_6\rangle \\ &= [A_{(\lambda,\mu,\nu)}, A_{(\lambda,\mu,\nu)}] + \mathrm{Sp}\langle y_4, y_5, y_6\rangle. \end{aligned}$$

It follows that $A_{(\lambda,\mu,\nu)}$ is isomorphic to $A_{(\lambda',\mu',\nu')}$ if and only if $A_{(\lambda,\mu,\nu)}$ has a set of generators $y_1, y_2, \ldots, y_6$ satisfying the defining relations of $A_{(\lambda',\mu',\nu')}$, and that this can only happen if the map $x_i + \langle x_{10}\rangle \mapsto y_i + \langle x_{10}\rangle$ $(i = 1, 2, \ldots, 6)$ extends to an automorphism of L_p, and if

$$[A_{(\lambda,\mu,\nu)}, A_{(\lambda,\mu,\nu)}] + \mathrm{Sp}\langle x_4, x_5, x_6\rangle = [A_{(\lambda,\mu,\nu)}, A_{(\lambda,\mu,\nu)}] + \mathrm{Sp}\langle y_4, y_5, y_6\rangle. \tag{4}$$

The first thing to observe is that if we let $y_1 = x_1$, $y_2 = x_2$, $y_3 = x_3$, $y_4 = \delta x_4$, $y_5 = \delta x_5$, $y_6 = \delta x_6$ in $A_{(\lambda,\mu,\nu)}$, then $y_1, y_2, \ldots, y_6$ satisfy the defining relations of $A_{(\delta\lambda,\delta\mu,\delta\nu)}$. (This is easy to check.) So the triples (λ, μ, ν) and $(\delta\lambda, \delta\mu, \delta\nu)$ define isomorphic algebras, and the isomorphism type of $A_{(\lambda,\mu,\nu)}$ depends only on the ratios $\lambda : \mu$, $\lambda : \nu$, $\mu : \nu$. The next thing to note is that if $y_1, y_2, \ldots, y_6 \in A_{(\lambda,\mu,\nu)}$ satisfy the defining relations of $A_{(\lambda',\mu',\nu')}$ then the ratios $\lambda' : \mu'$, $\lambda' : \nu'$, $\mu' : \nu'$ depend only on the values of y_4, y_5, y_6, and not on the values of y_1, y_2, y_3. The calculations in Section 8, together with Eq. (4) and the fact that the map $x_i + \langle x_{10}\rangle \mapsto y_i + \langle x_{10}\rangle$ $(i = 1, 2, \ldots, 6)$ extends to an automorphism of L_p, imply that

$$\begin{bmatrix} y_4 \\ y_5 \\ y_6 \end{bmatrix} = \delta A \begin{bmatrix} x_4 \\ x_5 \\ x_6 \end{bmatrix} + \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix}$$

where $b_1, b_2, b_3 \in [A_{(\lambda,\mu,\nu)}, A_{(\lambda,\mu,\nu)}]$, where $\delta \neq 0$, and where

$$A = \begin{bmatrix} u & 0 & 0 \\ 0 & u^{-1} & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

with $u^4 = 1$, or

$$A = \begin{bmatrix} a & ab & ac \\ df & -f & -def \\ 1 & d & e \end{bmatrix},$$

as described in Section 8. Furthermore, since x_4, x_5, x_6 centralize $[A_{(\lambda,\mu,\nu)}, A_{(\lambda,\mu,\nu)}]$ the values of $[y_5, y_4]$, $[y_6, y_4]$, $[y_6, y_5]$ depend only on δA, and not on b_1, b_2, b_3.

We now show that

$$\begin{bmatrix} y_4 \\ y_5 \\ y_6 \end{bmatrix} = \delta A \begin{bmatrix} x_4 \\ x_5 \\ x_6 \end{bmatrix}$$

can arise for all δA of the form just described. Specifically, we show that if we set

$$\begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} = \alpha A \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}, \qquad \begin{bmatrix} y_4 \\ y_5 \\ y_6 \end{bmatrix} = \delta A \begin{bmatrix} x_4 \\ x_5 \\ x_6 \end{bmatrix}$$

where $\alpha, \delta \neq 0$, and where A is as just described, then $y_1, y_2, \ldots, y_6$ *do* satisfy the defining relations of the algebra $A_{(\lambda',\mu',\nu')}$, for some (λ', μ', ν') which we will determine below. One possible way of checking this is to compute $[y_i, y_j]$ in terms of x_7, x_8, x_9, x_{10} for all $i > j$, and check all the relations one by one. But there is a shortcut. We know that the map $x_i + \langle x_{10} \rangle \mapsto y_i + \langle x_{10} \rangle$ $(i = 1, 2, \ldots, 6)$ extends to an automorphism of L_p. We also know that y_4, y_5, y_6 centralize $[A_{(\lambda,\mu,\nu)}, A_{(\lambda,\mu,\nu)}]$. In particular $[y_4, y_1, y_5] = 0$. So if we set $y_7 = [y_4, y_1]$, $y_8 = [y_4, y_2]$, $y_9 = [y_4, y_3]$, $y_{10} = [y_4, y_1, y_2]$, then $y_1, y_2, \ldots, y_{10}$ must satisfy relations of the form (3) for some scalars $\varepsilon, \zeta, \ldots, \sigma$. However we must have $\varepsilon = \zeta = \eta = 0$ since the linear span of y_1, y_2, y_3 is the same as the linear span of x_1, x_2, x_3, and

$$[x_2, x_1] = [x_3, x_1] = [x_3, x_2] = 0.$$

We must also have $\theta = \kappa = \lambda = \nu = \xi = \pi = 0$ since if $4 \leqslant r \leqslant 6$ and $1 \leqslant s \leqslant 3$ then

$$[y_r, y_s] \in \mathrm{Sp}\big\langle [x_i, x_j] \bigm| i \in \{4, 5, 6\},\ j \in \{1, 2, 3\} \big\rangle = \mathrm{Sp}\langle x_7, x_8, x_9 \rangle.$$

It remains to compute $[y_5, y_4]$, $[y_6, y_4]$, $[y_6, y_5]$.

Consider the case when

$$A = \begin{bmatrix} u & 0 & 0 \\ 0 & u^{-1} & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Then

$$[y_5, y_4] = \delta^2[x_5, x_4] = \delta^2\lambda x_{10},$$
$$[y_6, y_4] = \delta^2 u[x_6, x_4] = \delta^2 u\mu x_{10},$$
$$[y_6, y_5] = \delta^2 u^{-1}[x_6, x_5] = \delta^2 u^{-1}\nu x_{10}.$$

Now

$$y_{10} = [y_4, y_1, y_2] = \alpha^2\delta u[x_4, x_1, x_2] = \alpha^2\delta u x_{10},$$

and so $y_1, y_2, \dots, y_{10}$ satisfy the defining relations of $A_{(k\lambda, ku\mu, ku^{-1}\nu)}$ where $k = \alpha^{-2}\delta u^{-1}$. Note that as α and δ take on all possible non-zero values, k takes on all possible non-zero values.

Next consider the case when

$$A = \begin{bmatrix} a & ab & ac \\ df & -f & -def \\ 1 & d & e \end{bmatrix}.$$

Then

$$[y_5, y_4] = \delta^2\big(-(af + abdf)[x_5, x_4] - (adef + acdf)[x_6, x_4] - (abdef - acf)[x_6, x_5]\big),$$
$$[y_6, y_4] = \delta^2\big((ad - ab)[x_5, x_4] + (ae - ac)[x_6, x_4] + (abe - acd)[x_6, x_5]\big),$$
$$[y_6, y_5] = \delta^2\big(\big(d^2 f + f\big)[x_5, x_4] + 2def[x_6, x_4] - \big(ef - d^2 ef\big)[x_6, x_5]\big).$$

So $y_1, y_2, \dots, y_{10}$ satisfy the defining relations of $A_{(\lambda', \mu', \nu')}$ where

$$\begin{bmatrix} \lambda' \\ \mu' \\ \nu' \end{bmatrix} = k \begin{bmatrix} -abdf - af & -acdf - adef & -abdef + acf \\ -ab + ad & -ac + ae & abe - acd \\ d^2 f + f & 2def & d^2 ef - ef \end{bmatrix} \begin{bmatrix} \lambda \\ \mu \\ \nu \end{bmatrix},$$

for some non-zero scalar k which takes on all possible values as α and δ take on all possible values. Substituting the solutions for a, c, d, f in terms of d and e, and using the fact that $e^2 = \frac{d^2-1}{d}$, we obtain

$$\begin{bmatrix} \lambda' \\ \mu' \\ \nu' \end{bmatrix} = k \begin{bmatrix} \frac{1}{2d}(d^2+1)^2 & -e(d^2+1) & \frac{1}{2d}e(d^4+4d^2+3) \\ \frac{1}{2}du\frac{e}{d^2-1}(d^2+1)^2 & -\frac{u}{d}(d^2+1) & -\frac{1}{2}u(d^4+4d^2+3) \\ 2u^{-1}e & 4u^{-1}\frac{d^2-1}{d^2+1} & \frac{2u^{-1}}{d}\frac{(d^2-1)^2}{d^2+1} \end{bmatrix} \begin{bmatrix} \lambda \\ \mu \\ \nu \end{bmatrix}.$$

So we have an action on $\mathbb{F}_p^3$ of the form

$$\begin{bmatrix} \lambda \\ \mu \\ \nu \end{bmatrix} \to kB \begin{bmatrix} \lambda \\ \mu \\ \nu \end{bmatrix}, \tag{5}$$

where k is an arbitrary non-zero scalar, and where B is a matrix of the form

$$B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & u & 0 \\ 0 & 0 & u^{-1} \end{bmatrix} \tag{6}$$

(with $u^4 = 1$) or a matrix of the form

$$B = \begin{bmatrix} \frac{1}{2d}(d^2+1)^2 & -e(d^2+1) & \frac{1}{2d}e(d^4+4d^2+3) \\ \frac{1}{2}du\frac{e}{d^2-1}(d^2+1)^2 & -\frac{u}{d}(d^2+1) & -\frac{1}{2}u(d^4+4d^2+3) \\ 2u^{-1}e & 4u^{-1}\frac{d^2-1}{d^2+1} & \frac{2u^{-1}}{d}\frac{(d^2-1)^2}{d^2+1} \end{bmatrix} \tag{7}$$

(with d and e solutions of $d^4+6d^2-3=0$ and $1-d^2+de^2=0$ and with $u^4=1$). The actual matrices that occur depend on the residue class of p modulo 12. If $p=1$ mod 12 then we have 4 matrices of the form (6) and either 0 or 32 matrices of the form (7). So when $p=1$ mod 12 we either have a group of order $4(p-1)$ acting on $\mathbb{F}_p^3$, or we have a group of order $36(p-1)$. If $p=5$ mod 12 then we have 4 matrices of the form (6) and none of the form (7). So we have a group of order $4(p-1)$ acting on $\mathbb{F}_p^3$. If $p=7$ mod 12 then there are 2 matrices of the form (6) and none of the form (7), so we have a group of order $2(p-1)$ acting on $\mathbb{F}_p^3$. Finally, if $p=11$ mod 12 then we have 2 matrices of the form (6) and 4 matrices of the form (7), so that we have a group of order $6(p-1)$ acting on $\mathbb{F}_p^3$.

The number of isomorphism classes of algebras $A_{(\lambda,\mu,\nu)}$ is the number of orbits in the action of these groups on $\mathbb{F}_p^3$. We compute the number of orbits in each case by computing the number of vectors in $\mathbb{F}_p^3$ fixed by each transformation of the form (5). First note that all the transformations fix $\begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$. On the other hand, a non-zero vector $\begin{bmatrix} \lambda \\ \mu \\ \nu \end{bmatrix}$ can only be fixed by a transformation of the form (5) if it is an eigenvector of B, and in that case it is fixed if and only if k is the multiplicative inverse of the eigenvalue. So we need to count the (non-zero) eigenvectors for each of the matrices B. A matrix of the form (6) has p^3-1 eigenvectors if $u=1$, p^2+p-2 eigenvectors if $u=-1$, and $3p-3$ eigenvectors if $u^2=-1$. If $u=1$ then a matrix of the form (7) has characteristic polynomial $x^3-\frac{256}{3}(d^3-d)$, and an eigenvalue $-\frac{4}{3}(d^3+3d)$. So if $p=11$ mod 12 then the matrix has a single eigenvalue of multiplicity 1, and $p-1$ eigenvectors. But if $p=1$ mod 12 then the matrix has 3 distinct eigenvalues and $3p-3$ eigenvectors. If $u=-1$ then a matrix of the form (7) is diagonalizable with eigenvalues $\frac{4}{3}(d^3+3d)$, $\frac{4}{3}(d^3+3d)$, $-\frac{4}{3}(d^3+3d)$, and p^2+p-2 eigenvectors. Finally, if $u^2=-1$ then a matrix of the form (7) has 3 distinct eigenvalues $-4du+\frac{2}{3}(d^3+3d)$, $4d+\frac{2}{3}(d^3+3d)u$, $-4d-\frac{2}{3}(d^3+3d)u$, and so has $3p-3$ eigenvectors.

It follows that if $p=1$ mod 12 and if there are no solutions to the equations $d^4+6d^2-3=0$ and $1-d^2+de^2=0$, or if $p=5$ mod 12, then the number of orbits (i.e. the number of descendants of L_p of dimension 10) is

$$\frac{4(p-1)+(p^3-1)+(p^2+p-2)+2(3p-3)}{4(p-1)} = \frac{(p+1)^2}{4}+3.$$

If $p=1$ mod 12 and if there are solutions to the equations $d^4+6d^2-3=0$ and $1-d^2+de^2=0$, then the number of orbits is

$$\frac{36(p-1)+(p^3-1)+(p^2+p-2)+2(3p-3)+8(p^2+p-2)+24(3p-3)}{36(p-1)}$$
$$= \frac{(p-1)^2}{36}+\frac{p-1}{3}+4.$$

If $p=7$ mod 12 then the number of orbits is

$$\frac{2(p-1)+(p^3-1)+(p^2+p-2)}{2(p-1)} = \frac{(p+1)^2}{2}+2.$$

And finally if $p = 11 \bmod 12$ then the number of orbits is

$$\frac{6(p-1)+(p^3-1)+3(p^2+p-2)+2(p-1)}{6(p-1)} = \frac{(p+1)^2}{6} + \frac{p+1}{3} + 2.$$

This completes the proof of Theorem 1.

References

[1] S.R. Blackburn, P.M. Neumann, G. Venkataraman, Enumeration of Finite Groups, Cambridge Tracts in Math., vol. 173, Cambridge Univ. Press, 2007.

[2] N. Bourbaki, Groupes et Algebres de Lie, Hermann, Paris, 1972.

[3] M.P.F. du Sautoy, Zeta functions and counting finite p-groups, Electron. Res. Announc. Amer. Math. Soc. 5 (1999) 112–122.

[4] M.P.F. du Sautoy, Counting finite p-groups and nilpotent groups, Publ. Math. Inst. Hautes Études Sci. 92 (2000) 63–112.

[5] M.P.F. du Sautoy, Counting subgroups in nilpotent groups and points on elliptic curves, J. Reine Angew. Math. 549 (2002) 1–21.

[6] M.P.F. du Sautoy, F.J. Grunewald, Analytic properties of Euler products of Igusa-type zeta functions and subgroup growth of nilpotent groups, C. R. Acad. Sci. Paris 329 (1999) 351–356.

[7] M.P.F. du Sautoy, F.J. Grunewald, Analytic properties of zeta functions and subgroup growth, Ann. of Math. 152 (2000) 793–833.

[8] A. Evseev, Higman's PORC conjecture for a family of groups, Bull. London Math. Soc. 40 (2008) 415–431.

[9] F.J. Grunewald, D. Segal, G.C. Smith, Subgroups of finite index in nilpotent groups, Invent. Math. 93 (1988) 185–223.

[10] G. Higman, Enumerating p-groups, II, Proc. London Math. Soc. 10 (1960) 566–582.

[11] K. Ireland, M. Rosen, A Classical Introduction to Modern Number Theory, second ed., Grad. Texts in Math., vol. 84, Springer-Verlag, New York–Berlin–Heidelberg, 1993.

[12] F. Lemmermeyer, Reciprocity laws, From Kummer to Hilbert, preprint.

[13] M.F. Newman, E.A. O'Brien, M.R. Vaughan-Lee, Groups and nilpotent Lie rings whose order is the sixth power of a prime, J. Algebra 278 (2004) 383–401.

[14] E.A. O'Brien, The p-group generation algorithm, J. Symbolic Comput. 9 (1990) 677–698.

[15] E.A. O'Brien, M.R. Vaughan-Lee, The groups with order p^7 for odd prime p, J. Algebra 292 (2005) 243–358.

[16] Hans Rademacher, Über die Anzahl der Primzahlen eines reell-quadratischen Zahlkörpers, deren Konjugierte unterhalb gegebener Grenzen liegen, Acta Arith. 1 (1935) 67–77.