The Mal'cev correspondence for counting problems in groups and rings

15 June 2009

1 Introduction

In the 1980s it became popular to study the subgroup growth of a finitely generated (discrete) group. This is embodied in the sequence (a_n) which counts the number of index-n subgroups of a given group G. One might reasonably ask how one even begins to study this sequence. An attractive possibility is that one might try to encode some of the group structure in a simpler algebraic object. It is not obvious that this can be done in general. The authors of the paper [GSS88] realised that if one specialises to a certain subclass of these groups, namely finitely generated torsion-free nilpotent groups (or $\mathscr{T}$-groups), one can attach a certain Lie algebra over the ring $\mathbb{Z}$. This object looks additively just like the lattice $\mathbb{Z}^d$ for some $d \in \mathbb{N}$. Their beautiful result shows that for this special subclass of groups, counting (finite index) subgroups is essentially the same as counting (finite index) subrings in the ring. Their result is the subject of this note.

A proof of the result is given in Grunewald, Segal and Smith (see [GSS88]). However, it is not self-contained, relying heavily on the 'Mal'cev correspondence' which is described in a book of Segal ([Seg83]). Consequently, the reader has to do some work to identify and adapt certain results appearing in the book in order to reconstruct a coherent argument.

The purpose of these notes is to give a detailed account of this result and its proof in a mostly self-contained manner. We will need to assume two important structural results, whose proofs lie beyond the scope of these notes: the existence of an embedding of any given $\mathscr{T}$-group into a group of upper unitriangular matrices over $\mathbb{Z}$, and the Baker-Campbell-Hausdorff formula.

2 Statement of the Theorem

The result we shall be discussing is the following. We first give the statement, then explain the various notations and terminology.

Theorem 1 ([GSS88], Theorem 4.1) *Let G be a $\mathscr{T}$-group of Hirsch length n. Then there exists $f \in \mathbb{N}$, depending only on n, such that G^f is an LR group, and such that if $L = \log G^f$ then*

$$\zeta_{G,p} = \zeta_{L,p}, \;\; \zeta^{\triangleleft}_{G,p} = \zeta^{\triangleleft}_{L,p}, \;\; \zeta^{\wedge}_{G,p} = \zeta^{\wedge}_{L,p}$$

for all primes p not dividing f.

We will define the Hirsch length of a $\mathscr{T}$-group in Section 3. In Section 4 we will define a map called $\log$ which maps H into an algebra of upper triangular matrices; for H to be an LR group (Lie Ring group) means that the image of H under $\log$ is a $\mathbb{Z}$-lattice and is closed under the induced Lie bracket. If $*$ refers to some property of a subgroup or subring, we write

$$\zeta^*_{G,p}(s) = \sum_{i=0}^{\infty} a^*_{p^k} p^{-ks}, \;\; \zeta^*_{L,p}(s) = \sum_{i=0}^{\infty} b^*_{p^k} p^{-ks}$$

where

$$a^*_{p^k} = |\{H \leq G \mid H \text{ has property } *\}|$$

and

$$b^*_{p^k} = |\{H \leq L \mid H \text{ has property } *\}|.$$

For $* \in \{\leq, \lhd, \wedge\}$, we interpret $\leq$ to mean subgroup (respectively, subring), $\lhd$ to mean normal subgroup (respectively ideal) and $\wedge$ to mean subgroup whose profinite completion is isomorphic to the profinite completion of the original group (respectively subring H of L such that for all primes p, $H \otimes \mathbb{Z}_p$ is isomorphic to $L \otimes \mathbb{Z}_p$).

3 Preliminaries

We start off with some basic facts about $\mathscr{T}$-groups. First, a reminder about nilpotency. For any group G, we can define the lower central series

$$G = \gamma_1(G) \geq \gamma_2(G) \geq \ldots \geq \ldots$$

where the members are defined inductively by $\gamma_2(G) = [G, G]$, $\gamma_{i+1}(G) = [\gamma_i(G), G]$. The group G is called nilpotent if this sequence terminates at 1, and has class c if $\gamma_c(G) \neq 1$ and $\gamma_{c+1}(G) = 1$. The Hirsch length of a group is the number of infinite factors in a chain

$$G = G_1 \geq G_2 \geq \ldots \geq G_k = 1$$

of cyclic extensions (provided that at least one such chain exists, this number is independent of the choice of chain).It may be shown that any $\mathscr{T}$-group has finite Hirsch length.

Now let R denote a commutative ring with identity, and $\mathrm{Tr}_1(m, R)$ the group of upper unitriangular matrices over R (i.e. matrices with entries in R, 1's along the diagonal and zeroes below the diagonal). The first result we need is the following:

Theorem 2 ([Seg83], Chapter 5) *Let G be a $\mathscr{T}$-group. There exists an embedding $G \hookrightarrow \mathrm{Tr}_1(m, \mathbb{Z})$ for some $m \in \mathbb{N}$.*

We will not prove this; rather, we refer the interested reader to the book cited. Often we will only need an embedding of G into $\mathrm{Tr}_1(m, \mathbb{Q})$. In general, groups which admit an embedding into $\mathrm{Tr}_1(m, k)$, where k is a field of characteristic zero, can be studied using the Mal'cev correspondence. This given by a map (called $\log$) from $\mathrm{Tr}_1(m, k)$ to $\mathrm{Tr}_0(m, k)$, where $\mathrm{Tr}_0(m, k)$ is the Lie algebra over k of strictly upper triangular matrices. The map is given by the usual formal power series for $\log$, which will have only finitely many non-zero coefficients since $\mathrm{Tr}_1(m, k)$ is unipotent. It will turn out that $\log$ is a bijection, with inverse $\exp$. The image of the restriction of $\log$ to an arbitrary group G embedded in $\mathrm{Tr}_1(m, k)$ could fail to be closed under addition and the standard Lie bracket $(u, v) = uv - vu$ in $\mathrm{Tr}_0(m, k)$. In the special situation that $\log G$ does enjoy both these properties, we call G an LR group.

The proof of Theorem 2 relies on the following facts:

1. There exists some $f \in \mathbb{N}$ such that G^f is an LR group

2. If H is an LR group then for almost all primes p, the local zeta functions at p of H and $\log H$ are equal

3. If H is a finite index subgroup of G, then for almost all primes p, the zeta functions at p of G and H are equal

The reader who has studied the paper [GSS88] will have noticed that in that paper they package all the 'bad' primes into their definition of f, presumably to streamline the statement of Theorem 2. We find it more intuitive to separate the 'bad' primes according to the three items listed above.

We now begin with a detailed description of the argument.

4 The $\log$ and $\exp$ maps

Most of the material in this section is taken directly from the book [Seg83]. Let k be a field of characteristic zero. For $x \in \mathrm{Tr}_1(m, k)$ put

$$\log x = (x-1) - (x-1)^2/2 + \cdots + (-1)^n (x-1)^{n-1}/(n-1)$$

and for $v \in \mathrm{Tr}_0(m, k)$ put

$$\exp v = 1 + v^2/2! + \cdots + v^{n-1}/(n-1)!$$

Note that $(x-1)^n = 0 = v^n$ so these functions are actually the same as the respective power series. Therefore they are mutually inverse bijections. We next present a formula allowing us to express the group operation in $\mathrm{Tr}_1(m, k)$ in terms of Lie brackets via the $\log$ map. First we need some notation. For $l > 2$ and x_i elements of $\mathrm{Tr}_1(m, k)$, write

$$[x_1, x_2, \ldots, x_l] = [[x_1, x_2, \ldots, x_{l-1}], x_l]$$

which we call a repeated (group) commutator, and for v_i elements of $\mathrm{Tr}_0(m, k)$ write

$$(v_1, v_2, \ldots, v_l) = ((v_1, v_2, \ldots, v_{l-1}), v_l).$$

It will also be useful to have notation to deal with repeated commutators or Lie brackets involving only two arguments repeated in various orders. If $\boldsymbol{e} = (e_1, \ldots, e_j)$ is a vector of positive integers, $x, y \in \mathrm{Tr}_0(m, k)$ and $u, v \in \mathrm{Tr}_1(m, k)$, write

$$[x, y]_{\boldsymbol{e}} = [x, \underbrace{y, \ldots, y}_{e_1}, \underbrace{x, \ldots, x}_{e_2}, \ldots]$$

and

$$(u, v)_{\boldsymbol{e}} = (u, \underbrace{v, \ldots, v}_{e_1}, \underbrace{u, \ldots, u}_{e_2}, \ldots).$$

The following theorem is a technical fact vital to all that follows.

Theorem 3 (Baker-Campbell-Hausdorff formula) *There exist constants $q_{\boldsymbol{e}} \in \mathbb{Q}$, one for each vector $\boldsymbol{e}$ of positive integers, such that $q_{(1)} = 1/2$ and such that for any two matrices $u, v \in \mathrm{Tr}_0(m, k)$, the matrix*

$$u * v = u + v + \sum_{\boldsymbol{e}} q_{\boldsymbol{e}}(u, v)_{\boldsymbol{e}}$$

has the property

$$(\exp u).(expv) = \exp(u * v).$$

When we come to applying this theorem, we will usually not need to know anything more about the actual coefficients involved, except possibly the first one $q_{(1)}$. It is remarkable and by no means obvious that the group operation can be recovered inside the Lie algebra by suitable 'correction' terms coming from Lie commutators. The theorem in fact holds in greater generality than what we see here, namely for formal power series in two non-commuting variables.

5 Lattice groups - a criterion

We will soon discuss a sequence of technical results which will eventually allow us to formulate a condition ensuring that a given subgroup G of $\mathrm{Tr}_1(m, k)$ is an LR group. In fact, the hardest part will be to ensure that G is a lattice group; namely, that its image under $\log$ is closed under addition. Given an element x of $\mathrm{Tr}_1(m, k)$ and a positive integer j, we define $x^{1/j} := \exp((1/j)\log(x))$. It is clear that this defines a unique j^{th} root of x. If x belongs to some subgroup G of $\mathrm{Tr}_1(m, k)$, $x^{1/j}$ may or may not lie in G. We define $G^{1/j}$ to be the subgroup $\langle x^{1/j} \mid x \in G\rangle$ of $\mathrm{Tr}_1(m, k)$ generated by all the j^{th} roots of elements of G. Our main goal in the following section will be to prove the following result.

Theorem 4 ([Seg83], Chapter 6, Theorem 4) *There exists $t \in \mathbb{N}$, depending only on m, such that, if $H \leq \mathrm{Tr}_1(m, \mathbb{Q})$ and $H \lhd H^{1/t}$, then H is an LR group.*

Actually we will show that t can be chosen so that it depends explicitly on the coefficients in the Baker-Campbell-Hausdorff formula up to the terms of (bracket) length $m - 1$.

Now assume that Theorem 4 holds. Suppose we are given a subgroup G of $\mathrm{Tr}_1(m, \mathbb{Q})$. Recall that the first of our three main objectives stated above is to prove that there exists some $f \in \mathbb{N}$ such that G^f is an LR group. (Note that to do this we will not end up using the fact that G is finitely generated.) We claim that we can take $f := t^{m-1}$. We will need the following result about nilpotent groups.

Proposition 1 ([Seg83], Chapter 6, Proposition 2) *If G is a nilpotent group of class at most c and $s \in \mathbb{N}$, then every element of the subgroup*

$$G^{s^c} = \langle g^{s^c} \mid g \in G\rangle$$

is the s^{th} power of an element of G.

Let us assume both Theorem 4 and Proposition 1, and deduce the desired result. Given $G \leq \mathrm{Tr}_1(m, \mathbb{Q})$, note that G has class at most $m-1$. Pick t as in Theorem 4 and put $f := t^{m-1}$. By Proposition 1, every element of G^f is expressible as a t^{th} power of an element of G. Therefore $(G^f)^{1/t}$ is contained in G. However, $G^f \lhd G$ since the image of a product of f^{th} powers under any automorphism is again a product of f^{th} powers. Thus $G^f \lhd (G^f)^{1/t}$ and by Theorem 4, G^f is an LR group.

We close this section by proving Proposition 1. We begin with the technical

Lemma 1 ([Seg83], Chapter 6, Lemma 4) *Let G be a group with $\gamma_{c+1}(G) = 1$ and let $x_1, \ldots, x_r \in G$. Then for every $k \in \mathbb{N}$ we have*

$$(\gamma_c\langle x_1, \ldots, x_r\rangle)^{k^c} = \gamma_c\langle x_1^k, \ldots, x_r^k\rangle.$$

Proof. If $c = 1$ the result is trivial. We argue by induction on c. We may assume that $G = \langle x_1, \ldots, x_r\rangle$. By inductive hypothesis,

$$(\gamma_{c-1}(G))^{k^{c-1}}.\gamma_c(G) = \gamma_{c-1}\langle x_1^k, \ldots, x_r^k\rangle.\gamma_c(G).$$

We will repeatedly make use of the following special identities: if at least one of z and x lies in $\gamma_{c-1}(G)$ then we have

$$[z, xy] = [z, x]^y[z, y] \quad = \quad [z, x][z, y] \tag{1}$$
$$[z^i, x] = [z, x]^i \quad = \quad [z, x^i] \tag{2}$$

(1) holds since $[z, x]$ is central, and (2) follows. From (1) it follows that if S generates a subgroup H of G, and K is any subset of G, then $[K, H] = \langle [K, S]\rangle$. By (2), for any subsets S and T of G, and any $j \in \mathbb{N}$, $\langle [S, T]\rangle^j = \langle S, T^j\rangle$. These facts will be used in what follows without further reference. Now

$$\begin{aligned}
(\gamma_c(G))^{k^c} &= \langle [\gamma_{c-1}(G), g] \mid g \in G\rangle^{k^c} \\
&= \langle [u, x_i] \mid u \in \gamma_{c-1}(G);\ i = 1, \ldots, r\rangle^{k^c} \\
&= \langle [u, x_i]^{k^c} \mid u \in \gamma_{c-1}(G);\ i = 1, \ldots, r\rangle \\
&= \langle [u^{k^{c-1}}, x_i^k] \mid u \in \gamma_{c-1}(G);\ i = 1, \ldots, r\rangle \\
&= \langle [\gamma_{c-1}(G)^{k^{c-1}}, x_i^k] \mid i = 1, \ldots, r\rangle \\
&= \langle [\gamma_{c-1}\langle x_1^k, \ldots, x_r^k\rangle, x_i^k] \mid i = 1, \ldots, r\rangle \qquad \text{by inductive hypothesis} \\
&= \gamma_c\langle x_1^k, \ldots, x_r^k\rangle \qquad .
\end{aligned}$$

□

We are now ready to prove Proposition 1. We have $\gamma_{c+1}(G) = 1$. The case $c = 1$ is trivial; we proceed by induction on c. Consider a typical element

$$g = x^{s^c} \ldots x^{s^c}$$

of G^{s^c}. Put $H = \langle x_1^s, \ldots, x_r^s \rangle$. By Lemma 1,

$$\gamma_c(H) = (\gamma_c\langle x_1, \ldots, x_r\rangle)^{s^c}.$$

Since $g \in H^{s^{c-1}}$, by inductive hypothesis applied to $H/\gamma_c(H)$, there exist $y \in H$, $z \in \gamma_c(H)$ such that $g = y^s z$. However, $\gamma_c\langle x_1, \ldots, x_r\rangle$ is abelian so we can write $z = u^{s^c}$ for some $u \in \gamma_c\langle x_1, \ldots, x_r\rangle$. Thus

$$g = (yu^{s^{c-1}})^s,$$

as required.

6 Proof of Theorem 4

In this section we will state and prove some important technical results needed to prove Theorem 4. The philosophy is that one can 'approximate' a Lie commutator by a group commutator via the Mal'cev correspondence in such a way that the correction terms are either 'longer' group commutators, or 'longer' Lie commutators. As a spin-off, we will show how to construct the 'Mal'cev completion' or 'radicable hull' of a group embedded in $\mathrm{Tr}_1(m, k)$.

Lemma 2 ([Seg83], Chapter 6, Corollary 2) *Let k be a field of characteristic zero. For $x_1, \ldots, x_s \in \mathrm{Tr}_1(m, k)$, we have*

$$\log[x_1, \ldots, x_s] - (\log x_1, \ldots, \log x_s) = \sum_i r_i c_i$$

where each c_i is a repeated Lie bracket of length at least $s+1$ in $\log x_1, \ldots, \log x_s$, each of which appears at least once; and the coefficients r_i are universal constants lying in $\mathbb{Q}$ and are independent of m.

Proof. We first prove this in the case $s = 2$. Let $x_1, x_2 \in \mathrm{Tr}_1(m, k)$ and put $u_i = \log x_i$. Let M be the Lie algebra generated by u_1, u_2 and let L be the subalgebra generated by all commutators in u_1, u_2 of length at least 3. Note that L is in fact an ideal in M. Now we have

$$\begin{aligned} \log[x_1, x_2] &= \log x_1^{-1} * \log x_2^{-1} * \log x_1 * \log x_2 \\ &= (-u_1) * (-u_2) * u_1 * u_2 \\ &= (-u - v + (1/2)(u, v) + w_1) * (u + v + (1/2)(u, v) + w_2) \quad \text{for some } w_1, w_2 \in L \\ &= (u, v) + w_3 \quad \text{for some } w_3 \in L. \end{aligned}$$

Now apply induction: for $x_1, \ldots, x_s \in \mathrm{Tr}_1(m, k)$, let L_s be the Lie algebra generated by commutators of length at least $s+1$ in $\log x_1, \ldots, \log x_s$ in which each of these arguments occurs at least once, and let L_2 be the Lie algebra generated by commutators of length at least 3 in $\log[x_1, \ldots, x_{s-1}]$ and $\log x_s$ in which each occurs at least once. Then by induction we have

$$\begin{aligned} \log[x_1, \ldots, x_s] + L &= \log[[x_1, \ldots, x_{s-1}], x_s] \\ &= (\log[x_1, \ldots, x_{s-1}], \log x_s) + c + L \quad (c \in L_2) \\ &= (\log x_1, \ldots, \log x_s) + c + L \\ &= (\log x_1, \ldots, \log x_s) + L. \end{aligned}$$

It follows that suitable constants r_i exist but may depend on the choice of elements x_i. To see that they are actually independent of this choice, we can start by working over a field k containing some field of fractions of a polynomial ring over an arbitrary field with a large number of variables, and choosing our elements x_i to be matrices with entries involving independent indeterminates. The coefficients r_i obtained will remain valid if we specialize by choosing values for the indeterminates. This effectively allows us to choose any s-tuple of group elements and obtain the same constants, hence these constants are universal. □

Lemma 3 ([Seg83], Chapter 6, Corollary 3) *Let k be a field of characteristic zero. For $x_1, \ldots, x_s \in \mathrm{Tr}_1(m,k)$, we have*

$$(\log x_1, \ldots, \log x_s) = \log[x_1, \ldots, x_s] + \sum_i s_i \log v_i$$

where each v_i is a repeated commutator of length at least $s+1$ in $x_1, \ldots, x_s$, each of which appears at least once; and the coefficients s_i are universal constants lying in $\mathbb{Q}$ which depend on m.

Proof. In the case $s \geq m-1$, this follows trivially from Lemma 2, since Lie commutators of length at least $s+1$ are trivial. The result now follows for all s by reverse induction and application of Lemma 2. Note that the number of steps in this induction depends on $m-s$, so the constants s_i depend on m. □

These two lemmas turn out to be extremely powerful. Before stating our next result, we observe the following:

Corollary 1 *There exists a positive integer r such that for every tuple $\boldsymbol{e}$ of positive integers and $x, y \in \mathrm{Tr}_1(m,\mathbb{Q})$,*

$$q_{\boldsymbol{e}}(\log x, \log y)_{\boldsymbol{e}} \in r^{-1} \sum_{\boldsymbol{f}} \mathbb{Z} \log[x,y]_{\boldsymbol{f}}$$

Proof. Recall that the $q_{\boldsymbol{e}}$ come from the Baker-Campbell-Hausdorff formula (Theorem 3). The fact that such r exists is a direct consequence of Lemma 3 (note that only finitely many vectors $\boldsymbol{e}$ give a non-zero Lie commutator). (For interest's sake, we note here that if $m=3$, so that $\mathrm{Tr}_1(m,\mathbb{Q})$ is of class two, we can take $r=2$.) □

From here on we assume that the positive integer r, which must exist by Corollary 1, has been fixed. Suppose now we are given an arbitrary subgroup G of $\mathrm{Tr}_1(m,\mathbb{Q})$. Let G_j be the subgroup of G consisting of all matrices having $n-j-1$ diagonals above the main diagonal consisting entirely of zeroes. Then in fact $G_j = G \cap \gamma_{m-j}(\mathrm{Tr}_1(m,\mathbb{Q}))$, and it is a standard fact that $G = G_{m-1} \geq \ldots \geq G_0 = 1$ is a central series for G. We have the following result.

Lemma 4 *Let r be as in Corollary 1. Then for each $1 \leq j \leq m-1$, we have*

$$r^{2^{j-1}-1}\mathbb{Z}\log G_j \subseteq \log G_j.$$

Proof. Note that Lemma 4 holds trivially in the case of $j = 1$, since G_1 is abelian. Now assume inductively that it holds for all $j < l$ for some $l \leq m-1$.

Note that for $x \in G_l, x \in G_j$, by construction of r we have

$$\begin{array}{rcl} r(\log xy - \log x - \log y) & = & r((\log x) * (\log y) - \log x - \log y) \\ & = & r(\sum_{q_e} (\log x, \log y)_{\boldsymbol{e}}) \\ & \in & \sum_{\boldsymbol{f}} \mathbb{Z}\log[x,y]_{\boldsymbol{f}} \end{array}$$

since $[x, y] \in G_{j-1}$. Moreover, for $g_1, \ldots, g_{s-1} \in G_l$, $g_s \in G_j$, it follows easily that

$$r(\log g_1 + \cdots + g_s) \in r\log(g_1 \ldots g_s) + \mathbb{Z}G_{j-1}. \tag{3}$$

We now have the following:

Lemma 5 *For each $2 \leq j < l$, we have that for all $x \in G_l$, $g_1, \ldots, g_s \in G_j$, there exists $y \in G_l$ such that*

$$r^{2^{j-1}}(\log x + (\log g_1 + \cdots + \log g_s)) \in \log y + \mathbb{Z}\log G_{j-1}. \tag{4}$$

Proof. We have

$$\begin{array}{rcll} r^{2^{j-1}}(\log x_1 + (\log g_1 + \ldots + \log g_s)) & = & r(\log x^{r^{2^{j-1}-1}} + \log h) & (h \in G_j) \\ & \in & \log(x^{r^{2^{j-1}-1}}h) + \mathbb{Z}\log G_{j-1}, & \end{array}$$

□

It remains to put everything together to complete the inductive step: for $g_1, \ldots, g_s \in G_l$ and writing $w := g_1 \ldots g_s$, we have

$$\begin{array}{rcll} r^{2^{l-1}-1}(\log g_1 + \cdots + \log g_s) & = & r^{2^{l-1}-2}(\log w^r + u_{l-1}) & \text{by (3))} \\ & = & r^{2^{l-1}-2-2^{l-2}-2^{l-3}-\cdots-2^1}(\log z + u_1) & \text{by repeated application of 4} \\ & = & \log z + u_1 & , \end{array}$$

where $u_{l-1} \in \mathbb{Z}\log G_{l-1}, u_1 \in \mathbb{Z}\log G_1, z \in G_l$. Since G_1 is abelian, we may write $u_1 = \log h$ where $h \in \log G_1$. Since G_1 is central, we have $(\log z + u_1) = \log zh \in G_l$, and we are done.
□

We now set a new constant.

Definition 1 *Put $t = r^{2^{m-2}}$.*

The following builds on Lemma 4:

Lemma 6 *Let $K \lhd G \leq \mathrm{Tr}_1(m, \mathbb{Q})$. Taking t as in Definition 1, we have for all $g \in G$ and $k \in K$ that*

$$\log g + t \log k \quad \in \log K\langle g\rangle \tag{5}$$

$$t \log g + \log k \quad \in \log K\langle g^t\rangle. \tag{6}$$

$$\tag{7}$$

Proof. We establish by induction that if $K \leq G_i$ then, replacing t by $r^{2^{i-1}}$, both (5) and (6) hold. If $K \leq G_1$ then K is central and $r^{2^{i-1}} = r$, giving $\log g + r \log k = \log gk^r$, $r \log g + \log k = \log g^r k$, as required. Suppose that the two equations have been established for all $i < j$ for some $j < m - 1$. Suppose that $K \leq G_j$ and put $H = [K, G]$. Since (G_i) is a central series, $H \leq G_{j-1}$; since $K \lhd G$, also $H \lhd G$. Write $t_j := r^{2^{j-1}}$. We have

$$\begin{array}{rcl} \log g + t_j \log k - \log gk^{t_j} & = & -\sum q_{\boldsymbol{e}}(\log g, t_j \log k)_{\boldsymbol{e}} \quad \text{by Theorem 3} \\ & \in & t_0 r^{-1} \sum \mathbb{Z} \log[g, k]_{\boldsymbol{f}} \end{array}$$

by Corollary 1 and since in each repeated commutator we can take out factors of t_0 at least once. Now $[g, k]_{\boldsymbol{f}} \in H$ for all f by definition of H. Thus

$$\log g + t_j \log k - \log gk^{t_j} \in r^{2^{j-1}-1} \mathbb{Z} \log H.$$

By Lemma 4 we have

$$r^{2^{j-2}-1} \mathbb{Z} \log H \subseteq \log H$$

so for some $h \in H$ we have

$$\begin{array}{rcl} \log g + t_j \log k & = & \log gk^{t_j} + r^{2^{j-2}} \log h \\ & \in & \log H\langle gk^{t_j}\rangle \end{array}$$

by the inductive hypothesis, since $H \leq G_{j-1}$. But $\log H\langle gk^{t_j}\rangle \leq \log K\langle g\rangle$, proving 5. Now arguing as before we have

$$\begin{array}{rcl} t_j \log g + \log k - \log g^{t_j} k & = & -\sum q_{\boldsymbol{e}}(t_j \log g, \log k)_{\boldsymbol{e}} \\ & \in & t_0 r^{-1} \sum \mathbb{Z} \log[g, k]_{\boldsymbol{f}}, \end{array}$$

hence

$$t_j \log g + \log k - \log g^{t_j} k \in r^{2^{j-1}-1} \mathbb{Z} \log H \subseteq r^{2^{j-2}} \log H.$$

Thus, for some $h \in H$ we have

$$\begin{array}{rcl} t_j \log g + \log k & = & \log g^{t_j} k + r^{2^{j-2}} \log h \\ & \in & \log H\langle g^{t_j} k\rangle, \end{array}$$

using again the inductive hypothesis for (5). But $\log H\langle g^{t_j} k\rangle \subseteq \log K\langle g^{t_j}\rangle$, proving (6). □

Now finally we can establish Theorem 4. Pick t as in Definition 1. Let $x, y \in H.$ Then by construction, there exists $g \in H^{1/t}$ such that $x = g^t$. Since $H \lhd H^{1/t}$ we have by Lemma 6 that

$$\begin{array}{rcl} \log x + \log y & = & t \log g + \log y \\ & \in & \log(H\langle g^t \rangle) \\ & = & \log H \end{array}$$

hence H is a lattice group. To complete the proof of Theorem 4 it remains to show that H is closed under the Lie operation. Given $x_1, x_2 \in H$, there exists $g \in H^{1/t}$ such that $x_1 = g^t$ (similarly for x_2, but we shall not need this). By Lemma 3 we have

$$(\log x_1, \log x_2) = t(\log g, \log x_2) = t \log[g, x_2] + t \sum_i s_i \log v_i$$

where the v_i are group commutators of length at least 3 involving both g and x_2. Now $r|t$, and by construction, r is a common denominator for the s_i (cf. Corollary 1 with $\boldsymbol{e} = (1)$ so that $q_{\boldsymbol{e}} = 1/2$). Furthermore, by assumption $H \lhd H^{1/t}$ hence each group commutator lies in H. Thus $(\log x_1, \log x_2) \in \mathbb{Z} \log H = \log H$.

7 A diversion: the radicable hull

8 Proof of Theorem 2

Actually we will not prove all the parts of Theorem 2. For a treatment of 'proisomorphic' subgroup counting $\zeta^{\wedge}_{G,p}$, we refer the interested reader to [GSS88] and [Seg83]. We start by tackling objective 2 mentioned in Section 3. This proceeds in a number of steps. The basic idea is fix an LR group and to show that for almost all primes p the log map gives an index-preserving correspondence between the subgroups of p-power index and the subrings of its image. We assume throughout that all groups are contained in $\mathrm{Tr}_1(m, \mathbb{Q})$, unless otherwise specified.

Lemma 7 *Let t be as in Definition 1. If t_0 is a non-zero multiple of t and H satisfies $H \lhd H^{1/t_0}$ then H is an LR group.*

Proof. $H^{1/t} \leq H^{1/t_0}$, hence $H \lhd H^{1/t}$, and the result follows from Theorem 4. □

Lemma 8 *For any $H \leq \mathrm{Tr}_1(m, \mathbb{Q})$ and $j \in \mathbb{N}$, we have $|H^{1/j} : H| < \infty$, $|H : H^j| < \infty$ and both $|H^{1/j} : H|$ and $|H : H^j|$ divide some power of j.*

Proof. The proof of this innocent-looking fact is too much of a diversion to present at this point. We will defer it to the end of this section. □

Lemma 9 *If $H \leq K$, K is an LR group and $(|K : H|, t) = 1$ then H is an LR group.*

Proof. The idea is to construct another LR group lying above H of index relatively prime to $|K : H|$, and then take its intersection with K. Put $t_0 = t^{m-1}$, $H_1 = H^{1/t_0}$, $H_2 = H_1^{t_0}$. Then $H \leq H_2 \leq H_1$. By Proposition 1, $H_2^{1/t} \leq H_1$ since H_1 is of class at most $m-1$. Now $H_2 \lhd H_1$ by construction, hence $H_2 \lhd H_2^{1/t}$. By Theorem 4, H_2 is an LR group. Now $|H_2 : H|$ divides some power of t, by Lemma 8, hence $|K \cap H_2 : H|$ divides 1 by Lagrange's Theorem, i.e. $K \cap H_2 = 1$. Thus $\log H = \log H_2 \cap \log K$ and $\log H$ is an LR group. □

Definition 2 *Let d_1 be a common denominator for the coefficients in the Baker-Campbell-Hausdorff formula (Theorem 3) of length at most $m-1$.*

Lemma 10 *Let K be an LR group and put $L = \log K$. If M is a Lie subring of L and $(|L : M|, td_1) = 1$ then $\exp M$ is a subgroup of K.*

Proof. Given $\lambda, \mu \in M$ let $x = \exp \lambda$ and $y = \exp \mu$. Then $xy \in K$ so $\log(xy) \in L$. Now $\log(xy) = \lambda * \mu$ so by the BCH formula and by the choice of d_1, $d_1 \log(xy)$ lies in M. Since $|L : M| \log(xy) \in M$ too, we have $\log(xy) \in M$, as required. □

By Lemma 2 and Lemma 3 there exist constants r_i, s_i depending only on m such that for all $x, y \in \mathrm{Tr}_1(m, \mathbb{Q})$

$$\log[x, y] - (\log x, \log y) = \sum_i r_i c_i = -\sum_i s_i \log v_i$$

where each c_i is a repeated Lie bracket of length at least 3 in $\log x$, $\log y$ and each v_i is a repeated group commutator in x and y.

Definition 3 *Let d_2 be a common denominator for all the (finitely many) coefficients r_i, s_i of non-zero terms in the above expressions.*

Lemma 11 *Let $H \leq K$ where K is an LR group and $(|K : H|, td_1 d_2) = 1$. Then $H \lhd K \iff \log H \lhd \log K$ (i.e. an ideal of $\log K$).*

Proof. Put $q = |K : H|$. Note that by Lemma 9, H is an LR group. Assume that $H \lhd K$. Let $h \in H$, $g \in K$. Then $g^q \in H$ so we have

$$q(\log h, \log g) = (\log h, \log g^q) \in \log H$$

since H is an LR group. Also

$$d_2(\log h, \log g) = d_2 \log[h, g] + \sum d_2 s_i \log v_i$$

as in Lemma 3. Since the v_i are group commutators in g and h, they are all contained in H. Further, by construction (Definition 3) $d_2 s_i \in \mathbb{Z}$ for each i. Since $\log H$ is a Lie ring, we conclude that $d_2(\log h, \log g) \in \log H$. But $(d_2, q) = 1$ so $(\log h, \log g) \in \log H$ and $\log H \lhd \log K$.

To prove the other direction, assume that $\log H \lhd \log K$. Using the definition of q above, we have

$$q \log[h, g] = \log([h, g])^q \in \log H.$$

Also,

$$d_2 \log[h, g] = d_2(\log h, \log g) + \sum_i d_2 r_i c_i \in \mathbb{Z} \log H = \log H.$$

As before, $(d_2, q) = 1$ so $\log[h, g] \in \log H$ and $H \lhd K$. For an alternative argument for this second part, see [Seg83], Chapter 6, Lemma 4.7. □

Lemma 12 *Let $H \leq K$, where K is an LR group, let p be a prime not dividing td_1d_2 and m a positive integer. Then $|K : H| = p^m$ if and only if $|\log K : \log H| = p^m$.*

Proof. Note that H is an LR group, by Lemma 9. Suppose that $|K : H| = p^m$. We may in fact assume that $m = 1$. For suppose that $m > 1$. If we can show that there exists at group J such that $H < J < K$ then $(|K : J|, t)$ so J is an LR group; furthermore, $|K : J|$ and $|J : H|$ are powers of p strictly less than p^m, and we can reduce to the case $m = 1$ by induction. To see that such a group J exists, let T be the normal closure of H (cf. Section 9). By factoring out by T, we can assume that K is finite. Then K is a direct product of its Sylow subgroups (see again Section 9); say $K = \prod_q S_q$. Put $R = \prod_{q \neq p} S_q$. Since $|K : H|$ is a p-power, $R \leq H$. Therefore we can factor out by R and assume that K is a p-group. We now argue by induction on the size of K that a suitable subgroup J exists lying strictly between H and K (the base case $K = p$ holds vacuously). The centre of K is non-trivial. If it is contained in H, we can factor it out and apply the inductive hypothesis. If not, then we can find an element x of the centre which is not contained in H. If $\langle H, x \rangle \neq K$ then we are done. If $\langle H, x \rangle = K$, write $|K : H| = p^a$ and observe that $\langle H, x^{p^{a-1}} \rangle$ is a subgroup of K of index p.

We now consider the case $m = 1$. Note that in fact $H \lhd K$: as in the above argument, we can factor out by the normal core of H and assume that K is finite. Now the normalizer of H in K is larger than H (cf. Section 9), hence it must be K. Let g be an element of $k \backslash H$ so that $K = H\langle g \rangle$. Define d_1 as in Definition 2. We claim that

$$\log K = \bigcup_{i=0}^{p-1} (\log H + id_1 \log g).$$

To see this, note that

$$\begin{array}{rcll} \log(Hg^{id_1}) & = & \{\log(hg^{id_1}) \mid h \in H\} & \\ & = & \{\log h + \log g^{id_1} + \sum_e q_e(\log h, \log g^{id_1})_e\} & \\ & \subseteq & \log H + \log g^{id_1} & (\log H \lhd \log K;\ d_1 q_e \in \mathbb{Z}) \\ & = & \log H + id_1 \log g, & \end{array}$$

hence

$$\log K = \bigcup_{i=0}^{p-1} \log(Hg^{id_1}) \subseteq \bigcup_{i=0}^{p-1} (\log H + id_1 \log g)$$

(here we use the fact that $(d_1, p) = 1$). It follows that $|\log K : \log H| \leq p$, but evidently $|\log K : \log H| \neq 1$ (since $g^{id_1} \notin H$ for all $i = 1, \ldots, p-1$). Thus $|\log K : \log H| = p$, as required.

Finally, we need to prove the reverse implication. Assume then that $|\log K : \log H| = p^m$. Write $|K : H| = a = p_1^{k_1} \ldots p_l^{k_l}$ with each $k_i > 0$. Let T be the normal core of H (cf. Section 9). Then K/T is a finite nilpotent group and we may write K/T as a direct product $\prod_q \overline{S_q}$, where $\overline{S_q}$ is the Sylow-q subgroup of K/T. Write S_q for the preimage of $\overline{S_q}$ under the quotient map $K \to K/T$. Set $H_1 = HS_{p_1}$. Then $|H_1 : H| = p_1^{k_1}$ and by the first part of the proof, $|\log H_1 : \log H| = p_1^{k_1}$. Hence $p = p_1$. Considering now $H_1 \leq K$ and repeating, we eventually get that $p_1 = \cdots = p_l = p$. Thus $|K : H|$ is a p-power and by the first part again, $\sum_{i=1}^{l} k_i = m$, as required. □

To complete the proof of Theorem 2 (excluding $\zeta^{\wedge}_{G,p}$), we require the following.

Lemma 13 *Let $K \leq G$ be $\mathscr{T}$-groups with $|G : K|$ finite and let p be a prime not dividing $|G : K|$. For each subgroup H of G, put $H_1 = K \cap H$. Then $H \mapsto H_1$ gives an index-preserving bijection between the (normal) subgroups of G of p-power index and the (normal) subgroups of K of p-power index.*

Proof. We first show that the map is index preserving. Let H be a subgroup of G of index p^m, for some $m \in \mathbb{N}$. Then

□

9 Finite nilpotent groups

Bibliography

[GSS88] F.J. Grunewald, D. Segal, and G.C. Smith, *Subgroups of finite index in nilpotent groups*, Invent. Math. **93** (1988), 185–223.

[Seg83] D. Segal, *Polycyclic groups*, Cambridge University Press, 1983.