An insoluble \((p - 2)\)-Engel group of exponent \(p\)

Michael Vaughan-Lee

Christ Church, Oxford, OX1 1DP, England, United Kingdom

**Abstract**

In 1971, Razmyslov [4] found a beautiful construction for insoluble, locally nilpotent groups of exponent \(p\) \((p \geq 5)\). In 1978, Razmyslov [5] refined his construction, and showed that it also gives insoluble groups of exponent 4. In this note, we show that Razmyslov’s method can be used to construct insoluble, locally nilpotent, \((p - 2)\)-Engel groups of exponent \(p\) for all primes \(p \geq 5\).

© 2009 Elsevier Inc. All rights reserved.

In 1970, Bachmuth, Mochizuki and Walkup [1] constructed an insoluble, locally nilpotent group of exponent 5, and in 1971, Bachmuth and Mochizuki [2] showed that the group constructed in [1] is a 3-Engel group—that is, it satisfies the identical relation \([x, y, y, y] = 1\). Independently of [1] and [2], Razmyslov [4] constructed insoluble locally nilpotent groups of exponent \(p\) for all \(p \geq 5\). Although Razmyslov’s construction was completely independent of Bachmuth, Mochizuki and Walkup’s, the two constructions are in fact quite similar. So it seems natural to ask whether Razmyslov’s groups satisfy the \((p - 2)\)-Engel condition. (We say that a group \(G\) satisfies the \(n\)-Engel condition if

\[
[x, y, y, \ldots, y] = 1
\]

for all \(x, y \in G\).) An additional reason for asking this question is that Razmyslov constructed insoluble, locally nilpotent, \((p - 2)\)-Engel Lie algebras over \(\text{GF}(p)\) \((p \geq 5)\) in [4], and the existence of these Lie algebras is closely related to the existence of his insoluble groups of exponent \(p\).

It turns out that Razmyslov’s construction does indeed provide \((p - 2)\)-Engel groups.

**Theorem 1.** For each prime \(p \geq 5\) there exists an insoluble, locally nilpotent, \((p - 2)\)-Engel group of exponent \(p\).
In fact we can prove a stronger result which implies Theorem 1.

**Theorem 2.** For each prime $p \geq 5$ there exists an insoluble group $G$ of exponent $p$ with the property that if $g \in G$ then the normal closure of $g$ in $G$ is nilpotent of class at most $p - 3$.

It is perhaps worth observing that insoluble, locally nilpotent Engel groups are not that easy to come by. Razmyslov [5] proved that there exist insoluble groups of exponent 4. Since groups of exponent 4 are central-by-(4-Engel), his theorem proves the existence of insoluble, locally nilpotent, 4-Engel groups of exponent 4. As mentioned above, Bachmuth and Mochizuki [2] established the existence of insoluble, locally nilpotent, 3-Engel groups of exponent 5. But, as far as I am aware, up till now the existence of further examples has relied on Zelmanov’s solution of the restricted Burnside problem [7,8]. Zelmanov’s theorem implies that for any prime power $q$ the class of locally nilpotent groups of exponent $q$ forms a variety $B_q$, and from the results mentioned above we know that $B_q$ is insoluble for $q = 4$ and for prime $q \geq 5$. Razmyslov [5] also proved that $B_9$ is insoluble. These varieties are all Engel varieties, since the two generator groups in these varieties are nilpotent of bounded class. So there are insoluble, locally nilpotent, Engel groups of exponent $q$ for $q = 4, 9$ and for prime $q \geq 5$. However, the Engel length of these groups is quite large—groups in $B_5$ (for example) are 6-Engel, and groups in $B_7$ are 10-Engel.

1. Razmyslov’s algebra

As mentioned above, Razmyslov refined his construction of insoluble, locally nilpotent groups of exponent $p$ in [5], and we refer the reader to that paper for details. Chapter 4 of my book [6] also contains a detailed treatment of Razmyslov’s construction. Razmyslov defines an associative algebra $A$, and then establishes a number of properties of this algebra. We give a full definition of the algebra $A$ in this note. We then state the key properties that we need, referring the reader to [5] and [6] for proofs of these properties.

Let $M_2$ be the full $2 \times 2$ matrix algebra over the complex field $\mathbb{C}$. Let $F$ be the commutative algebra over $\mathbb{C}$ with generators $x_{i1}, x_{i2}, x_{i3}$ for $i = 1, 2, \ldots$, and defining relations

$$x_{ij}x_{ik} = \delta_{jk}x_{i1}^2 \quad (i = 1, 2, \ldots, 1 \leq j, k \leq 3)$$

where $\delta_{jk}$ is the Kronecker symbol. It follows from these defining relations that

$$x_{i1}^3 = x_{i1}^2 x_{i1} = x_{i2}^2 x_{i1} = x_{i2}(x_{i2}x_{i1}) = 0$$

and hence that

$$x_{ir}x_{is}x_{it} = 0$$

for all $r, s, t \in \{1, 2, 3\}$. We denote the matrices

$$\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

in $M_2$ by $e_1, e_2, e_3$, and we form $F \otimes_{\mathbb{C}} M_2$. We let $A$ be the associative subalgebra of $F \otimes_{\mathbb{C}} M_2$ generated by the elements

$$x_i = x_{i1}e_1 + x_{i2}e_2 + x_{i3}e_3 \quad (i = 1, 2, \ldots).$$
We can think of $A$ as a Lie algebra over $\mathbb{C}$ under the operations of scalar multiplication, addition, and bracket multiplication $[x, y] = xy - yx$, and we let $H$ be the Lie subalgebra of $A$ generated by $x_1, x_2, \ldots$. Note that $[e_2, e_3] = 2e_1$, $[e_3, e_1] = 2e_2$, $[e_1, e_2] = 2e_3$, so that the elements of $H$ can all be expressed in the form $c_1 e_1 + c_2 e_2 + c_3 e_3$ with $c_1, c_2, c_3 \in F$. Also note that $x_2^2 \neq 0$.

We now state a number of properties of the algebra $A$.

**Lemma 3.** (See [5, Proposition 1], [6, Lemma 4.2.3].) If $x, y, z, v \in H$ and $i \geq 1$, then

1. $[(x \circ y), z] = 0$,
2. $x_i v x_i = -\frac{1}{1} v x_i^2$,
3. $x_i^3 = 0$,

where $(x \circ y) = xy + yx$.

All the remaining properties of $A$ that we need follow from the fact that $A$ is an associative algebra over $\mathbb{C}$ generated by $x_1, x_2, \ldots$, and that $A$ satisfies Lemma 3, and that $x_1^2 x_2^2 \ldots x_n^2 \neq 0$. The development from this point on in [5] and in [6] is very slightly different, and we will follow [6]. So we will refer to [6] for the proofs, when necessary.

**Lemma 4.** If $i, j \geq 1$ then $(x_i \circ x_j)x_i = \frac{2}{3} x_j x_i^2$.

**Proof.** This follows immediately from Lemma 3.

**Lemma 5.** If $i_1, i_2, \ldots, i_n \geq 1$ then

$$x_{i_1} x_{i_2} \ldots x_{i_n} x_i = \sum_{\sigma \in \text{Sym}(n)} \frac{1}{3} \alpha_\sigma x_{i_{\sigma(1)}} x_{i_{\sigma(2)}} \ldots x_{i_{\sigma(n)}} x_i^2$$

for some integers $\alpha_\sigma$ such that $\sum_{\sigma \in \text{Sym}(n)} \alpha_\sigma$ equals $3$ if $n$ is even, and equals $-1$ if $n$ is odd.

**Proof.** We express $x_i x_{i_1} x_{i_2} \ldots x_{i_n} x_i$ as an alternating sum

$$(x_i \circ x_{i_1})x_{i_2} \ldots x_{i_n} x_i - x_{i_1}(x_i \circ x_{i_2}) \ldots x_{i_n} x_i + \cdots$$

$$+ (-1)^n x_{i_1} x_{i_2} \ldots (x_i \circ x_{i_n}) x_i + (-1)^n x_{i_1} x_{i_2} \ldots x_{i_n} x_i^2.$$

The $r$th term in this sum is

$$(-1)^{r-1} x_{i_1} x_{i_2} \ldots x_{i_{r-1}} (x_i \circ x_{i_r}) x_{i_{r+1}} \ldots x_{i_n} x_i$$

and, since $(x_i \circ x_{i_r})$ is central by Lemma 3, this term equals

$$(-1)^{r-1} x_{i_1} x_{i_2} \ldots x_{i_{r-1}} x_{i_{r+1}} \ldots x_{i_n} (x_i \circ x_{i_r}) x_i = (-1)^{r-1} \frac{2}{3} x_{i_1} x_{i_2} \ldots x_{i_{r-1}} x_{i_{r+1}} \ldots x_{i_n} x_i^2.$$
We now let \( M \) be the closure of \( x_1, x_2, \ldots \) under the operations of addition, subtraction, \( \frac{1}{2}[x, y] \), and \( \frac{1}{2}(x \circ y) \). Note that \( M \) is closed under multiplication since \( xy = \frac{1}{2}[x, y] + \frac{1}{2}(x \circ y) \). The algebra \( M \) is multigraded, and it turns out that if \( a \in M \) is a multihomogeneous element with multiweight \( (w_1, w_2, \ldots, w_m) \) in the generators \( x_1, x_2, \ldots, x_m \) then \( a = 0 \) if \( w_i \geq 3 \) for any \( i \). This follows easily from Lemma 5 above. This lemma shows that any monomial in \( x_1, x_2, \ldots, x_m \) with multiweight \( (w_1, w_2, \ldots, w_m) \) (with \( w_i \geq 3 \)) can be expressed as a linear combination of monomials of the form \( bx_i^2 \) where \( b \) has multiweight \( (w_1, w_2, \ldots, w_i - 2, \ldots, w_m) \). Since \( x_i^2 \) is central, and since \( x_i^3 = 0 \), any monomial \( bx_i^3 \) of this form must equal zero.

If \( S \) and \( T \) are disjoint subsets of the generating set \( x_1, x_2, \ldots \) with \( S \cup T \) non-empty then we let \( SMT \) be the multihomogeneous component of \( M \) consisting of elements of weight \( |S| + 2|T| \) which have weight 1 in each of the generators occurring in \( S \), and have weight 2 in the generators occurring in \( T \). If \( S \) is empty then we use the notation \( M_T \), and if \( T \) is empty then we use the notation \( S_M \). As we have seen,

\[
M = \bigoplus_{S,T} SMT.
\]

**Lemma 6.** (See [6, Lemma 4.3.1].) If \( a \in SMT \) with \( S \) non-empty then \( a = b(\prod_{x \in T} x^2) \) for some \( b \in SM \), and if \( a \in MT \) then \( a = 3k(\prod_{x \in S} x^2) \) for some integer \( k \).

This lemma allows us to define a bilinear coupling on pairs of elements of \( S_M \). If \( f, g \in S_M \) then Lemma 6 implies that \( fg = 3k(\prod_{x \in S} x^2) \) for some integer \( k \). Since \( \prod_{x \in S} x^2 \neq 0 \) this integer \( k \) is uniquely defined, and we set \( \langle f, g \rangle = k \).

**2. Some insoluble varieties of Lie rings**

Let \( \Lambda \) be the free Lie ring freely generated by \( y_1, y_2, \ldots \), and let \( L \) be the Lie subring of \( M \) generated by \( x_1, x_2, \ldots \) with the Lie product of two elements \( x, y \in L \) defined to be \( \frac{1}{2}[x, y] \). Let \( \pi \) be the homomorphism from \( \Lambda \) onto \( L \) mapping \( y_i \) to \( x_i \) for \( i = 1, 2, \ldots \). Note that \( [y_{11}, y_{12}, \ldots, y_{ik}]\pi = 2^{-1} [x_{i1}, x_{i2}, \ldots, x_{ik}] \). Also note that if \( u \in \Lambda \) is multilinear in \( y_i, y_j, \ldots, y_k \) then \( u\pi \in L \cap S_M \) where \( S = \{x_i, x_j, \ldots, x_k\} \). If \( p \geq 5 \) is prime, then we define a set \( V_p \) of multilinear elements of \( \Lambda \) as follows:

**Definition 7.** If \( u \in \Lambda \) is multilinear in the generators \( y_i, y_j, \ldots, y_k \) then we set \( S = \{x_i, x_j, \ldots, x_k\} \), and we let \( u \in V_p \) if \( p \) divides \( \langle u\pi, g \rangle \) for all \( g \in S_M \).

Razmyslov proves two key properties of the sets \( V_p \), as stated in the following two lemmas.

**Lemma 8.** (See [6, Lemma 4.4.1].) If \( v \) is a multilinear element of \( \Lambda \) with the property that the identity \( v = 0 \) is a consequence of the identities \( \{u = 0 | u \in V_p\} \), then \( v \in V_p \).

**Lemma 9.** (See [6, Lemma 4.4.2].) If we let \( \delta_n \) be the derived length \( n \) word in the free generators \( y_1, y_2, \ldots, y_{2n} \) of \( \Lambda \), then \( \delta_n \notin V_p \) for any \( n \geq 1 \).

Here

\[
\delta_1 = [y_1, y_2];
\delta_2 = [[y_1, y_2], [y_3, y_4]];
\delta_3 = [[[y_1, y_2], [y_3, y_4]], [[y_5, y_6], [y_7, y_8]]].
\]
and so on. Note that \(py_1 \in V_p\), so the class of Lie rings satisfying the identical relations \(u = 0\) for all \(u \in V_p\) forms an insoluble variety of Lie rings of characteristic \(p\). These Lie rings can be thought of as Lie algebras over \(GF(p)\). We let \(\mathcal{U}_p\) denote this variety. Razmyslov proves that if \(p \geq 5\), then
\[
\sum_{\sigma \in \text{Sym}(p-2)} [y_{p-1}, y_1^\sigma, y_2^\sigma, \ldots, y_{(p-2)^\sigma}] \in V_p.
\]
(This is Lemma 4.4.4 from [6].) This shows that \(\mathcal{U}_p\) is an insoluble variety of \((p-2)\)-Engel Lie algebras over \(GF(p)\). Gunnar Traustason has pointed out to me in private communication that we do not need Lemma 9 to prove that \(\mathcal{U}_p\) is an insoluble variety. There is a theorem of Higgins [3] which implies that soluble \((p-2)\)-Engel Lie algebras over \(GF(p)\) are nilpotent. So to show that \(\mathcal{U}_p\) is insoluble we only have to show that it is not nilpotent. Lemma 3 easily implies that
\[
[x_1, x_2, \ldots, x_{n-1}, x_n]x_n x_{n-1} \ldots x_1
= [x_1, x_2, \ldots, x_{n-1}]x_n x_{n-1} \ldots x_1 - x_n[x_1, x_2, \ldots, x_{n-1}]x_n x_{n-1} \ldots x_1
= \frac{4}{3} x_n^2 [x_1, x_2, \ldots, x_{n-1}]x_n x_{n-1} \ldots x_1,
\]
and an easy induction then gives
\[
[x_1, x_2, \ldots, x_{n-1}, x_n]x_n x_{n-1} \ldots x_1 = \left(\frac{4}{3}\right)^{n-1} x_1^2 x_2^2 \ldots x_n^2.
\]
It follows that
\[
\langle [y_1, y_2, \ldots, y_n]x_n x_{n-1} \ldots x_1 \rangle = 2^{n-1},
\]
so that \([y_1, y_2, \ldots, y_n] \notin V_p\).

Before stating our next lemma we need to introduce some notation. Let \(A\) be a finite set of positive integers. If \(A = \{i, j, \ldots, k\}\) with \(i < j < \cdots < k\), and if \(a \in A\), then we define
\[
[a, y_A] = [a, y_i, y_j, \ldots, y_k].
\]
If \(A\) is empty, then we set
\[
[a, y_A] = a.
\]
Now let \(n \geq p - 1\) and let \(A_1, A_2, \ldots, A_{p-2}\) be pairwise disjoint sets of positive integers with
\[
A_1 \cup A_2 \cup \cdots \cup A_{p-2} = \{p-1, p, \ldots, n-1\}.
\]
So
\[
[y_n, y_{A_1}, y_1, y_{A_2}, y_2, \ldots, y_{A_{p-2}}, y_{p-2}]
\]
is a multilinear left-normed Lie product in the generators \(y_1, y_2, \ldots, y_n\). In Section 3 of this article we prove the following lemma.
Lemma 10.

\[
\sum_{\sigma \in \text{Sym}(p-2)} [y_n, y_{A_1}, y_{A_2}, y_{A_3}, \ldots, y_{A_{p-2}}, y_{(p-2)\sigma}] \in V_p.
\]

Note that if \( n = p - 1 \) and the subsets \( A_1, A_2, \ldots, A_{p-2} \) are all empty, then this is Razmyslov's result that

\[
\sum_{\sigma \in \text{Sym}(p-2)} [y_n, y_{A_1}, y_{A_2}, y_{A_3}, \ldots, y_{A_{p-2}}, y_{(p-2)\sigma}] \in V_p.
\]

Razmyslov's result implies that Lie algebras in \( \mathfrak{u}_p \) are \((p-2)\)-Engel Lie algebras, but Lemma 10 implies the stronger result that if \( C \) is a Lie algebra in \( \mathfrak{u}_p \), and if \( c \in C \), then the ideal of \( C \) generated by \( c \) is nilpotent of class at most \( p - 3 \).

We actually need an even stronger result, which is quite easy to deduce from Lemma 10.

Lemma 11. Let \( n > m \geq p - 2 \), and let \( A_1, A_2, \ldots, A_{p-2} \) be pairwise disjoint sets of positive integers with

\[
A_1 \cup A_2 \cup \cdots \cup A_{p-2} = \{m + 1, m + 2, \ldots, n - 1\}.
\]

Then

\[
\sum_{\sigma \in \text{Sym}(p-2)} [y_n, y_{A_1}, y_{B_1}, y_{A_2}, y_{B_2}, \ldots, y_{A_{p-2}}, y_{B_{p-2}}] \in V_p,
\]

where the sum is taken over all partitions of \( \{1, 2, \ldots, m\} \) into an ordered sequence of pairwise disjoint, non-empty subsets \( B_1, B_2, \ldots, B_{p-2} \).

Proof. Note that each partition of \( \{1, 2, \ldots, m\} \) into pairwise disjoint, non-empty subsets yields \((p-2)!\) choices of \( B_1, B_2, \ldots, B_{p-2} \) as the subsets are permuted among themselves. Note also that if \( m = p - 2 \) then all the subsets \( B_1, B_2, \ldots, B_{p-2} \) must be one element subsets, so that Lemma 11 reduces to Lemma 10.

We prove Lemma 11 by induction on \( m \), the base case being Lemma 10. Let \( m > p - 2 \), and assume the lemma is proved for smaller values of \( m \). Let

\[
s = \sum [y_n, y_{A_1}, y_{B_1}, y_{A_2}, y_{B_2}, \ldots, y_{A_{p-2}}, y_{B_{p-2}}],
\]

where the sum is taken over all partitions of \( \{1, 2, \ldots, m\} \) into an ordered sequence of pairwise disjoint, non-empty subsets \( B_1, B_2, \ldots, B_{p-2} \). Note that

\[
s = s(y_1, y_2, \ldots, y_m, y_{m+1}, \ldots, y_n)
\]

is multilinear in the generators \( y_1, y_2, \ldots, y_n \). We now define an element

\[
t = t(y_1, y_2, \ldots, y_{m-1}, y_{m+1}, \ldots, y_n)
\]

which is multilinear in the generators \( y_1, y_2, \ldots, y_{m-1}, y_{m+1}, \ldots, y_n \) by setting

\[
t = \sum [y_n, y_{A_1}, y_{B_1}, y_{A_2}, y_{B_2}, \ldots, y_{A_{p-2}}, y_{B_{p-2}}].
\]
where this sum is taken over all partitions of \(\{1, 2, \ldots, m-1\}\) into an ordered sequence of pairwise disjoint, non-empty subsets \(B_1, B_2, \ldots, B_{p-2}\). By our inductive hypothesis, \(t \in V_p\). We show that \(s\) is symmetric in the generators \(y_1, y_2, \ldots, y_m\) modulo consequences of the identical relation \(t = 0\).

So let \(1 \leq i < m\), and consider

\[
s(y_1, \ldots, y_i, y_{i+1}, \ldots, y_n) - s(y_1, \ldots, y_{i+1}, y_i, \ldots, y_n).
\]

In some of the summands in (1), \(i\) and \(i+1\) are in different subsets \(B_j\), and in other summands \(i\) and \(i+1\) are in the same subset. So we can write \(s = s_1 + s_2\), where \(s_1\) is the sum of all the terms

\[
[y_n, y_{A_1}, y_{B_1}, y_{A_2}, y_{B_2}, \ldots, y_{A_{p-2}}, y_{B_{p-2}}]
\]

where \(i\) and \(i+1\) are in different subsets, and where \(s_2\) is the sum of all the terms where \(i\) and \(i+1\) are in the same subset. Note that the terms

\[
[y_n, y_{A_1}, y_{B_1}, y_{A_2}, y_{B_2}, \ldots, y_{A_{p-2}}, y_{B_{p-2}}]
\]

where \(i\) and \(i+1\) lie in the same subset all have the form

\[
[y_n, \ldots, y_i, y_{i+1}, \ldots].
\]

Interchanging \(y_i\) and \(y_{i+1}\) leaves \(s_1\) unchanged, but changes every summand

\[
[y_n, \ldots, y_i, y_{i+1}, \ldots]
\]

in \(s_2\) into \([y_n, \ldots, y_{i+1}, y_i, \ldots]\). So

\[
s(y_1, \ldots, y_i, y_{i+1}, \ldots, y_n) - s(y_1, \ldots, y_{i+1}, y_i, \ldots, y_n)
= t(y_1, \ldots, [y_i, y_{i+1}], \ldots, y_n)
\in V_p \quad \text{by Lemma 8.}
\]

This implies

\[
(p-2)!s - \sum_{\sigma \in \text{Sym}(p-2)} s(y_{1\sigma}, y_{2\sigma}, \ldots, y_{(p-2)\sigma}, y_{p-1}, \ldots, y_m, \ldots, y_n) \in V_p.
\]

But

\[
\sum_{\sigma \in \text{Sym}(p-2)} s(y_{1\sigma}, y_{2\sigma}, \ldots, y_{(p-2)\sigma}, y_{p-1}, \ldots, y_m, \ldots, y_n) \in V_p
\]

by Lemma 10, and so \(s \in V_p\). \(\Box\)
3. Proof of Lemma 10

Let \( n \geq p - 2 \), and let \( A_0, A_1, \ldots, A_{p-2} \) be monomials in the generators \( x_1, x_2, \ldots, x_n \) of \( A \). For each \( i = 0, 1, \ldots, p - 2 \), let \( A_i \) have multiweight \( w_i = (w_{i1}, w_{i2}, \ldots, w_{in}) \) in \( x_1, x_2, \ldots, x_n \), where

\[
w_0 + w_1 + \cdots + w_{p-2} = (1, 1, \ldots, 1, 2, 2, \ldots, 2).
\]

We allow the possibility that some of the \( A_i \) have length 0 and multiweight \((0, 0, \ldots, 0)\). So \( A_0 x_1 A_1 x_2 A_2 \ldots A_{p-3} x_{p-2} A_{p-2} \) has multiweight \((2, 2, \ldots, 2)\). Thus, by Lemma 6,

\[
A_0 x_1 A_1 x_2 A_2 \ldots A_{p-3} x_{p-2} A_{p-2} = \frac{k}{3^{n-1}} x_1^2 x_2^2 \cdots x_n^2
\]

for some integer \( k \). Lemma 10 follows immediately from the following result on associative products in the algebra \( A \).

Lemma 12.

\[
\sum_{\sigma \in \text{Sym}(p-2)} A_0 x_1 A_1 x_2 A_2 \ldots A_{p-3} x_{(p-2)\sigma} A_{p-2} = \frac{pk}{3^{n-1}} x_1^2 x_2^2 \cdots x_n^2
\]

for some integer \( k \).

Proof. The proof is by induction on \( n \). Note that since \( n \geq p - 2 \), the base case for the induction is when \( n = p - 2 \), and we consider this case first.

So let \( n = p - 2 \). Suppose first that \( A_0, A_1, \ldots, A_{p-3} \) all have length 0, and that \( A_{p-2} \) has length \( p - 2 \). There is no loss in generality in assuming that \( A_{p-2} = x_{p-2} x_{p-3} \cdots x_1 \), so that we need to consider the sum

\[
\sum_{\sigma \in \text{Sym}(p-2)} x_{1\sigma} x_{2\sigma} \cdots x_{(p-2)\sigma} x_{p-2} x_{p-3} \cdots x_1.
\]

We split this sum up into \( p - 2 \) separate sums

\[
\sum_{\sigma \in \text{Sym}(p-3)} x_{p-2} x_{1\sigma} x_{2\sigma} \cdots x_{(p-3)\sigma} x_{p-2} x_{p-3} \cdots x_1
\]

\[
+ \sum_{\sigma \in \text{Sym}(p-3)} x_{1\sigma} x_{p-2} x_{2\sigma} \cdots x_{(p-3)\sigma} x_{p-2} x_{p-3} \cdots x_1
\]

\[
+ \cdots
\]

\[
+ \sum_{\sigma \in \text{Sym}(p-3)} x_{1\sigma} x_{2\sigma} \cdots x_{(p-3)\sigma} x_{p-2} x_{p-3} \cdots x_1.
\]

By Lemma 5 this equals

\[
\left(1 - \frac{1}{3} + 1 - \frac{1}{3} + 1 - \cdots + 1\right) \sum_{\sigma \in \text{Sym}(p-3)} x_{1\sigma} x_{2\sigma} \cdots x_{(p-3)\sigma} x_{p-3} \cdots x_1 x_{p-2}^2.
\]
The sum in the brackets in this expression equals
\[
\frac{p-1}{2} \times 1 - \frac{p-3}{2} \times \frac{1}{3} = \frac{p}{3},
\]
so
\[
\sum_{\sigma \in \text{Sym}(p-2)} x_{1\sigma} x_{2\sigma} \ldots x_{(p-2)\sigma} x_{p-2} x_{p-3} \ldots x_1 = \frac{p}{3} \sum_{\sigma \in \text{Sym}(p-3)} x_{1\sigma} x_{2\sigma} \ldots x_{(p-3)\sigma} x_{p-3} \ldots x_1 x_{p-2}^2
\]
\[
= \frac{p k}{3p-3} x_1^2 x_2^2 \ldots x_{p-2}^2
\]
for some integer \(k\), by Lemma 6.

Now consider the case when \(n = p - 2\), and at least one of \(A_0, A_1, \ldots, A_{p-3}\) has positive length. We show that the lemma still holds in this case by reverse induction on the length of \(A_{p-2}\). (The case we have already dealt with when \(A_{p-2}\) has length \(p-2\) is the base case for the induction.) Suppose that \(A_r (r < p-2)\) has positive length, but that \(A_{r+1}, A_{r+2}, \ldots, A_{p-3}\) have zero length. Write \(A_r = B x_{i}\).

There is no loss in generality in taking \(i = p - 2\). So
\[
\sum_{\sigma \in \text{Sym}(p-2)} A_0 x_{1\sigma} A_1 x_{2\sigma} A_2 \ldots A_{p-3} x_{(p-2)\sigma} A_{p-2}
\]
\[
= \sum_{\sigma \in \text{Sym}(p-2)} A_0 x_{1\sigma} \ldots x_{r\sigma} B x_{p-2} x_{(r+1)\sigma} \ldots x_{(p-2)\sigma} A_{p-2}.
\]

Now \(x_{p-2} x_{(r+1)\sigma} \ldots x_{(p-2)\sigma}\) can be expressed as an alternating sum
\[
(x_{p-2} \circ x_{(r+1)\sigma}) \ldots x_{(p-2)\sigma} - x_{(r+1)\sigma} (x_{p-2} \circ x_{(r+2)\sigma}) \ldots x_{(p-2)\sigma} + \cdots
\]
\[
\pm x_{(r+1)\sigma} \ldots x_{(p-3)\sigma} (x_{p-2} \circ x_{(p-2)\sigma}) \mp x_{(r+1)\sigma} \ldots x_{(p-2)\sigma} x_{p-2}.
\]

By our reverse induction on the length of \(A_{p-2}\) we know that
\[
\sum_{\sigma \in \text{Sym}(p-2)} A_0 x_{1\sigma} \ldots x_{r\sigma} B x_{(r+1)\sigma} \ldots x_{(p-2)\sigma} x_{p-2} A_{p-2} = \frac{p k}{3p-3} x_1^2 x_2^2 \ldots x_{p-2}^2
\]
for some integer \(k\), and so we only need to consider terms of the form
\[
\sum_{\sigma \in \text{Sym}(p-2)} A_0 x_{1\sigma} \ldots x_{s\sigma} B x_{(r+1)\sigma} \ldots x_{(p-2)\sigma} A_{p-2}
\]
where \(r + 1 \leq s \leq p - 2\). Using the fact that \(x_{p-2} \circ x_{s\sigma}\) is central we can write this as
\[
\sum_{\sigma \in \text{Sym}(p-2)} (x_{p-2} \circ x_{s\sigma}) A_0 x_{1\sigma} \ldots x_{s\sigma} B x_{(r+1)\sigma} \ldots x_{(p-2)\sigma} A_{p-2},
\]
and then changing notation slightly we can express this as
\[
\sum_{\sigma \in \text{Sym}(p-2)} (x_{p-2} \circ x_{1\sigma}) B_1 x_{2\sigma} B_2 x_{3\sigma} B_3 \ldots B_{p-3} x_{(p-2)\sigma} B_{p-2}
\]
for some monomials \( B_1, B_2, \ldots, B_{p-2} \). We split this sum into \( p-2 \) separate sums

\[
\sum_{\sigma \in \text{Sym}(p-3)} (x_{p-2} \circ x_{p-2}) B_1 x_{1\sigma} B_2 x_{2\sigma} \cdots B_{p-3} x_{(p-3)\sigma} B_{p-2}
\]

\[
+ \sum_{\sigma \in \text{Sym}(p-3)} (x_{p-2} \circ x_{1\sigma}) B_1 x_{p-2} B_2 x_{2\sigma} B_3 \cdots B_{p-3} x_{(p-3)\sigma} B_{p-2}
\]

\[
+ \cdots
\]

\[
+ \sum_{\sigma \in \text{Sym}(p-3)} (x_{p-2} \circ x_{1\sigma}) B_1 x_{2\sigma} B_2 x_{3\sigma} B_3 \cdots x_{(p-3)\sigma} B_{p-3} x_{p-2} B_{p-2}.
\]

The first of these \( p-2 \) separate sums equals

\[
2 x_{p-2}^2 \sum_{\sigma \in \text{Sym}(p-3)} B_1 x_{1\sigma} B_2 x_{2\sigma} \cdots B_{p-3} x_{(p-3)\sigma} B_{p-2}.
\]

Using the fact that \((x_{p-2} \circ x_{1\sigma})\) is central, we see that the second sum equals

\[
\sum_{\sigma \in \text{Sym}(p-3)} B_1 (x_{p-2} \circ x_{1\sigma}) x_{p-2} B_2 x_{2\sigma} B_3 \cdots B_{p-3} x_{(p-3)\sigma} B_{p-2}
\]

\[
= \frac{2}{3} x_{p-2}^2 \sum_{\sigma \in \text{Sym}(p-3)} B_1 x_{1\sigma} B_2 x_{2\sigma} \cdots B_{p-3} x_{(p-3)\sigma} B_{p-2}.
\]

Similarly, we see that the remaining \( p-4 \) separate sums are all equal to

\[
\frac{2}{3} x_{p-2}^2 \sum_{\sigma \in \text{Sym}(p-3)} B_1 x_{1\sigma} B_2 x_{2\sigma} \cdots B_{p-3} x_{(p-3)\sigma} B_{p-2}.
\]

Lemma 6 implies that

\[
\sum_{\sigma \in \text{Sym}(p-3)} B_1 x_{1\sigma} B_2 x_{2\sigma} \cdots B_{p-3} x_{(p-3)\sigma} B_{p-2} = \frac{k}{3^{p-4}} x_1^2 x_2^2 \cdots x_{p-3}^2
\]

for some integer \( k \), and so

\[
\sum_{\sigma \in \text{Sym}(p-2)} (x_{p-2} \circ x_{1\sigma}) B_1 x_{2\sigma} B_2 x_{3\sigma} B_3 \cdots B_{p-3} x_{(p-2)\sigma} B_{p-2}
\]

\[
= \left( 2 + (p-3) \right) \frac{2}{3} \frac{k}{3^{p-4}} x_1^2 x_2^2 \cdots x_{p-2}^2
\]

\[
= \frac{2pk}{3^{p-3}} x_1^2 x_2^2 \cdots x_{p-2}^2.
\]

This completes the proof of Lemma 12 for the base case \( n = p-2 \).
Now suppose that \( n > p - 2 \), and that the lemma holds true for \( n - 1 \). We consider the positions of the two occurrences of \( x_n \) in

\[
\sum_{\sigma \in \text{Sym}(p-2)} A_0 x_{1\sigma} A_1 x_{2\sigma} A_2 \ldots A_{p-3} x_{(p-2)\sigma} A_{p-2},
\]

and we use Lemma 5 which implies that

\[
x_n x_{i_1} x_{i_2} \ldots x_{i_m} x_n = \frac{1}{3} x_n^2 \sum_{\tau} \alpha_{\tau} x_{i_1\tau} x_{i_2\tau} \ldots x_{i_m\tau} \tag{2}
\]

for some permutations \( \tau \) of \( \{1, 2, \ldots, m\} \) and some integers \( \alpha_{\tau} \). So suppose that the two occurrences of \( x_n \) are in \( A_r \) and \( A_s \) for some \( r \leq s \).

If \( r = s \) then

\[
A_r = \frac{1}{3} x_n^2 \sum_{\tau} \alpha_{\tau} B_{\tau}
\]

for some integers \( \alpha_{\tau} \) and some monomials \( B_{\tau} \). So

\[
\sum_{\sigma \in \text{Sym}(p-2)} A_0 x_{1\sigma} \ldots x_{r\sigma} A_r x_{(r+1)\sigma} \ldots A_{p-3} x_{(p-2)\sigma} A_{p-2}
\]

\[
= \frac{1}{3} x_n^2 \sum_{\tau} \alpha_{\tau} \left( \sum_{\sigma \in \text{Sym}(p-2)} A_0 x_{1\sigma} \ldots x_{r\sigma} B_{\tau} x_{(r+1)\sigma} \ldots A_{p-3} x_{(p-2)\sigma} A_{p-2} \right)
\]

\[
= \frac{p}{3} x_n^2 \sum_{i=1}^{n-1} x_i^2
\]

for some integer \( k \), by induction on \( n \).

On the other hand, if \( r < s \) then write \( A_r = B x_n C \), \( A_s = D x_n E \). So

\[
\sum_{\sigma \in \text{Sym}(p-2)} A_0 x_{1\sigma} A_1 x_{2\sigma} A_2 \ldots A_{p-3} x_{(p-2)\sigma} A_{p-2}
\]

\[
= \sum_{\sigma \in \text{Sym}(p-2)} A_0 x_{1\sigma} \ldots x_{r\sigma} B x_n C x_{(r+1)\sigma} \ldots x_{s\sigma} D x_n E \ldots x_{(p-2)\sigma} A_{p-2}.
\]

We apply Eq. (2) with \( x_{i_1} x_{i_2} \ldots x_{i_m} = C x_{(r+1)\sigma} \ldots x_{s\sigma} D \), and this shows that

\[
\sum_{\sigma \in \text{Sym}(p-2)} A_0 x_{1\sigma} A_1 x_{2\sigma} A_2 \ldots A_{p-3} x_{(p-2)\sigma} A_{p-2}
\]

is an integral linear combination of terms of the form

\[
\frac{1}{3} x_n^2 \sum_{\sigma \in \text{Sym}(p-2)} A_0 x_{1\sigma} \ldots x_{r\sigma} B \ldots x_{(r+1)\sigma} \ldots x_{s\sigma} \ldots E \ldots x_{(p-2)\sigma} A_{p-2}.
\]
By induction on \( n \) every term of the form

\[
\sum_{\sigma \in \text{Sym}(p-2)} A_0 x_{1\sigma} \cdots x_{r\sigma} B \cdots x_{(r+1)\sigma} \cdots x_{s\sigma} \cdots E \cdots x_{(p-2)\sigma} A_{p-2}
\]

equals \( \frac{p^k}{3^2} x_1^2 x_2^2 \cdots x_{p-1}^2 \) for some integer \( k \).

This completes the inductive step, and so completes the proof of Lemma 12. \( \square \)

4. Proof of Theorem 2

There are various ways to construct insoluble, locally nilpotent, \((p-2)\)-Engel groups of exponent \( p \). One way is follows. Let \( F \) be the free Lie algebra of the variety \( U_p \) of countably infinite rank, with free generators \( y_1, y_2, \ldots \). Since the identical relations defining the variety \( U_p \) are all multilinear, \( F \) is multigraded, and is a direct sum of multihomogeneous components. Let \( I \) be the ideal of \( F \) generated by all Lie products of the generators which have a repeated entry. In other words, if we let \( A_i \) be the ideal of \( F \) generated by \( y_i \), we let \( I = \sum_{i=1}^{\infty} [A_i, A_i] \). Let \( L = F/I \). Now pick a vector space basis \( b_1, b_2, \ldots \) for \( L \) consisting of left-normed Lie products in the generators \( y_1 + I, y_2 + I, \ldots \). For each pair of basis elements \( b_i, b_j \) with \( i > j \) we obtain a relation

\[
[b_i, b_j] = \sum_k \alpha_{ijk} b_k
\]

where \( 0 \leq \alpha_{ijk} < p \) for all \( i, j, k \). Now we let \( G \) be the group with generators \( a_1, a_2, \ldots \), with power relations

\[
a_i^p = 1 \quad \text{for} \quad i = 1, 2, \ldots ,
\]

and with commutator relations

\[
[a_i, a_j] = \prod_k \alpha_{ijk} a_k \quad \text{for} \quad i > j.
\]

This is a consistent power-commutator presentation, and \( G \) is an insoluble, locally nilpotent, \((p-2)\)-Engel group of exponent \( p \). In addition, if \( g \in G \), then the normal closure of \( g \) is nilpotent of class at most \( p - 3 \). So \( G \) is an insoluble Fitting group with Fitting degree \( p - 3 \).

See Appendix B of [6] for a discussion of consistent power-commutator presentations. The basis chosen for \( L \) has the property that for each \( i = 1, 2, \ldots \) the ideal generated by \( b_i \) is abelian. It follows from this that the normal closure of \( a_i \) in \( G \) is elementary abelian for \( i = 1, 2, \ldots \). The fact that the presentation for \( G \) is consistent follows easily from this fact. Note that \( L \) is the associated Lie ring of \( G \), and that the fact that \( L \) is insoluble implies that \( G \) is insoluble.

To prove that the normal closure of an element \( g \in G \) is nilpotent of class at most \( p - 3 \), we need to show that if \( c \) is any left-normed commutator in \( G \) with \( p - 2 \) entries equal to \( g \), then \( c = 1 \). It is sufficient to consider the case when the entries other than \( g \) in the commutator \( c \) are defining generators from the set \( \{a_1, a_2, \ldots \} \). We adapt the notation used in Lemmas 10 and 11 to describe this situation. Thus if \( A \) is a finite ordered sequence \( (i_1, i_2, \ldots, i_k) \) of positive integers, and if \( h \in G \), then we set

\[
[h, a_A] = [h, a_{i_1}, a_{i_2}, \ldots, a_{i_k}].
\]
(We do not require $i_1 < i_2 < \cdots < i_k$.) If $A$ is the empty sequence then we let $[h, a_A] = h$. We need to show that if $n \geq 1$, and if $A_1, A_2, \ldots, A_{p-2}$ are finite ordered sequences of positive integers, then

$$[a_n, a_{A_1}, g, a_{A_2}, g, \ldots, a_{A_{p-2}}, g] = 1.$$  

Let $g = a_{j_1}a_{j_2} \ldots a_{j_m}$. If $d$ is any left-normed commutator in $G$, with entries from the generating set $\{a_1, a_2, \ldots\}$, then the normal closure of $d$ is abelian, and so

$$[d, g] = \prod [d, a_B].$$

where the product is taken over all non-empty ordered subsequences $B$ of the ordered sequence $(j_1, j_2, \ldots, j_m)$. Thus

$$[a_n, a_{A_1}, g, a_{A_2}, g, \ldots, a_{A_{p-2}}, g] = \prod [a_n, a_{A_1}, a_{B_1}, a_{A_2}, a_{B_2}, \ldots, a_{A_{p-2}}, a_{B_{p-2}}],$$

where the product is taken over all possible choices of non-empty ordered subsequences $B_1, B_2, \ldots, B_{p-2}$ of $(j_1, j_2, \ldots, j_m)$. If $a_i$ is one of the defining generators of $G$, then the normal closure of $a_i$ is abelian, and so we can assume that the ordered subsequences $B_1, B_2, \ldots, B_{p-2}$ are pairwise disjoint. But then Lemma 11 implies that

$$[a_n, a_{A_1}, g, a_{A_2}, g, \ldots, a_{A_{p-2}}, g] = 1.$$

It is now very easy to show that $G$ has exponent $p$. Let $b = a_{j_1}a_{j_2} \ldots a_{j_m} \in G$. We show by induction on $m$ that $b^p = 1$. Certainly this is true for $m = 1$, since the defining generators of $G$ all have order $p$. So suppose that this is true for $m - 1$ and let $g = a_{j_1}a_{j_2} \ldots a_{j_{m-1}}$. By induction, we have $g^p = 1$. Since the normal closure of $a_{j_m}$ in $G$ is elementary abelian we see that

$$b^p = (ga_{j_m})^p$$

$$= g^p a_{j_m}^p [a_{j_m}, g]^{(p)}[a_{j_m}, g, g]^{(p)} \cdots [a_{j_m}, g, g, \ldots, g]^{(p)}[a_{j_m}, g, g, \ldots, g]^{(p-1)}$$

$$= 1.$$

So $G$ has exponent $p$, as claimed.

References