MILD PRO-p-GROUPS AND GALOIS GROUPS OF p-EXTENSIONS OF $\mathbb{Q}$

JOHN LABUTE

ABSTRACT. In this paper we introduce a new class of finitely presented pro-p-groups G of cohomological dimension 2 called mild groups. If $d(G), r(G)$ are respectively the minimal number of generators and relations of G, we give an infinite family of mild groups G with $r(G) \geq d(G)$ and $d(G) \geq 2$ arbitrary. These groups can be constructed with $G/[G,G]$ finite, answering a question of Kuzmin. If $G = G_S(p)$ is the Galois group of the maximal p-extension of $\mathbb{Q}$ unramified outside a finite set of primes S and $p \neq 2$, we show that G is mild for a co-final class of sets S, even in the case $p \notin S$.

To John Tate

1. Statement of Results

1.1. **Mild pro-p-groups.** Let p be a prime number; for simplicity, we assume that p is odd. Let $G = F/R$ be a finitely presented pro-p-group with F the free pro-p-group on $x_1, \ldots, x_m$ and $R = (r_1, \ldots, r_d)$ the closed normal subgroup generated by nonidentity elements $r_1, \ldots, r_d \in F^p[F,F]$, where $[F,F]$ is the closed subgroup generated by the commutators $[x,y] = x^{-1}y^{-1}xy$. Let $d(G) = \dim_{\mathbb{F}_p} H^1(G, \mathbb{Z}/p\mathbb{Z})$ and $r(G) = \dim_{\mathbb{F}_p} H^2(G, \mathbb{Z}/p\mathbb{Z})$. Then $d(G), r(G)$ are respectively the minimal number of generators and relations for G (cf.[26]). For the above presentation $G = F/R$ we have $d(G) = m$. The presentation is said to be minimal if $r(G) = d$.

The lower p-central series $(G_n)_{n\geq 1}$ of a pro-p-group G is defined inductively by $G_1 = G$, $G_{n+1} = G_n^p[G, G_n]$. The quotient groups $\mathrm{gr}_n(G)$, denoted additively, are vector spaces over the finite field $\mathbb{F}_p$. The graded vector space

$$\mathrm{gr}(G) = \oplus_{n\geq 1}\mathrm{gr}_n(G)$$

has a Lie algebra structure over the polynomial ring $\mathbb{F}_p[\pi]$, where multiplication by π is induced by $x \mapsto x^p$ and the bracket operation for homogeneous elements is induced by the commutator operation in G (cf.[22]).

If ξ_i is the image of x_i in $\mathrm{gr}_1(F)$ then $\mathrm{gr}(F)$ is the free Lie algebra on $\xi_1, \ldots, \xi_m$ over $\mathbb{F}_p[\pi]$. If $r \in F$, $r \neq 1$, and n is largest with $r \in F_n$ then $n = \omega(r)$ is called the filtration degree of r and the image of r in $\mathrm{gr}_n(F)$ is called the initial form of r. Let $h_i = \omega(r_i)$ and let $\rho_i \in \mathrm{gr}_{h_i}(F)$ be the initial form of r_i. If $\mathfrak{r}$ is the ideal of $L = \mathrm{gr}(F)$ generated

Date: February 26, 2006.

1991 *Mathematics Subject Classification.* 11R34, 20E15, 12G10, 20F05, 20F14, 20F40.

This paper was written while on leave at the Mathematics Department of the University of Western Ontario. We wish to thank the Department for providing a stimulating environment and excellent computer facilities . Special thanks to Jan Mináč for his enthusiastic support.

by $\rho_1, \ldots, \rho_d$ and $\mathfrak{g} = L/\mathfrak{r}$ then $\mathfrak{r}/[\mathfrak{r}, \mathfrak{r}]$ is a module over the enveloping algebra $U_{\mathfrak{g}}$ of $\mathfrak{g}$ via the adjoint representation.

Definition 1.1. The sequence $\rho_1, \ldots, \rho_d$ with $d \geq 1$ is said to be strongly free if $U_{\mathfrak{g}}$ is a free $\mathbb{F}_p[\pi]$-module and $M = \mathfrak{r}/[\mathfrak{r}, \mathfrak{r}]$ is a free $U_{\mathfrak{g}}$-module on the images of $\rho_1, \ldots, \rho_d$ in M. In this case we say that the presentation $G = F/R$ is strongly free. A pro-p-group is said to be mild if it has a strongly free presentation.

Let $U_{\mathfrak{g}}(t)$ be the Poincaré series of $U_{\mathfrak{g}}$ for the natural grading of $U_{\mathfrak{g}}$ by finite dimensional vector spaces over $\mathbb{F}_p$. If $\rho_1, \ldots, \rho_d$ is a strongly free sequence then

$$U_{\mathfrak{g}}(t) = \frac{1}{(1-t)(1 - mt + t^{h_1} + \ldots + t^{h_d})},$$

by Theorem 3.9 with $e_i = \deg(\xi_i) = 1$ for all i. If

The term *mild group* is due to Anick[2]. Mild groups have a lot of nice properties.

Theorem 1.2. *Let G be a mild group and $G = F/(r_1, \ldots, r_d)$ a strongly free presentation of G with F a free pro-p-group of rank m. Let ρ_i be the initial form of r_i and let $R = (r_1, \ldots, r_d)$. Then*

(a) $\mathrm{gr}(G) = \mathrm{gr}(F)/(\rho_1, \ldots, \rho_d)$.
(b) *$R/[R, R]$ is a free $\mathbb{Z}_p[[G]]$-module on the images of $r_1, \ldots, r_d$.*
(c) *The presentation $G = F/R$ is minimal and* $\mathrm{cd}(G) = 2$.
(d) *The enveloping algebra of* $\mathrm{gr}(G)$ *is the graded algebra* $\mathrm{gr}(B)$ *associated to the filtration of $B = \mathbb{Z}_p[[G]]$ by powers of the augmentation ideal* $\mathrm{Ker}(\mathbb{Z}_p[[G]] \to \mathbb{Z}/p\mathbb{Z})$.
(e) *The Poincaré series of* $\mathrm{gr}(B)$ *is* $1/(1-t)(1 - mt + t^{h_1} + \ldots + t^{h_d})$.

A related result is proved in [18] for discrete groups in the case of the lower central series. Theorem 1.2 can be proven in greater generality, including $p = 2$ in some cases (cf. Theorem 4.1). A proof for the case $p = 2$ can be found in [21]. That a mild group is of cohomological dimension 2 also follows from [15] and Theorem 3.10 (cf. Theorem 5.1).

Not much is known about mild groups but we produce a large supply of them (cf. Corollary 3.5). They also appear strikingly often as Galois groups of maximal p-extensions of $\mathbb{Q}$ with restricted ramification even when the ramification is tame.

1.2. **Galois groups of p-extensions of $\mathbb{Q}$ with restricted ramification.** Let S be a finite set of rational primes not containing the prime p and let $G_S(p)$ be the Galois group of the maximal p-extension of $\mathbb{Q}$ unramified outside S. If $p \neq 2$, we can assume that $S = \{q_1, \ldots, q_m\}$ with $q_i \equiv 1 \bmod p$. If $p = 2$, we have to assume that the infinite prime lies in S.

In [12],[14] Koch shows that $G = G_S(p)$ has a minimal presentation $G = F/R$ where F is the free pro-p-group on $x_1, \ldots, x_m$ and $R = (r_1, \ldots, r_m)$ with

$$r_i = x_i^{q_i - 1}[x_i^{-1}, y_i^{-1}], \quad y_i \equiv \prod_{j \neq i} x_j^{\ell_{ij}} \bmod F^p[F, F], \quad \ell_{ij} \in \mathbb{Z}/p\mathbb{Z},$$

where the image of x_i in G is a generator of the cyclic inertia group at a fixed place $\mathfrak{Q}_i$ above q_i and the image of y_i is a lifting of the Frobenius automorphism at q_i. We thus have

$$r_i \equiv x_i^{q_i-1} \prod_{j\neq i}[x_i, x_j]^{\ell_{ij}} \mod F_3.$$

The image of x_i in $F/[F,F] = G_S(p)/[G_S(p), G_S(p)]$ corresponds, under the reciprocity map, to an idele with component 1 at all places except for the component at q_i which is equal to g_i, a primitive root mod q_i. The image of y_i in $G_S(p)/[G_S(p), G_S(p)]$ corresponds to an idele with component q_i at the place q_i and component 1 at the other places. Then ℓ_{ij} is the image in $\mathbb{Z}/p\,\mathbb{Z}$ of any integer r satisfying

$$q_i \equiv g_j^{-r} \bmod q_j.$$

We call ℓ_{ij} the linking number of the pair (q_i, q_j). Note that if g is another primitive root mod q_j and $g_j \equiv g^c \bmod q_j$ then the linking number ℓ_{ij} would be multiplied by c if g were used instead of g_j.

There is an analogy between the arithmetic of $\mathbb{Z}$ and the topology of the 3-sphere S_3 in which ℓ_{ij} plays the role of the linking number of two loops in S_3 (cf. [28]). This analogy is not perfect as we can have $\ell_{ij} \neq \ell_{ji}$. However, it is this fact that allows $G = G_S(p)$ to be a mild group for certain S. Our work was greatly influenced by this analogy and corresponding results for link groups (cf. [24], [19],[2]).

Let $\Gamma_S(p)$ be the directed graph with vertices the primes of S with a directed edge q_iq_j from q_i to q_j if $\ell_{ij} \neq 0$. The directed graph $\Gamma_S(p)$ together with the function ℓ on $S \times S$ with values in $\mathbb{Z}/p\mathbb{Z}$ defined by $\ell(q_i, q_j) = \ell_{ij}$ if $i \neq j$ and 0 otherwise is called a **linking diagram** for S. Using the Čebotarev density theorem, one can show that, for any given finite directed graph Γ, there is a set of primes S as above with $\Gamma_S(p) = \Gamma$ (cf. Corollary 6.2).

Example 1.3. If $S = \{7, 13, 19\}$, the edges of $\Gamma_S(3)$ are $(19, 7)$, $(7, 13)$, $(13, 19)$, $(19, 13)$ and, choosing $g_7 = 3$, $g_{13} = g_{19} = 2$, we have $\ell(19, 7) = \ell(7, 13) = \ell(13, 19) = \ell(19, 13) = 1$ with $\ell(q_i, q_j) = 0$ otherwise.

A linking diagram Γ can be assigned to any presentation $< x_1, \ldots, x_m \mid r_1, \ldots, r_d >$ where

$$r_i \equiv x_i^{p\,a_i} \prod_{j\neq i}[x_i, x_j]^{a_{ij}} \bmod F_3 \quad (a_i, a_{ij} \in \mathbb{Z}/p\mathbb{Z}, a_{ii} = 0, d \leq m).$$

We shall call such a presentation of Koch type. The vertices of Γ are the generators x_i and $\ell(x_i, x_j) = a_{ij}$ if $i \leq d$ and zero otherwise. We have $d = m$ if every vertex of Γ is the source of some edge.

Definition 1.4. We call a linking diagram Γ a non-singular circuit if the the following conditions hold.

(a) There is an ordering $v_1, \ldots, v_m$ of the vertices of Γ such that $v_1v_2 \cdots v_mv_1$ is a circuit.

(b) If $\ell_{ij} = \ell(v_i, v_j)$ then $\ell_{ij} = 0$ if i, j are odd and

$$\Delta(v_1, v_2, \ldots, v_m) = \ell_{12}\ell_{23} \cdots \ell_{m-1,m}\ell_{m1} - \ell_{1m}\ell_{21}\ell_{32} \cdots \ell_{m,m-1} \neq 0.$$

In this case we also call $v_1v_2 \cdots v_mv_1$ a non-singular circuit.

Note that if (a) holds then $\Delta(v_1, v_2, \ldots, v_m) \neq 0$ if there is an edge v_iv_j of the circuit $v_1v_2\cdots v_mv_1$ such that v_jv_i is not an edge of Γ. Also note that (a) and (b) imply that m is even and ≥ 4. For $\Gamma = \Gamma_S(p)$ condition (b) is independent of the choice of primitive roots g_j since

$$\Delta(v_1, v_2, \ldots, v_m) \neq 0 \iff \frac{\ell_{1m}}{\ell_{m-1,m}}\frac{\ell_{21}}{\ell_{m1}}\frac{\ell_{32}}{\ell_{12}}\cdots\frac{\ell_{m,m-1}}{\ell_{m-2,m-1}} \neq 1,$$

where each ratio in the product is independent of the choice of primitive roots.

If $m = |S| \geq 2$ the linking diagram $\Gamma_S(p)$ can always be enlarged to a non-singular circuit $\Gamma_{S'}(p)$ with $|S'| = 2m$ (cf. Corollary 6.3).

Example 1.5. For $S = \{7, 19, 61, 163\}$ the edges of $\Gamma_S(3)$ are

$$\{(19, 7), (7, 61), (61, 7), (61, 19), (19, 61), (19, 163), (7, 163), (163, 7)\}$$

Using the primitive roots $2, 2, 2, 3$ for these primes and setting $v_1 = 61, v_2 = 19, v_3 = 163, v_4 = 7$, we find

$$\ell_{12} = \ell_{21} = \ell_{14} = \ell_{23} = \ell_{24} = \ell_{34} = 1, \ell_{43} = \ell_{41} = -1$$

with all other $\ell_{ij} = 0$. Then $v_1v_2v_3v_4v_1$ is a circuit with v_1v_3, v_3v_1, v_3v_2 not edges of $\Gamma_S(3)$. Hence $\Gamma_S(3)$ is a non-singular circuit. The initial forms of the relations in the Koch presentation for $G_S(3)$ are

$$\begin{aligned}
\rho_1 &= 2\pi\xi_1 + [\xi_1, \xi_2] + [\xi_1, \xi_4]\\
\rho_2 &= [\xi_2, \xi_1] + [\xi_2, \xi_3] + [\xi_2, \xi_4]\\
\rho_3 &= 2\pi\xi_3 + [\xi_3, \xi_4]\\
\rho_4 &= -[\xi_4, \xi_1] - [\xi_4, \xi_3].
\end{aligned}$$

By virtue of Theorems 3.10 and 3.12 we obtain that $G_S(3)$ is a mild group . More generally, these two theorems yield the following result.

Theorem 1.6. *A presentation of Koch type is strongly free if $p \neq 2$ and the vertices of its linking diagram Γ form a non-singular circuit.*

Theorem 1.6 can be proven under other conditions on the linking diagram when the number of vertices is odd and ≥ 5 (cf. Theorem 3.14).

The groups $G_S(p)$ are very mysterious and their structure is related to the Fontaine-Mazur Conjecture (cf.[4],[5],[9]). All that was known previously about these groups was that they were non-analytic for $m \geq 4$ and in certain cases for $m = 2, 3$ (cf. [26],[13],[23]). The group $G_S(3)$ with $S = \{7, 19, 61, 163\}$ seems to be the first known example where such a group is of cohomological dimension 2. This group also seems to be the first known example of a finitely generated pro-p-group G of cohomological dimension 2 with the same number of generators and relations and $G/[G, G]$ finite. This answers a question of Kuzmin[16],§6. Moreover, it has the property that $H/[H, H]$ is finite for any subgroup H of finite index. By Theorem 4.1(g), the rank of the n-th 3-central series quotient of $G_S(3)$ is

$$2\sum_{k=1}^{n}\frac{1}{k}\sum_{d|k}\mu(k/d)2^d.$$

So, as a graded vector space, the Lie algebra associated to the lower 3-central series is the direct sum of two copies of the Lie algebra associated to the lower 3-central series of the free pro-3-group on 2 generators.

Theorem 1.6 produces a lot of mild groups. An interesting example with the same number of generators and relators is the group

$$\langle x_1, x_2, \ldots, x_m \mid x_1^p[x_1, x_2], \cdots, x_{m-1}^p[x_{m-1}, x_m], x_m^p[x_m, x_1] >\rangle$$

where $m \geq 4$ is even and p is odd. A consequence of Theorem 3.14 and Theorem 3.10 is that the group is mild if $m \geq 5$ is odd (cf. Example 3.16).

If $S_p = S \cup \{p\}$, it is well known that the cohomological dimension of $G_{S_p}(p)$ is 2 when p is odd; for the case $p = 2$ see [25]. However, we can also prove that, for $p \neq 2$, it is a mild group under certain conditions on the linking diagram associated to its Koch presentation. This presentation is the same as that for $G_S(p)$ except for an additional generator x_{m+1} corresponding to a generator of the inertia group at p. Its linking diagram $\Gamma_{S_p}(p)$ is obtained from $\Gamma_S(p)$ by adding the vertex p which corresponds to x_{m+1} and an edge (q, p) for every $q \in S$ not congruent to 1 mod p^2. The linking number $\ell_{qp} \in \mathbb{Z}/p\mathbb{Z}$ is defined by

$$q \equiv (1+p)^{-\ell_{qp}} \mod p^2.$$

By definition $\ell_{pq} = 0$ for all $q \in S$ and $\ell_{pp} = 0$.

Theorem 1.7. *If $p \neq 2$, the pro-p-group G_{S_p} is a mild group if either of the following two conditions hold:*

(A) *$q_i \not\equiv 1$ mod p^2 for all $q_i \in S$,*

(B) *There is a prime $q \in S$, $q \not\equiv 1$ mod p^2 with $\ell(q_i, q) \neq 0$ for all $q_i \in S$ distinct from q.*

That condition (A) implies that G_{S_p} is a mild group follows from Theorems 3.10, 3.18. That condition (B) implies that G_{S_p} is a mild group follows from Theorems 3.10, 3.19. If condition (B) is not satisfied then it can be made so by the addition of a single prime (cf. Proposition 6.1). It would be interesting to find more general conditions on Γ_{S_p} which imply that G_{S_p} is a mild group

2. Algebraic Preliminaries

In this section we will review the more important algebraic techniques and results that we use in our paper. The most important of these is the Birkhoff-Witt Theorem.

Theorem 2.1 (Birkhoff-Witt)**.** *Let $\mathfrak{g}$ be a Lie algebra over a commutative ring k and let ϕ be the canonical mapping of $\mathfrak{g}$ into its enveloping algebra $U_{\mathfrak{g}}$. If $\mathfrak{g}$ is a free k-module with ordered basis $(e_i)_{i \in I}$ then $U_{\mathfrak{g}}$ is a free k-module with ordered basis the family of elements*

$$\phi(e_{i_1})\phi(e_{i_2}) \cdots \phi(e_{i_n})$$

with $n \geq 0$, $i_1 \leq i_2 \leq \cdots \leq i_n$.

In particular, if $\mathfrak{g}$ is a free k-module, the canonical mapping of $\mathfrak{g}$ into $U_{\mathfrak{g}}$ is injective and we can identify $\mathfrak{g}$ with a Lie subalgebra of $U_{\mathfrak{g}}$. Let U_n be the k-module generated by all products $x_1 x_2 \cdots x_m$ with $x_i \in \mathfrak{g}$ and $m \leq n$. Then $U_i U_j \subseteq U_{i+j}$ and $\mathrm{gr}(U_{\mathfrak{g}}) = \sum_{n \neq 0} U_{n+1}/U_n$ is a commutative associative algebra.

Corollary 2.2. *If $\mathfrak{g}$ is a free k-module then $\mathrm{gr}(U_{\mathfrak{g}})$ is isomorphic to $S_{\mathfrak{g}}$, the symmetric algebra of $\mathfrak{g}$. If, in addition, k is an integral domain then $U_{\mathfrak{g}}$ is an integral domain.*

Corollary 2.3. *Let $\mathfrak{g}$ be a Lie algebra over k and let $\mathfrak{h}$ be a Lie subalgebra such that $\mathfrak{h}$ and $\mathfrak{g}/\mathfrak{h}$ are free k-modules. If V, U are respectively the enveloping algebras of $\mathfrak{h}$, $\mathfrak{g}$ then U is a free left (right) V-module with basis*

$$f_{j_1} f_{j_2} \cdots f_{j_n} \quad (n \geq 0, j_1 \leq j_2 \leq \cdots \leq j_n$$

where $(f_j)_{j \in J}$ is any lifting of an ordered basis for $\mathfrak{g}/\mathfrak{h}$.

The Birkhoff-Witt Theorem has the following converse result.

Theorem 2.4. *Let $\mathfrak{g}$ be a graded Lie algebra over a principal ideal ring k and suppose that the homogeneous components are finitely generated k-modules. If the enveloping algebra of $\mathfrak{g}$ is a free k-module then so is $\mathfrak{g}$.*

Proof. Let $\mathfrak{a}, \mathfrak{b}$ be respectively the kernel and image of the canonical map ϕ of $\mathfrak{g}$ into $U_{\mathfrak{g}}$. Then $\mathfrak{b}$ is a free k-module and so the exact sequence

$$0 \to \mathfrak{a} \to \mathfrak{g} \to \mathfrak{b} \to 0$$

splits as k-modules. If π is an irreducible element of k and we let $\overline{M} = M/\pi M = M \otimes_k (k/\pi k)$ for any k-module M, we obtain the exact sequence

$$0 \to \overline{\mathfrak{a}} \to \overline{\mathfrak{g}} \to \overline{\mathfrak{b}} \to 0.$$

But the composite of the two arrows $\overline{\mathfrak{g}} \to \overline{\mathfrak{b}} \to \overline{U}_{\mathfrak{g}}$ is injective by the Birkhoff-Witt Theorem over the field $k/\pi k$. Hence $\overline{\mathfrak{g}} \to \overline{\mathfrak{b}}$ is injective. This implies that $\overline{\mathfrak{a}} = 0$. Since this is true for every homogeneous component of $\mathfrak{a}$ for any π, we obtain that the homogenous components of $\mathfrak{a}$ are all zero as they are finitely generated. This implies that $\mathfrak{a} = 0$ which is what we wanted to prove. □

If A is a graded k-module with homogeneous components A_n with A_n a finitely generated free k-module of rank c_n the Poincaré series of A is the power series

$$A(t) = \sum_{n \geq 0} c_n t^n.$$

By definition $A(t) \geq 0$ if $c_n \geq 0$ for all n. If B is another graded k-module with homogeneous components free finitely generated k-modules then $A(t) \geq B(t)$ if $A(t) - B(t) \geq 0$. We also have $(A \oplus B)(t) = A(t) + B(t)$ and $(A \otimes_k B)(t) = A(t)B(t)$. If

$$0 \to A \to B \to C \to O$$

is exact and C is also a free k-module then

$$B(t) = A(t) + C(t).$$

Proposition 2.5. *Let $\mathfrak{g} = \oplus_{n \geq 1} \mathfrak{g}_n$ be a graded Lie algebra over k with $\mathfrak{g}_n$ $(n \geq 1)$ a free k-module of finite rank a_n. Then the enveloping algebra $U_{\mathfrak{g}}$ of $\mathfrak{g}$ is a graded k-module whose homogenous components U_n are free k-modules of finite rank and*

$$U_{\mathfrak{g}}(t) = \prod_{n \geq 1} (1 - t^n)^{-a_n}.$$

Proof. By the Birkhoff-Witt Theorem $U_{\mathfrak{g}}(t) = S_{\mathfrak{g}}(t)$. Since $\mathfrak{g} = \oplus_{n\geq 1}\mathfrak{g}_n$ we have

$$S_{\mathfrak{g}}(t) = \prod_{n\geq 1} S_{\mathfrak{g}_n}(t^n)$$

which implies the result as $S_M(t) = (1-t)^{-r}$ for any free k-module M of rank r. $\square$

Now let $k = k_0[\pi]$, the polynomial algebra over the field k_0. Let $\mathcal{M}_k$ be the category of k-modules M such that M also has the structure of a graded module over k_0 where π sends the homogeneous component M_n into M_{n+1}. We say that M is of finite type if each component M_n is finite-dimensional. In the following we let $\overline{M} = M/\pi M = M \otimes_k (k/\pi k)$.

Proposition 2.6. *Let $M \in \mathcal{M}_k$. Then*
(a) $M = 0 \iff M/\pi M = 0$;
(b) *A subset of M generates $M \iff$ it generates M modulo πM.*
(c) *M is a free k-module $\iff$ multiplication by π is injective $\iff$ M is torsion free;*
(d) *M is a free k-module $\iff M \cong \overline{M} \otimes_{k_0} k$.*

For a proof see [22], §1.2.

Corollary 2.7. *If $M \in \mathcal{M}_k$ then $M(t) \leq \overline{M}/(1-t)$ with equality $\iff$ M is a free k-module.*

Proposition 2.8. *Let $\mathfrak{g}$ be a Lie algebra over $k_0[\pi]$ which has the structure of a graded Lie algebra over k_0 with homogeneous components $\mathfrak{g}_n$ satisfying $\pi\mathfrak{g}_n \subseteq \mathfrak{g}_{n+1}$. Then $\mathfrak{g}$ is a free $k_0[\pi]$-module if its enveloping algebra $U_{\mathfrak{g}}$ is a free $k_0[\pi]$-module.*

The proof of this is the same as the proof of Proposition 2.4 except that only the irreducible element π is required.

3. Strongly Free Sequences

Let k be a principal ideal domain and let L be the free Lie algebra over k on $\xi_1, \dots, \xi_m$. We view L as graded algebra where the degree of ξ_i is $e_i \geq 1$. Let $\rho_1, \dots, \rho_m$ be homogeneous elements of L with ρ_i of degree h_i and let $\mathfrak{r} = (\rho_1, \dots, \rho_d)$ be the ideal of L generated by $\rho_1, \dots, \rho_d$. Let $\mathfrak{g} = L/\mathfrak{r}$ and let $U = U_{\mathfrak{g}}$ be the enveloping algebra of $\mathfrak{g}$. Then $M = \mathfrak{r}/[\mathfrak{r}, \mathfrak{r}]$ is a U-module via the adjoint representation.

Definition 3.1. The sequence $\rho_1, \dots, \rho_d$ is said to be strongly free if
(a) $U_{\mathfrak{g}}$ is a free k-module,
(b) $M = \mathfrak{r}/[\mathfrak{r}, \mathfrak{r}]$ is a free U-module on the images of the ρ_i in M.

By the Birkhoff-Witt Theorem and Proposition 2.4, $U_{\mathfrak{g}}$ is a free k-module if and only if $\mathfrak{g}$ is a free k-module.

Let V (resp. W) be the enveloping algebra of L (resp. $\mathfrak{r}$) and I (resp. J) be the augmentation ideal of V (resp. W). If $\mathcal{R}$ is the ideal of V generated by $\mathfrak{r}$, we have an exact sequence

$$\mathrm{Tor}_1^W(k, V) \to M \to I/\mathcal{R}I \to V/\mathcal{R} \to k \to 0.$$

It is obtained from the exact sequence $0 \to I \to V \to k \to 0$ by tensoring with $k = W/J$ over W and using the fact that

(1) If M is a W-module then $M \otimes_W (W/J) = M/JM$;
(2) $\mathcal{R} = \mathfrak{r}V = V\mathfrak{r}$;
(3) $\mathrm{Tor}_1^W(k,k) = \mathfrak{r}/[\mathfrak{r},\mathfrak{r}]$ (cf. [7], Ch. XIII, §2).

The map $M \to I/\mathcal{R}I$ is induced by the inclusion $\mathfrak{r} \subseteq I$. The algebra V is the free associative algebra over k on $\xi_1,\ldots,\xi_m$ and I is the direct sum of the left ideals $V\xi_i$. The U-module $I/\mathcal{R}I$ is the direct sum of the free U-submodules Ug_i where g_i is the image of ξ_i in $U = V/\mathcal{R}$. If $\mathfrak{g}$ is free as a k-module then V is a free W-module by Corollary 2.3 since $\mathfrak{r}$ is a free k-module. In this case we have the exact sequence

$$0 \to M \to I/\mathcal{R}I \to V/\mathcal{R} \to k \to 0.$$

Expressing M as a quotient U^d/N using the relators ρ_i, we obtain the exact sequence of graded modules whose homogeneous components are finitely generated free k-modules

$$0 \to N \to \oplus_{j=1}^d U[h_j] \to \oplus_{j=1}^m U[e_j] \to U \to k \to 0$$

where $U[d] = U$ but with degrees shifted by d; by definition, $U[d](t) = t^d U(t)$. We have $N = 0$ if and only if M is a free U-module on the images of the ρ_i.

Taking Poincaré series in long exact sequence, we get

$$N(t) - (t^{h_1} + \cdots + t^{h_d})U(t) + (t^{e_1} + \cdots + t^{e_m})U(t) - U(t) + 1 = 0.$$

Solving for $U(t)$, we get $U(t) = P(t) + N(t)P(t)$, where

$$P(t) = \frac{1}{1 - (t^{e_1} + \cdots + t^{e_m}) + t^{h_1} + \cdots + t^{h_d}}.$$

We thus obtain

Proposition 3.2. *If $\rho_1,\ldots,\rho_d$ is a strongly free sequence and U is the enveloping algebra of $\mathfrak{g} = L/(\rho_1,\ldots,\rho_d)$ then $U(t) = P(t)$. Conversely, if $\mathfrak{g}$ is a free k-module and $U(t) = P(t)$ then $\rho_1,\ldots,\rho_d$ is a strongly free sequence. Moreover, if $P(t) \geq 0$ then $U(t) \geq P(t)$ with equality if and only if $\rho_1,\ldots,\rho_d$ is a strongly free sequence.*

The condition $P(t) \geq 0$, i.e, the coefficients of the powers of t^n are ≥ 0, is a serious restriction on the the sequences (e_i) and (h_j). For example, $1/(1-3t+4t^3)$ is a positive series whereas $1/(1-3t+5t^3)$ is not. If all $e_i = 1$ and all $h_i = h > 1$ then in [1], Lemma 3.5 Anick proved that

$$P(t) \geq 0 \implies d < \frac{m^h}{(h-1)e},$$

where $e = 2.718\cdots$.

Strongly free sequence were studied by Anick in [1] in the context of algebras over a field. They are the analogues of regular sequences in commutative algebra. They also arose in the work of Halperin-Lemaire[10] and in the paper of Koch[15].

In general, it is difficult to determine whether a sequence is strongly free but we can construct a large supply of them using the elimination theorem. Let $L(X)$ be the free Lie algebra over k on the set X. Let S be a subset of X and let $\mathfrak{a}$ be the ideal of $L(X)$ generated by $X - S$. Then the elimination theorem [3], §2, Proposition 10 states that $\mathfrak{a}$ is a free Lie algebra over k with basis consisting of the elements

$$ad(\sigma_1)ad(\sigma_2)\cdots ad(\sigma_n)(\xi)$$

with $n \geq 0$, $\sigma_i \in S$, $\xi \in X - S$. If B is the enveloping algebra of $L(S) = L(X)/\mathfrak{a}$, it follows that $\mathfrak{a}/[\mathfrak{a}, \mathfrak{a}]$ is a B-free module with basis the images of the elements ξ with $\xi \in X - S$.

Theorem 3.3. *Suppose that k is a field. Let S be a subset of $X = \{\xi_1, \dots, \xi_m\}$ and let $\mathfrak{a}$ be the ideal of the free Lie algebra L on X generated by $X - S$. Let $T = \{\tau_1, \dots, \tau_t\} \subset \mathfrak{a}$ whose elements are homogeneous and B-independent modulo $[\mathfrak{a}, \mathfrak{a}]$. If $\rho_1, \dots, \rho_d$ are homogeneous elements of $\mathfrak{a}$ which lie in the k-span of T modulo $[\mathfrak{a}, \mathfrak{a}]$ and which are linearly independent over k modulo $[\mathfrak{a}, \mathfrak{a}]$ then the sequence $\rho_1, \dots, \rho_d$ is strongly free (in L).*

Proof. If $\mathfrak{r}$ is the ideal of L generated by $\rho_1, \dots, \rho_d$, the elements

$$ad(\sigma_1)ad(\sigma_2)\cdots ad(\sigma_n)(\rho_j)$$

with $1 \leq j \leq d$, $n \geq 0$, $\sigma_i \in S$ generate $\mathfrak{r}$ as an ideal of the Lie algebra $\mathfrak{a}$. Suppose that these elements form part of a basis of the free Lie algebra $\mathfrak{a}$. The elimination theorem then shows that $M = \mathfrak{r}/[\mathfrak{r}, \mathfrak{r}]$ is a free module over the enveloping algebra C of $\mathfrak{a}/\mathfrak{r}$ with the images of these elements as basis. To show that this implies that M is a free U-module on the images m_i of the ρ_i suppose that $\sum_i u_i \cdot m_i = 0$ with $u_i \in U$. By the Corollary 2.3 every u_i can be written in the form

$$u_i = \sum c_{ij} w_j$$

where the w_j are distinct products of elements of S. Then

$$0 = \sum_i u_i \cdot m_i = \sum_{i,j} c_{ij}\, w_j \cdot m_i$$

which implies that all c_{ij} are zero and hence that each u_i is zero.

To show that the elements of the form $ad(\sigma_1)ad(\sigma_2)\cdots ad(\sigma_n)(\rho_j)$ are part of a Lie algebra basis of $\mathfrak{a}$ it suffices to show that $\rho_1, \dots, \rho_d$ are B-independent modulo $[\mathfrak{a}, \mathfrak{a}]$. We now work modulo $[\mathfrak{a}, \mathfrak{a}]$. If H is the k-span of $\rho_1, \dots, \rho_d$, we can find a basis $\gamma_1, \dots, \gamma_d$ of H such that

$$\gamma_i = a_i\alpha_i + \sum_{j=1}^{s} a_{ij}\beta_j$$

where $a_i, a_{ij} \in k$, $a_i \neq 0$, $d + s = t$, $T = \{\alpha_1, \dots, \alpha_d, \beta_1, \dots, \beta_s\}$. If $u_1, \dots, u_d \in B$, we have

$$\sum_{i=1}^{d} u_i \cdot \gamma_i = \sum_{i=1}^{d} a_i u_i \cdot \alpha_i + \sum_{j=1}^{s}(\sum_{i=1}^{d} a_{ij}u_i) \cdot \beta_j.$$

By the B-independence of the elements of T,

$$\sum_{i=1}^{d} u_i \cdot \gamma_i = 0 \mod [\mathfrak{a}, \mathfrak{a}] \implies \sum_{i=1}^{d} a_i u_i \cdot \alpha_i = 0 \mod [\mathfrak{a}, \mathfrak{a}]$$

and hence that $a_i u_i = 0$ so that $u_i = 0$ for all i which implies the B-independence of $\gamma_1, \dots, \gamma_d$ and hence of $\rho_1, \dots, \rho_d$. □

Remark 3.4. Note that for strongly free sequences $\rho_1, \dots, \rho_d$ produced by the above method, the Lie algebra $L/(\rho_1, \dots, \rho_d)$ is an extension of two free Lie algebras.

Corollary 3.5. *Let* $\{1, \dots, m\} = I \cup J$ *with* $I \cap J = \emptyset$, $|I| = k$ *and let* $S = \{\xi_j \mid j \in J\}$. *Then, for any* $h \geq 0$, *any subset of the* $k(m-k)^h$ *elements*

$$\xi_{j_1} \cdots \xi_{j_h} \cdot \xi_i = [\xi_{j_1}, [\xi_{j_2}, \cdots, [\xi_{j_h}, \xi_i]] \cdots]]$$

with $j_1, \dots, j_h \in J$, $i \in I$ *is strongly free as is, modulo* $[\mathfrak{a}, \mathfrak{a}]$, *any linearly independent subset of the space they span.*

Example 3.6. If we take $S = \{\xi_2, \dots, \xi_m\}$ we see that

$$[\xi_1, \xi_2], [\xi_1, \xi_3], \dots, [\xi_1, \xi_m]$$

is a strongly free sequence. If $m \geq 4$ is even and we take $S = \{\xi_n \mid n \text{ odd}\}$ we see that

$$[\xi_1, \xi_2], [\xi_2, \xi_3], \dots, [\xi_{m-1}, \xi_m], [\xi_m, \xi_1]$$

is a strongly free sequence. We shall show later this this is also true for $m > 4$ odd (cf. Example 3.16).

Note that the above implies the maximum length $s(m)$ of a strongly free sequence of elements of degree 2 in the free Lie algebra on $\xi_1, \dots, \xi_m$ satisfies

$$\max_k k(m-k) \leq s(m) < m^2/e.$$

Let $t(m) = \max_k k(m-k)$. We have $4 \leq s(4) \leq 5$. However, $s(4) = 5$ is not possible as $P(t)$ is not positive in this case; so $s(4) = t(4) = 4$. We have $6 \leq s(5) \leq 9$ and $7, 8, 9$ are not possible; so $s(5) = t(5) = 6$. In this case, an example of a strongly free sequence of length 6 is

$$[\xi_1, \xi_2], [\xi_1, \xi_4], [\xi_3, \xi_2], [\xi_3, \xi_4], [\xi_5, \xi_2], [\xi_5, \xi_4].$$

We conjecture that $t(m) = s(m)$ for all $m \geq 4$.

Our examples of strongly free sequences over a field can also be obtained using Anick's criterion for strong freeness developed in [1], §6. We will need this criterion to construct examples when the number of variables is 2. Let L be the free Lie algebra on $\xi_1, \dots, \xi_m$ with coefficients in the field k and A be the enveloping algebra of L. A sequence of non-identity monomials $\alpha_1, \dots, \alpha_d$ in the ξ_i is said to be combinatorially free if (1) no monomial α_i is a submonomial of α_j for $i \neq j$ and (2) if $\alpha_i = u_1 v_1$, $\alpha_j = u_2 v_2$ is a proper factorization with u_i, v_i monomials then $u_1 \neq v_2$. Let an ordering of $\xi_1, \dots, \xi_m$ be given and order the monomials lexicographically. By the leading term of an element w of L we mean the largest monomial appearing in w (with a non-zero coefficient).

Proposition 3.7 (Anick's Criterion)**.** *The sequence* $\rho_1, \dots, \rho_d$ *in* L *is strongly free if the sequence of leading terms of these elements is combinatorially free.*

Example 3.8. In the case $m = 2$, any sequence of distinct elements of the form

$$\rho_{rs} = [\mathrm{ad}(\xi_2)^r \mathrm{ad}(\xi_1)^{s+1} \xi_2, \mathrm{ad}(\xi_2)^{r+1} \mathrm{ad}(\xi_1)^{s+1} \xi_2],$$

where $r, s \geq 0$, is strongly free since the leading term of ρ_{rs} for the ordering $\xi_1 < \xi_2$ is $\lambda_{r,s} = \xi_2^{r+1} \xi_1^{s+1} \xi_2^{r+2} \xi_1^{s+2}$ and the $\lambda_{r,s}$ form a combinatorially free sequence.

Now let $k = k_0[\pi]$ where k_0 is a field. We view k as a graded algebra over k_0 with π of degree 1. Again L is the free Lie algebra over k on $\xi_1, \dots, \xi_m$ with the ξ_i being assigned the degree $e_i \geq 1$. Then L has a natural grading by finite-dimensional vector spaces L_n over k_0 in which multiplication by π sends L_n into L_{n+1}. Let $\overline{L} = L/\pi L = L \otimes_k k_0$ and let $\overline{\rho}_1, \dots, \overline{\rho}_m$ be the images of $\rho_1, \dots, \rho_m$ in $\overline{L}$. The Lie algebra $\overline{L}$ is the free Lie algebra over k_0 on the images of $\xi_1, \dots, \xi_m$ which we can and do identify with $\xi_1, \dots, \xi_m$. If $\overline{\mathfrak{r}} = (\overline{\rho}_1, \dots, \overline{\rho}_d)$, the enveloping algebra of $\overline{\mathfrak{g}} = \overline{L}/\overline{\mathfrak{r}}$ is $\overline{U} = U/\pi U$.

Proposition 3.2 holds if $P(t)$ is replaced by

$$Q(t) = \frac{P(t)}{1-t} = \frac{1}{(1-t)(1-(t^{e_1}+\cdots+t^{e_m})+t^{h_1}+\cdots+t^{h_d})}.$$

Proposition 3.9. *If $\rho_1, \dots, \rho_d$ is a strongly free sequence and U is the enveloping algebra of $\mathfrak{g} = L/(\rho_1, \dots, \rho_d)$ then $U(t) = Q(t)$. Conversely, if $\mathfrak{g}$ is a free k-module and $U(t) = Q(t)$ then $\rho_1, \dots, \rho_d$ is a strongly free sequence. Moreover, if $Q(t) \geq 0$ then $U(t) \geq Q(t)$ with equality if and only if $\rho_1, \dots, \rho_d$ is a strongly free sequence.*

Theorem 3.10. *We have $\overline{\rho}_1, \dots, \overline{\rho}_d$ strongly free $\iff$ $\rho_1, \dots, \rho_d$ strongly free.*

Proof. ($\Leftarrow$) From 3.9 we have $U \cong \overline{U} \otimes_{k_0} k$ as k_0-modules which implies

$$\overline{U}(t) = (1-t)Q(t) = \frac{1}{1-(t^{e_1}+\cdots+t^{e_m})+t^{h_1}+\cdots+t^{h_d}} = P(t)$$

and hence that $\overline{\rho}_1, \dots, \overline{\rho}_d$ is strongly free by Proposition 3.2.

($\Rightarrow$) If $M = \mathfrak{r}/[\mathfrak{r}, \mathfrak{r}]$ we have an exact sequence of graded vector spaces over k_0

$$0 \to K \to M \to U[e_1] \oplus \cdots \oplus U[e_m] \to U \to k \to 0.$$

Taking Poincaré series we get

$$K(t) - M(t) + (t^{e_1}+\cdots+t^{e_m})U(t) - U(t) + \frac{1}{1-t} = 0$$

from which we get $M(t) = K(t) - (1-(t^{e_1}+\cdots+t^{e_m}))U(t) + 1/(1-t)$. Hence

$$\frac{M(t)}{1-(t^{e_1}+\cdots+t^{e_m})} = \frac{K(t)}{1-(t^{e_1}+\cdots+t^{e_m})} + \frac{1}{(1-t)(1-(t^{e_1}+\cdots+t^{e_m}))} - U(t).$$

Now suppose that $\overline{\rho}_1, \dots, \overline{\rho}_d$ is strongly free. Then, if $\overline{\mathfrak{r}}$ is the ideal of $\overline{L}$ generated by $\overline{\rho}_1, \dots, \overline{\rho}_d$, we have surjections

$$\overline{U}[h_1] \oplus \cdots \oplus \overline{U}[h_d] \to \overline{M} \to \overline{\mathfrak{r}}/[\overline{\mathfrak{r}}, \overline{\mathfrak{r}}]$$

whose composite is an isomorphism. It follows that

$$\overline{M} \cong \overline{\mathfrak{r}}/[\overline{\mathfrak{r}}, \overline{\mathfrak{r}}] \cong \overline{U}[h_1] \oplus \cdots \oplus \overline{U}[h_d],$$

$$M(t) \leq \frac{\overline{M}(t)}{1-t} = \frac{1}{1-t} \cdot \frac{t^{h_1}+\cdots+t^{h_d}}{1-(t^{e_1}+\cdots+t^{e_m})+t^{h_1}+\cdots+t^{h_d}},$$

$$U(t) \leq \frac{\overline{U}(t)}{1-t} = \frac{1}{1-t} \cdot \frac{1}{1-(t^{e_1}+\cdots+t^{e_m})+t^{h_1}+\cdots+t^{h_d}}.$$

Using the fact that $K(t) \geq 0$, we get

$$\frac{M(t)}{1-(t^{e_1}+\cdots+t^{e_m})} \geq \frac{1}{(1-t)(1-(t^{e_1}+\cdots+t^{e_m}))} - \frac{\overline{U}(t)}{1-t}$$
$$= \frac{1}{1-t}\left(\frac{1}{(1-(t^{e_1}+\cdots+t^{e_m})} - \frac{1}{1-(t^{e_1}+\cdots+t^{e_m})+t^{h_1}+\cdots+t^{h_d}}\right)$$
$$= \frac{\overline{M}(t)}{(1-t)(1-(t^{e_1}+\cdots+t^{e_m}))} \geq \frac{M(t)}{1-(t^{e_1}+\cdots+t^{e_m})}.$$

It follows that $K(t)=0$, $U(t)=\overline{U}(t)/(1-t)$ and $M(t)=\overline{M}/(1-t)$. Hence U is a free k-module and M is a free U-module since we have a natural surjection

$$U[h_1]\oplus\cdots U[h_d]\to M$$

with both sides having the same Poincaré series. $\square$

Corollary 3.11. *If $\rho \notin \pi L$ then ρ is a strongly free sequence consisting of a single element.*

Proof. We use the fact that $\overline{M} \to \overline{U}^m$ is injective. Hence, if $\overline{\rho} \neq 0$ then $\overline{M}$ is a submodule of $\overline{U}^m$ and is generated by a single non-zero element. So it must be free since $\overline{U}$ has no zero-divisors by the Birkhoff-Witt Theorem. $\square$

Let us apply the above results to the relators in Example 1.5. Reducing mod π we get the relators

$$\begin{aligned}
\rho_1 &= [\xi_1,\xi_2]+[\xi_1,\xi_4]\\
\rho_2 &= -[\xi_1,\xi_2]+[\xi_2,\xi_3]+[\xi_2,\xi_4]\\
\rho_3 &= [\xi_3,\xi_4]\\
\rho_4 &= -[\xi_4,\xi_1]-[\xi_4,\xi_3]
\end{aligned}$$

in the free Lie algebra over $\mathbb{F}_3$ on ξ_1,ξ_2,ξ_3,ξ_4. We apply Theorem 3.3 with $S=\{\xi_1,\xi_3\}$ and $T=\{[\xi_1,\xi_2],[\xi_3,\xi_2],[\xi_3,\xi_4],[\xi_1,\xi_4]\}$. Modulo $[\mathfrak{a},\mathfrak{a}]$, the relators $\rho_1,\ldots,\rho_4$ are linearly independent and lie in the subspace spanned by T. Hence $\rho_1,\ldots,\rho_4$ is strongly free.

Now let L be the free Lie algebra on $X=\{\xi_1,\ldots,\xi_m\}$ over a field k and let $\rho_1,\ldots,\rho_m$ be elements of L with

$$\rho_i = \sum_{j\neq i} \ell_{ij}[\xi_i,\xi_j].$$

Let Γ be the linking diagram whose vertices are $\xi_1,\ldots,\xi_n$ with (ξ_i,ξ_j) an edge if $j\neq i$ and the linking number $\ell_{ij}\neq 0$.

Theorem 3.12. *The sequence $\rho_1,\ldots,\rho_m$ is strongly free if the vertices of Γ form a non-singular circuit.*

Proof. After permuting the vertices we can assume that the path showing that Γ is non-singular is $\xi_1\xi_2\cdots\xi_m\xi_1$. We apply Theorem 3.3 with $S=\{\xi_i \mid i \text{ odd}\}$ and $T=\{[\xi_i,\xi_j] \mid i \text{ odd}, j \text{ even}\}$. In this case, we have ρ_i in the span H of T modulo $[\mathfrak{a},\mathfrak{a}]$ since no $[\xi_i,\xi_j]$ appears in ρ_i with i,j both odd. Let $e_i=[\xi_i,\xi_{i+1}]$ for $1\leq i\leq m-1$, let

$e_m = [\xi_m, \xi_1]$ and complete $e_1, \ldots, e_m$ to a basis of H modulo $[\mathfrak{a}, \mathfrak{a}]$. The transpose of the coefficient matrix of $e_1, \ldots, e_m$ in $\rho_1, \ldots, \rho_n$ is

$$\begin{bmatrix} \ell_{12} & 0 & 0 & \cdots & 0 & -\ell_{1m} \\ -\ell_{21} & \ell_{23} & 0 & \cdots & 0 & 0 \\ 0 & -\ell_{32} & \ell_{34} & \cdots & 0 & 0 \\ 0 & 0 & -\ell_{43} & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \ell_{m,m-1} & 0 \\ 0 & 0 & 0 & \cdots & -\ell_{m,m-1} & \ell_{m1} \end{bmatrix}.$$

The determinant of this matrix is

$$\Delta(\xi_1, \xi_2, \ldots, \xi_m) = \ell_{12}\ell_{23}\cdots\ell_{m-1,m}\ell_{m1} - \ell_{1m}\ell_{21}\ell_{32}\cdots\ell_{m,m-1}.$$

□

Example 3.13. Let $S = \{181, 163, 7, 61\}$ and let $\Gamma = \Gamma_S(3)$. Using the primitive roots $2, 2, 3, 2$ for $v_1 = 181, v_2 = 163, v_3 = 7, v_4 = 61$ respectively, we find

$$\ell_{12} = \ell_{23} = \ell_{34} = \ell_{21} = \ell_{43} = 1, \ell_{41} = \ell_{14} = \ell_{32} = -1, \ell_{13} = \ell_{31} = 0$$

so that $\Delta(v_1, v_2, v_3, v_4) = 1$. Hence $\Gamma_S(3)$ is a non-singular circuit.

Theorem 3.14. *Suppose that $m \geq 5$ is odd and $\ell_{ij} = 0$ for $i, j \neq m$ and i, j odd. If $\ell_{m1} \neq 0$ and $\xi_1\xi_2\cdots\xi_{m-1}\xi_1$ is a non-singular circuit then the sequence $\rho_1, \ldots, \rho_m$ is strongly free.*

Proof. We apply Theorem 3.3 with $S = \{\xi_i \mid i \neq m,\ i \text{ odd}\}$ and T the set of $[\xi_i, \xi_j]$ with $\xi_i \in S$, $\xi_j \notin S$. In this case, we have ρ_i in the span H of T modulo $[\mathfrak{a}, \mathfrak{a}]$ since no $[\xi_i, \xi_j]$ appears in ρ_i with i, j both odd and $i, j \neq m$. Let $e_i = [\xi_i, \xi_{i+1}]$ for $1 \leq i \leq m-3$, $e_{m-1} = [\xi_{m-1}, \xi_1]$, $e_m = [\xi_m, \xi_1]$ and complete $e_1, \ldots, e_m$ to a basis of H modulo $[\mathfrak{a}, \mathfrak{a}]$. The transpose of the coefficient matrix of $e_1, \ldots, e_m$ in $\rho_1, \ldots, \rho_m$ is

$$\begin{bmatrix} \ell_{12} & 0 & 0 & \cdots & -\ell_{1,m-1} & -\ell_{1m} \\ -\ell_{21} & \ell_{23} & 0 & \cdots & 0 & 0 \\ 0 & -\ell_{32} & \ell_{34} & \cdots & 0 & 0 \\ 0 & 0 & -\ell_{43} & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \ell_{m-1,1} & 0 \\ 0 & 0 & 0 & \cdots & 0 & \ell_{m1} \end{bmatrix}.$$

The determinant of this matrix is $\ell_{m1}\Delta(\xi_1, \xi_2, \ldots, \xi_{m-1})$ which is non-zero by hypothesis. □

Example 3.15. If we take $S = \{61, 7, 163, 43, 19\}$ then, for the given ordering of S, we have

$$\ell_{13} = \ell_{31} = 0, \quad \ell_{12} = \ell_{32} = \ell_{34} = \ell_{43} = \ell_{14} = \ell_{51} = 1, \quad \ell_{21} = \ell_{23} = \ell_{41} = \ell_{45} = -1.$$

Since $\ell(19, 61) = 1$ and $\Delta(61, 7, 163, 43) = -1$ Theorem 3.14 applies and $G_S(3)$ is a mild group.

Example 3.16. The presentation with defining relators

$$\rho_1 = [\xi_1, \xi_2],\ \ \rho_2 = [\xi_2, \xi_3],\ \ \rho_3 = [\xi_3, \xi_4], \ldots, \rho_{m-1} = [\xi_{m-1}, \xi_m], \rho_m = [\xi_m, \xi_1]$$

is equivalent to the presentation with ρ_{m-1} replaced by

$$[\xi_{m-1}, \xi_m] + [\xi_{m-1}, \xi_1].$$

The graph Γ associated to this presentation satisfies the conditions of Theorem 3.14 when $m \geq 5$ is odd.

One can develop rank criteria for strong freeness based on the size of the set S in Theorem 3.3. For example, one has the following result for size 2.

Theorem 3.17. *Suppose that $\ell_{12} = \ell_{21} = 0$. Then $\rho_1, \ldots, \rho_m$ is strongly free if the matrix*

$$\begin{bmatrix} \ell_{13} & \ell_{14} & \ell_{15} & \cdots & \ell_{1m} & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 & \ell_{23} & \ell_{24} & \ell_{25} & \cdots & \ell_{2m} \\ -\ell_{31} & 0 & 0 & \cdots & 0 & -\ell_{32} & 0 & 0 & \cdots & 0 \\ 0 & -\ell_{41} & 0 & \cdots & 0 & 0 & -\ell_{42} & 0 & \cdots & 0 \\ 0 & 0 & -\ell_{51} & \cdots & 0 & 0 & 0 & -\ell_{52} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & -\ell_{m1} & 0 & 0 & 0 & \cdots & -\ell_{m2} \end{bmatrix}$$

of size $m \times 2(m-2)$ has rank m.

Proof. We apply Theorem 3.3 with $S = \{\xi_1, \xi_2\}$ and

$$T = \{[\xi_1, \xi_3], [\xi_1, \xi_4], \ldots, [\xi_1, \xi_m], [\xi_2, \xi_3], [\xi_2, \xi_4], \ldots, [\xi_2, \xi_m]\}.$$

The given matrix is the transpose of the coefficient matrix of $\rho_1, \ldots, \rho_m$ with respect to T modulo $[\mathfrak{a}, \mathfrak{a}]$. $\square$

We now consider the case L is the free Lie algebra on $X = \{\xi_1, \ldots, \xi_m\}$ over a field k and $\rho_1, \ldots, \rho_d$ are $d < m$ elements of L with

$$\rho_i = \sum_{j \neq i} \ell_{ij} [\xi_i, \xi_j].$$

The associated linking diagram Γ has vertices $\xi_1, \ldots, \xi_m$ with (ξ_i, ξ_j) an edge if $i \neq j$ and the linking number $\ell(\xi_i, \xi_j) = \ell_{ij} \neq 0$. We want to find conditions on Γ which imply the strong freeness of the sequence $\rho_1, \ldots, \rho_d$ in the case $d < m$.

Theorem 3.18. *The sequence $\rho_1, \ldots, \rho_{m-1}$ is strongly free if $\ell(\xi_i, \xi_m) \neq 0$ for $1 \leq i < m$.*

Proof. We apply Theorem 3.3 with $S = \{\xi_m\}$, $T = \{[\xi_i, \xi_m] \mid 1 \leq i < m\}$. We get the required result since $\rho_1, \ldots, \rho_{m-1}$ are in $\mathfrak{a}$, and modulo $[\mathfrak{a}, \mathfrak{a}]$ are a basis for the span of T. $\square$

Theorem 3.19. *Suppose that $\ell(\xi_{m-1}, \xi_m) \neq 0$ and $\ell(\xi_i, \xi_{m-1}) \neq 0$ for $i < m - 1$. Then $\rho_1, \ldots, \rho_{m-1}$ is a strongly free sequence.*

Proof. We apply Theorem 3.3 with $S = \{\xi_{m-1}\}$ and

$$T = \{[\xi_1, \xi_{m-1}], [\xi_2, \xi_{m-1}], \ldots, [\xi_{m-2}, \xi_{m-1}], [\xi_{m-1}, \xi_m]\}.$$

We get the required result since $\rho_1, \ldots, \rho_{m-1}$ are in $\mathfrak{a}$, and modulo $[\mathfrak{a}, \mathfrak{a}]$ is a basis for the span of T. □

Definition 3.20. We call Γ rooted at the vertex v if for every vertex $w \neq v$ there is a path from w to v.

We don't know if $\rho_1, \ldots, \rho_{m-1}$ is a strongly free sequence if Γ is rooted at ξ_m. For example, we don't know whether or not the sequence,

$$\rho_1 = [\xi_1, \xi_3], \quad \rho_2 = [\xi_2, \xi_1] + [\xi_2, \xi_4], \quad \rho_3 = [\xi_3, \xi_4] + [\xi_3, \xi_5], \quad \rho_4 = [\xi_4, \xi_5],$$

which is rooted at ξ_5, is strongly free. Computer evidence using GAP suggests that it is.

4. Computing the Lower p-Central Series

Let F be the free pro-p-group on $x_1, \ldots, x_m$. The completed group algebra $A = \mathbb{Z}_p[[F]]$ over the p-adic integers $\mathbb{Z}_p$ is isomorphic to the Magnus algebra of formal power series in the non-commuting indeterminates $X_1, \ldots, X_m$ over $\mathbb{Z}_p$. Identifying F with its image in A, we have $x_i = 1 + X_i$ (cf. [26], p. I-7).

If $e_1, \ldots, e_m$ are integers > 0, we define a valuation w of A in the sense of Lazard by setting

$$w\Big(\sum_{i_1,\ldots,i_k} a_{i_1,\ldots,i_k} X_{i_1} \cdots X_{i_k}\Big) = \inf_{i_i,\ldots,i_k} (v(a_{i_1,\ldots,i_k}) + e_{i_1} + \cdots + e_{i_k}),$$

where v is the p-valuation of $\mathbb{Z}_p$ with $v(p) = 1$. Let

$$A_n = \{u \in A \mid w(u) \geq n\}, \ \mathrm{gr}_n(A) = A_n/A_{n+1}, \ \mathrm{gr}(A) = \oplus_{n\geq 0}\mathrm{gr}_n(A).$$

Then $\mathrm{gr}(A)$ is a graded k-algebra where k is the graded ring $\mathbb{F}_p[\pi] = \mathrm{gr}(\mathbb{Z}_p)$ with π the image of p in $p\mathbb{Z}_p/p^2\mathbb{Z}_p$. If ξ_i is the image of X_i in $\mathrm{gr}_{e_i}(A)$ then $\mathrm{gr}(A)$ is the free associative k-algebra on $\xi_1, \ldots, \xi_m$ with a grading in which ξ_i is of degree e_i and multiplication by π increases the degree by 1. The Lie subalgebra L of $\mathrm{gr}(A)$ generated by the ξ_i is the free Lie algebra over k on $\xi_1, \ldots, \xi_m$ by the Birkhoff-Witt Theorem. Note that when $e_i = 1$ for all i we have $A_n = I^n$, where I is the augmentation ideal $(p, X_1, \ldots, X_m)$ of A.

For $n \geq 1$, let $F_n = (1 + A_n) \cap F$ and for $x \in F$ let $\omega(x) = w(x-1)$ be the filtration degree of x. Then (F_n) is a decreasing sequence of closed subgroups of F with the following properties:

$$F_1 = F, \ [F_n, F_k] \subseteq F_{n+k}, \ F_n^p \subseteq F_{n+1},$$

where $[F_n, F_k]$ is the closed normal subgroup generated by the commutators $[u, v] = u^{-1}v^{-1}uv$ with $u \in F_n, v \in F_k$. Such a sequence of subgroups of a pro-p-group F is called a p-central series of F. An important example of a p-central series of a pro-p-group G is the lower p-central series defined by

$$G_1 = G, \quad G_{n+1} = G_n^p[G, G_n].$$

If (G_n) is a p-central series of G, let $\mathrm{gr}_n(G) = G_n/G_{n+1}$ with the group operation denoted additively. Then $\mathrm{gr}(G) = \oplus_{n\geq 1}\mathrm{gr}_n(G)$ is a graded vector space over $\mathbb{F}_p$ with a bracket operation $[\xi,\eta]$ which is defined for $\xi \in G_n$, $\eta \in G_k$ to be the image in $\mathrm{gr}_{n+k}(F)$ of $[x,y]$ where x,y are representatives of ξ,η in $\mathrm{gr}_n(G),\mathrm{gr}_k(G)$ respectively. Under this bracket operation, $\mathrm{gr}(G)$ is a Lie algebra over $\mathbb{F}_p$. The mapping $x \mapsto x^p$ induces an operator P on $\mathrm{gr}(G)$ sending $\mathrm{gr}_n(G)$ into $\mathrm{gr}_{n+1}(G)$. For homogeneous ξ,η, we have

$$P(\xi+\eta) = P(\xi) + P(\eta), \quad [P(\xi),\eta] = P([\xi,\eta]).$$

unless $p = 2$ and $\xi,\eta \in \mathrm{gr}_1(F)$ in which case

$$P(\xi+\eta) = P(\xi) + P(\eta) + [\xi,\eta], \quad [P(\xi),\eta] = P([\xi,\eta]) + [\xi,[\xi,\eta]].$$

In the case $G = F$ and $F_n = (1 + A_n) \cap F$, the mapping $x \mapsto x - 1$ induces an injective Lie algebra homomorphism of $\mathrm{gr}(F)$ into $\mathrm{gr}(A)$. Identifying $\mathrm{gr}(F)$ with its image in $\mathrm{gr}(A)$, we have $P(\xi) = \pi\xi$ unless $p = 2$ and $\xi \in \mathrm{gr}_1(F)$ in which case

$$P(\xi) = \xi^2 + \pi\xi.$$

The Lie algebra $\mathrm{gr}(F)$ is the smallest $\mathbb{F}_p$-subalgebra of $\mathrm{gr}(A)$ which contains $\xi_1, \dots \xi_m$ and is stable under P. To see this, let X_n be the set of elements x_i with $e_i = n$ and define subsets T_n inductively as follows: $T_1 = X_1$ and, for $n > 1$, $T_n = T_n' \cup T_n''$ where

$$T_n' = \{x^p \mid x \in T_{n-1}\}, \quad T_n'' = X_n \cup \{[x,y] \mid x \in T_r'', y \in T_s'',\ r+s = n\}.$$

If F_n' is the closed subgroup of F generated by the T_k with $k \geq n$, then (F_n') is a p-central series of F (cf. [22], §1.2). If $\mathrm{gr}'(F)$ is the associated graded Lie-algebra, the inclusions $F_n' \subseteq F_n$ induce a Lie algebra homomorphism $\mathrm{gr}'(F) \to \mathrm{gr}(F)$. If $p \neq 2$ or if $p = 2$ and $e_i > 1$ for all i, we obtain a sequence of Lie algebra homomorphisms over $\mathbb{F}_p[\pi]$

$$L \to \mathrm{gr}'(F) \to \mathrm{gr}(F) \to \mathrm{gr}(A),$$

where the homomorphism $L \to \mathrm{gr}'(F)$ sends ξ_i to ξ_i', the image of ξ_i in $\mathrm{gr}'_{e_i}(F)$, and hence is surjective since the ξ_i' generate $\mathrm{gr}'(F)$ as a Lie algebra over $\mathbb{F}_p[\pi]$. The composite of these homomorphisms sends ξ_i to ξ_i and hence is injective. Thus $\mathrm{gr}'(F) \to \mathrm{gr}(F)$ is injective from which it follows inductively that $F_n' = F_n$ for all n and hence that $L = \mathrm{gr}(F)$.

If $p = 2$ and $e_i = 1$ for some i, we have to replace L by the free mixed Lie algebra on $\xi_1,\dots,\xi_m$ and the result follows by the Birkhoff-Witt theorem for mixed Lie algebras (cf. [22], §1.2).

The above filtration (F_n) is called the (x,e)-filtration of F. If $e_i = 1$ for all i then (F_n) is the lower p-central series of F. We will prove Theorem 1.2 in the more general context of an (x,e)-filtration.

Let $r_1,\dots,r_d \in F$ and let $R = (r_1,\dots,r_d)$ be the closed normal subgroup of F generated by $r_1,\dots,r_d$. Let $\rho_i \in \mathrm{gr}_{h_i}$ be the initial form of r_i with respect to the (x,e)-filtration (F_n) of F. The presentation $G = F/(r_1,\dots,r_d)$ is said to be strongly free with respect to the (x,e)-filtration if $\rho_1,\dots,\rho_d$ is a strongly free sequence of Lie polynomials in $\xi_1,\dots,\xi_m$ with coefficients in $\mathbb{F}_p[\pi]$. In this case, the pro-p-group G is called mild with respect to the (x,e)-filtration. If $G = F/R$ and G_n is the image of F_n in $G = F/R$ then $(G_n)_{n\geq 1}$ is a p-filtration of G.

Theorem 4.1. *Let F be the free pro-p-group on $x_1, \ldots, x_m$ and let $G = F/(r_1, \ldots, r_d)$, with r_i in $F^p[F,F]$ and $d \geq 1$. Suppose that the initial forms $\rho_1, \ldots, \rho_d$ of $r_1, \ldots, r_d$ are strongly free with respect to the (x,e)-filtration (F_n) of F. Let $R = (r_1, \ldots, r_d)$ and let G_n be the image of F_n in G. Then*

(a) *We have* $\mathrm{gr}(G) = \mathrm{gr}(F)/(\rho_1, \ldots, \rho_d)$*,*
(b) *The group $R/[R,R]$ is a free $\mathbb{Z}_p[[G]]$-module on the images of $r_1, \ldots, r_d$,*
(c) *The presentation $G = F/R$ is minimal and cd(G)=2.*
(d) *The enveloping algebra of* $\mathrm{gr}(G)$ *is the graded algebra associated to the filtration w_B of $B = \mathbb{Z}_p[[G]]$ induced by the (x,e)-valuation w of $\mathbb{Z}_p[[F]]$.*
(e) *The algebra $\mathbb{Z}_p[[G]]$ is an integral domain with valuation w_B.*
(f) *The Poincaré series of* $\mathrm{gr}(B)$ *is* $1/(1-t)(1-(t^{e_1}+\cdots+t^{e_m})+t^{h_1}+\ldots+t^{h_d}))$.
(g) *If* $1-(t^{e_1}+\cdots+t^{e_m})+t^{h_1}+\ldots+t^{h_d} = (1-\alpha_1 t)(1-\alpha_2 t)\cdots(1-\alpha_s t)$ *then*

$$\dim_{\mathbb{F}_p}(gr_n(G)) = \sum_{k=1}^{n} \frac{1}{k} \sum_{r|k} \mu(k/r)(\alpha_1^r + \alpha_2^r + \cdots + \alpha_s^r).$$

Proof. Let $R_n = R \cap F_n$ and let $\mathrm{gr}(R)$ be the Lie algebra associated to the p-filtration (R_n) of R. Identifying $\mathrm{gr}(R)$ with its image in $\mathrm{gr}(F)$ the ideal $\mathfrak{r} = (\rho_1, \ldots, \rho_d)$ is contained in $\mathrm{gr}(R)$. An easy inductive argument shows that $\mathfrak{r} = \mathrm{gr}(R)$ if and only if the induced homomorphism

$$\theta : \mathfrak{r}/[\mathfrak{r},\mathfrak{r}] \to \mathrm{gr}(R)/[\mathrm{gr}(R), \mathrm{gr}(R)]$$

is surjective (and hence bijective). Let U and U' be respectively the enveloping algebras of $\mathfrak{g} = \mathrm{gr}(F)/\mathfrak{r}$ and $\mathrm{gr}(G) = \mathrm{gr}(F)/\mathrm{gr}(R)$. The canonical homomorphism $\psi : U \to U'$ is surjective and is compatible with θ; which means that for $x \in \mathfrak{r}/[\mathfrak{r},\mathfrak{r}],\ u \in U$ we have

$$\theta(u \cdot x) = \psi(u) \cdot \theta(x).$$

Let $M = R/[R,R]$ and let M_n be the image of R_n in M. Then (M_n) is a p-filtration of M and we have $\mathrm{gr}(M) = \mathrm{gr}(R)/\mathrm{gr}([R,R])$ where $\mathrm{gr}([R,R])$ is the Lie algebra associated to the filtration $([R,R]_n)$ with $[R,R]_n = [R,R] \cap F_n$. Since $\mathrm{gr}(M)$ is an abelian Lie algebra, we have a canonical surjection

$$\theta' : \mathrm{gr}(R)/[\mathrm{gr}(R), \mathrm{gr}(R)] \to \mathrm{gr}(M)$$

which is injective in degree n if and only if

$$\mathrm{gr}_n([R,R]) = [\mathrm{gr}(R), \mathrm{gr}(R)]_n.$$

Let $B = \mathbb{Z}_p[[G]]$ be the completed group algebra of G over $\mathbb{Z}_p$ and let B_n be the image of A_n in B under the canonical surjection $A \to B$. The graded ring $\mathrm{gr}(B)$ associated to the filtration (B_n) is an algebra over $F_p[\pi]$. If $\mathcal{R}$ is the ideal of $\mathrm{gr}(A)$ generated by $\mathrm{gr}(R)$ then U' is canonically isomorphic to $\mathrm{gr}(A)/\mathcal{R}$ and the kernel of the canonical homomorphism of $\mathrm{gr}(A)$ onto $\mathrm{gr}(B)$ contains $\mathcal{R}$. Hence we obtain a surjective homomorphism

$$\psi' : U' \to \mathrm{gr}(B).$$

In addition, $\mathrm{gr}(M)$ is a $\mathrm{gr}(B)$-module since $B_n \cdot M_k \subseteq M_{n+k}$ and θ' is compatible with ψ'.

We now show that θ and θ' are bijective. The proof is by induction on the degrees. Suppose then that θ and θ' are bijective in degrees $n < k$. Since $\mathfrak{r}_n = \mathrm{gr}(R)_n$ for $n < h = \min(h_1, \ldots, h_d)$, we may assume that $k \geq h$.

(I) *θ is injective in degree k.* Since θ is surjective in degrees $< k$ we have $\mathfrak{r}_n = \mathrm{gr}_n(R)$. Hence

$$[\mathfrak{r}, \mathfrak{r}]_k = [\mathrm{gr}(R), \mathrm{gr}(R)]_k$$

which shows that θ is injective in degree k.

(II) *θ' is bijective in degree k.* We have to show that $\mathrm{gr}_k([R,R]) = [\mathrm{gr}(R), \mathrm{gr}(R)]_k$. For this we will construct a closed subgroup H of R generated by a finite number of elements $z_1, \ldots, z_s$ such that

(i) H is a free pro-p-group with basis $z_1, \ldots, z_s$;

(ii) If $e'_i = \omega(z_i)$ is the filtration degree of z_i and if $H_n = H \cap R_n$ then (H_n) is the (z, e')-filtration of H;

(iii) $\mathrm{gr}_n(H) = \mathrm{gr}_n(R)$ for $n < k$.

If we grant the existence of such a subgroup H we have $\mathrm{gr}_n([H,H]) = \mathrm{gr}_n([R,R])$ for $n \leq k$ and

$$\mathrm{gr}_n([H,H]) = [\mathrm{gr}(H), \mathrm{gr}(H)]_n$$

for all n. Thus

$$\mathrm{gr}_k([R,R]) = \mathrm{gr}_k([H,H]) = [\mathrm{gr}(H), \mathrm{gr}(H)]_k = [\mathrm{gr}(R), \mathrm{gr}(R)]_k.$$

Let us now construct H. We first note that $\mathfrak{r}$ is a free Lie algebra over $\mathbb{F}_p[\pi]$ since $L/\mathfrak{r}$ is a free $\mathbb{F}_p[\pi]$-module (cf.[17], Proposition 4). Choose a homogeneous free generating set for $\mathfrak{r}$ and let $\zeta_1, \ldots, \zeta_s$ the elements of this generating set which are of degree $< k$. If e'_i is the degree of ζ_i let $z_i \in R_{e'_i}$ whose image in $\mathrm{gr}_{e'_i}(R)$ is ζ_i. Let H be the closed subgroup of R generated by $z_1, \ldots, z_s$. Then property (iii) holds by construction. To verify (i) and (ii), let E be the free pro-p-group on the letters $z_1, \ldots, z_s$ and let (E_n) be the (z, e')-filtration of E. The homomorphism $\alpha : E \to H$ defined by $\alpha(z_i) = z_i$ sends E_n into H_n and, if $\overline{z}_i$ is the image of z_i in $\mathrm{gr}_{e'_i}(E)$, the induced homomorphism

$$\alpha_* : \mathrm{gr}(E) \to \mathrm{gr}(H) \subset \mathrm{gr}(R)$$

sends $\overline{z}_i$ to ζ_i. But $\mathrm{gr}(E)$ is a free Lie algebra over $\mathbb{F}_p[\pi]$ with basis $\overline{z}_1, \ldots, \overline{z}_s$ since $e'_i > 1$ for all i. Since $\zeta_1, \ldots, \zeta_s$ is part of a basis for the free Lie algebra $\mathfrak{r}$, the homomorphism α_* is injective. It follows that α is injective and hence bijective.

It remains to show $\alpha(E_n) = H_n$. Suppose that we have shown that $\alpha(E_k) = H_k$ for $1 \leq k \leq n$; this is true for $n = 1$. Let $y \in H_{n+1}$ and suppose that $y \notin H'_{n+1}$. Then there exists $k \leq n$ such that $y \in H'_k, y \notin H'_{k+1}$. Let $x \in E_k$ with $\alpha(x) = y$. Then $x \notin E_{k+1}$ and so $\xi = \mathrm{gr}_k(x) \neq 0$. But $\alpha_*(\xi) = 0$ since $y = \alpha(x) \in H_{k+1}$. This contradicts the injectivity of α_*. So $H'_{n+1} = H_{n+1}$ and so, by induction, it follows that (H_n) is the (z, e')-filtration of H.

(III) *θ is surjective in degree k.* To show this it suffices to show that $\theta'' = \theta' \circ \theta$ is surjective in degree k. If $e_i = \omega(r_i)$, we may assume that $e_i \leq e_j$ for $i \leq j$ and that $e_i > k$ for $i > t$. Let β be a non-zero element of $\mathrm{gr}_k(M)$ and let $b \in M_k$ be an element whose image in $\mathrm{gr}_k(M)$ is β. If $\overline{r}_i$ is the image of r_i in M_{e_i}, we can choose b so that

$$b = v_1 \cdot \overline{r}_1 + \ldots + v_t \cdot \overline{r}_t,$$

where $v_i \in B$. Since $B_i \cdot M_j \subseteq M_{i+j}$ we can suppose that the above expression for b involves only those terms $v_i \cdot \overline{r}_i$ with $w_B(v_i) + e_i \leq k$, where $w_B(v) = \sup\{n \mid v \in B_n\}$. Since $b \notin M_{k+1}$, this expression is not empty. Let g be the smallest integer of the form $w_B(v_i) + e_i$ and let D be the set of integers i with $w_B(v_i) + e_i = g$. Let u_i be a homogeneous element of U with $\psi''(u_i) = \overline{v}_i$, where $\psi'' = \psi' \circ \psi$ and $\overline{v}_i$ is the image of v_i in $\mathrm{gr}_n(B)$ with $n = g - e_i$. Let $\overline{\rho}_i$ be the image of ρ_i in $\mathfrak{r}/[\mathfrak{r}, \mathfrak{r}]$ and let $\xi = \sum_{i \in D} u_i \cdot \overline{\rho}_i$. If $g < k$, we have $\theta(\xi) = 0$ which implies that $\xi = 0$ since ξ is of degree g and θ is injective in degree g. But this contradicts the fact that $\mathfrak{r}/[\mathfrak{r}, \mathfrak{r}]$ is a free U-module. Hence $g = k$ and $\beta = \theta''(\xi)$ which implies the surjectivity of of θ'' in degree k.

From the above it follows that the homomorphism $\psi' : \mathrm{gr}(A)/\mathcal{R} \to \mathrm{gr}(B)$ is bijective. Since $\mathfrak{r} = \mathrm{gr}(R)$, we have $U = \mathrm{gr}(A)/\mathcal{R}$ which yields (d) and (e).

From the fact that $\mathrm{gr}(M)$ is a free $\mathrm{gr}(B)$-module on the images of $\overline{r}_1, \ldots, \overline{r}_d$, it follows that M is a free B-module on $r_1, \ldots, r_d$ which gives (b). Using this, we obtain

$$H^2(G, \mathbb{Z}/p\mathbb{Z}) \cong H^1(R, \mathbb{Z}/p\mathbb{Z})^F \cong \mathrm{Hom}(R/[R,R], \mathbb{Z}/p\mathbb{Z})^F \cong (\mathbb{Z}/p\mathbb{Z})^d,$$

which implies that d is the minimal number of relations for G. Finally, using the standard exact sequence

$$0 \to R/[R,R] \to B^m \to B \to \mathbb{Z}_p \to 0,$$

we obtain that the cohomological dimension of G is 2 (cf. [6], p.459). This gives (c). To get (g) we take logarithms on both sides of the identity

$$\prod_{n \geq 1} (1 - t^n)^{b_n} = (1 - \alpha_1 t)(1 - \alpha_2 t) \cdots (1 - \alpha_d t),$$

where b_n is the dimension of the n-th homogeneous component of $\mathrm{gr}(G)/\pi\mathrm{gr}(G)$, and use the fact that $\dim_{\mathbb{F}_p} \mathrm{gr}_n(G) = \sum_{k=1}^n b_k$. □

Since the (x, e)-filtration of F is the lower p-central series of F when $e_i = 1$ for all i and the filtration of A is given by powers of the ideal I which is the kernel of the augmentation homomorphism of $\mathbb{Z}_p[[F]]$, we obtain that the induced filtration of $B = \mathbb{Z}_p[[G]]$ is given by powers of the augmentation ideal J of B. Moreover, our proof shows that $G_n = G \cap (1 + I^n)$; in other words, the lower p-central series of G is induced by the J-adic filtration of $\mathbb{Z}_p[[G]]$. This yields Theorem 1.2.

When $p = 2$ and the initial forms ρ_i of the relators r_i in a minimal presentation for G are of degree 2, that the ρ_i are Lie polynomials with coefficients in $\mathbb{F}_2[\pi]$ is equivalent to the torsion subgroup of $G/[G,G]$ having exponent ≥ 4. For example, this shows that the group

$$\langle x_1, x_2, \ldots, x_m \mid x_1^4[x_1, x_2] = x_2^4[x_2, x_3] = \cdots = x_{m-1}^4[x_{m-1}, x_m] = x_m^4[x_m, x_1] = 1 \rangle$$

is a mild pro-2-group if $m \geq 4$ since

$$\rho_1 = [\xi_1, \xi_2], \rho_2 = [\xi_2, \xi_3], \ldots, \rho_m = [\xi_m, \xi_1].$$

More generally, the torsion subgroup of $G/[G,G]$ has exponent ≥ 4 if and only if the initial forms ρ_i are Lie polynomials $\overline{\rho}_i$ over $\mathbb{F}_2$ modulo $\pi\mathrm{gr}(F)^*$, where $\mathrm{gr}(F)^* = \oplus_{n \geq 2} \mathrm{gr}(F)$. In this case, the given presentation can be shown to be strongly free if $\overline{\rho}_1, \ldots, \overline{\rho}_d$ is a strongly free sequence over $\mathbb{F}_2$ (cf.[21]).

5. Zassenhaus Filtrations

Theorem 4.1 can be extended to the case of filtrations induced by valuations of the completed group ring $\mathbb{F}_p[[F]]$. The Lie algebras associated to these filtrations are restricted Lie algebras in the sense of Jacobson[11].

Let F be the free pro-p-group on $x_1,\ldots,x_m$. The completed group algebra $\bar{A} = \mathbb{F}_p[[F]]$ over the finite field $\mathbb{F}_p$ is isomorphic to the algebra of formal power series in the non-commuting indeterminates $X_1,\ldots,X_m$ over $\mathbb{F}_p$. Identifying F with its image in $\bar{A}$, we have $x_i = 1+X_i$.

If $e_1,\ldots,e_m$ are integers >0, we define a valuation $\bar{w}$ of $\bar{A}$ by setting

$$\bar{w}(\sum_{i_1,\ldots,i_k} a_{i_1,\ldots,i_k}X_{i_1}\cdots X_{i_k}) = \inf_{i_i,\ldots,i_k}(e_{i_1}+\cdots+e_{i_k}).$$

Let

$$\bar{A}_n = \{u\in\bar{A}\mid \bar{w}(u)\geq n\},\ \mathrm{gr}_n(\bar{A}) = \bar{A}_n/\bar{A}_{n+1},\ \mathrm{gr}(\bar{A}) = \oplus_{n\geq 0}\mathrm{gr}_n(\bar{A}).$$

Then $\mathrm{gr}(\bar{A})$ is a graded $\mathbb{F}_p$-algebra. If ξ_i is the image of X_i in $\mathrm{gr}_{e_i}(\bar{A})$ then $\mathrm{gr}(\bar{A})$ is the free associative $\mathbb{F}_p$-algebra on $\xi_1,\ldots,\xi_m$ with a grading in which ξ_i is of degree e_i . The Lie subalgebra $\bar{L}$ of $\mathrm{gr}(\bar{A})$ generated by the ξ_i is the free Lie algebra over $\mathbb{F}_p$ on $\xi_1,\ldots,\xi_m$ by the Birkhoff-Witt Theorem. Note that when $e_i=1$ for all i we have $\bar{A}_n = \bar{I}^n$, where $\bar{I}$ is the augmentation ideal $(X_1,\ldots,X_m)$ of $\bar{A}$.

A decreasing sequence (G_n) of closed subgroups of a pro-p-group G which satisfies

$$[G_i,G_j]\subseteq G_{i+j},\quad G_i^p\subseteq G_{pi}.$$

is called a called, after Lazard [22], a p-restricted filtration of G.

For $n\geq 1$, let $F_n = (1+\bar{A}_n)\cap F$. Then (F_n) is a p-restricted filtration of F. This filtration is also called the Zassenhaus (x,e)-fitration of F. The mapping $x\mapsto x^p$ induces an operator P on $\mathrm{gr}(F)$ sending $\mathrm{gr}_n(F)$ into $\mathrm{gr}_{pn}(F)$. With this operator, $\mathrm{gr}(F)$ is a restricted Lie algebra over $\mathbb{F}_p$. If $e_i=1$ for all i, the subgroups F_n are the so-called dimension subgroups mod p. They can be defined by

$$F_n = <[y_1,[\cdots[y_{r-1},y_r]\cdots]]^{p^s}\mid y_1,\ldots,y_r\in F,\ rp^s\geq n> .$$

Let $r_1,\ldots,r_d\in F$ and let $R=(r_1,\ldots,r_d)$ be the closed normal subgroup of F generated by $r_1,\ldots,r_d$. Let $\rho_i\in\mathrm{gr}_{h_i}$ be the initial form of r_i with respect to the Zassenhaus (x,e)-filtration (F_n) of F. The presentation $G=F/(r_1,\ldots,r_d)$ is said to be strongly free with respect to the Zassenhaus (x,e)-filtration if $\rho_1,\ldots,\rho_d$ is a strongly free sequence of Lie polynomials in $\bar{L}$. In this case, the pro-p-group G is called mild with respect to the Zassenhaus (x,e)-filtration. If $G=F/R$ and G_n is the image of F_n in $G=F/R$ then $(G_n)_{n\geq 1}$ is a p-restricted filtration of G.

Theorem 5.1. *Let F be the free pro-p-group on $x_1,\ldots,x_m$ and let $G=F/(r_1,\ldots,r_d)$, with r_i in $F^p[F,F]$ and $d\geq 1$. Suppose that the initial forms $\rho_1,\ldots,\rho_d$ of $r_1,\ldots,r_d$ are strongly free with respect to the Zassenhaus (x,e)-filtration (F_n) of F. Let $R=(r_1,\ldots,r_d)$ and let G_n be the image of F_n in G. Then*

(a) *We have $\mathrm{gr}(G)=\mathrm{gr}(F)/(r_1,\ldots,r_d)$,*
(b) *The group $R/R^p[R,R]$ is a free $\mathbb{F}_p[[G]]$-module on the images of $\rho_1,\ldots,\rho_d$,*
(c) *The presentation $G=F/R$ is minimal and cd(G)=2.*

(d) *The enveloping algebra of* $\mathrm{gr}(G)$ *is the graded algebra associated to the filtration* $w_{\bar{B}}$ *of* $\bar{B} = \mathbb{F}_p[[G]]$ *induced by the* (x, e)*-valuation* $\bar{w}$ *of* $\bar{A} = \mathbb{F}_p[[F]]$.
(e) *The algebra* $\bar{B}$ *is an integral domain and* $w_{\bar{B}}$ *is a valuation of* $\bar{B}$.
(f) *The valuation* $w_{\bar{B}}$ *of* $\bar{B}$ *induces the filtration* (G_n) *of* G.
(g) *The Poincaré series of* $\mathrm{gr}(\bar{B})$ *is* $1/(1-(t^{e_1}+\cdots+t^{e_m})+t^{h_1}+\ldots+t^{h_d})$.
(h) *If* $e_i = 1$ *for all* i *and* $a_n = \dim \mathrm{gr}_n(G)$ *then*

$$\prod_{n\geq 1} \frac{(1-t^{pn})}{1-t^n}^{a_n} = \frac{1}{1-mt+t^d}.$$

Proof. In [15], Koch proves that if $\bar{\mathcal{R}}/\bar{\mathcal{R}}\bar{I}$ is a free $\bar{A}/\bar{\mathcal{R}}$ module on the images of $\rho_1, \ldots, \rho_m$ then $\mathrm{gr}(\bar{\Gamma}) = \bar{A}/\bar{\mathcal{R}}$, where $\bar{\mathcal{R}}$ is the ideal of $\bar{A} = \mathrm{gr}(\bar{\Lambda})$ generated by $\rho_1, \ldots, \rho_m$. The former is true if $\rho_1, \ldots, \rho_m$ lie in $\tilde{L}$ and are strongly free since $\bar{\mathcal{R}}/\bar{\mathcal{R}}\bar{I}$ is the image of the free $\bar{A}/\bar{\mathcal{R}}$-module $\tilde{\mathfrak{r}}/[\tilde{\mathfrak{r}}, \tilde{\mathfrak{r}}]$ under the injective mapping

$$\tilde{\mathfrak{r}}/[\tilde{\mathfrak{r}}, \tilde{\mathfrak{r}}] \to \bar{I}/\bar{\mathcal{R}}\bar{I}$$

where $\tilde{\mathfrak{r}}$ is the ideal of the quadratic Lie algebra $\tilde{L}$ generated by $\rho_1, \ldots, \rho_m$. This proves (e).

Now consider the exact sequence

$$0 \to \bar{\mathfrak{r}}/[\bar{\mathfrak{r}}, \bar{\mathfrak{r}}] \to \mathrm{gr}(\bar{B})^m \to \mathrm{gr}(\bar{B}) \to \mathbb{F}_p \to 0,$$

where $\bar{\mathfrak{r}}$ is the ideal of $\bar{L}$ generated by $\rho_1, \ldots, \rho_d$. Since by assumption, $\bar{\mathfrak{r}}/[\bar{\mathfrak{r}}, \bar{\mathfrak{r}}]$ is a free $\mathrm{gr}(\bar{B})$-module of rank d, we obtain the exact sequence

$$0 \to \mathrm{gr}(\bar{B})^d \to \mathrm{gr}(\bar{B})^m \to \mathrm{gr}(\bar{B}) \to \mathbb{F}_p \to 0.$$

By a result of Serre (cf. [22], V, 2.1), we obtain the exact sequence

$$0 \to \bar{B}^d \to \bar{B}^m \to \bar{B} \to \mathbb{F}_p \to 0.$$

This yields (g) and, by a result of [6], it proves (b) and (c). If $\mathfrak{R} = (\rho_1, \ldots, \rho_d)$ is the ideal of the restricted Lie algebra $\mathrm{gr}(F)$ generated by $\rho_1, \ldots, \rho_d$, we have canonical homomorphisms of restricted Lie algebras

$$\mathrm{gr}(F)/\mathfrak{R} \to \mathrm{gr}(G) \to \mathrm{gr}'(G) \to \mathrm{gr}(\bar{B}),$$

where the first arrow is surjective and $\mathrm{gr}'(G)$ is the restricted Lie algebra associated to the Zassenhaus filtration (G'_n) of G induced by the filtration $w_{\bar{B}}$ of B. Since $\mathrm{gr}(\bar{B})$ is the enveloping algebra of the restricted Lie algebra $\mathrm{gr}(F)/\mathfrak{R}$, the Birkhoff-Witt Theorem for restricted Lie algebras shows that all arrows are injective which yields (a) and (d). The injectivity of $\mathrm{gr}(G) \to \mathrm{gr}'(G)$ yields $G_n = G'_n$ for all n by induction which proves (f). The assertion (h) follows from (g) and [22], Proposition A.3.10. □

Corollary 5.2. *If* G *is a mild pro-*p*-group with* $r(G) \geq d(G)$ *then* G *is non-analytic.*

This follows from [22], A3.12.1 and the fact the the reciprocal of the Poincaré series $P(t)$ of $\mathrm{gr}(\bar{B})$ has a root strictly between 0 and 1 which implies that the coefficients of $P(t)$ have exponential growth.

6. Examples of Mild Groups

The groups $G_S(p)$ and $G_{S_p}(p)$ are a rich source of mild groups due to the following fact pointed out to us by H. Kisilevsky and J. Sonn.

Proposition 6.1. *Let $p \neq 2$ and let S be a given set of primes congruent to 1 mod p. Then a prime $q \equiv 1$ mod p can be found with the additional edges of $\Gamma_{S\cup\{q\}}(p)$ and $\Gamma_{(S\cup\{q\})_p}(p)$ arbitrarily prescribed.*

Proof. Let $S = \{q_1, \dots, q_m\}$. The proof is based on the fact that the fields

$$\mathbb{Q}(\mu(pq_1)), \dots \mathbb{Q}(\mu(pq_m), \mathbb{Q}(\mu(p), \sqrt[p]{q_1}), \dots, \mathbb{Q}(\mu(p), \sqrt[p]{q_m}), \mathbb{Q}(\mu(p^2))$$

are linearly disjoint over $\mathbb{Q}(\mu(p))$. Let E_i be the unique extension of $\mathbb{Q}(\mu(p))$ of degree p and contained in $\mathbb{Q}(\mu(pq_i))$. If σ_j is a generator $\mathrm{Gal}(\mu(pq_j))$ over $\mathbb{Q}(\mu(p))$ then E_j is the fixed field of σ_j^p. Let K be composite of the fields

$$E_1, \dots, E_m, \mathbb{Q}(\mu(p), \sqrt[p]{q_1}), \dots, \mathbb{Q}(\mu(p), \sqrt[p]{q_m}), \mathbb{Q}(\mu(p^2)).$$

The field K is Galois over $\mathbb{Q}$ and the subgroup $H = \mathrm{Gal}(K/Q(\mu_p))$ of $\mathrm{Gal}(K/\mathbb{Q})$ is the direct product of the Galois groups of these fields over $\mathbb{Q}(\mu(p))$. These groups are cyclic of order p. If $F_{\mathfrak{Q}} \in \mathrm{Gal}(K/\mathbb{Q})$ is the Frobenius automorphism at the unramified prime $\mathfrak{Q}$ of K and $\mathfrak{Q}$ lies above the rational prime q then $F_{\mathfrak{Q}} \in H$ if and only if $q \equiv 1$ mod p.

If $F_{\mathfrak{Q}} \in H$ then the restriction of $F_{\mathfrak{Q}}$ to E_i is the identity if and only if q is a p-th power mod q_i and the restriction of $F_{\mathfrak{Q}}$ to $\mathbb{Q}(\sqrt[p]{q_i}, \mu(p))$ is the identity if and only if q_i is a p-th power mod q. The restriction of $F_{\mathfrak{Q}}$ to $\mathbb{Q}(\mu(p^2))$ is the identity if and only if $q \equiv 1$ mod p^2. By the Čebotarev density theorem, every $g \in H$ is is of the form $F_{\mathfrak{Q}}$ for some $\mathfrak{Q}$. Therefore, we can extend the directed graph $\Gamma_S(p)$ or $\Gamma_{S_p}(p)$ by a single prime $q \equiv 1$ mod p with prescribed edges joining the primes of S to q and q to the primes of S or S_p. □

Corollary 6.2. *Given a finite directed graph Γ, we have $\Gamma = \Gamma_S(p)$ for some S.*

We don't know if the linking numbers can be arbitrarily prescribed.

Corollary 6.3. *Let p be a prime and S a finite set of primes $\equiv 1$ mod p. If $|S| \geq 2$ then S can be extended to such a set S' with $|S'| = 2|S|$ and $\Gamma_{S'}(p)$ a non-singular circuit.*

Proof. Let $S = \{q_1, \dots, q_m\}$. We now extend S by a single prime r_1 so that q_1r_1, r_1q_2 are edges with r_1q_1 not an edge. Now extend the new graph $\Gamma_{S\cup\{r_1\}}$ by another prime r_2 so that q_2r_2 and r_2q_2 are the only new edges. Continuing in this way, we see that we can extend Γ_S to a non-singular circuit $\Gamma_{S'}$ having $2m$ vertices. If $1 \leq i \leq m$ let $v_{2i-1} = r_i$ and $v_{2i} = q_i$. Then $v_1 \cdots v_{2m}v_1$ is the required non-singular circuit. □

If $S = \{7, 13, 19, 31\}$ with the primes of S ordered as written, the initial forms of the relators in the Koch presentation of the group $G_S(3)$ are, modulo π,

$$\begin{aligned}
\rho_1 &= [\xi_1, \xi_2] - [\xi_1, \xi_4],\\
\rho_2 &= [\xi_2, \xi_3] + [\xi_2, \xi_4],\\
\rho_3 &= [\xi_3, \xi_1] + [\xi_3, \xi_2] - [\xi_3, \xi_4],\\
\rho_4 &= [\xi_1, \xi_4].
\end{aligned}$$

The circuit $\xi_1\xi_2\xi_3\xi_4\xi_1$ is not a non-singular circuit since $\xi_3\xi_1$ is an edge of Γ. However, if we add ρ_4 to ρ_1, make the change of variable

$$\xi_i \mapsto \xi_i \ (i \neq 4), \xi_4 \mapsto -\xi_4 + \xi_1 + \xi_2,$$

and subtract ρ_1 from ρ_4, we obtain the equivalent Koch presentation for $\overline{\mathfrak{g}} = \overline{L}/(\rho_1, \rho_2, \rho_3, \rho_4)$

$$\begin{aligned}
\rho_1 &= [\xi_1, \xi_2],\\
\rho_2 &= [\xi_2, \xi_1] + [\xi_2, \xi_3] - [\xi_2, \xi_4],\\
\rho_3 &= [\xi_3, \xi_4],\\
\rho_4 &= [\xi_4, \xi_1]
\end{aligned}$$

which is strongly free as $\xi_1\xi_2\xi_3\xi_4\xi_1$ is now a non-singular circuit since $\xi_1\xi_3$ and $\xi_3\xi_1$ are not edges of Γ. Hence G_S is a mild group. Note that, after adding ρ_1 to ρ_2 and making the change of variable $\xi_3 \mapsto \xi_3 + \xi_4$, $\xi_i \mapsto \xi_i$ $(i \neq 3)$, one obtains that the given presentation is equivalent modulo π to

$$\rho_1 = [\xi_1, \xi_2], \ \rho_2 = [\xi_2, \xi_3], \ \rho_3 = [\xi_3, \xi_4], \ \rho_4 = [\xi_4, \xi_1].$$

We can produce an infinite number of mild groups G with $d(G) = r(G) = 2, 3$. For example,

(1) the group
$$< x, y \mid x^{p^a}[[x, y], [y, [x, y]]]u, \quad y^{p^b}[[x, [x, y]], [y, [x, [x, y]]]]v >$$
with $a \geq 4, b \geq 5$, $u \in F_6, v \in F_8$ is mild,

(2) the group
$$< x, y, z \mid x^{p^a}[x, y]u = 1, \quad y^{p^b}[z, [z, y]]v, \quad z^{p^c}[x, [z, y]]w >$$
with $u \in F_3, v, w \in F_4, a \geq 1, b, c \geq 2$ is mild if $p \neq 2$ or if $p = 2$, $a > 1$,

(3) the group
$$< x, y, z | x^{p^a}[z, [x, y]]u, \quad y^{p^b}[z, [z, y]]u, \quad z^{p^c}[x, [z, y]]w >$$
with $u, v, w \in F_4, a, b, c \geq 2$ is mild.

For any $m \geq 4$ we can construct mild pro-p-groups with $d(G) = m$,

$$1 \leq r(G) \leq s(m) = \max_k k(m - k)$$

and the initial forms of these relators of degree 2. For example, if $p \neq 2$, the pro-p-group

$$G = \langle x_1, x_2, x_3, x_4, x_5 \mid x_1^p[x_1, x_2], x_2^p[x_1, x_4], x_3^p[x_3, x_2], x_4^p[x_3, x_4], x_5^p[x_5, x_2], [x_5, x_4]\rangle$$

is mild with $d(G) = 5$, $r(G) = s(5) = 6$. Moreover, we have $G/[G, G]$ finite.

7. The Group $G_{S_\infty}(2)$.

For $p = 2$, the group $G_{S_\infty}(2)$ with $S_\infty = S \cup \{\infty\}$ has the Koch presentation $< x_1, \ldots, x_m \mid r_1, \ldots, r_m >$ where

$$r_i = x_i^{q_i-1} \prod_{j \neq i} [x_i, x_j]^{\ell_{ij}} w_i$$

with $w_i \in F_3$.

If $q_i \equiv 1 \bmod 4$ and the initial forms ρ_i of these relators are of degree 2 then the ρ_i are Lie polynomials in $\xi_1, \ldots, \xi_m$ with coefficients in $\mathbb{F}_2$. In this case Theorem 1.2 applies. However, it is not of much use as the linking numbers are symmetric $\ell_{ij} = \ell_{ji}$ by quadratic reciprocity. This implies that

$$\rho_1 + \ldots + \rho_m = 0$$

and so the sequence $\rho_1, \ldots, \rho_m$ is not strongly free. However, the group $G_{S_\infty}(2)$ could still be shown to be a mild group by considering the modified presentation obtained by replacing r_m by $r'_m = r_1 r_2 \cdots r_m$. In this case the initial form of r'_m would be of degree > 2. However, the initial form of r'_i may not be a Lie polynomial in $\xi_1, \ldots, \xi_m$ with coefficients in $\mathbb{F}_2[\pi]$ but this will be true modulo π. In this case Theorem 4.1 does not apply but we are able to extend it to cover this case (cf.[21]). However, Theorem 5.1 does apply.

An example of this is furnished by the pro-2-group H having the presentation

$$< x_1, x_2, x_3, x_4 \mid x_1^5 = x_1^{x_3 x_2}, x_2^5 = x_2^{x_4 x_3}, x_3^5 = x_3^{x_1 x_4}, x_4^5 = x_4^{x_2 x_1} > .$$

This group appears as a subgroup of index 4 of the group on 2 generators x, y and relations $x^{y^2 xyxy} = x^5$, $y^4 = 1$ (cf.[5]). This group has a presentation whose initial forms of the relators are

$$\begin{aligned}
\rho_1 &= [\xi_1, \xi_2] + [\xi_1, \xi_3], \\
\rho_2 &= [\xi_2, \xi_3] + [\xi_2, \xi_4], \\
\rho_3 &= [\xi_3, \xi_4] + [\xi_3, \xi_1], \\
\rho_4 &= \pi P\xi_1 + \pi P\xi_2 + \pi P\xi_3 + \pi P\xi_4 + [\xi_1, [\xi_2, \xi_4]].
\end{aligned}$$

Working modulo π, these relators become

$$\begin{aligned}
\rho_1 &= [\xi_1, \xi_2] + [\xi_1, \xi_3], \\
\rho_2 &= [\xi_2, \xi_3] + [\xi_2, \xi_4], \\
\rho_3 &= [\xi_3, \xi_4] + [\xi_3, \xi_1], \\
\rho_4 &= [\xi_1, [\xi_2, \xi_4]].
\end{aligned}$$

We are unable to prove that these elements form a strongly free sequence over $\mathbb{F}_2$ with the methods in this paper but computations using GAP indicate that the Poincaré series of the enveloping of $L/(\rho_1, \rho_2, \rho_3, \rho_4)$ over $\mathbb{F}_2$ is

$$\frac{1}{1 - 4t + 3t^2 + t^3}.$$

In [27], [24] the case $\ell_{ij} = 0$ for all i, j is considered and the initial forms computed in certain cases in degree 3 modulo squares using the connection between the Rédei symbols and the Milnor μ_2-invariants. For example, in the case $S = \{5, 41, 61\}$, they find that

$$\begin{aligned}
\rho_1 &= [[\xi_1, \xi_2], \xi_2] + [[\xi_1, \xi_3], \xi_3] + [[\xi_2, \xi_3], \xi_1],\\
\rho_2 &= [[\xi_1, \xi_2], \xi_2] + [[\xi_1, \xi_3], \xi_2] + [[\xi_2, \xi_3], \xi_2] + [[\xi_2, \xi_3], \xi_3],\\
\rho_3 &= [[\xi_1, \xi_3], \xi_2] + [[\xi_1, \xi_3], \xi_3] + [[\xi_2, \xi_3], \xi_1] + [[\xi_2, \xi_3], \xi_2] + [[\xi_2, \xi_3], \xi_3]
\end{aligned}$$

in the restricted Lie algebra associated to the dimension subgroups mod p. Again, we are unable to prove that these elements form a strongly free sequence with the methods in this paper but computations using GAP indicate that they are. If they were then Theorem 5.1 would apply.

8. Questions

In view of these results and results of [5] which show that certain groups of Koch type on two generators have subgroups of finite index which behave like mild groups, we are led to ask the following questions.

Question 1. If $|S| \geq 4$, is $G_S(p)$ of cohomological dimension 2?
Question 2. Is $G_S(p)$ virtually of cohomological dimension 2 for all S?

References

[1] D. Anick, *Non-commutative Algebras and their Hilbert Series*, J. Algebra 78 (1982), 120-140.

[2] D. Anick, *Inert sets and the Lie algebra associated to a group*, J. Algebra, 111 (1987), 154-165.

[3] N. Bourbaki, *Groupes et algèbres de Lie*, Hermann, Paris, CH. 2 (1960).

[4] N. Boston, *p-adic Galois Representations and pro-p-Galois Groups*, "New Horizons in pro-p Groups", (edited by Du Sautoy, Segal, Shalev), Birhauser, Boston 2000.

[5] N. Boston, *Reducing the Fontaine-Mazur Conjecture to Group Theory*, (preprint).

[6] A. Brumer, *Pseudocompact algebras, profinite groups and class formations*, J. Algebra 4, 442-470 (1966).

[7] H. Cartan and S. Eilenberg, *Homological Algebra*, Princeton Math. Ser., No. 19, Princeton 1856.

[8] K. Haberland, *Galois Cohomology of Algebraic Number Fields*, Deutscher Verlag der Wiss., Berlin, 1978.

[9] F. Hajir, *Tame pro-p-galois groups: a survey of recent work*, to appear in Proceedings of the 9th conference on Algebraic Geometry and Coding Theory, Luminy.

[10] S. Halperin and J-M. Lemaire, *Suites inertes dans les algèbres de Lie graduées*, Math. Scand., 61 (1987), No. 1, 39-67.

[11] N. Jacobson, *Lie Algebras*, Interscience, New York, 1962.

[12] H. Koch. *Galois Theory of p-Extensions*, Springer, 2002.

[13] H. Koch, *Zum Satz von Golod-Shafarewitsch*, Math. Nachr. 42 (1969), 321-333.

[14] H. Koch,*On p-extensions with given ramification*, Appendix 1 in [8].

[15] H. Koch, *Über pro-p-Gruppen der kohomologischen Dimension* 2, Math. Nachr. 78 (1977), 285-289.

[16] L.V. Kuzmin, Homology of Profinite Groups, Schur Multipliers, and Class Field Theory, Izv. Akad. Nauk SSSR 33 (1969), 1149-1181.

[17] J. Labute, *Algèbres de Lie et pro-p-groupes définis par une seule relation*, Invent. Math. 4 (1967), 142-158.

[18] J. Labute, *The Determination of the Lie Algebra Associated to the Lower Central Series of a Group*, Trans. Amer. Math. Soc. 288 (1985), 51-57.

[19] J. Labute, *The Lie Algebra Associated to the Lower Central Series of a Link Group and Murasugi's Conjecture*, Proc. AMS, 109, 4 (1990), 951-956.
[20] J. Labute, Mild pro-p-groups and Galois groups of p-extensions of $\mathbb{Q}$, J. Reine Angew. Math. 596 (2006), 155-82.
[21] J. Labute, J. Mináč, *Mild pro-2-groups and 2-Extensions of $\mathbb{Q}$ with restricted ramification*, (work in progress).
[22] M. Lazard, *Groupes analytiques p-adiques*,Publ. Math. I.H.E.S., No. 26, Paris, 1965.
[23] A. Lubotzky, *Group presentations, p-adic analytic groups and lattices in* $\mathrm{SL}_2(\mathbb{C})$, Ann. Math. 118 (1983), 115-130.
[24] M. Morishita, *On Certain Analogies Between Knots and Primes*, J. Reine Angew. Math. 550 (2002), 141-167.
[25] A. Schmidt, *On the relation between* 2 *and* ∞, Compositio Math. 133 (2002), 267-288.
[26] J-P. Serre, *Cohomologie galoisienne*, Lecture Notes in Mathematics, No. 5, Springer, 1964; 5ème édition révisée et complétée, Springer, 1997.
[27] D. Vogel, *On the Galois Group of 2-Extensions with Restricted Ramification*, J. Reine Angew. Math. 581 (2003), 117-50.
[28] J-L. Waldspurger, *Entrelacements Sur* Spec*($\mathbb{Z}$)*, Bull. Sc. Math 100 (1976), 113-139.

Department of Mathematics and Statistics, McGill University, Burnside Hall, 805 Sherbrooke Street West, Montreal QC H3A 2K6, Canada
E-mail address: labute@math.mcgill.ca