MILD PRO-2-GROUPS AND 2-EXTENSIONS OF $\mathbb{Q}$ WITH RESTRICTED RAMIFICATION

JOHN LABUTE AND JÁN MINÁČ

Abstract. Using the mixed Lie algebras of Lazard, we extend the results of the first author on mild groups to the case $p = 2$. In particular, we show that for any finite set $S_0$ of odd rational primes we can find a finite set $S$ of odd rational primes containing $S_0$ such that the Galois group of the maximal 2-extension of $\mathbb{Q}$ unramified outside $S$ is mild. We thus produce a projective system of such Galois groups which converge to the maximal pro-2-quotient of the absolute Galois group of $\mathbb{Q}$ unramified at 2 and $\infty$. Our results also allow results of Alexander Schmidt on pro-$p$-fundamental groups of marked arithmetic curves to be extended to the case $p = 2$ over a global field which is either a function field of characteristic $\neq 2$ or a totally imaginary number field.

\section{Introduction}

In this paper we extend the theory of mild pro-$p$-groups developed in \cite{Labute} to the case $p = 2$. In particular, we obtain the following result which is the missing ingredient in extending the results of Alexander Schmidt in \cite{Schmidt} to the case $p = 2$ over a global field which is either a function field of characteristic $\neq 2$ or a totally imaginary number field. Let $H^i(G) = H^i(G, \mathbb{Z}/p\mathbb{Z})$.

\begin{theorem}
Let $G$ be a finitely generated pro-$p$-group. If $H^2(G) \neq 0$ and $H^1(G) = U \oplus V$ with the cup-product trivial on $U \times U$ and mapping $U \otimes V$ surjectively onto $H^2(G)$ then $G$ is mild.
\end{theorem}

For $p \neq 2$, Theorem 1.1 is a reformulation by Schmidt of a criterion for the mildness of a pro-$p$-group that was proven in \cite{Labute}. We will show that mild pro-$p$-groups are also of cohomological dimension 2 when $p = 2$. To prove our results we have to further develop the theory of certain mixed Lie algebras of Lazard \cite{Lazard}.

If $S$ is a finite set of odd rational primes we let $G_S(2)$ be the Galois group of the maximal 2-extension of $\mathbb{Q}$ unramified outside $S$.

\begin{theorem}
If $S_0$ is a finite set of odd rational primes there is a finite set $S$ of odd rational primes containing $S_0$ such that $G_S(2)$ is mild.
\end{theorem}

Date: October 13, 2009.
1991 Mathematics Subject Classification. 11R34, 20E15, 12G10, 20F05, 20F14, 20F40.
\textsuperscript{†}Research supported in part by NSERC grants 4344-06 and R0370A01.
Although the study of Galois groups of number fields with restricted ramification can be traced already to work of L. Kronecker and others in the 19-th century, the formal modern foundations were laid out by I.R. Šafarevič. His work was influenced by geometrical considerations of finite coverings of Riemann surfaces ramified in a given finite set of primes, class field theory and a deep understanding of the Galois groups of local fields. His papers [13], [14] as well as his paper with E.S. Golod [15] demonstrated the extraordinary power of his vision. Koch’s monograph [5], first published in 1970, summarized the important contributions to the subject. For example, information of the cohomological dimension of \(G_S(p)\) was obtained when \(p\) was odd and in \(S\). When \(p\) was not in \(S\), nothing was known about \(G_S(p)\), other that it could be infinite by the work of Golod and Shafarevich, until the recent work of the first author [8] where it was shown that for \(p\) odd this group was of cohomological dimension 2 for certain \(S\). The more difficult case \(p = 2\) was left open. This work finally extends these results to the case \(p = 2\).

2. Mixed Lie Algebras

Let \(G\) be a pro-2-group and let \(G_n\) \((n \geq 1)\) be the \(n\)-th term of the lower 2-central series of \(G\). We have

\[
G_1 = G, \quad G_{n+1} = G_n^2[G, G_n]
\]

where, for subgroups \(H, K\) of \(G\), \([H, K]\) is the closed subgroup generated by the commutators \([h, k] = h^{-1}k^{-1}hk\) with \(h \in H, k \in K\) and \(H^2\) is the subset of squares \(h^2\) of elements of \(H\). Let \(L(G)\) be the Lie algebra associated to the lower 2-central series of \(G\). We have

\[
L(G) = \oplus_{n \geq 1} L_n(G)
\]

where \(L_n(G) = G_n/G_{n+1}\) is denoted additively. This defines \(L(G)\) as a graded vector space over \(\mathbb{F}_2\). If \(l_n\) is the canonical homomorphism \(G_n \to L_n(G)\), the Lie bracket \([ξ, η]\) of \(ξ = l_n(x)\), \(η = l_n(y)\) is \(l_{m+n}([x, y])\). To the homogeneous element \(ξ = l_n(x)\) we associate the homogeneous element \(Pξ = l_{n+1}(x^2)\). If \(ξ, η \in L_n(G)\) then

\[
P(ξ + η) = \begin{cases} 
Pξ + Pη & \text{if } n > 1, \\ Pξ + Pη + [ξ, η] & \text{if } n = 1. \end{cases}
\]

If \(ξ \in L_m(G)\), \(η \in L_n(G)\) we have

\[
[Pξ, η] = \begin{cases} 
P[ξ, η] & \text{if } m > 1, \\ P[ξ, η] + [ξ, [ξ, η]] & \text{if } m = 1. \end{cases}
\]

Thus the operator \(P\) defines a mixed Lie algebra structure on \(L(G)\) in the terminology of Lazard, cf. [9], Ch.2, §1.2. The operator \(P\) extends to a linear operator on the Lie algebra

\[
L^+(G) = \oplus_{n > 1} L_n(G).
\]

It follows that \(L^+(G)\) is a module over the polynomial ring \(\mathbb{F}_2[π]\) where \(πu = P(u)\).
If $A = \sum_{n \geq 0} A_n$ is a graded associative algebra over the graded algebra $F_2[\pi]$, where multiplication by $\pi$ on homogeneous elements increases the degree by 1, then $A_+ = \sum_{n > 0} A_n$ has the structure of a mixed Lie algebra where

$$P_\xi = \begin{cases} \pi \xi & \text{if } \xi \text{ is of degree } > 1, \\ \pi \xi + \xi^2 & \text{if } \xi \text{ is of degree } 1. \end{cases}$$

Every mixed Lie algebra $g$ has an enveloping algebra $U_{\text{mix}}(g)$. This is graded associative algebra $U$ over $F_2[\pi]$ together with a mixed Lie algebra homomorphism $f$ of $g$ into $U_+$ such that, for every graded associative algebra $B$ over $F_2[\pi]$ and mixed Lie algebra homomorphism $\varphi_0$ of $g$ into $B_+$, there is a unique algebra homomorphism $\varphi$ of $U$ into $B$ satisfying $\varphi \circ f = \varphi_0$. The existence of $U_{\text{mix}}(g)$ is proven in [9], Th. 1.2.8. It is also shown there that the canonical mapping of $[\pi \xi]$ on homogeneous elements increases the degree by 1. The Lie subalgebra $F$ is a graded algebra over the graded ring $A$, $\pi$ into $\mathbb{A}$ is injective; this fact is referred to as the Birkhoff-Witt Theorem for mixed Lie algebras. Indeed, giving a mixed Lie algebra homomorphism $f: L_{\text{mix}}(X) \to B_+$ is the same as giving a graded map of $X$ into $B_+$ which is the same as giving a homomorphism of the graded algebra $A(X)$ into $B$. It is now a straight-forward argument to verify the following Proposition.

**Proposition 2.1.** If $0 \to r \to g \to h \to 0$ is an exact sequence of mixed Lie algebras, we have

$$U_{\text{mix}}(h) = U_{\text{mix}}(g)/\mathfrak{R}$$

where $\mathfrak{R}$ is the ideal of $U_{\text{mix}}(g)$ generated by the image of $r$.

Let $X = \{x_1, \ldots, x_d\}$ be a set and let $F = F(X)$ be the free pro-2-group on $X$. The completed group algebra $\Lambda = \mathbb{Z}_2[[F]]$ over the 2-adic integers $\mathbb{Z}_2$ is isomorphic to the Magnus algebra of formal power series in the non-commuting indeterminates $X_1, \ldots, X_d$ over $\mathbb{Z}_2$. Identifying $F$ with its image in $\Lambda$, we have $x_i = 1 + X_i$ (cf. [12], Ch. I, §1.5).

The lower 2-cental series of $F$ can be obtained by means of a valuation on $\Lambda$. More generally, if $\tau_1, \ldots, \tau_d$ are integers $> 0$, we define a valuation $w$ in the sense of Lazard by setting

$$w\left(\sum_{i_1, \ldots, i_k} a_{i_1, \ldots, i_k} X_{i_1} \cdots X_{i_k}\right) = \inf_{i_1, \ldots, i_k} (v(a_{i_1, \ldots, i_k}) + \tau_1 + \cdots + \tau_d),$$

where $v$ is the 2-adic valuation of $\mathbb{Z}_2$ with $v(2) = 1$. Let $\Lambda_n = \{u \in A \mid w(u) \geq n\}$. Then $(\Lambda_n)_{n \geq 0}$ is a filtration of $\Lambda$ by ideals and the associated graded algebra $\text{gr}(\Lambda)$ is a graded algebra over the graded ring $F_2[\pi] = \text{gr}(\mathbb{Z}_2)$ with $\pi$ the image of 2 in $2\mathbb{Z}_2/4\mathbb{Z}_2$. If $\xi_i$ is the image of $X_i$ in $\text{gr}_{\tau_i}(\Lambda)$ then $\text{gr}(\Lambda)$ is the free associative $F_2[\pi]$-algebra on $\xi_1, \ldots, \xi_d$ with a grading in which $\xi_i$ is of degree $\tau_i$ and multiplication by $\pi$ increases the degree by 1. The Lie subalgebra $L$ of $\text{gr}(\Lambda)$ generated by the $\xi_i$ is the free mixed Lie algebra over $F_2[\pi]$ on $\xi_1, \ldots, \xi_d$ by the Birkhoff-Witt Theorem. Note that when $\tau_i = 1$ for all $i$ we have $\Lambda_n = I^n$, where $I$ is the augmentation ideal $(2, X_1, \ldots, X_d)$ of $\Lambda$.  


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

\[
F_1 = F, \quad [F_n, F_k] \subseteq F_{n+k}, \quad F_n^2 \subseteq F_{n+1}.
\]

It is called the \((x, \tau)\)-filtration of \( F \). Such a sequence of subgroups of a pro-2-group \( G \) is called a 2-central series of \( G \). If \( \tau_i = 1 \) for all \( i \), then \( (F_n) \) is the lower 2-central series of \( F \).

If \( (G_n) \) is a 2-central series of \( G \), let \( \text{gr}_n(G) = G_n / G_{n+1} \) with the group operation denoted additively. Then \( \text{gr}(G) = \bigoplus_{n \geq 1} \text{gr}_n(G) \) is a graded vector space over \( \mathbb{F}_2 \) with a bracket operation \([\xi, \eta]\) which is defined for \( \xi \in G_n, \eta \in G_k \) by the image in \( \text{gr}_{n+k}(F) \) of \([x, y]\) where \( x, y \) are representatives of \( \xi, \eta \) in \( \text{gr}_n(G), \text{gr}_k(G) \) respectively. Under this bracket operation, \( \text{gr}(G) \) is a Lie algebra over \( \mathbb{F}_2 \). The mapping \( x \mapsto x^2 \) induces an operator \( P \) on \( \text{gr}(G) \) sending \( \text{gr}_n(G) \) into \( \text{gr}_{n+1}(G) \).

For homogeneous \( \xi, \eta \) of degree \( m, n \) respectively, we have

\[
\begin{align*}
P(\xi + \eta) &= P(\xi) + P(\eta) + [\xi, \eta] \quad \text{if } m = n = 1, \\
P(\xi + \eta) &= P(\xi) + P(\eta) \quad \text{if } m = n > 1, \\
[P(\xi), \eta] &= P([\xi, \eta]) + [\xi, [\xi, \eta]] \quad \text{if } m = 1, \\
[P(\xi), \eta] &= P([\xi, \eta]) \quad \text{if } m > 1.
\end{align*}
\]

Hence \( \text{gr}(G) \) is a mixed Lie algebra.

In the case \( F = F(X) \) and \( F_n = (1 + \Lambda_n) \cap F \), the mapping \( x \mapsto x - 1 \) induces an injective Lie algebra homomorphism of \( \text{gr}(F) \) into \( \text{gr}(\Lambda) \). Identifying \( \text{gr}(F) \) with its image in \( \text{gr}(\Lambda) \), we have \( P(\xi) = \pi \xi \) unless \( \xi \in \text{gr}_1(F) \) in which case

\[
P(\xi) = \xi^2 + \pi \xi.
\]

The Lie algebra \( \text{gr}(F) \) is the smallest \( \mathbb{F}_2 \)-subalgebra of \( \text{gr}(\Lambda) \) which contains \( \xi_1, \ldots, \xi_d \) and is stable under \( P \). To see this, let \( X_n \) be the set of elements \( x_i \) with \( \tau_i = n \) and define subsets \( T_n \) inductively as follows: \( T_1 = X_1 \) and, for \( n > 1 \),

\[
T_n' = \{ x^2 \mid x \in T_{n-1} \}, \quad T_n'' = X_n \cup \{ [x, y] \mid x \in T_n', y \in T_n', r + s = n \}.
\]

If \( F_n' \) is the closed subgroup of \( F \) generated by the \( T_k \) with \( k \geq n \), then \( (F_n') \) is a 2-central series of \( F \) (cf. [9], §1.2). If \( \text{gr}'(F) \) is the associated graded Lie-algebra, the inclusions \( F_n' \subseteq F_n \) induce a mixed Lie algebra homomorphism \( \text{gr}'(F) \to \text{gr}(F) \).

We obtain a sequence of mixed Lie algebra homomorphisms

\[
L_{\text{mix}}(X) \to \text{gr}'(F) \to \text{gr}(F) \to \text{gr}(\Lambda),
\]

where the homomorphism \( L_{\text{mix}}(X) \to \text{gr}'(F) \) sends \( \xi_i \) to \( \xi'_i \), the image of \( \xi_i \) in \( \text{gr}'(F) \), and hence is surjective since the \( \xi'_i \) generate \( \text{gr}'(F) \) as a mixed Lie algebra over \( \mathbb{F}_2[\pi] \). The composite of these homomorphisms sends \( \xi_i \) to \( \xi'_i \) and hence is injective. Thus \( \text{gr}'(F) \to \text{gr}(F) \) is injective from which it follows inductively that \( F_n' = F_n \) for all \( n \). Hence we obtain that \( \text{gr}(F(X)) = L_{\text{mix}}(X) \). The above 2-filtration \( (F_n) \) of \( F \) is called the \((x, \tau)\)-filtration of \( F \). If \( \tau_i = 1 \) for all \( i \), then \( (F_n) \) is the lower 2-central series of \( F \). Thus we have shown the following result.
Theorem 2.2. If \( L(F(X)) \) is the Lie algebra associated to the \((x, \tau)\)-filtration of the free pro-2-group \( F(X) \) on the weighted set \( X = \{x_1, \ldots, x_d\} \), with \( x_i \) of weight \( \tau_i \), then \( L(F(X)) = L_{\min}(X) \), the free mixed Lie algebra on \( X = \{\xi_1, \ldots, \xi_d\} \), where \( \xi_i \) is the image of \( x_i \) in \( L_{\tau_i}(F(X)) \).

Theorem 2.3. \( L^+(X) \) is a free Lie algebra over \( \mathbb{F}_2[\pi] \). If \( \xi_1, \ldots, \xi_m \) are the elements of \( X \) of weight 1 then, as a free Lie algebra, \( L^+(X) \) has a basis \( Y \) consisting of

1. the \( \binom{m+1}{2} \) elements
   \[ P\xi_1, \ldots, P\xi_m, [\xi_i, \xi_j] \quad (1 \leq i < j \leq m), \]
2. the elements
   \[ \xi_{m+1}, \ldots, \xi_d, [\xi_i, \xi_j] \quad (1 \leq i \leq m, m + 1 \leq j \leq d), \]
3. for \( 3 \leq k \), the \((k-1)\binom{m}{k-1}\) commutators
   \[ \text{ad}(\xi_{i_1})\text{ad}(\xi_{i_2}) \cdots \text{ad}(\xi_{i_{k-3}})\text{ad}(\xi_{i_{k-2}})\text{ad}(\xi_{i_{k-1}})^2(\xi_{i_{k-2}}), \]
   where \( m \geq i_1 > i_2 > \cdots > i_{k-2} \geq 1, 1 \leq j \leq m, j \neq i_1, \ldots, i_{k-2}, \)
4. for \( 3 \leq k \), the \((k-1)\binom{m}{k}\) commutators
   \[ \text{ad}(\xi_{i_1})\text{ad}(\xi_{i_2}) \cdots \text{ad}(\xi_{i_{k-1}})\text{ad}(\xi_{i_k}), \]
   where \( m \geq i_1 > i_2 > \cdots > i_{k-1} \geq 1, i_k < i_{k-1} \leq m, i_k \neq i_1, \ldots, i_{k-1}, \)
5. for \( 3 \leq k \), the \((k-1)\binom{d-m}{k}\) commutators
   \[ \text{ad}(\xi_{i_1})\text{ad}(\xi_{i_2}) \cdots \text{ad}(\xi_{i_{k-1}})\text{ad}(\xi_{i_k}), \]
   where \( m \geq i_1 > i_2 > \cdots > i_{k-1} \geq 1, i_k > m. \)

If \( A = A(X) \) is the free associative \( \mathbb{F}_2[\pi] \)-algebra on \( X \) and \( B \) is the subalgebra of \( A \) generated by \( Y \) then \( B \) is the free associative algebra over \( \mathbb{F}_2[\pi] \) on the weighted set \( Y \). Moreover, \( A \) is a free \( B \)-module with basis \( \xi_1^e \cdots \xi_m^e \) \( (e_i = 0, 1) \).

Proof. Let \( A \) be the free associative algebra on \( X = \{\xi_1, \ldots, \xi_d\} \) over \( \mathbb{F}_2[\pi] \) and let \( \bar{L} \) be the Lie subalgebra over \( \mathbb{F}_2 \) generated by \( Y \). Then \( \bar{L} \) is the free Lie algebra over \( \mathbb{F}_2 \) generated by \( X \). If \( L = L_{\min}(X) \) we have

\[
L_1 = \bar{L}_1 = \sum_{i=1}^{m} \mathbb{F}_2 \xi_i,
\]

\[
L_n = \pi^{n-2} \sum_{i=1}^{m} \mathbb{F}_2 P\xi_i + \pi^{n-2} \bar{L}_2 + \cdots + \pi \bar{L}_{n-1} + \bar{L}_n \quad (n \geq 2).
\]

Let \( Z \) be a homogeneous basis of \( \bar{L} \) containing \( X \) with \( \xi_1, \ldots, \xi_m \) the elements of \( Z \) of degree 1. If \( Z^+ \) is the set of elements of \( Z \) of degree \( > 1 \) then

\[
Z^* = \{P\xi_1, P\xi_2, \ldots, P\xi_m\} \cup Z^+
\]

is an \( \mathbb{F}_2 \)-basis for \( L^+ \) modulo \( \pi L^+ \) and hence is an \( \mathbb{F}_2[\pi] \)-basis for the free \( \mathbb{F}_2[\pi] \)-module \( L^+ \). If \( Z = \{\eta_i \mid i \geq 1\} \) is linearly ordered so that \( \eta_i \leq \eta_{i+1} \) and
degree(\eta_i) \leq \text{degree}(\eta_{i+1}) \text{ then, by the Birkhoff-Witt theorem for Lie algebras over } \mathbb{F}_2, \text{ the elements}
\eta^\alpha = \prod_{i \geq 1} \eta_i^{\alpha_i},
\text{where } \alpha = (\alpha_i)_{i \geq 1} \text{ with } \alpha_i = 0 \text{ for almost all } i, \text{ form a } \mathbb{F}_2\text{-basis of } \tilde{A} = A/\pi A, \text{ the enveloping algebra of } \tilde{L}. \text{ It follows that the elements}
\prod_{i=1}^m \eta_i^{\beta_i} \prod_{i=1}^m \eta_i^{2\gamma_i} \prod_{i > m} \eta_i^{\alpha_i},
\text{where } \beta_i = 0, 1 \text{ and } \gamma_i, \alpha_i \in \mathbb{N}, \text{ are also an } \mathbb{F}_2\text{-basis of } \tilde{A}. \text{ Note that, in our convention, } 0 \in \mathbb{N}. \text{ Hence the elements}
\prod_{i=1}^m P \eta_i^{\gamma_i} \prod_{i > m} \eta_i^{\alpha_i},
\text{where } \gamma_i, \alpha_i \in \mathbb{N}, \text{ are an } \mathbb{F}_2[\pi]\text{-basis for } \tilde{A}. \text{ This implies that } A \text{ is a free } B\text{-module with basis}
\xi_1^{i_1} \cdots \xi_m^{i_m} \quad (i_k = 0, 1).

\text{Let } a_n \text{ be the number of elements of } Z \text{ of degree } n. \text{ Then}
\prod_{n \geq 1} \frac{1}{(1 - t^n)^{-a_n}} = \frac{1}{1 - \sum m_i t^{e_i}},
\text{where } e_1 < e_2 < \cdots < e_r \text{ are the possible values of the } \tau_i = \text{deg}(\xi_i) \text{ and } m_i \text{ is the number of } j \text{ with } \tau_j = e_i. \text{ We can rewrite this equation in the form}
P(t) = (1 + t)^m P(t) = \left(1 - \sum m_i t^{e_i}\right)^{-1} \text{ where}
P(t) = (1 - t^2)^{-m} \prod_{n \geq 2} (1 - t^n)^{-a_n}
= (1 - t^2)^{-(a_2 + m)} \prod_{n \geq 3} (1 - t^n)^{-a_n}
\frac{1}{1 - (c_2 t^2 + c_3 t^3 + \cdots + c_{m+1} t^{m+1} + \sum_{k \geq 1} q_k(t))},
\text{where}
c_k = (k - 1) \binom{m + 1}{k}
= (k - 1) \binom{m}{k} + (k - 1) \binom{m}{k},
q_k(t) = \sum_{j \geq 2} \binom{m}{k-1} m_j t^{k-1+e_j}.
The power series $P(t)$ is the Poincaré series of $\tilde{B} = B/\pi B$; the Poincaré series of $B$ is $P(t)/(1 - t)$.

To show that the elements of $Y$ generate $L^+$ it suffices to show that they generate $L^+$ as a vector space over $\mathbb{F}_2$ modulo $\pi L^+ + [L^+, L^+]$. For $k > 2$, we have $L^+_k = \tilde{L}_k$ modulo $\pi L^+$. For $k \geq 2$, every element of $\tilde{L}_k$ can be uniquely written modulo $[\tilde{L}, \tilde{L}]$ as a linear combination of the sequence $S$ of elements of the form

$$\text{ad}(\xi_i)\text{ad}(\xi_2)\cdots\text{ad}(\xi_{i_k})\text{ad}(\xi_{i_k})$$

with $d \geq i_1 \geq i_2 \geq \cdots \geq i_{k-1} \geq 1$ and $i_{k-1} < i_k$. Modulo $\pi L^+$ we have

$$[P(\xi_1), P(\xi_j)] = \text{ad}(\xi_i)\text{ad}(\xi_j)^2(\xi_i),$$

$$[P(\xi_i), u] = \text{ad}(\xi_i)^2(u) \text{ if } u \in L^+$$

and $\text{ad}(\xi_i)\text{ad}(\xi_j)(u) = \text{ad}(\xi_j)\text{ad}(\xi_i)(u)$ modulo $[L^+, L^+]$ if $u \in L^+$. If follows that the only terms of the sequence $S$ which possibly do not lie in $\pi L^+ + [L^+, L^+]$ are the terms of the subsequence $T$ of elements of the form

(A) \quad \text{ad}(\xi_{i_1})\text{ad}(\xi_{i_2})\cdots\text{ad}(\xi_{i_{k-2}})\text{ad}(\xi_{i_{k-1}})\text{ad}(\xi_{i_k})$

with $m \geq i_1 > i_2 > \cdots > i_{k-1} \geq 1$ and $i_{k-1} < i_k$, or of the form

(B) \quad \text{ad}(\xi_{i_1})\text{ad}(\xi_{i_2})\cdots\text{ad}(\xi_{i_{k-2}})\text{ad}(\xi_{i_{k-1}})^2(\xi_{i_{k-1}})$

with $m \geq i_1 > i_2 > \cdots > i_{k-2} \geq 1$, $i_{k-2} < i_{k-1} \leq m$, or of the form

(C) \quad \text{ad}(\xi_{i_1})\text{ad}(\xi_{i_2})\cdots\text{ad}(\xi_{i_{k-2}})\text{ad}(\xi_{i_{k-1}})\text{ad}(\xi_{i_k})$

with $m \geq i_1 > i_2 > \cdots > i_{k-1} \geq 1$ and $i_{k-1} < i_k = i_1$. Working modulo $\pi L^+ + [L^+, L^+]$, this last element is equal to

$$\text{ad}(\xi_{i_2})\cdots\text{ad}(\xi_{i_{k-2}})\text{ad}(\xi_{i_1})\text{ad}(\xi_{i_{k-1}})\text{ad}(\xi_{i_k}) = \text{ad}(\xi_{i_2})\cdots\text{ad}(\xi_{i_{k-2}})\text{ad}(\xi_{i_1})^2(\xi_{i_{k-1}})$$

which is an element in the family (3) in the statement of the theorem. Using the identity

$$\text{ad}(x)\text{ad}(y)^2\text{ad}(z) = \text{ad}(z)\text{ad}(y)^2\text{ad}(x) \pmod{\pi L^+ + [L^+, L^+]}$$

the elements of the form (B) can be also written in the form (3). The elements in (A) with $i_k \leq m$ account for the elements in (4) and the elements in (A) with $i_k > m$ account for the elements in (5). The later account for the terms $q_k(t)$ in $P(t)$. Thus $Y$ generates $L^+(X)$ and so the canonical mapping of $L(Y)$, the free Lie algebra over $\mathbb{F}_2[\pi]$ on the weighted set $Y$, into $L^+$ is surjective. It is injective since $L(Y)$ and $L^+$ have the same Poincaré series. \qed

**Corollary 2.4.** Let $L_{\text{mix}}(X) = L_{\text{mix}}(X)/\pi L_{\text{mix}}(X)^+$ and let $Y$ be as in Theorem 2.3. Then $L_{\text{mix}}(X)^+ = L(Y)$, the free Lie algebra over $\mathbb{F}_2$ on $Y$. Its enveloping algebra $B$ is the subalgebra of $\tilde{A} = \tilde{A}(X)$ (the free associative $\mathbb{F}_2$-algebra on $X$) generated by $L(X)^+$. The $B$-module $\tilde{A}$ is free with basis consisting of the elements $\xi_1^i \cdots \xi_m^i$ ($i_k = 0, 1$).

This follows immediately from the fact that $A$ is a free $B$-module with basis $\xi_1^i \cdots \xi_m^i$ ($i_k = 0, 1$).
3. Quadratic Lie Algebras

If \( g \) is a mixed Lie algebra we let \( \tilde{g} = g/\pi g^+ \). Then \( \tilde{g} \) is a Lie algebra over \( \mathbb{F}_2 \) which we call the reduced algebra of \( g \). The operator \( P \) on \( g \) induces an operator on \( \tilde{g} \), also denoted by \( P \), which is zero in degree > 1 and which, for homogeneous elements \( \xi, \eta \), satisfies

\[
\begin{align*}
&\text{(QL1)} & P(\xi + \eta) &= P(\xi) + P(\eta) + [\xi, \eta] &\text{if } \xi, \eta \text{ are of degree 1,} \\
&\text{(QL2)} & [P\xi, \eta] &= [\xi, [\xi, \eta]] &\text{if } \xi \text{ is of degree 1.}
\end{align*}
\]

Thus \( \tilde{g} \) satisfies the axioms for a mixed Lie algebra where \( P(\xi) = 0 \) if \( \xi \) is homogeneous of degree > 1. It is an example of what we call a quadratic Lie algebra.

**Definition 3.1** (Quadratic Lie Algebra). A quadratic Lie algebra is a graded Lie algebra \( h = \oplus_{i \geq 1} h_i \) over \( \mathbb{F}_2 \) together with a mapping \( P : h_1 \to h_2 \) satisfying (QL1) and (QL2).

A homomorphism \( f : h \to h' \) of quadratic Lie algebras is a homomorphism of graded Lie algebras (over \( \mathbb{F}_2 \)) such that \( f(P(s)) = P(f(s)) \) for every homogenous element \( s \) of degree 1. By an ideal of \( h \) we mean an ideal \( a \) of \( h \) as a Lie algebra over \( \mathbb{F}_2 \) such that \( P(s) \in a \) for every element \( s \) of \( a \) of degree 1. Every quadratic Lie algebra is a mixed Lie algebra if we set \( P\xi = 0 \) for every homogeneous element \( \xi \) of degree 1. In this way Quadratic Lie algebras form a full subcategory of the category of mixed Lie algebras.

If \( A = \oplus_{i \geq 0} A_i \) is a graded associative algebra over \( \mathbb{F}_2 \) then the mapping \( P : x \mapsto x^2 \) of \( A_1 \) into \( A_2 \) together with the bracket \( [x, y] = xy + yx \) defines the structure of a quadratic Lie algebra on \( A_+ = \oplus_{i > 0} A_i \). Indeed, we have \((x+y)^2 = x^2 + y^2 + xy + yx\) and

\[
[x, [x, y]] = [x, xy + yx] = x^2y + xyx + yx + yx^2 = [x^2, y].
\]

**Definition 3.2** (Derivation of a quadratic Lie algebra). If \( h \) is a quadratic Lie algebra then by a derivation of \( h \) we mean an additive mapping \( D : h \to h \) that

\[
\begin{align*}
&\text{(Der 1)} & \text{There is an integer } s \geq 1 \text{ such that } D(h_n) \subseteq h_{n+s} \text{ (} s \text{ is the degree of } D), \\
&\text{(Der 2)} & D(P(\xi)) = [\xi, D(\xi)] &\text{if } \xi \text{ is homogeneous of degree 1,} \\
&\text{(Der 3)} & D[\xi, \eta] = [D(\xi), \eta] + [\xi, D(\eta)].
\end{align*}
\]

The set \( \text{Der}_{\text{quad}}(h) \) of derivations of the quadratic Lie algebra \( h \) is a quadratic Lie algebra under the operations of addition and Lie bracket \( [D_1, D_2] = D_1 D_2 + D_2 D_1 \) with \( P(D) = D^2 \) if \( D \) is of degree 1. The grading is defined by the degree of a derivation.

If \( a \) and \( h \) are Lie algebras over \( \mathbb{F}_2 \) and \( f \) is a homomorphism of \( h \) into the Lie algebra of derivations of \( a \), the semi-direct product of \( a \) and \( h \) is the direct product \( a \times h \) as vector spaces with the Lie algebra structure given by

\[
[(\xi, \sigma), (\xi', \sigma')] = ([\xi, \xi'] + f(\sigma)(\xi') + f(\sigma')(\xi), [\sigma, \sigma']).
\]
We denote this Lie algebra by $a \times_f h$. We will agree to identify $a$ and $h$ with their canonical images in $a \times_f h$. If $a$ and $h$ are graded then so is $a \times_f h$ with $n$-th homogeneous component $a_n \times h_n = a_n + h_n$.

**Theorem 3.3.** Let $a$ and $h$ be quadratic Lie algebras and $f$ is a homomorphism of $h$ into $\text{Der}_{\text{quad}}(a)$. If $(\xi, \sigma)$ is an element of $a \times h$ of degree 1 then

$$P(\xi, \sigma) = (P(\xi) + f(\sigma)(\xi), P(\sigma))$$

defines the structure of a quadratic Lie algebra on $a \times h$.

**Proof.** Let $\xi + \sigma$, $\xi' + \sigma'$ be elements of $a \times h$ of degree 1. Then

$$P(\xi + \sigma) + \xi' + \sigma' = P(\xi + \xi' + \sigma + \sigma') =$$

$$P(\xi + \xi' + f(\sigma + \sigma')(\xi + \xi')) + P(\sigma + \sigma') =$$

$$P(\xi) + P(\xi') + [\xi, \xi'] + f(\sigma)(\xi) + f(\sigma)'(\xi') + f(\sigma')(\xi) + f(\sigma')(\xi') +$$

$$P(\sigma) + P(\sigma') + [\sigma, \sigma'] =$$

$$P(\xi + \sigma) + P(\xi' + \sigma') + [\xi + \sigma, \xi' + \sigma'].$$

If $\xi + \sigma$ is of degree 1 we have

$$[P(\xi + \sigma), \xi' + \sigma'] = [P(\xi) + f(\sigma)(\xi) + P(\sigma), \xi' + \sigma'] =$$

$$[P(\xi) + f(\sigma)(\xi), \xi'] + f(P(\sigma))(\xi') + f(\sigma')(P(\xi)) + f(\sigma)'(f(\xi) + [P(\sigma), \sigma'] =$$

$$[P(\xi), \xi'] + [f(\sigma)\xi, \xi'] + f(\sigma)^2\xi' + [\xi, f(\sigma')(\xi)] + f(\sigma)f(\sigma)(\xi) + [\sigma, [\sigma, \sigma'] =$$

$$[\xi, [\xi, \xi']] + [\xi, f(\sigma)(\xi')] + [\xi, f(\sigma')(\xi)] + f(\sigma)([\xi, \xi'] + f(\sigma)^2(\xi') + f(\sigma)f(\sigma')(\xi) +$$

$$f([\sigma, \sigma'])(\xi) + [\sigma, [\sigma, \sigma'] =$$

$$[\xi + \sigma, [\xi, \xi'] + f(\sigma)(\xi') + f(\sigma')(\xi) + [\sigma, [\sigma, \xi' + \sigma'] =$$

$$[\xi + \sigma, [\xi, \xi'] + f(\sigma)(\xi') + f(\sigma')(\xi) + [\sigma, [\sigma, \xi' + \sigma'] =$$

\[\square\]

If $X$ is a homogeneous subset of the quadratic Lie algebra $h$ generated by $X$ is the smallest Lie subalgebra $a$ of $h$ which contains $X$ and which contains $P(x)$ for every $x \in X$ of degree 1. Let $h^* = P(h_1) + [h, h]$. Then $h^*$ is a vector subspace of $h$ by (QL1). The proof of the following result is left to the reader.

**Proposition 3.4.** The subset $X$ generates the quadratic Lie algebra $h$ if and only its image in the vector space $h/h^*$ is a generating set.

If $X$ is a weighted set then the natural map of $\tilde{L}_{\text{mix}}(X) = L_{\text{mix}}(X)/\pi L_{\text{mix}}(X)^+$ into $A(X) = A(X)/\pi A(X)$ is injective map of quadratic Lie algebras. We use this to identify $\tilde{L}_{\text{mix}}(X)$ with the quadratic subalgebra of the free associative algebra $\tilde{A}(X)$ over $F_2$ generated by $X$. If $\tilde{L}(X)$ is the Lie subalgebra of $\tilde{A}(X)$ generated by $X$ we have

$$\tilde{L}_{\text{mix}}(X) = \tilde{L}(X) + \sum_{s \in S} F_2 s^2,
where $S$ is the set of elements of $X$ of degree 1 and $P(s) = s^2$ for $s \in S$. The Lie algebra $\hat{L}(X)$ is the free Lie algebra over $\mathbb{F}_2$ on $X$. Note that $\hat{L}_{\text{mix}}(X)/\hat{L}_{\text{mix}}(X)^* = \hat{L}(X)/[\hat{L}(X), \hat{L}(X)]$.

**Proposition 3.5.** The Lie algebra $\hat{L}_{\text{mix}}(X)$ is the free quadratic Lie algebra on the set $X$.

**Proof.** Let $f$ be a weight preserving map of $X$ into a quadratic Lie algebra $\mathfrak{h}$. Then $f$ extends uniquely to a Lie algebra homomorphism $\varphi_0$ of $\hat{L}(X)$ into $\mathfrak{h}$. The only way to extend $\varphi_0$ to a quadratic Lie algebra homomorphism $\varphi$ of $\hat{L}_{\text{mix}}(X)$ into $\mathfrak{h}$ is to define $\varphi(P(s)) = P(\varphi(s))$ for any $s \in S$ and to extend by linearity to all of $\hat{L}_{\text{mix}}(X)$. A straightforward verification yields that $\varphi([P(s), y]) = [\varphi(P(s)), \varphi(y)]$ for any $y \in \hat{L}(X)$ and that $\varphi([P(s), P(t)]) = [\varphi(P(s)), \varphi(P(t))]$ for any $s, t \in S$ and hence that $\varphi$ is a homomorphism of quadratic Lie algebras. \hfill $\square$

Every quadratic Lie algebra $\mathfrak{h}$ has a universal enveloping algebra $U = U_\text{quad}(\mathfrak{h})$. More precisely, there is a graded associative algebra $U$ over $\mathbb{F}_2$ and a quadratic Lie algebra homomorphism $f$ of $\mathfrak{h}$ into $U_+$ such that for every quadratic Lie algebra homomorphism $\varphi_0$ of $\mathfrak{h}$ into an associative algebra $B$ over $\mathbb{F}_2$ there is a unique algebra homomorphism $\varphi$ of $U$ into $B$ satisfying $\varphi \circ f = \varphi_0$. We have $U_\text{quad}(\hat{L}_{\text{mix}}(X)) = \hat{A}(X)$ since $\hat{A}(X)$ has the correct universal property. More generally, we have

**Proposition 3.6.** Let $\mathfrak{g} = \hat{L}_{\text{mix}}(X)/\mathfrak{r}$ be a presentation of a quadratic Lie algebra $\mathfrak{g}$ and let $\mathfrak{R}$ be the ideal of $\hat{A}(X) = U_\text{quad}(\hat{L}_{\text{mix}}(X))$ generated by the image of $\mathfrak{r}$. Then

$$\hat{A}(X)/\mathfrak{R} = U_\text{quad}(\mathfrak{g}).$$

**Proposition 3.7.** Let $\mathfrak{g}$ be a mixed Lie algebra and $\tilde{\mathfrak{g}} = \mathfrak{g}/\pi\mathfrak{g}^+$ the reduced algebra of $\mathfrak{g}$. If $U = U_{\text{mix}}(\mathfrak{g})$ then $U_{\text{quad}}(\tilde{\mathfrak{g}}) = U/\pi U$.

**Proof.** If $\mathfrak{g} = L_{\text{mix}}(X)/\mathfrak{r}$ then $\tilde{\mathfrak{g}} = \hat{L}_{\text{mix}}(X)/\tilde{\mathfrak{r}}$, where $\tilde{\mathfrak{r}}$ is the image of $\mathfrak{r}$ in $\hat{L}_{\text{mix}}(X)$. Then

$$U_{\text{quad}}(\tilde{\mathfrak{g}}) = \hat{A}(X)/\mathfrak{R},$$

where $\mathfrak{R}$ is the image of $\mathfrak{R}$ in $\hat{A}(X)$. \hfill $\square$

4. **Strongly Free Sequences**

Let $\rho_1, \ldots, \rho_m \in L = L_{\text{mix}}(X)$ with $\rho_i$ homogeneous of degree $h_i > 1$ and let $\mathfrak{r}$ be the ideal of the free mixed Lie algebra $L$ generated by $\rho_1, \ldots, \rho_m$. Let $\mathfrak{g} = L/\mathfrak{r}$. Then $M = \mathfrak{r}/[\mathfrak{r}, \mathfrak{r}]$ is a module over the enveloping algebra $U = U_{\text{mix}}(\mathfrak{g})$ via the adjoint representation.

**Definition 4.1.** The sequence $\rho_1, \ldots, \rho_m$ is said to be strongly free in $L$ if the following conditions hold.

(i) The $\mathbb{F}_2[\pi]$-module $U$ is torsion free.

(ii) The $U$-module $M$ is free on the images of $\rho_1, \ldots, \rho_m$. 
Let \( \tilde{\rho}_i \) be the image of \( \rho_i \) in \( \tilde{L} = \tilde{L}_{\text{mix}}(X) \) and let \( \tilde{r} \) be the ideal of \( \tilde{L} \) generated by \( \tilde{\rho}_1, \ldots, \tilde{\rho}_m \). Let \( \tilde{\mathfrak{g}} = \tilde{L}/\tilde{r} \). Then \( \tilde{M} = \tilde{r}/[\tilde{r}, \tilde{r}] \) is a module over the enveloping algebra \( \tilde{U} = U_{\text{quad}}(\tilde{\mathfrak{g}}) \) via the adjoint representation.

**Definition 4.2.** The sequence \( \tilde{\rho}_1, \ldots, \tilde{\rho}_m \) is said to be a strongly free in \( \tilde{L} \) if the \( \tilde{U} \)-module \( \tilde{M} \) is free on the images of \( \tilde{\rho}_1, \ldots, \tilde{\rho}_m \).

Let \( X = \{\xi_1, \ldots, \xi_d\} \) with \( \xi_i \) of weight \( e_i \).

**Theorem 4.3.** The sequence \( \tilde{\rho}_1, \ldots, \tilde{\rho}_m \) is strongly free in \( \tilde{L} \) if and only if the Poincaré series of \( \tilde{U} \) is

\[
\frac{1}{1 - (t^{e_1} + \cdots + t^{e_d}) + t^{h_1} + \cdots + t^{h_m}).
\]

**Proof.** Let \( \mathcal{R} \) be the ideal of \( \tilde{A}(X) \) generated by \( \tilde{r} \). Then \( \tilde{A}(X)/\mathcal{R} = U_{\text{quad}}(\tilde{\mathfrak{g}}) = \tilde{U} \). If \( I \) is the augmentation ideal of \( V = \tilde{A}(X) \) and \( J \) is the augmentation ideal of \( W = U_{\text{quad}}(\tilde{r}) \) then, by tensoring the exact sequence \( 0 \to I \to V \to \mathbb{F}_2 \to 0 \) with \( \mathbb{F}_2 = W/J \) over \( W \), we obtain the exact sequence

\[
\text{Tor}^W_1(\mathbb{F}_2, V) \to \tilde{r}/[\tilde{r}, \tilde{r}] \to I/\mathcal{R}I \to V/\mathcal{R} \to \mathbb{F}_2 \to 0
\]

using the fact that

1. If \( M \) is a \( W \)-module then \( M \otimes_W (W/J) = M/JM \);
2. \( \mathcal{R} = \tilde{V} = V \tilde{r} \);
3. \( \text{Tor}^W_1(\mathbb{F}_2, \mathbb{F}_2) = \tilde{r}/[\tilde{r}, \tilde{r}] \) (cf. [3], Ch. XIII, §2).

The map \( \tilde{r}/[\tilde{r}, \tilde{r}] \to I/\mathcal{R}I \) is induced by the inclusion \( \tilde{r} \subseteq I \). Since \( I \) is the direct sum of the left ideals \( V \xi_i \). The \( \tilde{U} \)-module \( I/\mathcal{R} \) is the direct sum of the free \( \tilde{U} \)-submodules \( U\xi_i \), where \( g_i \) is the image of \( \xi_i \) in \( U = \tilde{A}(X)/\mathcal{R} \). Since \( \tilde{r} \subseteq \tilde{L} \) the algebra \( V = \tilde{A}(X) \) is a free \( W \)-module by Corollary [2.3] and the Birkhoff-Witt Theorem for Lie algebras over \( \mathbb{F}_2 \). In this case we have the exact sequence

\[
0 \to \tilde{r}/[\tilde{r}, \tilde{r}] \to I/\mathcal{R}I \to \tilde{A}(X)/\mathcal{R} \to \mathbb{F}_2 \to 0.
\]

Expressing \( \tilde{M} = \tilde{r}/[\tilde{r}, \tilde{r}] \) as a quotient \( \tilde{U}^m/N \) using the relators \( \tilde{\rho}_i \), we obtain the exact sequence of graded modules whose homogeneous components are finitely generated free \( \mathbb{F}_2 \)-modules

\[
0 \to N \to \bigoplus_{j=1}^m \tilde{U}[h_j] \to \bigoplus_{j=1}^d \tilde{U}[e_j] \to U \to \mathbb{F}_2 \to 0
\]

where \( \tilde{U}[n] = \tilde{U} \) but with degrees shifted by \( n \); by definition, \( \tilde{U}[n](t) = t^n \tilde{U}(t) \). We have \( N = 0 \) if and only if \( \tilde{M} \) is a free \( \tilde{U} \)-module on the images of the \( \tilde{\rho}_i \).

Taking Poincaré series in the above long exact sequence, we get

\[
N(t) - (t^{h_1} + \cdots + t^{h_m})\tilde{U}(t) + (t^{e_1} + \cdots + t^{e_d})\tilde{U}(t) - \tilde{U}(t) + 1 = 0.
\]

Solving for \( \tilde{U}(t) \), we get \( \tilde{U}(t) = P(t) + N(t)P(t) \), where

\[
P(t) = \frac{1}{1 - (t^{e_1} + \cdots + t^{e_d}) + t^{h_1} + \cdots + t^{h_m}}.
\]

Hence \( N(t) = 0 \iff \tilde{U}(t) = P(t) \). \( \square \)
Theorem 4.4. The sequence $\rho_1, \ldots, \rho_m$ is strongly free in $L = L_{\text{mix}}(X)$ if and only if the sequence $\hat{\rho}_1, \ldots, \hat{\rho}_m$ is strongly free in $\hat{L}$.

Proof. If $\rho_1, \ldots, \rho_m$ is a strongly free sequence then the enveloping algebra $U$ of the mixed Lie algebra $g = L/\tau$ is a torsion free $\mathbb{F}_2[\pi]$-module. By the Birkhoff-Witt Theorem for mixed Lie algebras, the canonical mapping of the enveloping algebra $W$ into $U$ is injective. Hence $g^+ = L^+/\tau$ is a torsion free $\mathbb{F}_2[\pi]$-module. If $B$ is the subalgebra of $A = A(X)$ generated by $L^+$ then $B$ is the enveloping algebra of $L^+$. By Birkhoff-Witt the canonical mapping of the enveloping algebra $W$ of $\tau$ into $B$ is injective and $B$ is a free $W$-module. Since $A$ is a free $B$-module it follows that $A$ is a free $W$-module. Thus, if $M = \tau/\langle \tau, \rho \rangle$ and $\mathcal{R}$ the ideal of $A$ generated by $\tau$ and $I$ the augmentation ideal of $A$, we have an exact sequence

$$0 \to M \to I/\mathcal{R}I \to A/\mathcal{R} \to \mathbb{F}_2[\pi] \to 0.$$  

As in the proof of Theorem 4.3 we obtain that the Poincaré series of $U$ is

$$Q(t) = \frac{1}{(1-t)(1-(t^{e_1} + \cdots + t^{e_d}) + t^{h_1} + \cdots + t^{h_m})}.$$  

If $\hat{U}$ is the enveloping algebra of $\hat{L}/(\hat{\rho}_1, \ldots, \hat{\rho}_m)$ we have $\hat{U} = U/\pi U = U \otimes_{\mathbb{F}_2} \mathbb{F}_2[\pi]$. Since $U$ is torsion free over $\mathbb{F}_2[\pi]$ the Poincaré series of $\hat{U}$ is $(1-t)Q(t)$ which proves that the sequence $\hat{\rho}_1, \ldots, \hat{\rho}_m$ is strongly free. 

Conversely, suppose that the sequence $\hat{\rho}_1, \ldots, \hat{\rho}_m$ is strongly free in $\hat{L}$. We have the exact sequence of graded vector spaces over $\mathbb{F}_2$

$$0 \to K \to M \to U[e_1] \oplus \cdots \oplus U[e_d] \to U \to \mathbb{F}_2 \to 0.$$  

Taking Poincaré series we get

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

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

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

Now suppose that $\hat{\rho}_1, \ldots, \hat{\rho}_m$ is strongly free. Then, if $\tilde{\tau}$ is the ideal of $\hat{L}$ generated by $\hat{\rho}_1, \ldots, \hat{\rho}_m$ and $\hat{M} = \tilde{\tau}/[\tilde{\tau}, \hat{\tau}]$, we have surjections

$$\hat{U}[h_1] \oplus \cdots \oplus \hat{U}[h_m] \to \hat{M} \to \tilde{\tau}/[\tilde{\tau}, \hat{\tau}]$$  

whose composite is an isomorphism. It follows that

$$\hat{M} \cong \tilde{\tau}/[\tilde{\tau}, \hat{\tau}] \cong \hat{U}[h_1] \oplus \cdots \oplus \hat{U}[h_m],$$

$$M(t) \leq \hat{M}(t) = \frac{1}{1-t} \cdot \frac{t^{h_1} + \cdots + t^{h_m}}{1 - (t^{e_1} + \cdots + t^{e_d}) + t^{h_1} + \cdots + t^{h_m}}.$$

$$U(t) \leq \hat{U}(t) = \frac{1}{1-t} \cdot \frac{1}{1 - (t^{e_1} + \cdots + t^{e_d}) + t^{h_1} + \cdots + t^{h_m}}.$$
Using the fact that \( K(t) \geq 0 \), we get
\[
\frac{M(t)}{1 - (t^{e_1} + \cdots + t^{e_d})} \geq \frac{1}{(1 - t)(1 - (t^{e_1} + \cdots + t^{e_d}))},
\]
\[
\frac{1}{1 - t} \left( \frac{1}{1 - (t^{e_1} + \cdots + t^{e_d})} \right) - \frac{1}{1 - (t^{e_1} + \cdots + t^{e_d} + t^{h_1} + \cdots + t^{h_m})} = \frac{\tilde{M}(t)}{(1 - t)(1 - (t^{e_1} + \cdots + t^{e_d}))} \geq \frac{M(t)}{1 - (t^{e_1} + \cdots + t^{e_d})}.
\]

It follows that \( K(t) = 0, U(t) = \tilde{U}(t)/(1 - t) \) and \( M(t) = \tilde{M}/(1 - t) \). Hence \( U \) is a free \( \mathbb{F}_2[\pi] \)-module and \( M \) is a free \( U \)-module since we have a natural surjection
\[
U[h_1] \oplus \cdots \oplus U[h_m] \twoheadrightarrow M
\]
with both sides having the same Poincaré series.

\[\square\]

In general it is very difficult to determine whether a sequence in \( \tilde{L} \) is strongly free but we can construct a large supply using the following elimination theorem for free quadratic Lie algebras.

**Theorem 4.5 ((Elimination Theorem)).** Let \( S \) be a subset of the weighted set \( X \) and let \( \mathfrak{a} \) be the ideal of the free quadratic Lie algebra \( \tilde{L}_{\text{mix}}(X) \) generated by \( X - S \). Then \( \mathfrak{a} \) is a free quadratic Lie algebra with basis
\[
ad(\sigma_1)ad(\sigma_2)\cdots ad(\sigma_n)(\xi), \quad (n \geq 0, \ \sigma_i \in S, \ \xi \in X - S).
\]

**Proof.** We first show that the quadratic Lie algebra \( \tilde{L}_{\text{mix}}(X) \) is the semi-direct product of the quadratic Lie algebras \( \mathfrak{a} \) and \( L_{\text{mix}}(S) \). Let \( f \) be the adjoint representation of \( \tilde{L}_{\text{mix}}(S) \) on \( \mathfrak{a} \). Then \( f \) is a homomorphism of the quadratic Lie algebra \( \tilde{L}_{\text{mix}}(S) \) into the quadratic Lie algebra \( \text{Der}_{\text{quad}}(\mathfrak{a}) \) of derivations of the quadratic Lie algebra \( \mathfrak{a} \). More precisely, if \( f(\sigma) = D \) then \( f(P(\sigma)) = D^2 \) and \( D(P(\xi)) = [\xi, D(\xi)] \) if \( \sigma, \xi \) are homogeneous of degree 1. Every element of \( \tilde{L}_{\text{mix}}(X) \) can be uniquely written in the form \( \xi + \sigma \) with \( \xi \in \mathfrak{a}, \sigma \in L_{\text{mix}}(S) \). We have
\[
[x_1 + \sigma_1, x_2 + \sigma_2] = [x_1, x_2] + f(\sigma_1)(x_2) + f(\sigma_2)(x_1) + [\sigma_1, \sigma_2]
\]
and \( P(\xi + \sigma) = P(\xi) + f(\sigma)(\xi) + P(\sigma) \) if \( \xi, \sigma \) are of degree 1. As a quadratic Lie algebra, \( \mathfrak{a} \) is generated by the family of elements
\[
ad(\sigma_1)ad(\sigma_2)\cdots ad(\sigma_n)(\xi), \quad (n \geq 0, \ \sigma_i \in S, \ \xi \in X - S).
\]

If \( \sigma \in S \) and \( f(\sigma) = D \) then
\[
D(ad(\sigma_1)ad(\sigma_2)\cdots ad(\sigma_n)(\xi)) = ad(\sigma)ad(\sigma_1)ad(\sigma_2)\cdots ad(\sigma_n)(\xi).
\]

Let \( T \) be the family of elements \( \{\sigma_1, \sigma_2, \ldots, \sigma_n, \xi\} \) with \( n \geq 0, \ \sigma_i \in S, \ \xi \in X - S \) and weight equal to the sum of the weights of the components \( \sigma_i, \xi \). Let \( \varphi_1 \) be the quadratic Lie algebra homomorphism of \( \tilde{L}_{\text{mix}}(T) \) into \( \mathfrak{a} \) such that
\[
\varphi_1(\sigma_1, \sigma_2, \ldots, \sigma_n, \xi) = ad(\sigma_1)ad(\sigma_2)\cdots ad(\sigma_n)(\xi).
\]
Since \( \varphi_1 \) is surjective it suffices to prove \( \varphi_1 \) is injective. Let \( g \) be the quadratic Lie algebra homomorphism of \( \tilde{L}_{\text{mix}}(S) \) into \( \text{Der}_{\text{quad}}(\tilde{L}_{\text{mix}}(T)) \) where, for \( \sigma \in S \), we define \( g(\sigma) \) be the derivation which takes \( \{\sigma_1, \sigma_2, \ldots, \sigma_n, \xi\} \) into \( \{\sigma, \sigma_1, \sigma_2, \ldots, \sigma_n, \xi\} \).
That such a derivation exists follows from the fact that the derivations $D$ of the free Lie algebra $\tilde{L}(T)$ can be assigned arbitrarily and can be uniquely extended to derivations of the quadratic Lie algebra $\tilde{L}(T)$ by defining $D(\xi) = [\xi, D(\xi)]$ if $\xi$ is an element of $T$ of degree 1. Let $L$ be the semi-direct product of $\tilde{L}_{\text{mix}}(T)$ and $\tilde{L}_{\text{mix}}(S)$ with respect to the homomorphism $\varphi$. Every element of $L$ can be uniquely written in the form $\xi + \sigma$ with $\xi \in L_{\text{mix}}(T), \sigma \in L_{\text{mix}}(S)$. Then

$$[\xi_1 + \sigma_1, \xi_2 + \sigma_2] = [\xi_1, \xi_2] + g(\sigma_1)(\xi_2) + g(\sigma_2)(\xi_1) + [\sigma_1, \sigma_2].$$

and $P(\xi + \sigma) = P(\xi) + g(\sigma)(\xi) + P(\sigma)$ if $\xi, \sigma$ are of degree 1. Since $\varphi_1(g(\sigma)(\xi)) = f(\sigma)(\varphi_1(\xi))$ we see that there is a unique homomorphism $\varphi$ of $L$ into $\tilde{L}_{\text{mix}}(X)$ which restricts to $\varphi_1$ and is the identity on $\tilde{L}_{\text{mix}}(S)$. If $\psi$ is the homomorphism of $\tilde{L}(X)$ into $L$ which is the identity on $X$ we have $\varphi \circ \psi$ and $\psi \circ \varphi$ identity maps so that $\varphi$ and hence $\varphi_1$ is bijective.

\begin{corollary}
If $B$ is the enveloping algebra of $\tilde{L}_{\text{mix}}(S) = \tilde{L}_{\text{mix}}(X)/\mathfrak{a}$ then, via the adjoint representation, $\mathfrak{a}/[\mathfrak{a}, \mathfrak{a}]$ is a free $B$-module with basis the images of the elements $\xi \in X - S$.
\end{corollary}

Let $X$ be a finite weighted set and let $S \subset X$. Let $\mathfrak{a}$ be the ideal of $\tilde{L} = \tilde{L}_{\text{mix}}(X)$ generated by $X - S$ and let $B$ be the enveloping algebra of $\tilde{L}/\mathfrak{a}$.

\begin{theorem}
Let $T = \{\tau_1, \ldots, \tau_t\} \subset \mathfrak{a}$ whose elements are homogeneous of degree $\geq 2$ and $B$-independent modulo $\mathfrak{a}^*$. If $\rho_1, \ldots, \rho_m$ are homogeneous elements of $\mathfrak{a}$ which lie in the $\mathbb{F}_2$-span of $T$ modulo $\mathfrak{a}^*$ and which are linearly independent over $\mathbb{F}_2$ modulo $\mathfrak{a}^*$ then the sequence $\rho_1, \ldots, \rho_m$ is strongly free in $\tilde{L}$.
\end{theorem}

\begin{proof}
Let $\mathfrak{r}$ is the ideal of $\tilde{L}$ generated by $\rho_1, \ldots, \rho_m$ and let $U = U_{\text{quad}}$ be the enveloping algebra of $\tilde{L}/\mathfrak{r}$. The elements

$$\text{ad}(\sigma_1)\text{ad}(\sigma_2)\cdots\text{ad}(\sigma_n)(\rho_j)$$

with $1 \leq j \leq m, n \geq 0, \sigma_i \in S$ generate $\mathfrak{r}$ as an ideal of the quadratic Lie algebra $\mathfrak{a}$. Suppose that these elements form part of a basis of the free quadratic 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. Now let $\mu_i$ be the image of $\rho_i$ in $M$ and suppose that $\sum_i u_i \mu_i = 0$ with $u_i \in U$. Then, since 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 $S$ and $c_{ij} \in C$ with $\bar{c}_{ij}$ its image in $U$, the dependence relation

$$0 = \sum_i u_i \mu_i = \sum_{i,j} (\bar{c}_{ij} w_j) \mu_i = \sum_{i,j} c_{ij} (w_j \mu_i)$$

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

To show that the elements of the form $\text{ad}(\sigma_1)\text{ad}(\sigma_2)\cdots\text{ad}(\sigma_n)(\rho_j)$ are part of a Lie algebra basis of $\mathfrak{a}$ it suffices to show that $\rho_1, \ldots, \rho_m$ are $B$-independent modulo
If Example 4.9. If $H$ is the $\mathbb{F}_2$-span of $\rho_1, \ldots, \rho_m$, we can find a basis $\gamma_1, \ldots, \gamma_m$ of $H$ such that

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

where $a_i, a_{ij} \in \mathbb{F}_2$, $a_i \neq 0$, $m + s = t$, $T = \{\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_s\}$. If $u_1, \ldots, u_m \in B$, we have

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

If $\sum_{j=1}^{m} u_i \gamma_i = 0 \mod \mathfrak{a}^*$ then by the $B$-independence of the elements of $T$ we $a_i u_i = 0$ so that $u_i = 0$ for all $i$ which implies the $B$-independence of $\gamma_1, \ldots, \gamma_m$ and hence of $\rho_1, \ldots, \rho_m$. □

**Corollary 4.8.** Let $X = \{\xi_1, \ldots, \xi_d\}$ with $d \geq 4$ even and let $\rho_1, \ldots, \rho_d \in \tilde{L}_{\text{mix}}(X)$ with

$$\rho_i = a_i \xi_i^2 + \sum_{j=1}^{d} \ell_{ij} [\xi_i, \xi_j],$$

where (a) $a_i = 0$ if $i$ is odd, (b) $\ell_{ij} = 0$ if $i, j$ odd, (c) $\ell_{12} = \ell_{23} = \ldots = \ell_{d-1,d} = \ell_{d1} = 1$ and (d) $\ell_{1d} \ell_{d,d-1} \cdots \ell_{32} \ell_{21} = 0$. Then the sequence $\rho_1, \ldots, \rho_d$ is strongly free.

**Proof.** Let $\mathfrak{a}$ be the ideal of $\tilde{L}_{\text{mix}}(X)$ generated by the $\xi_i$ with $i$ even and let $\mathfrak{b}$ be the subspace of $\mathfrak{a}^2$ generated by the $\xi_i^2$, $[\xi_i, \xi_j]$ with $i, j$ even. Then the $\rho_i$ are in $\mathfrak{a}$ and their images in $V = (\mathfrak{a}/\mathfrak{a}^*\mathfrak{a})_2 = \mathfrak{a}_2/\mathfrak{b}$ are linearly independent. Indeed, the images in $V$ of the elements $[\xi_i, \xi_j]$ with $i$ odd, $j$ even $i < j$ form a basis for $V$ which we order lexicographically. If $A$ is the matrix representation of $\rho_1, \ldots, \rho_d$ with respect to this basis, the $d$ columns $(1, 2), (2, 3), (3, 4), \ldots, (1, d)$ of $A$ form the matrix

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

which has determinant $\ell_{12} \ell_{23} \cdots \ell_{m-1,m} \ell_{m1} + \ell_{1m} \ell_{21} \ell_{32} \cdots \ell_{m,m-1} = 1$. □

**Example 4.9.** If $d \geq 4$ is even then

$$a_i \xi_i^2 + [\xi_1, \xi_2], a_2 \xi_2^2 + [\xi_2, \xi_3], \ldots, a_d \xi_d^2 + [\xi_d, \xi_1]$$

is a strongly free sequence if $a_i = 0$ for $i$ odd.
5. Mild Groups

Let $F = F(x_1, \ldots, x_d)$ be the free pro-2-group on $x_1, \ldots, x_d$ and let $G = F/R$ with $R$ the closed normal subgroup of $F$ generated by $r_1, \ldots, r_m$. Let $(F_n)$ be the filtration of $F$ induced by the $(x, \tau)$-filtration of $F$. It is induced by the $(x, \tau)$-filtration of $\Lambda = \mathbb{Z}_2[[F]]$. Let $G_n$ be the image of $F_n$ in $G$ and let $\Gamma_n$ be the image of $\Lambda_n$ in $\Gamma = \mathbb{Z}_2[[G]]$.

Let $\rho_i$ be the initial form of $r_i$ with respect to the $(x, \tau)$-filtration of $F$; by definition, if $r \in F_k$, $r \notin F_{k+1}$, the initial form of $r$ is the image of $r$ in $L_k(F) = \text{gr}_k(F)$. We assume that the degree $h_i$ of $\rho_i$ is $> 1$.

**Definition 5.1** ((Strongly Free Presentation)). The presentation $G = F/R$ is strongly free if $\rho_1, \ldots, \rho_m$ is strongly free in $L_{\text{mix}}(F)$.

**Definition 5.2** ((Mild Group)). A pro-2-group $G$ is said to be weakly mild if it has a minimal presentation $G = F/R$ of finite type which is strongly free with respect to some $(x, \tau)$-filtration of $F$. It is called mild if the $\tau_i = 1$ for all $i$ in which case the $(x, \tau)$-filtration is the lower 2-central series of $F$.

**Theorem 5.3.** Let $F/R$ be a strongly free presentation of $G$ with $R = (r_1, \ldots, r_m)$. Let $\tau$ be the ideal of $L(F(X))$ generated by the initial forms $\rho_1, \ldots, \rho_m$ of the defining relations $r_1, \ldots, r_m$. Then

(a) $L(G) = L(F)/\tau$.

(b) The group $R[[R, R]]$ is a free $\mathbb{Z}_2[[G]]$-module on the images of $r_1, \ldots, r_m$.

(c) The presentation $G = F/R$ is minimal and $cd(G) = 2$.

(d) The enveloping algebra of $L(G)$ is the graded algebra associated to the filtration $(\Gamma_n)$ of $\Gamma = \mathbb{Z}_2[[G]]$, where $\Gamma_n$ is the image of $\Lambda_n$ in $G$.

(e) The filtration $(G_n)$ of $G$ is induced by the filtration $(\Gamma_n)$ of $\Gamma$.

(f) The Poincaré series of $\text{gr}(\Gamma)$ is $1/(1-t)(1-(t^{r_1} + \cdots + t^{r_d}) + t^{h_1} + \cdots + t^{h_m})$.

(g) If $b_n = \dim \tilde{L}_n$ then the Poincaré series of $\text{gr}(\Gamma)/\pi \text{gr}(\Gamma)$ is equal to

$$(1 + t)^r \prod_{n \geq 2} (1 - t^n)^{-b_n},$$

where $r = b_1$ is the number of $i$ with $\tau_i = 1$.

(h) If $b_n, r$ are as in (g) and

$$1 - (t^{r_1} + \cdots + t^{r_d}) + t^{h_1} + \cdots + t^{h_m} = (1 - \alpha_1 t) \cdots (1 - \alpha_s t)$$

then $a_n = \sum_{k=2}^n b_k$ with

$$b_n = \frac{1}{n} \sum_{i \leq n} \mu(\frac{n}{\ell})(\alpha_1^\ell + \cdots + \alpha_s^\ell + (-1)^\ell r).$$

Except for (g) and (h), the proof this theorem is the same as the proof of Theorem 4.1 in [S] except that the freeness of the Lie algebra $\tau$ over $\mathbb{F}_2[\pi]$ is deduced from the fact that $\tau$ is an ideal of the free Lie algebra $L_{\text{mix}}(X)^+$ and that $L_{\text{mix}}(X)^+/\tau$ a torsion free $\mathbb{F}_2[\pi]$-module.
To prove \((g)\) and \((h)\) let \(A\) be the enveloping algebra of the mixed Lie algebra \(L = L_{\text{mix}}(F(X))\) and let \(B\) be the enveloping algebra of the \(\mathbb{F}_2[\pi]\)-Lie algebra \(L^+\). Then \(L\) is the free mixed Lie algebra on \(\xi_1, \ldots, \xi_d\), where \(\xi_i\) is the image of \(x_i\) in \(\text{gr}_{r_i}(F)\). By Theorem 2.3 \(L^+\) is a free Lie algebra over \(\mathbb{F}_2[\pi]\) and the canonical map of \(B\) into \(A\) is injective. Moreover, assuming that \(\xi_1, \ldots, \xi_s\) the \(\xi_i\) of degree 1, then \(A\) is a free \(B\)-module with basis \(\xi_1^{e_1} \cdots \xi_s^{e_s}\) \((e_i = 0, 1)\). If \(\tau_B\) be the ideal of \(B\) generated by \(r\) then

\[
\tau_A = \sum_{e_i=0,1} \xi_1^{e_1} \cdots \xi_s^{e_s} \tau_B
\]

is the ideal of \(A\) generated by \(r\). It follows that the canonical map of \(B/\tau_B\) into \(A/\tau_A\) is injective and that \(A/\tau_A\) is a free \(B/\tau_B\)-module with basis \(\xi_1^{e_1} \cdots \xi_s^{e_s}\) \((e_i = 0, 1)\). The algebra \(U = A/\tau_A\) is the enveloping algebra of the mixed Lie algebra \(g = L/r\) and \(V = B/\tau_B\), the enveloping algebra of the Lie algebra \(L^+/r\) over \(\mathbb{F}_2[\pi]\). If \(\bar{U} = U/\pi U\) and \(\bar{V} = V/\pi V\) we obtain that the canonical map of \(V\) into \(\bar{U}\) is injective and that \(\bar{U}\) is a free \(\bar{V}\)-module with basis \(\xi_1^{e_1} \cdots \xi_s^{e_s}\) \((e_i = 0, 1)\). The algebra \(\bar{U}\) is the enveloping algebra of the quadratic Lie algebra \(\bar{g}\) and \(\bar{V}\) is the enveloping algebra of the Lie algebra \(\bar{g}^+\) over \(\mathbb{F}_2\).

We now use the fact that \(\bar{L}/\bar{r}\), where \(\bar{r}\) is the image of \(r\) in \(\bar{L}\), is a strongly free presentation to deduce that \(P(\xi) \not\in \bar{r}\) for every non-zero element \(\xi\) of \(\bar{L}\) of degree 1. Indeed, if \(P(\xi)\) lies in \(\bar{r}\) then, if \(\xi\) is the image of \(P(\xi)\) in \(\bar{L}/\bar{r}\) and \(\bar{\xi}\) the image of \(\xi\) in \(\bar{g}\), we would have \(\xi, \bar{\xi} \neq 0\)

\[
ad(\bar{\xi}) = 0
\]

which contradicts the fact that \(\bar{r}/[\bar{r}, \bar{r}]\) is a free \(\bar{V}\)-module via the adjoint representation and the fact that \(\bar{V}\) is an integral domain. Thus multiplication by \(P(\xi) = \xi^2\) maps \(\bar{V}\) injectively in to \(\bar{V}\) which implies that multiplication by \(\xi\) is injective on \(\bar{V}\). This in turn implies that

\[
P_{\bar{V}}(t) = tP_{\bar{V}}(t).
\]

We thus obtain that \(P_{\bar{U}}(t) = (1 + t)^s P_{\bar{V}}(t)\). This implies \((g)\) since

\[
P_{\bar{V}}(t) = \prod_{n \geq 2} (1 - t^n)^{-b_n}
\]

and \(U_{\text{mix}}(\text{gr}(G)) = U\). The assertion \((h)\) follows form the fact that \(\text{gr}(G)^+\) is a free \(\mathbb{F}_2[\pi]\)-module and a standard argument to compute \(b_n\) using the formula

\[
(1 + t)^s \prod_{n \geq 2} (1 - t^n)^{-b_n} = \frac{1}{(1 - \alpha_1 t) \cdots (1 - \alpha_s t)}
\]

6. Zassenhaus Filtrations

Theorem 2.3 can be extended under certain conditions to filtrations induced by valuations of the completed group ring \(\mathbb{F}_2[[F]]\). The Lie algebras associated to these filtrations are restricted Lie algebras in the sense of Jacobson [4]. A sufficient condition is that the initial forms of the relators lie in a Lie subalgebra over \(\mathbb{F}_2\) which is quadratic and that these initial forms are strongly free. This will
give a second proof that the pro-2-group with these relations is of cohomological dimension 2.

Let $F$ be the free pro-2-group on $x_1, \ldots, x_d$. The completed group algebra $\tilde{A} = \mathbb{F}_2[[F]]$ over the finite field $\mathbb{F}_2$ is isomorphic to the algebra of formal power series in the non-commuting indeterminates $X_1, \ldots, X_d$ over $\mathbb{F}_2$. Identifying $F$ with its image in $\tilde{A}$, we have $x_i = 1 + X_i$.

If $\tau_1, \ldots, \tau_d$ are integers $> 0$, we define a valuation $\bar{w}$ of $\tilde{A}$ by setting

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

Let

$$\hat{A}_n = \{ u \in \tilde{A} \mid \bar{w}(u) \geq n \}, \quad \text{gr}_n(\tilde{A}) = \hat{A}_n/\hat{A}_{n+1}, \quad \text{gr}(\tilde{A}) = \bigoplus_{n \geq 0} \text{gr}_n(\tilde{A}).$$

Then $\text{gr}(\tilde{A})$ is a graded $\mathbb{F}_2$-algebra. If $\xi_i$ is the image of $X_i$ in $\text{gr}_{\tau_i}(\tilde{A})$ then $\text{gr}(\tilde{A})$ is the free associative $\mathbb{F}_2$-algebra $\bar{A}$ on $\xi_1, \ldots, \xi_d$ with a grading in which $\xi_i$ is of degree $\tau_i$. Note that when $\tau_i = 1$ for all $i$ we have $\hat{A}_n = \bar{I}^n$, where $\bar{I}$ is the augmentation ideal $(X_1, \ldots, X_d)$ of $\bar{A}$.

The Lie subalgebra $\bar{L}$ of $\tilde{A}$ generated by the $\xi_i$ is the free Lie algebra over $\mathbb{F}_2$ on $\xi_1, \ldots, \xi_m$ by the Birkhoff-Witt Theorem. The Lie subalgebra $L$ generated by $\xi_1, \ldots, \xi_d$ and the $\xi_i^2$ where $\xi_i$ is of degree 1 is the free quadratic Lie algebra on $\xi_1, \ldots, \xi_d$.

A decreasing sequence $(G_n)$ of closed subgroups of a pro-2-group $G$ which satisfies

$$[G_i, G_j] \subseteq G_{i+j}, \quad G_i^2 \subseteq G_{2i}.$$

is called a called, after Lazard [9], a 2-restricted filtration of $G$.

For $n \geq 1$, let $F_n = (1 + \hat{A}_n) \cap F$. Then $(F_n)$ is a 2-restricted filtration of $F$. This filtration is also called the Zassenhaus $(x, \tau)$-filtration of $F$. The mapping $x \mapsto x^2$ induces an operator $P$ on gr$(F)$ sending gr$_n(F)$ into gr$_{2n}(F)$. With this operator, gr$(F)$ is a restricted Lie algebra over $\mathbb{F}_2$. If $\tau_i = 1$ for all $i$, the subgroups $F_n$ are the so-called dimension subgroups mod 2. They can be defined by

$$F_n = \langle \{[y_1, \ldots, [y_{r-1}, y_r], \ldots]^{2^s} \mid y_1, \ldots, y_r \in F, \ r2^s \geq n \rangle.$$

Let $r_1, \ldots, r_m \in F^2[F, F]$ and let $R = (r_1, \ldots, r_m)$ be the closed normal subgroup of $F$ generated by $r_1, \ldots, r_m$. Let $\rho_i \in \text{gr}_{h_i}(F)$ be the initial form of $r_i$ with respect to the Zassenhaus $(x, \tau)$-filtration $(F_n)$ of $F$. 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 2-restricted filtration of $G$. Let $\Gamma_n$ be the image of $\hat{A}_n$ in $\Gamma = \mathbb{F}_2[[G]]$.

**Theorem 6.1.** Suppose that the initial forms $\rho_1, \ldots, \rho_m$ of $r_1, \ldots, r_m$ are in $\bar{L}$ and are strongly free. Then

(a) We have $\text{gr}(G) = \text{gr}(F)/(\rho_1, \ldots, \rho_m)$.

(b) The group $R/R^2 \cong [R, R]$ is a free $\mathbb{F}_2[[G]]$-module on the images of $r_1, \ldots, r_m$.

(c) The presentation $G = F/R$ is minimal and $\text{cd}(G) = 2$.

(d) The enveloping algebra of $\text{gr}(G)$ is the graded algebra associated to the filtration $(\Gamma_n)$. 

(e) The filtration \((\tilde{\Gamma}_n)\) of \(\tilde{\Gamma}\) induces the filtration \((G_n)\) of \(G\).

(f) The Poincaré series of \(gr(\tilde{\Gamma})\) is \(1/(1 - (t^1 + \cdots + t^d) + t^{h_1} + \cdots + t^{h_m})\).

(g) If \(\tau_i = 1\) for all \(i\) and \(a_n = \dim gr_n(G)\) then

\[
\prod_{n \geq 1} (1 + t^n)^{a_n} = \frac{1}{1 - dt + mt^2}.
\]

**Proof.** In [6], Koch proves that if \(R/R\tilde{I}\) is a free \(\tilde{A}/R\) module on the images of \(\rho_1, \ldots, \rho_m\) then \(gr(\tilde{\Gamma}) = \tilde{A}/R\), where \(R\) is the ideal of \(\tilde{A} = gr(\tilde{\Lambda})\) 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 \(R/R\tilde{I}\) is the image of the free \(\tilde{A}/R\)-module \(\tilde{t}/[\tilde{t}, \tilde{t}]\) under the injective mapping

\[
\tilde{t}/[\tilde{t}, \tilde{t}] \rightarrow I/R\tilde{I}
\]

where \(\tilde{t}\) is the ideal of the quadratic Lie algebra \(\tilde{L}\) generated by \(\rho_1, \ldots, \rho_m\). Now consider the exact sequence

\[
0 \rightarrow \tilde{t}/[\tilde{t}, \tilde{t}] \rightarrow gr(\tilde{\Gamma})^d \rightarrow gr(\tilde{\Gamma}) \rightarrow F_2 \rightarrow 0,
\]

Since \(\tilde{t}/[\tilde{t}, \tilde{t}]\) is a free \(gr(\tilde{\Gamma})\)-module of rank \(m\), we obtain the exact sequence

\[
0 \rightarrow gr(\tilde{\Gamma})^m \rightarrow gr(\tilde{\Gamma})^d \rightarrow gr(\tilde{\Gamma}) \rightarrow F_2 \rightarrow 0.
\]

This yields (f). By a result of Serre (cf. [9], V, 2.1), we obtain the exact sequence

\[
0 \rightarrow \tilde{\Gamma}^m \rightarrow \tilde{\Gamma}^d \rightarrow \tilde{\Gamma} \rightarrow F_2 \rightarrow 0.
\]

By a result of [2], section 5, this proves (b) and (c). If \(\mathcal{R} = (\rho_1, \ldots, \rho_m)\) is the ideal of the restricted Lie algebra \(gr(F(X))\) generated by \(\rho_1, \ldots, \rho_m\), we have canonical homomorphisms of restricted Lie algebras

\[
gr(F(X))/\mathcal{R} \rightarrow gr(G) \rightarrow gr'(G) \rightarrow gr(\tilde{\Gamma}),
\]

where the first arrow is surjective and \(gr'(G)\) is the restricted Lie algebra associated to the Zassenhaus filtration \((G_n')\) of \(G\) induced by the filtration of \(\Gamma\). Since \(gr(\tilde{\Gamma})\) is the enveloping algebra of the restricted Lie algebra \(gr(F)/\mathcal{R}\), the Birkhoff-Witt Theorem for restricted Lie algebras shows that all arrows are injective which yields (a) and (d). The injectivity of \(gr(G) \rightarrow gr'(G)\) yields \(G_n = G'_n\) for all \(n\) by induction which proves (e). The proof of (g) follows from (d), (e), (f) and Proposition A3.10 of [9].

**Remark.** The formula given in (g) partially answers a question of Morishita stated in [10] in a remark after Theorem 3.6.

### 7. Proof of Theorem

Let \((\chi_i)_{1 \leq i \leq d}\) be a basis of \(H^1(G)\) with \((\chi_i)_{i \in S}\) a basis of \(U\) and \((\chi_j)_{j \in S'}\) a basis of \(V\). Let \((\xi_i)_{i \in S}\) be the dual basis of \(H^1(G)^* = L_1(G)\) and let \(g_i\) be any lift of \(\xi_i\) to \(G\). Let \(F\) be the free pro-2-group on \(x_1, \ldots, x_d\) and let \(f : F \rightarrow G\) be the homomorphism sending \(x_i\) to \(g_i\). Then the induced mapping of \(L_1(F)\) into \(L_1(G)\) is an isomorphism which we use to identify these two groups. If \(R\) is the kernel of \(f\) the presentation \(G = F/R\tilde{I}\) is minimal and the transgression map \(tg : H^1(R/R^2[R, F]) \rightarrow H^2(G)\) is an isomorphism. Hence \(tg^* : H^2(G)^* \rightarrow R/R^2[R, F]\)
is the symmetric tensor product of 
which is surjective since, by assumption, the cup-product maps 
Since the annihilator of 
ξ generated by the 
elements of the form 
have 
the composite 
By Theorems 4.4 and 4.7, the elements 
ρ, if their images in 
ξ elements 
neighborhood of 
the ideal of 
U generated by the elements of the form 
Let 
The cup product 
H1(G) ⊗ H1(G) → H2(G) vanishes on the subspace W generated by elements of the form \(a \otimes b + b \otimes a\) and so, by duality, induces a homomorphism

\[H^2(G)^* \to L_1(F) \otimes L_1(F) = (H^1(G) \otimes H^1(G))^*,\]

whose image is contained in \(W^0\), the annihilator of the subspace \(W\). Since \(\dim W = d(d-1)/2\) we have \(\dim W^0 = d(d +1)/2\). Now \(L_2(F)\) can be identified with the subspace of the tensor algebra of \(L_1(F)\) generated by the elements of the form \(ξ^2\) and \([ξ, η] = ξη + ηξ\). Since these elements lie in \(W^0\) and \(\dim L_2(F) = \dim W^0\) we obtain that \(W^0 = L_2(F)\). If 
\(H^1(G) \otimes' H^1(G) = (H^1(G) \otimes H^1(G))/W\)
is the symmetric tensor product of \(H^1(G)\) with itself we have 
\(H^1(G) \otimes' H^1(G) = U \otimes' U \oplus V \otimes' V \oplus U \otimes' V\), 
where \(U \otimes' V\) is the image of \(U \otimes V\) in \(H^1(G) \otimes' H^1(G)\). Since the cup-product vanishes on \(U \otimes' U\) it induces a homomorphism 
\(φ : V \otimes' V \oplus U \otimes' V = (H^1(G) \otimes' H^1(G))/U \otimes' U \to H^2(G)\)
which is surjective since, by assumption, the cup-product maps \(U \otimes V\) onto \(H^2(G)\). Since the annihilator of \(U \otimes' U\) is contained in \(a_2\), where \(a\) is the ideal of \(L(F)\) generated by the \(ξ_i\) with \(i \in S'\), we get an injective homomorphism 
\(φ^* : H^2(G)^* \to a_2\).

Let \(r_1, \ldots, r_m\) generate \(R\) as a closed normal subgroup of \(F\). Since \(r_i \in F_2\) we have

\[r_k = \prod_{i=1}^{d} a_i^{2a_{ik}} \prod_{i<j} [x_i, x_j]^{a_{ijk}} \mod F_3\]

with \(a_{ik} = r_k(χ_i \cup χ_i)\) and \(a_{ijk} = r_k(χ_i \cup χ_j)\) (cf. [7], Prop. 3). Moreover, if \(ρ_k\) is the initial form of \(r_k\), we have

\[φ^*(r_k) = ρ_k = \sum_{i=1}^{d} a_{ik}ξ_i^2 + \sum_{i<j} a_{ijk}[ξ_i, ξ_j].\]

By Theorems 4.4 and 4.7, the elements \(ρ_1, \ldots, ρ_m\) form a strongly free sequence if their images in \((a/\alpha')_2 = a_2/b\), where \(b\) is the subspace of \(a_2\) generated by the elements \(ξ_i^2, [ξ_i, ξ_j]\) with \(i, j \in S'\), are linearly independent. If \(c\) is the subspace of \(a_2\) generated by the elements \([ξ_i, ξ_j]\) with \(i \in S, j \in S'\) then \(a_2 = b \oplus c\). The images of the \(ρ_i\) in \(a_2/b\) form a linearly independent sequence if and only if the projections of the \(ρ_i\) on \(c\) form an independent sequence. But this is equivalent to the composite

\[H^2(G)^* \to a_2 \to c\]

being injective. Now \(a_2\) is the dual space of 
\((H^1(G) \otimes' H^1(G))/U \otimes' U = V \otimes' V \oplus U \otimes' V\)
and, with respect to this duality, we have \( c = (V \otimes V)^0 \) which implies that the canonical injection
\[
\iota : U \otimes V \to V \otimes V \oplus U \otimes V
\]
is dual to the projection of \( a_2 \) onto \( c \). Since \( \phi \circ \iota \) is surjective it dual \( \iota^* \circ \varphi^* \) is injective. But the latter is the composite \( H^2(G)^* \to a_2 \to c \).

8. Proof of Theorem 1.2 and Examples

Without loss of generality, we may assume \( S_0 = \{q_1, \ldots, q_m\} \) with \( m \geq 2 \), \( q_1 \equiv 1 \mod 4 \) and \( q_m \equiv 3 \mod 4 \). Let \( q'_1, \ldots, q'_m \) be primes \( \equiv 1 \mod 4 \) which are not in \( S_0 \) and such that
(a) \( q'_i \) is a square mod \( q'_j \) for all \( i, j \).
(b) \( q'_i \) is not a square mod \( q_i \) and \( q'_i \) is not a square mod \( q_i \) and \( q_{i-1} \) for \( 1 < i \leq m \).

Let \( S = \{q'_1, q'_1, q'_2, q'_2, \ldots, q'_m, q_m, q_{m+1}\} \) where \( q_{m+1} \) is a prime \( \equiv 3 \mod 4 \) distinct from \( q_1, \ldots, q_m \) and such that \( q_m \) is not a square mod \( q'_i \) but is a square mod \( q'_i \) for all \( i \neq 1 \).

Let
\[
(p_1, \ldots, p_{2m+1}) = (q'_1, q'_1, q'_2, q'_2, \ldots, q'_m, q_m, q_{m+1}).
\]
and let \( x_1, \ldots, x_{2m+1} \) be generators for the inertia subgroups of \( G_{S}(2) \) at the primes \( p_1, \ldots, p_{2m+1} \) respectively. Then, by \( [5] \), Theorem 11.10 and Example 11.12, the group \( G = G_{S}(2) \) has the presentation \( G = F(X)/R = \langle x_1, \ldots, x_{2m+1} \mid r_1, \ldots, r_{2m+1}, r \rangle \), where
\[
r_i \equiv x_i^{2a_i} \prod_{j=1}^{2m+1} [x_i, x_j]^{\ell_{ij}} \mod F_3,
\]
\[
r \equiv \prod_{i=1}^{2m+1} x_i^{a_i} \mod F_2
\]
with \( a_i = 0 \) if and only if \( p_i \equiv 1 \mod 4 \) and \( \ell_{ij} = 1 \) if \( p_i \) is not a square mod \( p_j \) and 0 otherwise. Moreover, we can omit the relator \( r_{2m+1} \). By construction we have
\[
r \equiv \prod_{i=2}^{m-1} x_i^{2q_i} x_{2m} x_{2m+1} \mod F_2
\]
so that \( x_{2m+1} \equiv x_{2m} x_{2m}^{-2} \cdots x_{2m-2} \mod F_2 \). Hence \( G = \langle x_1, \ldots, x_{2m} \mid r'_1, \ldots, r'_{2m} \rangle \) where
\[
r'_i \equiv x_i^{2a_i} \prod_{j=1}^{2m} [x_i, x_j]^{\ell'_{ij}}
\]
with \( \ell'_{ij} = 0 \) if \( i, j \) are odd and
\[
\ell'_{12} = \ell'_{23} = \ell'_{34} = \cdots = \ell'_{2m-1,2m} = \ell'_{2m-1,2m} = 1
\]
but \( \ell'_{1,2m} = 0 \). The image of the initial form of \( r'_i \) in \( \tilde{L}_{mix}(X) \) (here \( \tau_i = 1 \) for all \( i \)) is
\[
\rho'_i = \xi_{2a_i} + \sum_{j=1}^{2m} \ell'_{ij} [\xi_i, \xi_j].
\]
By Corollary \[4.8\] the sequence $\rho_1', \ldots, \rho_{2m}'$ is strongly free in $\hat{L}_{\text{mix}}(X)$ and therefore $G$ is mild by Theorem \[4.4\].

**Example 1.** To illustrate the above proof, let $S_0 = \{13, 3\} = \{q_1, q_2\}$. Then $q_1' = 41$, $q_2' = 5$, $q_3 = 19$ satisfy the required conditions. Then

$$S = \{41, 13, 5, 3, 19\} = \{p_1, p_2, p_3, p_4, p_5\}$$

and the relators for the first presentation are

$$
\begin{align*}
    r_1 &\equiv [x_1, x_2][x_1, x_4][x_1, x_5] \mod F_3, \\
    r_2 &\equiv [x_2, x_1][x_2, x_3][x_2, x_5] \mod F_3, \\
    r_3 &\equiv [x_3, x_2][x_3, x_4] \mod F_3, \\
    r_4 &\equiv x_3^2[x_4, x_1][x_4, x_3][x_4, x_5] \mod F_3, \\
    r_5 &\equiv x_3^2[x_5, x_1][x_5, x_2] \mod F_3, \\
    r &\equiv x_4x_5 \mod F_2.
\end{align*}
$$

Hence $G = G_S(2)$ has the presentation $< x_1, x_2, x_3, x_4 | r_1', r_2', r_3', r_4' >$ where

$$
\begin{align*}
    r_1' &\equiv [x_1, x_2] \mod F_3, \\
    r_2' &\equiv [x_2, x_1][x_2, x_3][x_2, x_4] \mod F_3, \\
    r_3' &\equiv [x_3, x_2][x_3, x_4] \mod F_3, \\
    r_4' &\equiv x_3^2[x_4, x_1][x_4, x_3] \mod F_3.
\end{align*}
$$

**Example 2.** This example is due to Denis Vogel and while it does not illustrate exactly the above proof it does contain the basic idea which led to the result. Let $S = \{5, 29, 7, 11, 3\}$. Using the above notation for a Koch presentation of $G_S(2)$ with $p_1 = 5, p_2 = 29, p_3 = 7, p_4 = 11, p_5 = 3$ we have

$$
\begin{align*}
    r_1 &\equiv [x_1, x_3][x_1, x_5] \mod F_3, \\
    r_2 &\equiv [x_2, x_4][x_2, x_5] \mod F_3, \\
    r_3 &\equiv x_3^2[x_3, x_1][x_3, x_4] \mod F_3, \\
    r_4 &\equiv x_3^2[x_4, x_2][x_4, x_5] \mod F_3, \\
    r_5 &\equiv x_5^2[x_5, x_1][x_5, x_2] \mod F_3, \\
    r &\equiv x_3x_4x_5 \mod F_2.
\end{align*}
$$

Omitting $r_5$ and setting $x_5 = x_3x_4 \mod F_2$, we get

$$
\begin{align*}
    r_1' &\equiv [x_1, x_4] \mod F_3, \\
    r_2' &\equiv [x_2, x_3] \mod F_3, \\
    r_3' &\equiv x_3^2[x_3, x_1][x_3, x_4] \mod F_3, \\
    r_4' &\equiv x_4^2[x_4, x_2][x_4, x_3] \mod F_3.
\end{align*}
$$
The images of the initial forms of these relators in $\tilde{L}_{mix}(X)$ (all $\tau_i = 1$) are

$$
\rho'_1 = [\xi_1, \xi_4],
$$

$$
\rho'_2 = [\xi_2, \xi_3],
$$

$$
\rho'_3 = \xi_3^2 + [\xi_3, \xi_1] + [\xi_3, \xi_4],
$$

$$
\rho'_4 = \xi_4^2 + [\xi_4, \xi_2] + [\xi_4, \xi_3].
$$

If $a$ is the ideal of $\tilde{L}_{mix}(X)$ generated by $\xi_3, \xi_4$ the $\rho'_i$ are in $a$ and their images in $a/a^*$ are the classes of

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

which are part of a basis for $(a/a^*)_2$. Hence $G_S(2)$ is mild. If $a_n = \dim L(G_S)$ then $a_1 = 4$ and

$$
a_n = \sum_{k=2}^{n} \frac{1}{k} \sum_{\ell | k} \mu\left(\frac{k}{\ell}\right)(2^{\ell+1} + (-1)^{\ell/4})
$$

for $n \geq 2$ by Theorem 5.3.

References

[1] N. Bourbaki, Groupes et algébres de Lie, Hermann, Paris, 1960.
[2] A. Brumer, Pseudocompact algebras, profinite groups and class formations, J. Algebra 4, 442-470 (1966).
[3] H. Cartan and S. Eilenberg, Homological Algebra, Princeton Math. Ser., No. 19, Princeton 1956.
[4] N. Jacobson, Lie Algebras, Interscience, New York, 1962.
[5] H. Koch, Galois Theory of p-Extensions, Springer, 2002.
[6] H. Koch, Über Pro-p-Gruppen der kohomologischen Dimension 2, Math. Nachr. 78 (1977), 285-289.
[7] J. Labute, Classification of Demuskin Groups, Can. J. Math., 19 (1967), 142-158.
[8] J. Labute, Mild pro-p-groups and Galois groups of p-extensions of $\mathbb{Q}$, J. Reine Angew. Math. 596 (2006), 115-130.
[9] M. Lazard, Groupes analytiques p-adiques, Publ. I.H.E.S., No. 26, Paris, 1965.
[10] H. Morishita, Analogies Between Knots and Primes, 3-Manifolds and Number Fields, arXiv:0904.3399 [math.GT].
[11] A. Schmidt, Über Pro-p-Fundamentalgruppen markierter arithmetischer Kurven, to appear in J. Reine Angew. Math. Engl. Transl.: arXiv:0906.1863 [math.NT].
[12] J.-P. Serre, Cohomologie galoisienne, Lecture Notes in Mathematics, No. 5, Springer, 1964; 5ème édition révisée et complétée, Springer, 1997.
[13] I.R. Šafarevič, Algebraic Number Fields (Russian), Proc. Cong. Stockholm (1962), 163-172 (English Translation: AMS Transl. 31, (1963), 25-39).
[14] I.R. Šafarevič, Extensions with prescribed ramification points (Russian: French Summary), IHES Publ. Math. 18 (1963), 71-95.
[15] E.S. Golod and I.R. Šafarevič, On the Class Field Tower, Izv. Akad. Nauk. SSSR 28 (1964), 261-272.

E-mail address: labute@math.mcgill.ca

Department of Mathematics and Statistics, McGill University, Burnside Hall, 805 Sherbrooke Street West, Montreal QC H3A 2K6, Canada

E-mail address: minac@uwo.ca
