Journal of the Iranian Mathematical Society
ISSN (on-line): 2717-1612
J. Iranian Math. Soc. 1 (2020), no. 2, 129-143

UNDERSTANDING WALL'S THEOREM ON DEPENDENCE OF LIE RELATORS IN BURNSIDE GROUPS

M. VAUGHAN-LEE

Abstract. G.E. Wall [*J. Algebra* 104 (1986), no. 1, 1–22; Lecture Notes in Mathematics, pp. 191–197, 1456, Springer-Verlag, Berlin, 1990] gave two different proofs of a remarkable result about the multilinear Lie relators satisfied by groups of prime power exponent q. He showed that if q is a power of the prime p, and if f is a multilinear Lie relator in n variables where $n \neq 1 \bmod (p-1)$, then $f = 0$ is a consequence of multilinear Lie relators in fewer than n variables. For years I have struggled to understand his proofs, and while I still have not the slightest clue about his proof in [*J. Algebra* 104 (1986), no. 1, 1–22], I finally have some understanding of his proof in [Lecture Notes in Mathematics, pp. 191–197, 1456, Springer-Verlag, Berlin, 1990]. In this note I offer my insights into Wall's second proof of this theorem.

1. Introduction

This note is concerned with the multilinear Lie relators which hold in the associated Lie rings of groups of prime-power exponent. I refer the reader to Chapter 2 of my book [5] for the definition of the associated Lie ring of a group, and the definition of a Lie relator (or Lie identity). In that chapter, for every prime power $q = p^k$ I explicitly construct a sequence of Lie elements K_n $(n = 1, 2, \ldots)$ where K_n is multilinear in $x_1, x_2, \ldots, x_n$. (We can think of K_n as an element of the free Lie ring on generators $x_1, x_2, \ldots, x_n$. It is a linear combination of Lie products $[y_1, y_2, \ldots, y_n]$ where $y_1, y_2, \ldots y_n$ is a permutation of $x_1, x_2, \ldots, x_n$. The element K_1 equals qx_1.) I prove that the associated Lie ring of any group of exponent q satisfies the identity $K_n = 0$ for all n. I also prove that if $f = 0$ is a multilinear identity which holds in the associated Lie ring of every group of exponent q, then $f = 0$ is a consequence of the identities $K_n = 0$ $(n = 1, 2, \ldots)$.

Communicated by Alireza Abdollahi

MSC(2020): Primary: 20F50; Secondary: 17B60.

Keywords: Lie relators; Burnside groups; Wall's theorem.

Received: 25 March 2020, Accepted: 17 May 2020.

DOI: http://dx.doi.org/10.30504/jims.2020.107524

.

G.E. Wall [7,8] gave two proofs of the following remarkable theorem which shows that in some sense most of the identities $K_n = 0$ are redundant.

Theorem 1.1. *If* $n \neq 1 \bmod (p-1)$ *then the identity* $K_n = 0$ *is a consequence of the identities* $K_m = 0$ *for* $m < n$.

This result ties in with (but vastly extends) previously known results about groups of exponent p. It has been known for many years that the associated Lie rings of groups of exponent p have characteristic p and satisfy the $(p-1)$-Engel identity. These identities have helped enormously in the study of finite groups of exponent p. The identity $px = 0$ is the identity $K_1 = 0$ (in exponent p), and the $(p-1)$-Engel identity is equivalent to $K_p = 0$ in characteristic p. Magnus [3] proved that all Lie identities of weight at most $p-1$ that hold in the associated Lie rings of groups of exponent p are consequences of the identity $px = 0$, and Sanov [4] extended this result to show that all Lie identities of weight at most $2p-2$ are consequences of the identity $px = 0$ and the $(p-1)$-Engel identity. On the other hand, Wall [6] found a multilinear identity of weight $2p-1$ which holds in the associated Lie rings of groups of exponent p, and he showed that for $p = 5, 7, 11$ this identity is not a consequence of the $(p-1)$-Engel identity in characteristic p. Havas and Vaughan-Lee [2] extended this result to the primes $13, 17, 19$. (It follows that $K_{2p-1} = 0$ is *not* a consequence of the identities $\{K_n = 0 \,|\, n < 2p-1\}$ for $p = 5, 7, 11, 13, 17, 19$.)

Most of Wall's proof in [8] involves calculations in the free associative algebra with unity over the rationals $\mathbb{Q}$, with free generators $x_1, x_2, \ldots$. Wall calls this algebra A, and turns A into a Lie algebra over $\mathbb{Q}$ by setting $[a,b] = ab - ba$. He lets L be the Lie subalgebra of A generated by $x_1, x_2, \ldots$. It is well known that L is a free Lie algebra, freely generated by $x_1, x_2, \ldots$. For a proof of this fact see [5, Corollary 1.4.2]. Wall then lets R be the set of all linear mappings $\theta : A \to A$ which commute with all algebra endomorphisms $\varepsilon : A \to A$ such that $\varepsilon(L) \subseteq L$. Wall implicitly assumes a number of properties of R, and states other important properties without proof. No doubt these properties are straightforward enough (even elementary) for those who are familiar with R, and in fact their proofs are not hard. But I had never come across R before, and I could not begin to understand Wall's proof of Theorem 1.1 until I had found my own proofs of these properties. So in the section below I develop the properties of R which Wall needs. I give the definitions of the relators K_n $(n = 1, 2, \ldots)$ in Section 3, and establish some of their properties. Then in the final section I give his proof of Theorem 1.1. The proof itself is quite short, but it takes quite a lot of work in Section 2 and Section 3 to set up the machinery needed.

We end the introduction stating and proving a standard result about products of the free generators of A. The proof is easy enough, but we use the result below (several times) and so it is convenient to state it as a lemma.

Lemma 1.2. *Let* $W_r \subset A$ *be the set of all sums* $\sum_j m_j$ *where the summands* m_j *are products*

$$y_1 y_2 \cdots y_{i-1} [y_i, y_{i+1}] y_{i+2} \cdots y_r$$

DOI: http://dx.doi.org/10.30504/jims.2020.107524

where $1 \leq i < r$ and where $y_1, y_2, \ldots, y_r$ is a permutation of $x_1, x_2, \ldots, x_r$. Let π be a permutation in the symmetric group S_r. Then $x_{\pi 1} x_{\pi 2} \ldots x_{\pi r} = x_1 x_2 \ldots x_r + w$ for some $w \in W_r$.

Proof. We apply a "bubble sort" to the product $x_{\pi 1} x_{\pi 2} \ldots x_{\pi r}$. If $\pi = 1_{S_r}$ then there is nothing to prove. If $\pi \neq 1_{S_r}$, look for the first integer i such that $\pi i > \pi(i+1)$. Then

$$\begin{aligned} & x_{\pi 1} \ldots x_{\pi i} x_{\pi(i+1)} \ldots x_{\pi r} \\ & = x_{\pi 1} \ldots x_{\pi(i+1)} x_{\pi i} \ldots x_{\pi r} + x_{\pi 1} \ldots [x_{\pi i}, x_{\pi(i+1)}] \ldots x_{\pi r} \\ & = x_{\pi 1} \ldots x_{\pi(i+1)} x_{\pi i} \ldots x_{\pi r} + w \text{ with } w \in W_r. \end{aligned}$$

We replace $x_{\pi 1} \ldots x_{\pi i} x_{\pi(i+1)} \ldots x_{\pi r}$ by $x_{\pi 1} \ldots x_{\pi(i+1)} x_{\pi i} \ldots x_{\pi r}$, and iterate. After a number of iterations we obtain $x_1 x_2 \ldots x_r$. □

2. The algebra R

As mentioned above, Wall defines R to be the set of all linear mappings $\theta : A \to A$ which commute with all algebra endomorphisms $\varepsilon : A \to A$ such that $\varepsilon(L) \subseteq L$. It is clear from the definition of R that it is closed under addition, scalar multiplication, and composition of mappings. So R is an algebra over $\mathbb{Q}$.

Lemma 2.1. *If $\theta \in R$ then $\theta(1) \in \mathbb{Q}$, and if $r > 0$, then*

$$\theta(x_1 x_2 \ldots x_r) = \sum_{\pi \in S_r} a_\pi x_{\pi 1} x_{\pi 2} \ldots x_{\pi r}$$

for some $a_\pi \in \mathbb{Q}$.

Proof. First consider $\theta(1)$. If we let ε be the endomorphism of A mapping x_i to 0 for all i, then the fact that $\varepsilon\theta = \theta\varepsilon$ implies that $\theta(1) \in \mathbb{Q}$.

Next consider $\theta(x_1)$. If we let ε be the endomorphism of A mapping x_1 to x_1 and mapping all other free generators of A to zero, then the fact that $\varepsilon\theta = \theta\varepsilon$ implies that $\theta(x_1)$ is a polynomial in x_1. Let $\theta(x_1) = f(x_1)$ where f is a polynomial. If $k \in \mathbb{Q}$, then θ commutes with the endomorphism of A mapping x_1 to kx_1 and mapping x_i to x_i for $i > 1$. So $\theta(kx_1) = f(kx_1)$. But θ is linear, and so $\theta(kx_1) = kf(x_1)$ This implies that $f(x_1) = ax_1$ for some $a \in \mathbb{Q}$.

Similar considerations imply that $\theta(x_1 x_2 \ldots x_r)$ lies in the subalgebra of A generated by $x_1, x_2, \ldots, x_r$, and by considering endomorphisms of A mapping x_i to $k_i x_i$ for $i = 1, 2, \ldots, r$ ($k_i \in \mathbb{Q}$) we see that either $\theta(x_1 x_2 \ldots x_r) = 0$, or $\theta(x_1 x_2 \ldots x_r)$ is homogeneous of degree 1 in each of $x_1, x_2, \ldots, x_r$. □

Note that the fact that θ commutes with all L preserving endomorphisms of A implies that if

$$\theta(x_1 x_2 \ldots x_r) = \sum_{\pi \in S_r} \alpha_\pi x_{\pi 1} x_{\pi 2} \ldots x_{\pi r}$$

then

$$\theta(y_1 y_2 \ldots y_r) = \sum_{\pi \in S_r} \alpha_\pi y_{\pi 1} y_{\pi 2} \ldots y_{\pi r}$$

DOI: http://dx.doi.org/10.30504/jims.2020.107524

for all $y_1, y_2, \ldots, y_r \in L$. So the values of $\theta(x_1x_2\ldots x_r)$ for $r = 0, 1, 2, \ldots$ determine θ. We let $\sigma_0(\theta) = \theta(1)$, and if

$$\theta(x_1x_2\ldots x_r) = \sum_{\pi\in S_r} \alpha_\pi x_{\pi1}x_{\pi2}\ldots x_{\pi r}$$

then we let $\sigma_r(\theta) = \sum_{\pi\in S_r} \alpha_\pi \pi^{-1}$ in the group ring $\mathbb{Q}S_r$. So θ is determined by the sequence $(\sigma_0(\theta), \sigma_1(\theta), \ldots)$. It is straightforward to show that if $\theta, \varphi \in R$, and if we define $\theta \circ \varphi$ by setting

$$(\theta \circ \varphi)(x_1x_2\ldots x_r) = (\theta(\varphi(x_1x_2\ldots x_r))$$

then $\sigma_r(\theta \circ \varphi) = \sigma_r(\theta)\sigma_r(\varphi)$ for $r = 0, 1, 2, \ldots$.

Now let x be an indeterminate and let $\mathbb{Q}[[x]]$ be the power series ring in x over $\mathbb{Q}$. If $w \in \mathbb{Q}[[x]]$ then we define the linear transformation $\psi_w : A \to A$ as follows. First we set $\psi_w(1) = w(0)$. Next, for $r > 0$ we let $\psi_w(x_1x_2\ldots x_r)$ be the $\{x_1, x_2, \ldots, x_r\}$-multilinear component of

$$w((1 + x_1)(1 + x_2)\ldots(1 + x_r) - 1).$$

Let $y_1, y_2, \ldots, y_r$ be any sequence of the free generators of A (possibly with repetitions). Then if

$$\psi_w(x_1x_2\ldots x_r) = \sum_{\pi\in S_r} \alpha_\pi x_{\pi1}x_{\pi2}\ldots x_{\pi r}$$

we set

$$\psi_w(y_1y_2\ldots y_r) = \sum_{\pi\in S_r} \alpha_\pi y_{\pi1}y_{\pi2}\ldots y_{\pi r}.$$

Note that if $n > r$ then $((1+x_1)(1+x_2)\ldots(1+x_r)-1)^n$ has no terms of degree r, so that $\psi_w(x_1x_2\ldots x_r)$ is well defined. In fact, if $w = \sum_{n=0}^{\infty} \beta_n x^n$ then

$$\psi_w(x_1x_2\ldots x_r) = \psi_{w'}(x_1x_2\ldots x_r)$$

where $w' = \sum_{n=0}^{r} \beta_n x^n$. So $\psi_w : A \to A$ is a well defined linear transformation. (There is no problem over convergence, since if $a \in A$ has degree r then $\psi_w(a) = \psi_{w'}(a)$.) In addition, it is clear that if we let V be the $\mathbb{Q}$-linear span of $x_1, x_2, \ldots$, then ψ_w commutes with any endomorphism $\varepsilon : A \to A$ such that $\varepsilon(V) \subseteq V$.

Lemma 2.2. *If $w \in \mathbb{Q}[[x]]$ then $\psi_w \in R$.*

Proof. By linearity, it is sufficient to show that $\psi_{x^m} \in R$ for $m = 1, 2, \ldots$. To this end we introduce some notation to enable us to describe the form of $\psi_{x^m}(x_1x_2\ldots x_r)$. If $S = \{i_1, i_2, \ldots, i_k\}$ is a subset of $\{1, 2, \ldots, r\}$ with $i_1 < i_2 < \ldots < i_k$ then we define $x_S = x_{i_1}x_{i_2}\ldots x_{i_k}$. So

$$\psi_{x^m}(x_1x_2\ldots x_r) = \sum x_{S_1}x_{S_2}\ldots x_{S_m}$$

where the summation is taken over all partitions of $\{1, 2, \ldots, r\}$ into an ordered sequence of disjoint non-empty subsets $S_1, S_2, \ldots, S_m$. Each partition of $\{1, 2, \ldots, r\}$ into m disjoint non-empty subsets yields $m!$ ordered sequences $S_1, S_2, \ldots, S_m$. If $y_1, y_2, \ldots, y_r \in A$ we let $U_r(y_1, y_2, \ldots, y_r)$ be the image of $\psi_{x^m}(x_1x_2\ldots x_r)$ under an endomorphism of A mapping x_i to y_i for $i = 1, 2, \ldots, r$. We need to show that if $y_1, y_2, \ldots, y_r \in L$ then $\psi_{x^m}(y_1y_2\ldots y_r) = U_r(y_1, y_2, \ldots, y_r)$, and by linearity it is sufficient

DOI: http://dx.doi.org/10.30504/jims.2020.107524

to establish this in the case when the y_i are Lie products of the form $[x_{j_1}, x_{j_2}, \ldots, x_{j_k}]$. The key to proving this is to show that if $1 \leq i \leq r$ then

$$\begin{aligned}&U_{r+1}(x_1, \ldots, x_i, x_{i+1}, \ldots, x_{r+1}) - U_{r+1}(x_1, \ldots, x_{i+1}, x_i, \ldots, x_{r+1})\\&= U_r(x_1, \ldots, [x_i, x_{i+1}], \ldots, x_{r+1}).\end{aligned}$$

To see this write

$$U_{r+1}(x_1, \ldots, x_i, x_{i+1}, \ldots, x_{r+1}) = \sum x_{S_1} x_{S_2} \ldots x_{S_m},$$

where now the sum is over all partitions of $\{1, 2, \ldots, r, r+1\}$ into an ordered sequence of disjoint non-empty subsets $S_1, S_2, \ldots, S_m$. Decompose the sum

$$\sum x_{S_1} x_{S_2} \ldots x_{S_m}$$

into $B + C$, where B is the sum of all $x_{S_1} x_{S_2} \ldots x_{S_m}$ where i and $i+1$ lie in different subsets, and where C is the sum of all $x_{S_1} x_{S_2} \ldots x_{S_m}$ where i and $i+1$ lie in the same subset. Note that

$$C = U_r(x_1, \ldots, x_i x_{i+1}, \ldots, x_{r+1}).$$

Interchanging x_i and x_{i+1} leaves B unchanged (although it permutes the summands) and maps C to $U_r(x_1, \ldots, x_{i+1} x_i, \ldots, x_{r+1})$. So

$$\begin{aligned}&U_{r+1}(x_1, \ldots, x_i, x_{i+1}, \ldots, x_{r+1}) - U_{r+1}(x_1, \ldots, x_{i+1}, x_i, \ldots, x_{r+1})\\&= U_r(x_1, \ldots, x_i x_{i+1}, \ldots, x_{r+1}) - U_r(x_1, \ldots, x_{i+1} x_i, \ldots, x_{r+1})\\&= U_r(x_1, \ldots, [x_i, x_{i+1}], \ldots, x_{r+1})\end{aligned}$$

as claimed.

Now consider $\psi_{x^m}(y_1 y_2 \ldots y_r)$ where the y_i are Lie products of the free generators of L. We need to prove that $\psi_{x^m}(y_1 y_2 \ldots y_r) = U_r(y_1, y_2, \ldots, y_r)$, and we do this by induction on $\sum_{i=1}^r \deg(y_i) - r$. If $\sum_{i=1}^r \deg(y_i) - r = 0$, then all the y_i have weight 1 and there is nothing to prove. So suppose that $1 \leq i \leq r$ and that $y_i = [z, t]$ for some $z, t \in L$. Then

$$\begin{aligned}&\psi_{x^m}(y_1 y_2 \ldots y_r)\\&= \psi_{x^m}(y_1 \ldots [z, t] \ldots y_r)\\&= \psi_{x^m}(y_1 \ldots zt \ldots y_r) - \psi_{x^m}(y_1 \ldots tz \ldots y_r)\end{aligned}$$

and

$$\begin{aligned}&U_r(y_1, y_2, \ldots, y_r)\\&= U_r(y_1, \ldots, [z, t], \ldots, y_r)\\&= U_{r+1}(y_1, \ldots, z, t, \ldots, y_r) - U_{r+1}(y_1, \ldots, t, z, \ldots, y_r).\end{aligned}$$

So it is sufficient to show that

$$\psi_{x^m}(y_1 \ldots zt \ldots y_r) = U_{r+1}(y_1, \ldots, z, t, \ldots, y_r)$$

DOI: http://dx.doi.org/10.30504/jims.2020.107524

and that

$$\psi_{x^m}(y_1 \dots tz \dots y_r) = U_{r+1}(y_1, \dots, t, z, \dots, y_r)$$

and this follows by induction. □

Lemma 2.3. *If $\psi \in R$ then $\psi = \psi_w$ for some unique $w \in \mathbb{Q}[[x]]$.*

Proof. Let $\psi \in R$ and let $\psi(1) = \alpha_0$, $\psi(x_1) = \alpha_1 x_1$ with $\alpha_0, \alpha_1 \in \mathbb{Q}$. Let $\varphi = \psi - \alpha_0\psi_1 - \alpha_1\psi_x$. Then $\varphi(1) = \varphi(x_1) = 0$. Let $\varphi(x_1x_2) = \alpha x_1x_2 + \beta x_2x_1$. Since $\varphi \in R$ it follows that $\varphi([x_1, x_2]) = 0$ so that $\varphi(x_1x_2) = \varphi(x_2x_1)$. Hence $\alpha = \beta$. Let $\alpha_2 = \alpha$, and let $\varphi_2 = \psi - \alpha_0\psi_1 - \alpha_1\psi_x - \alpha_2\psi_{x^2}$. Then $\sigma_0(\varphi_2) = \sigma_1(\varphi_2) = \sigma_2(\varphi_2) = 0$. Suppose by induction that for some $n > 2$ we have found $\alpha_0, \alpha_1, \dots, \alpha_{n-1} \in \mathbb{Q}$ such that

$$\varphi_{n-1} = \psi - \alpha_0\psi_1 - \alpha_1\psi_x - \dots - \alpha_{n-1}\psi_{x^{n-1}}$$

has the property that $\sigma_i(\varphi_{n-1}) = 0$ for $i = 0, 1, \dots, n-1$. Then $\varphi_{n-1}(y_1y_2\dots y_m) = 0$ whenever $m < n$ and $y_1, y_2, \dots, y_m \in L$. It follows from Lemma 1.2 that

$$\varphi_{n-1}(x_{\pi 1}x_{\pi 2}\dots x_{\pi n}) = \varphi_{n-1}(x_1x_2\dots x_n)$$

for all permutation $\pi \in S_n$. So $\sigma_n(\varphi_{n-1}) = \alpha_n \sum_{\pi \in S_n} \pi$ for some $\alpha_n \in \mathbb{Q}$, and

$$\varphi_n = \varphi = \psi - \alpha_0\psi_1 - \alpha_1\psi_x - \dots - \alpha_{n-1}\psi_{x^{n-1}} - \alpha_n\psi_{x^n}$$

has the property that $\sigma_i(\varphi_n) = 0$ for $i = 0, 1, \dots, n$. Continuing in this way we obtain a sequence of rationals $\alpha_0, \alpha_1, \dots$ such that $\psi = \psi_w$ where

$$w = \sum_{i=0}^{\infty} \alpha_i x^i.$$

□

Lemma 2.4. *Let $X = x + 1$. Then $\psi_{X^m} \circ \psi_{X^n} = \psi_{X^{mn}}$ for all $m, n \geq 0$.*

Proof. It is easy to see that $\sigma_0(\psi_{X^m}) = 1$ and $\sigma_1(\psi_{X^m}) = m1_{S_1}$ for all m. So $\sigma_i(\psi_{X^m} \circ \psi_{X^n}) = \sigma_i(\psi_{X^{mn}})$ for $i = 0, 1$. Suppose by induction that we have shown that $\sigma_i(\psi_{X^m} \circ \psi_{X^n}) = \sigma_i(\psi_{X^{mn}})$ for $i = 0, 1, \dots, r-1$ for some $r > 1$. Let

$$\sigma_r(\psi_{X^m}) = \sum_{\pi \in S_r} \alpha_\pi \pi,\ \sigma_r(\psi_{X^n}) = \sum_{\pi \in S_r} \beta_\pi \pi.$$

Then the coefficients α_π, β_π are non-negative integers, and it is not hard to see that

$$\sum \alpha_\pi = m^r,\ \sum \beta_\pi = n^r.$$

So

$$\sigma_r(\psi_{X^m} \circ \psi_{X^n}) = \sigma_r(\psi_{X^m})\sigma_r(\psi_{X^n}) = \sum_{\pi \in S_r} \gamma_\pi \pi$$

for some non-negative integers γ_π with $\sum \gamma_\pi = (mn)^r$. It follows that

$$\sigma_r(\psi_{X^m} \circ \psi_{X^n} - \psi_{X^{mn}}) = \sum_{\pi \in S_r} \delta_\pi \pi$$

DOI: http://dx.doi.org/10.30504/jims.2020.107524

for some integers δ_π with $\sum \delta_\pi = 0$. But $\sigma_i(\psi_{X^m} \circ \psi_{X^n} - \psi_{X^{mn}}) = 0$ for $i = 0, 1, \ldots, r-1$, and as we saw in the proof of Lemma 2.3 this implies that

$$\sigma_r(\psi_{X^m} \circ \psi_{X^n} - \psi_{X^{mn}}) = \alpha \sum_{\pi \in S_r} \pi$$

for some $\alpha \in \mathbb{Q}$. It follows that $\sigma_r(\psi_{X^m} \circ \psi_{X^n} - \psi_{X^{mn}}) = 0$, and so by induction we see that $\sigma_i(\psi_{X^m} \circ \psi_{X^n}) = \sigma_i(\psi_{X^{mn}})$ for all $i \geq 0$. So $\psi_{X^m} \circ \psi_{X^n} = \psi_{X^{mn}}$, as claimed. □

Corollary 2.5. *The algebra R is commutative.*

Proof. Lemma 2.4 implies that $\psi_{X^m} \circ \psi_{X^n} = \psi_{X^n} \circ \psi_{X^m}$ for all $m, n \geq 0$. We can express x^m as a linear combination of $1, X, X^2, \ldots, X^m$, so that ψ_{x^m} is a linear combination of $\psi_1, \psi_X, \ldots, \psi_{X^m}$. So $\psi_{x^m} \circ \psi_{x^n} = \psi_{x^n} \circ \psi_{x^m}$ for all $m, n \geq 0$, and R is commutative. □

Now let

$$z = \log X = \log(1+x) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{x^n}{n} \in \mathbb{Q}[[x]].$$

Then

$$X = \mathrm{e}^z = \sum_{n=0}^{\infty} \frac{z^n}{n!}$$

and

$$X^m = \mathrm{e}^{mz} = \sum_{n=0}^{\infty} \frac{m^n z^n}{n!}.$$

It follows that

$$\psi_{X^m} = \sum_{n=0}^{\infty} \varepsilon_n m^n$$

where

$$\varepsilon_n = \psi_{\frac{z^n}{n!}} \text{ for } n = 0, 1, \ldots.$$

(There is no problem over convergence, since if $a \in A$ has degree r then $\varepsilon_n(a) = 0$ for $n > r$.)

Lemma 2.6. *The elements ε_n $(n = 0, 1, 2, \ldots)$ are orthogonal idempotents. That is, $\varepsilon_r \circ \varepsilon_s = 0$ if $r \neq s$ and $\varepsilon_r \circ \varepsilon_r = \varepsilon_r$ for $r, s = 0, 1, 2, \ldots$.*

Proof. It is enough to show that if $k \geq 0$ then

$$\sigma_k(\varepsilon_r \circ \varepsilon_s) = 0 \text{ if } r \neq s, \tag{2.1}$$

and

$$\sigma_k(\varepsilon_r \circ \varepsilon_r) = \sigma_k(\varepsilon_r). \tag{2.2}$$

Now $\sigma_k(\varepsilon_r \circ \varepsilon_s) = \sigma_k(\varepsilon_r)\sigma_k(\varepsilon_s)$ and $\sigma_k(\varepsilon_r) = 0$ if $r > k$. So equations (1) and (2) hold if $r > k$ or $s > k$. As noted above, $\psi_{X^m} = \sum_{r=0}^{\infty} \varepsilon_r m^r$, and so the equation $\psi_{X^m} \circ \psi_{X^n} = \psi_{X^{mn}}$ gives

$$\sum_{r,s=0}^{k} \sigma_k(\varepsilon_r)\sigma_k(\varepsilon_s) m^r n^s = \sum_{r=0}^{k} \sigma_k(\varepsilon_r)(mn)^r.$$

This equation holds for all m, n, and so equations (1) and (2) also hold when $r, s \leq k$. □

DOI: http://dx.doi.org/10.30504/jims.2020.107524

We need the following number theoretic result.

Lemma 2.7. *Let*

$$z = \log(1+x) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{x^n}{n}$$

as above, and let p be a prime. For $0 < i < p$ let t_i be the power series in x given by

$$t_i = \sum_{r=0}^{\infty} \frac{1}{(i + r(p-1))!} z^{i+r(p-1)}.$$

Then the denominators of the coefficients of t_i are coprime to p.

Proof. The constant term of t_i is 0 for all $i = 1, 2, \ldots, p-1$. Let $n \geq 1$ and let α_i be the coefficient of x^n in t_i ($0 < i < p$). (We fix n for the moment.) We want to show that $\alpha_i \in \mathbb{Z}_{(p)}$, the ring of rationals with denominators coprime to p. For $m = 1, 2, \ldots$ let β_m be the coefficient of x^n in $\frac{1}{m!} z^m$. Then $\beta_m = 0$ for $m > n$, and so if we pick R such that $1 + R(p-1) \geq n$ then

$$\alpha_i = \sum_{r=0}^{R} \beta_{i+r(p-1)}$$

for $0 < i < p$. Let k be a positive integer, so that $\mathrm{e}^{kz} = (1+x)^k$, and pick out the coefficient of x^n on both sides of the equation

$$(1+x)^k = \sum_{m=0}^{\infty} \frac{1}{m!} (kz)^m.$$

We obtain the equation

$$\binom{k}{n} = \sum_{m=1}^{n} k^m \beta_m = \sum_{i=1}^{p-1} \sum_{r=0}^{R} k^{i+r(p-1)} \beta_{i+r(p-1)}.$$

Now let N be the largest positive integer where p^N divides the denominator of any of $\beta_1, \beta_2, \ldots, \beta_n$. By Hensel's lemma we can find an integer k such that $k + p\mathbb{Z}$ is a primitive element in the finite field $\mathbb{Z}/p\mathbb{Z}$, and such that $k^{p-1} = 1 \bmod p^N$. If $r > 0$, then $k^{i+r(p-1)} - k^i$ is divisible by p^N (for any i) so that $k^{i+r(p-1)} \beta_{i+r(p-1)} - k^i \beta_{i+r(p-1)} \in \mathbb{Z}_{(p)}$. It follows that

$$\sum_{i=1}^{p-1} k^i \alpha_i = \sum_{i=1}^{p-1} \sum_{r=0}^{R} k^i \beta_{i+r(p-1)} \in \mathbb{Z}_{(p)}.$$

If we let $k_j = k^j$ for $j = 1, 2, \ldots, p-1$ then we obtain $p-1$ equations

$$\sum_{i=1}^{p-1} k_j^i \alpha_i \in \mathbb{Z}_{(p)},$$

and since the Vandermonde determinant $\prod_{1 \leq i < j \leq p-1} (k_i - k_j)$ is coprime to p this implies that $\alpha_i \in \mathbb{Z}_{(p)}$ for $i = 1, 2, \ldots, p-1$. ∎

DOI: http://dx.doi.org/10.30504/jims.2020.107524

Corollary 2.8. *Let*

$$\eta = \psi_{t_1} = \sum_{r=0}^{\infty} \varepsilon_{1+r(p-1)}.$$

Then $\sigma_0(\eta) = 0$, $\sigma_1(\eta) = 1_{S_1}$. *If* $n \geq 1$, *and if we write* $\sigma_n(\eta) = \sum_{\pi \in S_n} \alpha_\pi \pi$, *then the coefficients* α_π *have denominators which are coprime to* p. *Furthermore, if* $n \neq 1 \bmod (p-1)$ *then* $\sum_{\pi \in S_n} \alpha_\pi = 0$.

Proof. The constant term of t_1 is 0, and the coefficient of x is 1. So $\sigma_0(\eta) = 0$ and $\sigma_1(\eta) = 1_{S_1}$. Let $n \geq 1$ and let $\sigma_n(\eta) = \sum_{\pi \in S_n} \alpha_\pi \pi$. Then Lemma 2.7 implies that the coefficients α_π have denominators which are coprime to p. Finally, suppose that $n \neq 1 \bmod (p-1)$. Then $\varepsilon_n \circ \eta = 0$ since the elements ε_r $(r = 0, 1, 2, \ldots)$ are orthogonal idempotents. It is easy to see that $\sigma_n(\varepsilon_n) = \frac{1}{n!} \sum_{\pi \in S_n} \pi$ and so

$$\left(\sum_{\pi \in S_n} \alpha_\pi \right) \left(\frac{1}{n!} \sum_{\pi \in S_n} \pi \right) = \left(\frac{1}{n!} \sum_{\pi \in S_n} \pi \right) \left(\sum_{\pi \in S_n} \alpha_\pi \pi \right) = \sigma_n(\varepsilon_n)\sigma_n(\eta) = \sigma_n(\varepsilon_n \circ \eta) = 0.$$

This implies that $\sum_{\pi \in S_n} \alpha_\pi = 0$. □

3. The relators K_n $(n = 1, 2, \ldots)$

If $a \in L$ and if $x_i x_j \ldots x_k$ is a product of the free generators of A let $[a \,|\, x_i x_j \ldots x_k] = [a, x_i, x_j, \ldots, x_k] \in L$. If $b = \sum \beta_i m_i \in A$ is a linear combination of products m_i then let

$$[a \,|\, b] = \sum \beta_i [a \,|\, m_i].$$

Then $K_1(x_1) = q x_1$, and if $n > 0$ then using Wall's notation we have

$$K_{n+1}(x_1, x_2, \ldots, x_{n+1}) = \sum_{r=2}^{q} \binom{q}{r} [x_{n+1} \,|\, \psi_{x^{r-1}}(x_1 x_2 \ldots x_n)].$$

If G is any group of prime-power exponent q then the associated Lie ring of G satisfies the relations $K_n = 0$ $(n = 1, 2, \ldots)$. Furthermore, if $f = 0$ is any multilinear Lie relation satisfied by the associated Lie ring of every group of exponent q, then $f = 0$ is a consequence of the identities $K_n = 0$ $(n = 1, 2, \ldots)$. This is Theorem 2.4.7 and Theorem 2.5.1 of [5].

Let $L_{\mathbb{Z}}$ be the Lie subring of L generated by $x_1, x_2, \ldots$. Then $L_{\mathbb{Z}}$ consists of linear combinations

$$\sum \alpha_i [x_{i1}, x_{i2}, \ldots, x_{in_i}]$$

of Lie products of the generators $x_1, x_2, \ldots$ where the coefficients α_i are integers. So $K_n \in L_{\mathbb{Z}}$ for all n. For $n \geq 1$ let I_n be the Lie ideal of $L_{\mathbb{Z}}$ generated by elements $K_m(a_1, a_2, \ldots, a_m)$ with $m \leq n$ and $a_1, a_2, \ldots, a_m \in L_{\mathbb{Z}}$. So Theorem 1.1 says that if $n \neq 1 \bmod (p-1)$ then $K_n \in I_{n-1}$. Note that I_n is actually spanned by the elements $K_m(a_1, a_2, \ldots, a_m)$, since

$$[K_m(a_1, a_2, \ldots, a_m), b] = \sum_{i=1}^{m} K_m(a_1, \ldots, [a_i, b], \ldots, a_m).$$

We define a linear map $\delta : A \to L$ by setting $\delta(1) = 0$, and setting

$$\delta(x_i x_j \ldots x_k) = \begin{cases} [x_i, x_j, \ldots, x_k] \text{ if } i = 1, \\ 0 \text{ if } i \neq 1. \end{cases}$$

DOI: http://dx.doi.org/10.30504/jims.2020.107524

The map δ has the useful property that if $a \in L$ is multilinear in $x_1, x_2, \ldots, x_r$ then $\delta(a) = a$. (See [5, page 47].)

Lemma 3.1. *$\delta(\psi_{X^q}(x_1)) = \psi_{X^q}(x_1) = qx_1 = K_1(x_1)$, and if $n \geq 2$*

$$\delta(\psi_{X^q}(x_1 x_2 \ldots x_n)) = K_n(x_2, \ldots, x_n, x_1) \bmod I_{n-1}.$$

Proof. The first claim in the lemma is straighforward, and so we let $n \geq 2$.

$$\psi_{X^q} = \sum_{r=0}^{q} \binom{q}{r} \psi_{x^r}$$

and so

$$\psi_{X^q}(x_1 x_2 \ldots x_n) = qx_1 x_2 \ldots x_n + \sum_{r=2}^{q} \binom{q}{r} \psi_{x^r}(x_1 x_2 \ldots x_n).$$

If $r \geq 2$, then using the notation introduced in the proof of Lemma 2.2 we have

$$\psi_{x^r}(x_1 x_2 \ldots x_n) = \sum x_{S_1} x_{S_2} \ldots x_{S_r}$$

where the sum is taken over all partitions of $\{1, 2, \ldots, n\}$ into an ordered sequence of non-empty subsets $S_1, S_2, \ldots, S_r$. For each non-empty subset $S \subset \{1, 2, \ldots, n\}$ we gather together the summands where $S_1 = S$, and obtain

$$\psi_{x^r}(x_1 x_2 \ldots x_n) = \sum_S \left(\sum_{S_1 = S} x_{S_1} x_{S_2} \ldots x_{S_r} \right) = \sum_S x_S \psi_{x^{r-1}}(x_{\{1,2,\ldots,n\} \setminus S}).$$

So

$$\delta(\psi_{X^q}(x_1 x_2 \ldots x_n))$$
$$= q[x_1, x_2, \ldots, x_n] + \sum_S \left(\sum_{r=2}^{q} \binom{q}{r} [\delta(x_S) \,|\, \psi_{x^{r-1}}(x_{\{1,2,\ldots,n\} \setminus S})] \right).$$

If S is a non-empty subset of $\{1, 2, \ldots, n\}$, and if we write $\{1, 2, \ldots, n\} \setminus S = \{i, j, \ldots, k\}$ with $i < j < \ldots < k$ then

$$\sum_{r=2}^{q} \binom{q}{r} [\delta(x_S) \,|\, \psi_{x^{r-1}}(x_{\{1,2,\ldots,n\} \setminus S})] = K_{n+1-|S|}(x_i, x_j, \ldots, x_k, \delta(x_S)).$$

But $\delta(x_S) = 0$ unless $1 \in S$, and $K_{n+1-|S|}(x_i, x_j, \ldots, x_k, \delta(x_S)) \in I_{n-1}$ if $|S| > 1$. Clearly $q[x_1, x_2, \ldots, x_n] \in I_{n-1}$ and so

$$\delta(\psi_{X^q}(x_1 x_2 \ldots x_n)) = K_n(x_2, \ldots, x_n, x_1) \bmod I_{n-1}.$$

□

We now define Γ_n to be the subring of A generated by elements $K_m(a_1, a_2, \ldots, a_m)$ with $m \leq n$ and $a_1, a_2, \ldots, a_m \in L_{\mathbb{Z}}$. So Γ_n consists of integral linear combinations of products of elements $K_m(a_1, a_2, \ldots, a_m)$ ($m \leq n$). (Wall's definition of Γ_n is slightly different from this, in that he allows coefficients in the ring of rationals with denominators which are coprime to p. Wall also indexes Γ_n differently.)

DOI: http://dx.doi.org/10.30504/jims.2020.107524

Lemma 3.2. $\psi_{X^q}(x_1x_2\dots x_n) = K_n(x_2,\dots,x_n,x_1) \bmod \Gamma_{n-1}$.

Proof. First note that $\psi_{X^q}(x_1) = qx_1 = K_1(x_1)$. Next note that $K_2(x_2,x_1) = \binom{q}{2}[x_1,x_2]$ and that

$$\begin{aligned}
&\psi_{X^q}(x_1x_2)\\
&= \binom{q+1}{2}x_1x_2 + \binom{q}{2}x_2x_1\\
&= \binom{q+1}{2}[x_1,x_2] + q^2x_1x_2\\
&= \binom{q}{2}[x_1,x_2] + q[x_1,x_2] + q^2x_1x_2\\
&= K_2(x_2,x_1) \bmod \Gamma_1
\end{aligned}$$

since $q^2x_1x_2 = (qx_1)(qx_2) \in \Gamma_1$ and $q[x_1,x_2] \in \Gamma_1$.

We establish Lemma 3.2 for general n by induction on n. So suppose that $n > 2$ and that

$$\psi_{X^q}(x_1x_2\dots x_m) = K_m(x_2,\dots,x_m,x_1) \bmod \Gamma_{m-1}$$

for $m < n$. Note that this implies that $\psi_{X^q}(x_1x_2\dots x_m) \in \Gamma_m$ for $m < n$.

We extend A to the ring $\widehat{A}$ of formal power series consisting of formal sums

$$\sum_{r=0}^{\infty} u_r$$

where u_r is a homogeneous element of degree r in A. If $a \in \widehat{A}$ has zero constant term then we define

$$\mathrm{e}^a = \sum_{r=0}^{\infty} \frac{a^r}{r!}$$

in the usual way. So e^a is a unit in $\widehat{A}$ with inverse e^{-a}. It is well known that the group F generated by e^{x_1}, e^{x_2}, ..., e^{x_n} is a free group with free generators e^{x_1}, e^{x_2}, ..., e^{x_n}. (See [5, pages 41,42].) If $w \in F$ then

$$w = 1 + u_1 + u_2 + \dots$$

for some $u_1, u_2, \dots \in A$, where u_i is homogeneous of degree i for $i = 1, 2, \dots$. We set $u = u_1 + u_2 + \dots$, and set

$$z = \log w = \log(1+u) = \sum_{r=1}^{\infty} (-1)^{r+1}\frac{u^r}{r},$$

and then $w = \mathrm{e}^z$. If we write

$$z = z_1 + z_2 + \dots$$

where $z_i \in A$ is homogeneous of degree i for $i = 1, 2, \dots$, then $z_i \in L$ for $i = 1, 2, \dots$. This is known as the Baker-Campbell-Hausdorff formula. (See [5, Theorem 2.5.4].)

Now let $w = (\mathrm{e}^{x_1}\mathrm{e}^{x_2}...\mathrm{e}^{x_n})^q \in F$. We apply what Wall calls smoothing to w. For $i = 1, 2, \dots, n$ we let $\delta_i : \widehat{A} \to \widehat{A}$ be the endomorphism given by $\delta_i(x_i) = 0$, $\delta_i(x_j) = x_j$ if $j \neq i$. So δ_i induces a homomorphism $\delta_i : F \to F$. Note that $\delta_i^2 = \delta_i$ and that $\delta_i\delta_j = \delta_j\delta_i$ for all i, j.

DOI: http://dx.doi.org/10.30504/jims.2020.107524

We set $w_1 = w.(\delta_1 w)^{-1}$ so that $\delta_1(w_1) = 1$. Then we set $w_2 = w_1.\delta_2(w_1)^{-1}$ so that $\delta_i(w_2) = 1$ for $i = 1, 2$. Then we set $w_3 = w_2.\delta_3(w_2)^{-1}$ and so on. Eventually we obtain an element $w_n \in F$ such that $\delta_i(w_n) = 1$ for $1 \leq i \leq n$. Note that w_n is a product of 2^n elements of the form $(\delta_i\delta_j \ldots \delta_k(w))^{\pm 1}$ with one element for each subset $\{i, j, \ldots, k\} \subset \{1, 2, \ldots, n\}$. The exponent is $+1$ if $|\{i, j, \ldots, k\}|$ is even, and -1 if it is odd. Let $w_n = \mathrm{e}^z$ where $z = z_1 + z_2 + \ldots$, with $z_r \in L$ homogeneous of degree r for $r = 1, 2, \ldots$. Then $\delta_i(z_r) = 0$ for $i = 1, 2, \ldots, n$ (for all r) and we can write z_r as a linear combination of Lie products $[x_{j_1}, x_{j_2}, \ldots, x_{j_r}]$ with $\{j_1, j_2, \ldots, j_r\} = \{1, 2, \ldots, n\}$. It follows that $z_r = 0$ for $r < n$, and that z_n is an $\{x_1, x_2, \ldots, x_n\}$-multilinear element of L.

So $w_n = 1 + z_n + u_{n+1} + u_{n+2} + \ldots$ where $u_i \in A$ is homogeneous of degree i for $i = n+1, n+2, \ldots$.

Next consider w. We have

$$w = (e^{x_1} e^{x_2} \ldots e^{x_n})^q$$
$$= 1 + \sum \psi_{X^q}(x_i x_j \ldots x_k) + b$$

where the sum is taken over all non empty subsets $\{i, j, \ldots, k\} \subset \{1, 2, \ldots, n\}$, and where b is an infinite sum of terms αm where $\alpha \in \mathbb{Q}$ and where m is a non-multilinear product of (some of) the generators $x_1, x_2, \ldots, x_n$. By induction

$$w = 1 + \psi_{X^q}(x_1 x_2 \ldots x_n) + a + b$$

where $a \in \Gamma_{n-1}$. Similarly, if $\{i, j, \ldots, k\}$ is non-empty, $\delta_i\delta_j \ldots \delta_k(w) = 1 + c + d$ where $c \in \Gamma_{n-1}$ and where d is an infinite sum of terms αm where $\alpha \in \mathbb{Q}$ and where m is a non-multilinear product of the generators $x_1, x_2, \ldots, x_n$. Clearly $(\delta_i\delta_j \ldots \delta_k(w))^{-1}$ can be expressed in the same form. It follows that if we pick out the $\{x_1, x_2, \ldots, x_n\}$-multilinear terms in w_n then we obtain

$$\psi_{X^q}(x_1 x_2 \ldots x_n) + e$$

for some $e \in \Gamma_{n-1}$, so that

$$z_n = \psi_{X^q}(x_1 x_2 \ldots x_n) \bmod \Gamma_{n-1}.$$

This implies that

$$z_n = \delta(z_n) = \delta(\psi_{X^q}(x_1 x_2 \ldots x_n)) \bmod \Gamma_{n-1}.$$

So

$$\psi_{X^q}(x_1 x_2 \ldots x_n) = \delta(\psi_{X^q}(x_1 x_2 \ldots x_n)) \bmod \Gamma_{n-1}$$

and by Lemma 3.1 this implies that

$$\psi_{X^q}(x_1 x_2 \ldots x_n) = K_n(x_2, \ldots, x_n, x_1) \bmod \Gamma_{n-1}.$$

□

Corollary 3.3. $\psi_{X^q}(x_1 x_2 \ldots x_n) \in \Gamma_n$.

DOI: http://dx.doi.org/10.30504/jims.2020.107524

Lemma 3.4. *If $\pi \in S_n$ then*

$$\psi_{X^q}(x_{\pi 1}x_{\pi 2}\ldots x_{\pi n}) - \psi_{X^q}(x_1x_2\ldots x_n) \in \Gamma_{n-1}$$

and

$$K_n(x_{\pi 1}, x_{\pi 2}, \ldots, x_{\pi n}) - K_n(x_1, x_2, \ldots, x_n) \in I_{n-1}.$$

Proof. From Lemma 1.2 we see that

$$\psi_{X^q}(x_{\pi 1}x_{\pi 2}\ldots x_{\pi n}) - \psi_{X^q}(x_1x_2\ldots x_n)$$

is a sum of terms of the form

$$\psi_{X^q}(y_1y_2\ldots y_{i-1}[y_i, y_{i+1}]y_{i+2}\ldots y_n)$$

where $1 \leq i < n$ and where $y_1, y_2, \ldots, y_n$ is a permutation of $x_1, x_2, \ldots, x_n$. But

$$\psi_{X^q}(y_1y_2\ldots y_{i-1}[y_i, y_{i+1}]y_{i+2}\ldots y_n)$$

is the image of $\psi_{X^q}(x_1x_2\ldots x_{n-1})$ under an endomorphism $\varphi : A \to A$ mapping $x_1, x_2, \ldots, x_{n-1}$ into $y_1, y_2, \ldots, y_{i-1}, [y_i, y_{i+1}], y_{i+2}, \ldots, y_n$. We can assume that $\varphi(L_{\mathbb{Z}}) \leq L_{\mathbb{Z}}$, which implies that $\varphi(\Gamma_{n-1}) \subset \Gamma_{n-1}$, and so Corollary 3.3 implies that

$$\psi_{X^q}(y_1y_2\ldots y_{i-1}[y_i, y_{i+1}]y_{i+2}\ldots y_n) \in \Gamma_{n-1}.$$

So

$$\psi_{X^q}(x_{\pi 1}x_{\pi 2}\ldots x_{\pi n}) - \psi_{X^q}(x_1x_2\ldots x_n) \in \Gamma_{n-1}$$

as claimed.

This result, combined with Lemma 3.2 implies that

$$K_n(x_{\pi 1}, x_{\pi 2}, \ldots, x_{\pi n}) - K_n(x_1, x_2, \ldots, x_n) = a$$

for some $a \in \Gamma_{n-1}$, and hence that

$$\begin{aligned} &K_n(x_{\pi 1}, x_{\pi 2}, \ldots, x_{\pi n}) - K_n(x_1, x_2, \ldots, x_n) \\ &= \delta(K_n(x_{\pi 1}, x_{\pi 2}, \ldots, x_{\pi n}) - K_n(x_1, x_2, \ldots, x_n)) \\ &= \delta(a) \\ &\in I_{n-1} \end{aligned}$$

since $\delta(\Gamma_{n-1}) = I_{n-1}$. (Recall that I_{n-1} is the ideal of $L_{\mathbb{Z}}$ consisting of integer linear combinations of values $K_m(a_1, a_2, \ldots, a_m)$ with $m < n$ and $a_1, a_2, \ldots, a_m \in L_{\mathbb{Z}}$.) □

It is perhaps worth observing that the analysis in this section would have been simpler if in [5] I had defined $K_n(x_1, x_2, \ldots, x_n)$ to be $\delta(\psi_{X^q}(x_1x_2\ldots x_n))$. Of course that would have meant that the proofs of Theorem 2.4.7 and Theorem 2.5.1 in [5] would have to have been rewritten. But the proofs would have remained essentially the same. In fact the proof of Lemma 3.2 above shows that the associated Lie rings of groups of exponent q satisfy the identity $z_n = 0$. So Lemma 3.2 (and its proof) give a proof of Theorem 2.4.7 of [5].

DOI: http://dx.doi.org/10.30504/jims.2020.107524

4. Proof of Theorem 1.1

Recall from Section 2 that

$$z = \log(1+x) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{x^n}{n}$$

and that

$$\varepsilon_n = \psi_{\frac{z^n}{n!}} \text{ for } n = 0, 1, \ldots .$$

In Corollary 2.8 we defined

$$\eta = \sum_{r=0}^{\infty} \varepsilon_{1+r(p-1)}$$

and we proved that $\sigma_0(\eta) = 0$, $\sigma_1(\eta) = 1_{S_1}$, and that if $n \geq 1$, and $\sigma_n(\eta) = \sum_{\pi \in S_n} \alpha_\pi \pi$, then the coefficients α_π have denominators which are coprime to p. We also showed that if $n \neq 1 \bmod (p-1)$ then $\sum_{\pi \in S_n} \alpha_\pi = 0$.

So assume that $n \neq 1 \bmod (p-1)$, and let k be the least common multiple of the denominators of all the coefficients which appear in $\sigma_m(\eta)$ for $m = 1, 2, \ldots, n$. Let $\eta' = k\eta$. (Note that k is coprime to p.) Then $\sigma_n(\eta') = \sum_{\pi \in S_n} \beta_\pi \pi$ for some integers β_π satisfying $\sum \beta_\pi = 0$. Lemma 3.2 and Lemma 3.4 imply that

$$K_n(x_1, x_2, \ldots, x_n) = \psi_{X^q}(x_1 x_2 \ldots x_n) + a$$

for some $a \in \Gamma_{n-1}$. Since $\sigma_1(\eta) = 1_{S_1}$,

$$\begin{aligned} &= kK_n(x_1, x_2, \ldots, x_n) \\ &= \eta'(K_n(x_1, x_2, \ldots, x_n)) \\ &= (\eta' \circ \psi_{X^q})(x_1 x_2 \ldots x_n) + \eta'(a). \end{aligned}$$

Now R is commutative and so

$$\begin{aligned} &(\eta' \circ \psi_{X^q})(x_1 x_2 \ldots x_n) \\ &= \psi_{X^q}(\eta'(x_1 x_2 \ldots x_n)) \\ &= \sum_{\pi \in S_n} \beta_\pi \psi_{X^q}(x_{\pi^{-1}1} x_{\pi^{-1}2} \ldots x_{\pi^{-1}n}) \\ &\in \Gamma_{n-1} \end{aligned}$$

since $\psi_{X^q}(x_{\pi^{-1}1} x_{\pi^{-1}2} \ldots x_{\pi^{-1}n}) = \psi_{X^q}(x_1 x_2 \ldots x_n) \bmod \Gamma_{n-1}$ by Lemma 3.4, and since $\sum_{\pi \in S_n} \beta_\pi = 0$.

Next we show that $\eta'(a) \in \Gamma_{n-1}$. Since $a \in \Gamma_{n-1}$, we can express a as sum of terms of the form mb where m is an integer and where each b in the sum is a product $c_1 c_2 \ldots c_r$ where each c_i has the form $K_s(a_1, a_2, \ldots, a_s)$ $(s < n)$ with $a_i \in L_{\mathbb{Z}}$ for $i = 1, 2, \ldots, s$. So we need to show that $\eta'(c_1 c_2 \ldots c_r) \in \Gamma_{n-1}$ for each of these products $c_1 c_2 \ldots c_r$. We can take a to be homogeneous of degree n and so $r \leq n$. Our choice of k then implies that $\sigma_r(\eta') = \sum_{\pi \in S_r} \gamma_\pi \pi$ where the coefficients γ_π are integers. It follows that

$$\eta'(c_1 c_2 \ldots c_r) = \sum_{\pi \in S_r} \gamma_\pi c_{\pi^{-1}1} c_{\pi^{-1}2} \ldots c_{\pi^{-1}r} \in \Gamma_{n-1}.$$

DOI: http://dx.doi.org/10.30504/jims.2020.107524

We have shown that

$$kK_n(x_1, x_2, \ldots, x_n) \in \Gamma_{n-1}.$$

We also have

$$qK_n(x_1, x_2, \ldots, x_n) \in \Gamma_{n-1}$$

and since k is coprime to q this implies that

$$K_n(x_1, x_2, \ldots, x_n) \in \Gamma_{n-1}.$$

This in turn implies that

$$\begin{aligned} &K_n(x_1, x_2, \ldots, x_n) \\ &= \delta(K_n(x_1, x_2, \ldots, x_n)) \\ &\in \delta(\Gamma_{n-1}) \\ &= I_{n-1}. \end{aligned}$$

References

[1] M. Hall, The Theory of Groups, The Macmillan Co., New York, 1959.

[2] G. Havas and M. Vaughan-Lee, On counterexamples to the Hughes conjecture, *J. Algebra* **322** (2009), no. 3, 791–801.

[3] W. Magnus, A connection between the Baker-Hausdorff formula and a problem of Burnside, *Ann. of Math. (2)* **52** (1950) 111–126.

[4] I.N. Sanov, Establishment of a connection between periodic groups with period a prime number and Lie rings, *Izv. Akad. Nauk SSSR, Ser. Mat.* **16** (1952) 23–58.

[5] M.R. Vaughan-Lee, The restricted Burnside problem. Second edition, London Mathematical Society Monographs. New Series, 8, The Clarendon Press, Oxford University Press, New York, 1993.

[6] G.E. Wall, On Hughes' H_p-problem, *Proc. Internat. Conf. Theory of Groups (Canberra, 1965)*, pp. 357–362, Gordon and Breach, New York, 1967.

[7] G.E. Wall, On the multilinear identities which hold in the Lie ring of a group of prime-power exponent, *J. Algebra* **104** (1986), no. 1, 1–22.

[8] G.E. Wall, Dependence of Lie relators for Burnside varieties, pp. 191–197, Lecture Notes in Mathematics, 1456, Springer-Verlag, Berlin, 1990.

Michael Vaughan-Lee

Christ Church, University of Oxford, Oxford, OX1 1DP, England.

Email: michael.vaughan-lee@chch.ox.ac.uk

DOI: http://dx.doi.org/10.30504/jims.2020.107524