Groups Geom. Dyn. 1 (2007), 421–468 **Groups, Geometry, and Dynamics**

A partial extension of Lazard's correspondence for finite p-groups

George Glauberman

Dedicated to Professor Avinoam Mann

Abstract. M. Lazard established a correspondence between finite p-groups of nilpotence class less than p and finite nilpotent Lie rings of p-power order and nilpotence class less than p. This correspondence has had many applications, but cannot generally be extended to p-groups of class p or larger. However, in this paper, we obtain a partial extension of Lazard's result for a p-group that is a product of normal subgroups of class less than p.

Mathematics Subject Classification (2000). 20D15, 20F18, 20F40.

Keywords. Finite p-groups, Lie algebras.

1. Introduction and notation

Let S be a finite p-group for some prime p. If S is abelian, it is sometimes convenient to represent the operation in S as addition. If p is odd and S has nilpotence class at most two, then we may define new operations $+$ and $[\ ,\ ]$ on S under which S becomes a Lie ring, by a construction of R. Baer (below). M. Lazard extended Baer's construction to the case in which p is arbitrary and S has class at most $p-1$. Furthermore, Lazard established a correspondence (Theorem 4.8 below) between these p-groups and finite nilpotent Lie rings of p-power order and class at most $p-1$, since one may recover the group operation from the Lie ring operations. (Thus, this Lie ring differs from the more commonly used Lie ring ([13], Definition 6.1), which may be defined for any nilpotent group and which may be the same for non-isomorphic groups.)

Lazard's correspondence has many applications ([13], Remark 10.29). Unfortunately, examples (below) show that it is generally impossible to extend to a p-group S of class at least p. However, in this paper, we show that one may associate to S a Lie ring that reflects a large part of the structure of S in the case in which S is equal to a product $B_1 B_2 \dots B_n$ of normal subgroups of class at most $p-1$, e.g., normal abelian subgroups. We do this by making a slight change in the definition of the operations.

In the Lazard correspondence for a given group the Lie ring operations are defined by formulas

$$a + b = h_1(a, b) \quad \text{and} \quad [a, b] = h_2(a, b),$$

where each of $h_1(a, b)$ and $h_2(a, b)$ is a product of elements equal to a or b or to a commutator in a and b raised to a rational power (as defined below). However, h_1 and h_2 need not be well defined in a p-group of class at least p. We give below a family of examples in which $h_2(x, y)$, but not $h_1(x, y)$, is well defined for some pairs of elements x, y. More generally, there are conditions under which $h_2(x, y)$, but not $h_1(x, y)$, may become well defined by multiplying its product formula by some powers of commutators c^r for which the choice of x and y yields $c = 1$. Therefore, in this paper (in Remark 5.9), we modify the product formula for $h_2(a, b)$ in this way to obtain a product $h_2'(a, b)$ that is equal to $h_2(a, b)$ for p-groups of class at most $p - 1$, but is also well defined in some other situations. We then let $[a, b]$ be $h_2'(a, b)$ in these situations.

Lazard's correspondence was originally inspired by a correspondence of Mal'cev for infinite nilpotent groups (Theorem 4.6). Although its main applications concern finite p-groups, it is stated in a more general form. Our main results, too, are stated in a more general (and complicated) form in Section 6 of the paper. We also mention some open questions (Remark 6.11 and below).

Our main results are the following (for $[a, b]$ as above):

Theorem A. *Suppose p is a prime and S is a finite p-group. Then $[x, y]$ is well defined whenever x and y are elements of (possibly different) normal subgroups of S of nilpotence class at most $p - 1$.*

In addition, suppose A and B are normal subgroups of S of nilpotence class at most $p - 1$. Define $+$ and $[\,,]$ on A and B as in the Lazard correspondence. Then:

(i) *for each u in A and v in B, the elements $[u, v]$ and $[v, u]$ lie in $A \cap B$, and $[v, u] = [u, v]^{-1}$, and*

(ii) *for each u, u' in A and v in B,*

$$[u + u', v] = [u, v] + [u', v] \quad \textit{and} \quad [[u, u'], v] = [[u, v], u'] + [u, [u', v]].$$

Theorem B. *Suppose S is a finite p-group generated by a set $\mathcal{S}$ of normal subgroups N of S having nilpotence class at most $p - 1$. Let $\mathfrak{U}$ be the set-theoretic union of the elements of $\mathcal{S}$. For each N in $\mathcal{S}$, define $+$ on N by Lazard's definition. For each u, v in $\mathfrak{U}$, define $[u, v]$ as in Theorem A.*

Let $E = \mathrm{End}(\mathcal{S})$ be the set of all mappings ϕ from $\mathfrak{U}$ to $\mathfrak{U}$ such that, for each N in $\mathcal{S}$,

$$\phi \textit{ maps } N \textit{ into } N \textit{ and induces an endomorphism of } N \textit{ under } +.$$

Define addition and multiplication on E by

$$(\phi + \phi')(x) = \phi(x) + \phi'(x) \quad \textit{and} \quad (\phi\phi')(x) = \phi(\phi'(x)).$$

Then E forms an associative ring, and hence also a Lie ring under the definition

$$[\phi, \phi'] = \phi\phi' - \phi'\phi.$$

For each v in $\mathfrak{U}$, define a mapping ad v *on* $\mathfrak{U}$ *by*

$$(\operatorname{ad} v)(u) = [u, v].$$

Then

(i) ad v *lies in E for each v in* $\mathfrak{U}$,

(ii) *for each N in $\mathcal{S}$ and each v, w in N,* $\operatorname{ad}(v + w) = \operatorname{ad} v + \operatorname{ad} w$,

(iii) *for v, w in* $\mathfrak{U}$,

$$[\operatorname{ad} v, \operatorname{ad} w] = \operatorname{ad}[w, v] = -\operatorname{ad}[v, w], \quad \textit{and}$$

$$\operatorname{ad} v = \operatorname{ad} w \quad \textit{iff} \quad v \equiv w \pmod{Z(S)},$$

(iv) *the additive subgroup $L(\mathcal{S})$ of E spanned by the mappings* ad v *for v in* $\mathfrak{U}$ *is a Lie subring of E, and*

(v) *for $L(\mathcal{S})$ as in* (iv)*, each element of ϕ of $L(\mathcal{S})$ satisfies*

$$\phi([u, v]) = [\phi(u), v] + [u, \phi(v)], \quad \textit{for every } u, v \textit{ in } \mathfrak{U}.$$

Note that in Theorem B, we associate to S a Lie ring, $L(\mathcal{S})$, although it may be impossible to make S itself into a Lie ring by Lazard's methods. The elements of $L(\mathcal{S})$, together with the identity mapping on $\mathfrak{U}$, generate an associative subring of $E(\mathcal{S})$ that contains the inner automorphism group of $\mathcal{S}$ as a multiplicative subset (Remark 6.9). The condition that $\mathcal{S}$ generate S in Theorem B is used only for the second part of conclusion (iii).

Part (ii) of Theorem A shows that, for each v in $\mathfrak{U}$ and each N in $\mathcal{S}$, ad v induces a derivation of N, for N regarded as a Lie ring under Lazard's definition. Part (v) of Theorem B generalizes this.

To illustrate our methods, consider the case in which S has class two. For p odd, Baer's construction ([1], Theorem B.1) gives

$$x + y = x^{\frac{1}{2}} y x^{\frac{1}{2}} = xy(y, x)^{\frac{1}{2}} \quad \text{and} \quad [x, y] = (x, y),$$

where $\left(u^{\frac{1}{2}}\right)^2 = u$ and (u, v) is the group commutator $u^{-1}v^{-1}uv$, for all u, v in S. For $p = 2$, $[x, y]$ is still well defined, but $x + y$ is not, in general. (For groups of larger class, usually $[x, y]$ does not coincide with (x, y).)

An explanation for our results is that one almost seems to need S (or the subgroup generated by x and y) to have class at most $p - 1$ in order to define $x + y$, while one needs less to define $[x, y]$. For example, the original definition of $x + y$

(in [14], Théorème II.2.4, pp. 155–156) uses a formula for products $x^t y^t$ (for every integer t) that is a product of factors c_i in various terms $\gamma_{k_i}(S)$ of the lower central series $\{\gamma_k(S)\}$ of S, raised to powers $f_i(t)$ that are polynomials in t with rational coefficients. (Here, k_i tends to infinity as i increases.) For the factors c_i inside (but not outside) $\gamma_p(S)$, the rational coefficients may have denominators divisible by p, so that $c_i^{f_i(t)}$ may be undefined. This is why we assume that $\gamma_p(S) = 1$ (i.e., S has nilpotence class at most $p-1$) for the Lazard correspondence. In contrast, the bracket product $[x, y]$ is related to the formula for (x^t, y^t), which may be expressed similarly as a product of powers of extended commutators $c_i^{h_i(t)}$ in which the rational coefficients of $h_i(t)$ may have denominators divisible by p only if c_i has weight at least p in x or at least p in y. This was shown by T. Easterfield (in Theorem C of [5]) and is illustrated by the formulas above for Baer's construction.

For example, suppose S has class at most $p-1$. For a fixed element y of S, define

$$\delta(x) = (y^{-1}xy) + (x^{-1}) \quad \text{for every } x \text{ in } S.$$

Define powers of δ by composition and regard S as a Lie algebra over $\mathbb{Z}/|S|\mathbb{Z}$. Then (Corollary 6.2) for every x in S,

$$[x, y] = \delta(x) - \delta^2(x)/2 + \cdots + (-1)^{p-2}\delta^{p-1}(x)/(p-1). \tag{1.1}$$

(Thus, $[x, y] = (\mathrm{Log}\,\gamma)(x)$ for γ given by $\gamma(x) = y^{-1}xy$ for all x in S.) It turns out that if S has class greater than $p-1$, we may define $[x, y]$ by (1.1) if we have the situation of Theorem A (with x in A and y in B).

A special case of our results appears in the Section 5 of [7]. It concerns a p-group S of class p. Here, every element x lies in a normal subgroup $N_x = \langle x, S'\rangle$ of class at most $p-1$, so that $L(\mathcal{S})$ is isomorphic to the Lazard Lie ring of $S/Z(S)$ for $\mathcal{S} = \{N_x \mid x \text{ in } S\}$.

These results lead to further questions. In the Lazard correspondence, the entire group S becomes a Lie ring. In Theorem B, in effect, we turn each subgroup B in $\mathcal{S}$ into a Lie ring and then embed $BZ(S)/Z(S)$ into the Lie ring $L(\mathcal{S})$. Then $L(\mathcal{S})$ is spanned additively by the Lie rings $BZ(S)/Z(S)$. It would seem preferable to construct an analogous Lie ring in which we embed the Lie rings B, but we do not know whether this is possible. Some other questions are given in Remark 6.11.

It is easy to see that in the original situation of Lazard's correspondence, the elements of order 1 or p in the group S form a Lie subring of S (and thus a subgroup of S). Therefore, Lazard's correspondence cannot be extended to a dihedral group of order 8. Similarly, for any prime p, the Sylow p-subgroup of the symmetric group of degree p^2 (i.e., the wreath product of a group of order p by a group of order p) provides an example of a p-group of class p to which the Lazard correspondence cannot be extended.

This paper relies heavily on the proof of the Mal'cev and Lazard correspondences given in [13], which uses the free nilpotent associative $\mathbb{Q}$-algebra A of some arbitrary

class c. After some preliminary lemmas in Section 2, we devote Sections 3 and 4 to steps in the proof of the Lazard correspondence and to extensions of these steps. In Section 5, we study a quotient algebra A/I_d of A. The derivation of our main results from properties of A/I_d is analogous to the derivation of the Lazard correspondence from properties of A. Thus, we use Sections 3 and 4 as a basis and as a model for Section 5. Finally, in Section 6, we obtain our main results and some technical results intended for further applications.

Our notation is mainly standard and taken from [9] and [13]. We mention some exceptions and some possibly unfamiliar notation.

Suppose G is a group and H and K are subgroups of G. We write $H \lhd K$ to indicate that H is a normal subgroup of K. For an element x of G, we let x^H be the set of all elements $x^y (= y^{-1}xy)$ as y ranges over H. For elements x and y of G, we let (x, y) be the commutator $x^{-1}y^{-1}xy$. Here we differ from [9] and [13], which denote the commutator by $[x, y]$, because we often need to write $[x, y]$ for the bracket product of x and y given by the Lazard correspondence or by the formula $h_2'(x, y)$ of Remark 5.9.

As in [9] and [13], we use left-normed commutators, so that (x, y, z) denotes $((x, y), z)$ for elements x, y, z in a group G, and likewise for $(x_1, x_2, \ldots, x_n)$. We also let

$$(y, x; 0) = y \quad \text{and} \quad (y, x; n+1) = ((y, x; n), x)$$

for every positive integer n. For a subset T of G, we let

$$(T, x) = \langle (t, x) \mid t \in T \rangle$$

and define subgroups $(T, x; n)$ similarly. We adopt analogous notation for bracket products where a Lie ring is involved.

Now we take some further definitions and notation from [13] (especially pp. 18 and 121–122) that concern mainly infinite groups.

A group G is *torsion-free* if the identity is the only element of finite order in G; it is *divisible* if, for every element h of G and every positive integer n, there exists an nth root of h in G, i.e., an element g in G such that $g^n = h$.

Now suppose G is nilpotent, torsion-free, and divisible, and $h \in G$. Then ([13], Lemma 3.16) for every positive integer n, h has a *unique* nth root in G. A short argument shows that for every rational number r, there exists a unique element g in G such that

$$g^k = h^m, \text{ for all integers } m, k \text{ such that } k \neq 0 \text{ and } m/k = r; \tag{1.2}$$

we denote g by h^r. Moreover, for all r, s in $\mathbb{Q}$,

$$h^{r+s} = h^r h^s \quad \text{and} \quad (h^r)^s = h^{rs}. \tag{1.3}$$

Following [13], p. 18, we call G a $\mathbb{Q}$-*powered group*. If the operation of G is written additively, we usually write $r \cdot h$ or rh for h^r.

Conversely, a $\mathbb{Q}$-powered group must be torsion-free and divisible. Thus, a nilpotent group is $\mathbb{Q}$-powered if and only if it is torsion free and divisible.

Now let π be a set of primes. An integer is said to be a *π-number* if it is a product of powers of primes from π (we regard 1 as a π-number.) A group G is *π-divisible* if, for every π-number k, every element in G has a kth root in G. A group G is *π-torsion-free* if it has no non-identity elements whose orders are π-numbers.

Let $\mathbb{Q}_\pi$ be the ring of all rational numbers whose denominators are π-numbers.

Suppose G is a nilpotent group. If G is π-divisible and π-torsion-free, then Lemma 10.18 of [13] and our argument above show that for every element h of G and every number r in $\mathbb{Q}_\pi$, there exists a unique element g of G (denoted by h^r) such that (1.2) is valid. Moreover, (1.3) is satisfied for all r, s in $\mathbb{Q}_\pi$. Thus, G is a *$\mathbb{Q}_\pi$-powered* group, as defined in [13], pp. 18–19. Since a $\mathbb{Q}_\pi$-powered subgroup is obviously π-torsion-free and π-divisible, we see that a nilpotent group is $\mathbb{Q}_\pi$-powered if and only if it is π-torsion free and π-divisible. In the special case that π consists of all primes, then $\mathbb{Q}_\pi = \mathbb{Q}$, and the properties of being π-divisible and π-torsion-free coincide with the properties of being divisible and torsion-free.

For a subgroup H of a nilpotent group G, the set of all roots in G of elements from H is denoted by

$$_G\sqrt{H} = \{g \in G \mid g^n \in H \text{ for some positive integer } n\}.$$

Likewise, we let

$$_G\sqrt[\pi]{H} = \{g \in G \mid g^n \in H \text{ for some } \pi\text{-number } n\}.$$

If there is no danger of confusion, we may write $\sqrt{H}$ and $\sqrt[\pi]{H}$ for $_G\sqrt{H}$ and $_G\sqrt[\pi]{H}$.

2. $\mathbb{Q}$-powered groups and generalizations

In this section, we prove some preliminary results, mainly about infinite groups.

The following elementary result from ([9], p. 19) will be useful:

Lemma 2.1. *Suppose x and y are elements of a group G and $z = (x, y)$ commutes with both x and y. Then*

$$(x^i, y^j) = z^{ij} \quad \textit{for all integers } i, j.$$

Lemma 2.2. *Let π be a set of primes and H be a subgroup of a nilpotent $\mathbb{Q}_\pi$-powered group G. Assume H has nilpotence class at most c.*

Then $\sqrt[\pi]{H}$ is a $\mathbb{Q}_\pi$-powered subgroup of G of nilpotence class at most c.

Proof. Let $H_\pi = \sqrt[\pi]{H}$. By Theorem 10.19 of [13], H_π is a subgroup of G. Since G is a nilpotent $\mathbb{Q}_\pi$-powered group, H_π is nilpotent and π-torsion-free. Moreover, G is π-divisible and, therefore, H_π is π-divisible. Hence, H_π is a $\mathbb{Q}_\pi$-powered group.

One may use Theorem 10.20 of [13] to show that H_π has class at most c, but we give a short direct proof. Let d be the nilpotence class of H_π. We may assume that $d \geq 1$. Then $\gamma_{d+1}(H_\pi) = 1$ and, by Lemma 3.6 of [13], there exists an iterated commutator

$$h = (h_1, h_2, \ldots, h_d)$$

of elements $h_1, h_2, \ldots, h_d$ of H_π such that $h \neq 1$.

For each $j = 1, 2, \ldots, d$, there exists a π-number $k(j)$ such that $h_j^{k(j)}$ lies in H. Let $k = k(1)k(2)\ldots k(d)$. By Lemma 6.13 of [13],

$$\left(h_1^{k(1)}, h_2^{k(2)}, \ldots, h_d^{k(d)}\right) = (h_1, h_2, \ldots, h_d)^k = h^k.$$

As G is π-torsion-free and $h \neq 1, h^k \neq 1$. Therefore, $\gamma_d(H) > 1$. As H has class at most c, we have $d \leq c$ as desired. □

Lemma 2.3. *Let π be a set of primes and H and K be subgroups of a nilpotent group G. Assume $H \lhd K$. Then*

$$\sqrt[\pi]{H} \lhd \sqrt[\pi]{K}.$$

Proof. This is part of Theorem 10.19 of [13]. □

The remaining results in this section are not necessary for applications to finite groups, except for the easy special cases in which G is finite.

Lemma 2.4. *Suppose H and K are subgroups of a nilpotent group G. Let*

$$L = (H, K) = \langle (x, y) \mid x \in H, y \in K \rangle.$$

(a) *If K is π-divisible and $L \leq Z(G)$, then L is π-divisible.*

(b) *If H and K are both normal in G and π-divisible, then L is normal in G and π-divisible.*

Proof. (a) Here, L is abelian. Take any x in H and y in K, and let k be a π-number. We claim that (x, y) has a kth root in L.

Since K is π-divisible, there exists z in K such that $z^k = y$. Since (x, z) lies in $Z(G)$, Lemma 2.1 yields

$$(x, y) = (x, z^k) = (x, z)^k.$$

Thus, (x, y) has a kth root in L, as claimed. Since L is abelian and is generated by elements of the form (x, y) above, L is π-divisible.

(b) Let $M = \langle H, K\rangle$. Since G is nilpotent, so is M. Let d be the nilpotence class of M, and let

$$1 = Z_0(M) < Z_1(M) < \cdots < Z_d(M) = M$$

be the upper central series of M. Take r minimal such that $L \leq Z_r(M)$. Since $H, K \lhd G$, we have $L \lhd G$ ([9], p. 18).

We prove that L is π-divisible by induction on r. Part (a) handles the case in which r is 0 or 1.

Now assume $r \geq 2$. Then L is not contained in $Z(M)$. Take s minimal such that

$$L \cap Z_s(M) > L \cap Z(M).$$

Then

$$1 < (L \cap Z_s(M), M) \leq L \cap Z_{s-1}(M) = L \cap Z(M).$$

(This shows that $s = 2$, as is well known.) Let

$$L^\star = L \cap Z_s(M) \text{ and } Y = (L^\star, H)(L^\star, K). \tag{2.1}$$

Then $Y \leq L \cap Z(M)$.

Since Y is abelian and $(L^\star, H)$ and $(L^\star, K)$ are π-divisible by (a),

$$Y \text{ is } \pi\text{-divisible.} \tag{2.2}$$

Let $\bar{M} = M/Y$ and let $\bar{X} = XY/Y$ for every subgroup X of M. Since H and K are normal in G and π-divisible, $\bar{H}$ and $\bar{K}$ are normal in $\bar{M}$ and π-divisible. Moreover,

$$\bar{L} = \overline{(H, K)} = (\bar{H}, \bar{K}). \tag{2.3}$$

It is easy to see that $(\bar{L^\star}, \bar{M}) = 1$ (in fact, $Y = (L^\star, M)$). Therefore, by (2.1) and a short argument, we have

$$\bar{L} \leq Z_{r-1}(\bar{M}).$$

By (2.3) and the induction hypothesis,

$$\bar{L} \text{ is } \pi\text{-divisible.} \tag{2.4}$$

Take any element x of L and any π-number k. By (2.4), there exists y in L such that $\bar{y}^k = \bar{x}$. Then xy^{-k} lies in Y. By (2.2), there exists z in Y such that $z^k = xy^{-k}$. Since $Y \leq Z(M)$,

$$x = z^k y^k = (zy)^k.$$

Thus, L is π-divisible, as desired. □

Corollary 2.5. *Suppose G is a π-divisible nilpotent group. Then $\gamma_n(G)$ is π-divisible for every positive integer n.*

Proposition 2.6. *Suppose G is a nilpotent group generated by π-divisible subgroups. Then*

(a) *$Z(G)$ is π-divisible, and*

(b) *G is π-divisible.*

Proof. Let $Z = Z(G)$.

(a) Let $N = \sqrt[\pi]{Z}$. Since $Z \lhd G$, Lemma 2.3 yields

$$N = \sqrt[\pi]{Z} \lhd \sqrt[\pi]{G} = G.$$

Assume $N > Z$. We work toward a contradiction. Since $N \lhd G$ and G is nilpotent,

$$1 < N/Z \lhd G/Z \quad \text{and} \quad 1 < (N/Z) \cap Z(G/Z) = (N \cap Z_2(G))/Z.$$

Take x in $N \cap Z_2(G)$ such that x lies outside Z.

Since $N = \sqrt[\pi]{Z}$, $x^k \in Z$ for some π-number k. Since x lies outside Z, and G is generated by π-divisible subgroups, some π-divisible subgroup H of G does not centralize x. Take y in H such that y does not centralize x. Take z in H such that $z^k = y$.

Since x lies in $Z_2(G)$, the element (x, y) lies in Z. Therefore, by Lemma 2.1,

$$(x, y) = (x, z^k) = (x, z)^k = (x^k, z) = 1,$$

since x^k lies in Z. This contradicts the choice of y. Thus, Z is π-divisible.

(b) We use induction on the nilpotence class of G.

For every π-divisible subgroup H of G, the group HZ/Z is π-divisible. Therefore, by induction,

$$G/Z \text{ is } \pi\text{-divisible.} \tag{2.5}$$

Take any element x in G and any π-number k. By (2.5), there exists y in G such that $y^k \equiv x \pmod{Z}$. Then xy^{-k} lies in Z. By (a), $xy^{-k} = z^k$ for some z in Z. Then

$$x = z^k y^k = (zy)^k.$$

Thus, G is π-divisible. □

3. Group operations on algebras

In this section, we describe some relations among associative algebras, Lie algebras, and groups, taken mainly from [13], Chapters 9–10, that are extended in Sections 4 and 5.

All rings and algebras that we discuss will be associative unless otherwise specified. We use the following conditions:

Hypothesis 3.1. (i) R is a commutative ring with unity element 1.

(ii) B is an algebra over R with unity element (also denoted by 1).

(iii) A is a subalgebra (without unity element) of B over R.

(iv) c is a positive integer.

(v) A is nilpotent of class at most c, i.e., $a_1 a_2 \dots a_{c+1} = 0$ for all $a_1, a_2, \dots, a_{c+1}$ in A.

Suppose u is an element of B in Hypothesis 3.1. We define a mapping $\mathrm{ad}(u)$ on B by $\mathrm{ad}(u)(x) = xu - ux$. If u is in A, then $u^{c+1} = 0$ by condition (v). Assume further that, for some positive integer d,

$$d! \text{ is invertible in } R \text{ and } u^{d+1} = 0. \tag{3.1}$$

Then we may define

$$\mathrm{Exp}(u) = e^u = 1 + u + \frac{u^2}{2!} + \cdots + \frac{u^d}{d!}$$

and

$$\mathrm{Log}(1+u) = u - \frac{u^2}{2} + \cdots + (-1)^{d+1}\frac{u^d}{d}.$$

It is easy to see that $(\mathrm{Exp}(u) - 1)^{d+1} = (\mathrm{Log}(1+u))^{d+1} = 0$. By a proof similar to the usual proof for real numbers (e.g., by a small change in the proof of Proposition 2.1 of [2]), we have:

Lemma 3.2. *Suppose u is in B, d is a positive integer, $d!$ is invertible in R, and $u^{d+1} = 0$. Then*

$$u = \mathrm{Log}(\mathrm{Exp}(u)) \quad \textit{and} \quad 1 + u = \mathrm{Exp}(\mathrm{Log}(1+u)).$$

We sometimes use the following assumption.

Hypothesis 3.1′. (i) Hypothesis 3.1 is satisfied.

(ii) d is a positive integer and $d!$ is invertible in R.

(iii) u is an element of B and $u^i b u^{d+1-i} = 0$ for all b in B and for $i = 1, 2, \dots, d$.

Note that, by (iii) in Hypothesis 3.1′, $u^{d+1} = u1u^d = 0$.

The following result appears as Lemma 4.5.1 in [3].

Lemma 3.3. *Assume Hypothesis* 3.1′. *Let* $\gamma = \mathrm{Exp}(\mathrm{ad}(u))$ *and let* $(\gamma - 1)(x) = \gamma(x) - x$ *for all x in B. Then*

(a) $\mathrm{ad}(u) = \mathrm{Log}\ \gamma$ *and* $(\mathrm{ad}(u))^{d+1} = (\gamma - 1)^{d+1} = 0$,

(b) $\gamma(x) = e^{-u}xe^{u}$, *for all* x *in* B, *and*

(c) $\gamma(e^{x}) = e^{\gamma(x)}$ *whenever* x *is in* B *and* $x^{d+1} = 0$.

Proof. Let E be the ring of all endomorphisms of B as a module over R. Then E is an algebra over R, and E contains the mappings $r(u)$ and $l(u)$ on B given by

$$r(u)(x) = xu, \quad l(u)(x) = ux.$$

Clearly, $\mathrm{ad}(u) = r(u) - l(u)$ and $r(u)l(u) = l(u)r(u)$.

By Hypothesis 3.1′and the Binomial Theorem,

$$r(u)^{d+1} = l(u)^{d+1} = (\mathrm{ad}(u))^{d+1} = 0.$$

Therefore, by Lemma 3.2 (applied to E in place of B), $\mathrm{ad}(u) = \mathrm{Log}(\mathrm{Exp}(\mathrm{ad}(u))) = \mathrm{Log}\ \gamma$.

Since $r(u)l(u) = l(u)r(u)$,

$$\gamma = e^{\mathrm{ad}(u)} = e^{r(u)-l(u)} = e^{-l(u)}e^{r(u)}.$$

Moreover, $\gamma - 1$ is an element of E and since $(r(u)-l(u))^{d+1} = 0$ (by Hypothesis 3.1′ and the Binomial Theorem), $(\gamma - 1)^{d+1} = 0$.

For x in B,

$$e^{r(u)}(x) = \sum_{i=0}^{d} \frac{(r(u))^{i}(x)}{i!} = \sum_{i=0}^{d} \frac{xu^{i}}{i!} = xe^{u},$$

and similarly $e^{-l(u)}(x) = e^{-u}x$ and $\gamma(x) = e^{\mathrm{ad}(u)}(x) = e^{-u}xe^{u}$.

Now suppose $x^{d+1} = 0$. Since γ is conjugation by e^{u}, it is an algebra automorphism, and $(\gamma(x))^{d+1} = 0$.

Then

$$e^{\gamma(x)} = \sum_{i=0}^{d} \frac{(\gamma(x))^{i}}{i!} = \sum_{i=0}^{d} \frac{\gamma(x^{i})}{i!} = \gamma(e^{x}). \qquad \square$$

In B, let $1 + A$ be the subset $\{1 + x \mid x \text{ in } A\}$. For each x in A, the element $1 + x$ has a multiplicative inverse because $x^{c+1} = 0$ and

$$(1 + x)^{-1} = 1 - x + x^{2} - x^{3} + \cdots + (-1)^{c}x^{c}.$$

Now it is easy to see that $1 + A$ is a group under multiplication.

Note that B becomes a Lie algebra B^{-} over R under the bracket multiplication

$$[u, v] = uv - vu,$$

and A becomes a Lie subalgebra A^{-} of B^{-}.

Now suppose also that $c!$ is invertible in R. Then, for every u in A, since $u^{c+1} = 0$, we see that $\mathrm{Exp}(u)$ and $\mathrm{Log}(1+u)$ are well defined. Further, $u = \mathrm{Log}(\mathrm{Exp}(u))$ and $1 + u = \mathrm{Exp}(\mathrm{Log}(1+u))$, by Lemma 3.2. Therefore, the function Exp from A to $1 + A$ is a bijection for which Log is the inverse function. Since $1 + A$ is a group under multiplication, this bijection induces a group operation $\star$ on A, given by

$$\mathrm{Exp}(u \star v) = (\mathrm{Exp}\, u)(\mathrm{Exp}\, v) = e^u e^v, \quad \text{i.e.,}$$
$$u \star v = \mathrm{Log}(e^u e^v).$$

It is easy to see that, under $\star$, 0 is the identity element and the inverse of an element u is $-u$. For each natural number n, the nth power of an element u under $\star$ is the element nu in A.

For a set π of primes, recall that $\mathbb{Q}_\pi$ consists of all rational numbers that can be expressed in the form m/k, where m and k are integers and every prime divisor of k lies in π. For the next result, note that if $c!$ is invertible in R, then A may be regarded as an algebra over the ring $\mathbb{Z}[1/c!]$ obtained by adjoining $1/c!$ to the ring $\mathbb{Z}$ of integers. However, $\mathbb{Z}[1/c!]$ coincides with $\mathbb{Q}_\sigma$ for the set σ of all primes not exceeding c, since $\mathbb{Q}_\sigma$ is obtained from $\mathbb{Z}$ by adjoining $1/p$ for every such prime p.

Theorem 3.4 (Baker–Campbell–Hausdorff (BCH) formula; [13], Theorem 9.11 and Remark 9.17). *Assume Hypothesis* 3.1. *Suppose $c!$ is invertible in R. Let σ be the set of all primes not exceeding c, and regard A as an algebra over $\mathbb{Q}_\sigma$.*

Then, for u and v in A,

$$u \star v \text{ lies in the subalgebra of } A^- \text{ over } R \text{ generated by } u \text{ and } v,$$

and is given by a formula $H(u, v)$ over $\mathbb{Q}_\sigma$ that depends only on c, not on u and v.

The formula in the theorem is given as (9.16) in [13], p. 109; in particular ([4], p. 116), it gives

$$u \star v = u + v + \frac{1}{2}[u, v] + w, \tag{3.2}$$

where w is a linear combination over $\mathbb{Q}_\sigma$ of bracket products of weight at least three in u and v.

Recall that for u and v in B,

$$[v, u; 0] = v \quad \text{and} \quad [v, u; n+1] = [[v, u; n], u]$$

for every positive integer n, and that extended iterated commutators $(v, u; n)$ in a group are defined similarly.

Proposition 3.5. *Assume Hypothesis* 3.1′. *Let*

$$\gamma(x) = e^{-u}xe^{u}, \quad \textit{for all } x \textit{ in } B.$$

Then

(a) $(\mathrm{ad}(u))^{d+1} = (\gamma - 1)^{d+1} = 0, \gamma = \mathrm{Exp}(\mathrm{ad}(u))$ *and* $\mathrm{ad}(u) = \mathrm{Log}\,\gamma$ *and*

(b) *for all* v *in* A,

$$\gamma(v) = v + [v,u] + \cdots + [v,u;d]/d!$$

and

$$[v,u] = (\gamma - 1)(v) - \frac{1}{2}(\gamma - 1)^2(v) + \cdots + (-1)^{d+1}\frac{1}{d}(\gamma - 1)^d(v).$$

Moreover,

(c) *if* $c!$ *is invertible in* R, *then for all* v *in* A,

$$u^{-1} \star v \star u = \gamma(v),$$

where u^{-1} *is the inverse of* u *under* $\star$.

Proof. Lemma 3.3 gives (a), which gives (b).

To prove (c), take v in A and assume $c!$ is invertible in R. Then

$$\begin{aligned} u^{-1} \star v \star u &= u^{-1} \star (v \star u) = (-u) \star \mathrm{Log}(e^v e^u) = \\ &= \mathrm{Log}(e^{-u}\,\mathrm{Exp}(\mathrm{Log}(e^v e^u))) = \mathrm{Log}(e^{-u}e^v e^u) = \\ &= \mathrm{Log}(\gamma(e^v)) = \mathrm{Log}(e^{\gamma(v)}) = \gamma(v), \quad \text{by Lemma 3.3.} \end{aligned}$$

□

Proposition 3.6. *Assume Hypothesis* 3.1′. *Suppose* d *is a positive integer,* $d!$ *is invertible in* R, C *is a subalgebra of* A *that is nilpotent of class at most* d, T *is a Lie subalgebra of* C^-, *and* α *is an automorphism of* T.

For each positive integer i, *let* $(\alpha - 1)^i(T)$ *be the image of the additive group of* T *under the endomorphism* $(\alpha - 1)^i$. *Then:*

(a) C *is a group under* $\star$ *and* T *is a subgroup of* C,

(b) α *is an automorphism of* T *under* $\star$, *and*

(c) *in the semi-direct product of* T *(under* $\star$*) by the cyclic group generated by* α, *the subgroup* $(T, \alpha; i)$ *contains the set* $(\alpha - 1)^i(T)$ *above, for every* i.

Proof. (a) Since $d!$ is invertible in R and C is nilpotent of class at most d, C forms a group under $\star$. The BCH formula (Theorem 3.4) shows that T is closed under $\star$. Since T contains the negatives of its elements, it contains its inverses under $\star$. Therefore, T is a subgroup of C.

(b) This also follows from Theorem 3.4.

(c) This is an extension of Lemma 6.5 of [8], but follows from the proof of that lemma. □

4. The Mal'cev and Lazard correspondences

To prove our main results, we need a variation of the Mal'cev and Lazard correspondences. Here, we present part of Khukhro's exposition of these correspondences (Chapters 9 and 10 of [13], especially Sections 9.1 and 10.1 in pp. 101–104 and 113–121), together with some applications.

Take positive integers c and n such that $n \geq 2$. (We will later choose n to be 2 or 3, depending on our applications.) Let A be a free associative $\mathbb{Q}$-algebra of nilpotency class c with free (non-commuting) generators $x_1, \ldots, x_n$. Then A has a basis consisting of all monomials of the form

$$x_{i_1} x_{i_2} \ldots x_{i_k}, \quad 1 \leq k \leq c,\ 1 \leq i_j \leq n \text{ for } j = 1, 2, \ldots, k.$$

Thus, A is homogeneous: $A = A_1 \oplus \cdots \oplus A_c$, where A_i is the homogeneous component of A of degree i.

The bracket multiplication $[x, y] = xy - yx$ defines the structure of the Lie $\mathbb{Q}$-algebra A^- on the additive group of A; and $x_1, \ldots, x_n$ generate a Lie ring ($\mathbb{Z}$-algebra) L inside A^- and a Lie algebra $\mathbb{Q}L$ over $\mathbb{Q}$. Then L is a free nilpotent Lie ring of class c with free generators x_i (and, $\mathbb{Q}L$ is a similar free nilpotent Lie $\mathbb{Q}$-algebra). Both L and $\mathbb{Q}L$ are homogeneous with components $L_k = L \cap A_k$ and $\mathbb{Q}L_k = \mathbb{Q}L \cap A_k$ and are multihomogeneous with respect to the free generators x_i. Recall that certain Lie products of $x_1, \ldots, x_n$ are called *basic* Lie products. By Theorem 5.39 of [13],

> the additive group of L (respectively, of $\mathbb{Q}L$) has a free $\mathbb{Z}$-basis (respectively, a $\mathbb{Q}$-basis) consisting of the basic Lie products in $x_1, \ldots, x_n$ of weight at most c. (4.1)

We adjoin an outer unity 1 to A to form the associative $\mathbb{Q}$-algebra $B = A_0 \oplus A$, where 1 spans the one-dimensional algebra A_0. Then every ideal of A is an ideal of B and, as in Section 3, the set

$$1 + A = \{1 + a \mid a \in A\}$$

forms a group under multiplication. Moreover, Hypothesis 3.1 is satisfied with $R = \mathbb{Q}$.

Since $c!$ is invertible in $\mathbb{Q}$ and A is nilpotent of class c, Hypothesis 3.1′ is satisfied for every element u of A if we take d to be c. Therefore, we may define $e^u = \mathrm{Exp}(u)$ and $\mathrm{Log}(1+u)$ for every u in A, and the function Exp from A to $1 + A$ is a bijection for which Log is the inverse function. This bijection induces a group operation $\star$ on A, given by

$$u \star v = \mathrm{Log}(e^u e^v)$$

As in [13], let $H(u, v) = u \star v$ for all u, v in A. Since (Theorem 3.4) $H(u, v)$ is a linear combination of u, v, and Lie ring commutators involving u and v with rational

coefficients, $\mathbb{Q}L$ is a subgroup of A under $\star$. For $i = 1, \ldots, n$, let $y_i = e^{x_i} - 1 - x_i$, so that

$$1 + x_i + y_i = e^{x_i} = 1 + x_i + \frac{x_i^2}{2!} + \cdots + \frac{x_i^c}{c!}. \tag{4.2}$$

Then, for each i, y_i is a linear combination of powers of x_i of degree at least 2. Let F be the multiplicative subgroup of $1 + A$ generated by the elements $e^{x_1}, \ldots, e^{x_n}$.

For each positive integer k, let A^k be the sum $A_k \oplus \cdots \oplus A_c$. (Thus $A^k = 0$ if $k > c$.) Note that A^k is an ideal of A and of B. Because we make heavy use of both group commutators and Lie ring commutators, we denote the commutator of two group elements a, b by

$$(a, b) = a^{-1}b^{-1}ab,$$

unlike [13], which uses the notation $[a, b]$ for both group commutators and Lie ring commutators. For any group G and positive integer k, we let $\gamma_k(G)$ be the kth term of the lower central series of G:

$$\gamma_1(G) = G, \quad \text{and} \quad \gamma_{i+1}(G) = (G, \gamma_i(G)) \text{ for } i \geq 1.$$

As in [13], we consider a commutator κ to be an abstract bracket product of variables that may be all taken from a Lie ring or all taken from a group. In the latter case, we interpret each bracket product $[a, b]$ within κ to be a group commutator (a, b). (However, at the end of Section 4 and afterward, we will interpret a bracket product $[a, b]$ of group elements differently.)

Now we quote two important results from [13].

Lemma 4.1 (Special case of Lemma 9.1 in [13]). (a) *Suppose that κ is a commutator of weight k. Then the group commutator $\kappa(e^{x_i})$, the value of κ on the elements e^{x_i} in F, is equal to $1 + \kappa(x_i) + \lambda$, where $\lambda \in A^{k+1}$ and $\kappa(x_i)$ is the corresponding Lie ring commutator, the value of κ on the elements x_i in L.*

(b) *Suppose that $g \equiv \prod_j \kappa_j^{\alpha_j} \pmod{\gamma_{k+1}(F)}$, $\alpha_j \in \mathbb{Z}$, where the $\kappa_j = \kappa_j(e^{x_i})$ are group commutators of weight k in the e^{x_i}. Then $g = 1 + \sum_j \alpha_j \kappa_j(x_i) + \lambda$, where $\lambda \in A^{k+1}$ and the $\kappa_j(x_i)$ are the corresponding Lie ring commutators in the x_i.*

Theorem 4.2 (Special case of Theorem 9.2 of [13]). *The group F is free nilpotent of class c with free generators e^{x_i}.*

It is easy to see that the group A under the operation $\star$ is a nilpotent $\mathbb{Q}$-powered group in which a power u^r is simply the scalar multiple ru. The isomorphism of A under $\star$ onto $1 + A$ under multiplication shows that $1 + A$ is a $\mathbb{Q}$-powered group.

Remark 4.3. Let $F^\star$ be the set of all roots of elements of F in $1 + A$, i.e.,

$$F^\star = \sqrt{F} = \{g \in 1 + A \mid g^n \in F \text{ for some positive integer } n\}.$$

Then ([13]. Theorem 9.19 and Corollary 9.22),

> $F^\star$ is a subgroup of $1 + A$, and is a free nilpotent $\mathbb{Q}$-powered group of class c freely generated by the elements e^{x_i}.

Therefore, for any nilpotent $\mathbb{Q}$-powered group G of class at most c and elements $g_1, \ldots, g_n$ of G, there exists a unique homomorphism of $F^\star$ into G that maps e^{x_i} to g_i for each i.

Recall that L is the Lie subring of A^- generated by $x_1, \ldots, x_n$. Theorem 10.4 of [13] yields:

Proposition 4.4. *We have*

$$F^\star = e^{\mathbb{Q}L} = \{e^u \mid u \text{ in } \mathbb{Q}L\}.$$

Remark 4.5. Now let $f_i = e^{x_i}$ for $i = 1, \ldots, n$. We first consider the case in which $n = 2$. There $F = \langle e^{x_1}, e^{x_2}\rangle = \langle f_1, f_2\rangle$. Since $x_1 + x_2$ and $[x_1, x_2]$ lie in L (and hence in $\mathbb{Q}L$), $e^{x_1+x_2}$ and $e^{[x_1,x_2]}$ lie in $F^\star$. Thus, we may express them as "words" in f_1 and f_2 obtained by taking inverses, products, and rational powers:

$$e^{x_1+x_2} = h_1(f_1, f_2) \quad \text{and} \quad e^{[x_1,x_2]} = h_2(f_1, f_2). \tag{4.3}$$

Now consider any nilpotent $\mathbb{Q}$-powered group G of class at most c. For any elements u and v of G, there exists a unique homomorphism ϕ of $F^\star$ into G such that $\phi(f_1) = u$ and $\phi(f_2) = v$, by Remark 4.3. If we evaluate the "words" h_1 and h_2 on u and v in the natural manner, we see that

$$\begin{aligned} h_1(u, v) &= \phi(e^{x_1+x_2}) = \phi(h_1(f_1, f_2)) \quad \text{and} \\ h_2(u, v) &= \phi(e^{[x_1,x_2]}) = \phi(h_2(f_1, f_2)) \end{aligned} \tag{4.4}$$

This allows us to define operations $\hat{+}$ and $\hat{[\,,\,]}$ on G by

$$u \mathbin{\hat{+}} v = h_1(u, v) \quad \text{and} \quad \hat{[}u, v\hat{]} = h_2(u, v), \qquad \text{for all } u, v \text{ in } G.$$

We also define $r \cdot u$ to be u^r for r in $\mathbb{Q}$ and u in G. Since

$$h_1(f_2, f_1) = e^{x_2+x_1} = e^{x_1+x_2} = h_1(f_1, f_2),$$

we obtain for u, v in G,

$$v \mathbin{\hat{+}} u = h_1(v, u) = \phi(h_1(f_2, f_1)) = \phi(h_1(f_1, f_2)) = h_1(u, v) = u \mathbin{\hat{+}} v.$$

Likewise, as

$$e^{[x_1,x_1]} = e^0 = 1 \text{ and } e^{[x_2,x_1]} = e^{-[x_1,x_2]} = (e^{[x_1,x_2]})^{-1},$$

we obtain $\hat{[}u, u\hat{]} = 1$ and $\hat{[}v, u\hat{]} = (-1) \cdot \hat{[}u, v\hat{]} = \hat{[}u, v\hat{]}^{-1}$.

Similar arguments (some with $n = 2$ and some with $n = 3$) show that, under $\hat{+}$ and $\hat{[\,,\,]}$ and scalar multiplication as above, G becomes a nilpotent Lie algebra L_G over $\mathbb{Q}$ with class at most c ([13], pp. 116–117). In particular, the identity element of G is the zero element of L_G and the inverse of each element u of G is the element $-u = (-1) \cdot u$ of L_G.

Remark 4.5 gives part of the notation and proof for the Mal'cev correspondence, which is proved in full as Theorem 10.11 in pp. 116–118 of [13]:

Theorem 4.6 (Mal'cev correspondence). *Let c be a positive integer. For every nilpotent $\mathbb{Q}$-powered group G of class at most c, the corresponding nilpotent Lie $\mathbb{Q}$-algebra L_G of class at most c is defined on the same underlying set $L_G = G$, with Lie $\mathbb{Q}$-algebra operations*

$$a + b = h_1(a, b), \quad [a, b] = h_2(a, b), \quad ra = a^r$$

for $r \in \mathbb{Q}$.

Conversely, for every nilpotent Lie $\mathbb{Q}$-algebra M of class at most c, the corresponding nilpotent $\mathbb{Q}$-powered group G_M of class at most c is defined on the same underlying set $G_M = M$, with group operations

$$a \cdot b = H(a, b) \quad \textit{and} \quad a^r = ra \ \textit{ for } r \in \mathbb{Q},$$

where $H(a, b)$ is given by the Baker–Campbell–Hausdorff (BCH) formula as in Theorem 3.4.

These transformations are inverses of one another: $L_{G_M} = M$ as Lie $\mathbb{Q}$-algebras (that is, not only sets, but all operations coincide), and, similarly, $G_{L_G} = G$ as $\mathbb{Q}$-powered groups.

(For G as in Theorem 4.6 above, we write $+$ and $[\,,\,]$ for the Lie operations instead of $\hat{+}$ and $\hat{[\,,\,]}$ when there is no danger of confusion.)

Since the ideas in the proof of Theorem 4.6 are used in the proof of the Lazard correspondence and our main results, we have mentioned some of these ideas in Remark 4.5, and we mention some more now.

Returning to the original case in which G is the group $F^\star = e^{\mathbb{Q}L}$ for some n, we obtain ([13], p. 114) for all x, y in $\mathbb{Q}L$,

$$e^x \,\hat{+}\, e^y = e^{x+y} \quad \text{and} \quad \hat{[}e^x, e^y\hat{]} = e^{[x,y]}. \tag{4.5}$$

Since we have defined

$$r \cdot e^x = (e^x)^r = e^{rx} \quad \text{for all } e^x \text{ in } F^\star, \tag{4.6}$$

we see that the Lie $\mathbb{Q}$-algebra $L_{F^\star} = L_{e^{\mathbb{Q}L}}$ on the set $F^\star$ is isomorphic to the original Lie $\mathbb{Q}$-algebra $\mathbb{Q}L$ under the logarithm mapping, which takes e^x to x for each x.

The inverse of the logarithm mapping in the previous paragraph is the exponential bijection that takes each element x of $\mathbb{Q}L$ to the element e^x of $F^\star$. We used the exponential mapping earlier to define the group action $\star$ on A and on $\mathbb{Q}L$:

$$x \star y = H(x, y) = \mathrm{Log}(e^x e^y) \quad (\text{and } \mathrm{Exp}(x \star y) = (\mathrm{Exp}\, x)(\mathrm{Exp}\, y)). \tag{4.7}$$

The definition forces $\mathbb{Q}L$ under $\star$ to be isomorphic to $F^\star$ under multiplication. Similarly, the BCH formula can be applied to define a product $u \star v = H(u, v)$ for elements u, v in any nilpotent $\mathbb{Q}$-algebra M of class at most c. Moreover, take $n = 2$ and recall that $\mathbb{Q}L$ is a free nilpotent Lie $\mathbb{Q}$-algebra of class c with free generators x_1 and x_2. Then for any u, v and M as above, there is a unique Lie $\mathbb{Q}$-algebra homomorphism ϕ that takes x_1 to u and x_2 to v. Clearly,

$$u \star v = H(u, v) = \phi(H(x_1, x_2)).$$

We may show above that under $\star$, M satisfies the associative law and is a nilpotent $\mathbb{Q}$-powered group of class at most c (with u^r in the group equal to $r \cdot u$ in the Lie algebra for r in $\mathbb{Q}$ and u in M) by taking $n = 3$ and using arguments similar to those in the proof above that L_G is a Lie $\mathbb{Q}$-algebra for a suitable group G ([13], p. 178). We denote the set M under the group operation by G_M. Thus, by (4.7),

$$G_{\mathbb{Q}L} \cong F^\star = e^{\mathbb{Q}L}.$$

Now let us consider the special case in which M is $L_{F^\star}$,i.e., the set $F^\star$ considered as a Lie $\mathbb{Q}$-algebra. We saw in (4.5) and (4.6) that for all e^x, e^y in $F^\star$ and r in $\mathbb{Q}$,

$$e^x \mathbin{\hat{+}} e^y = e^{x+y}, \quad \hat{[}e^x, e^y\hat{]} = e^{[x,y]}, \quad \text{and} \quad r \cdot e^x = e^{rx}.$$

Therefore, the mapping $\mathrm{Log} : L\colon F^\star \to \mathbb{Q}L$ is a Lie $\mathbb{Q}$-algebra isomorphism. Hence, for e^x, e^y in $L_{F^\star}$,

$$\mathrm{Log}(e^x \star e^y) = \mathrm{Log}(e^x) \star \mathrm{Log}(e^y) = x \star y = H(x, y) = \mathrm{Log}(e^x e^y),$$

by (4.7), i.e., $e^x \star e^y = e^x e^y$. Thus, $L_{F^\star}$ under $\star$ and $F^\star$ under its usual multiplication are the same set with the same operation: $G_{L_{F^\star}} = F^\star$. This is a special case of the Mal'cev correspondence. In particular, the functions h_1 and h_2 in the formula (4.4) together give an *inversion* of the BCH formula by giving a Lie algebra structure on a group.

The derivation of the Mal'cev correspondence by algebraic means above was obtained by M. Lazard, inspired by Mal'cev's orginal work, which used analytic methods ([14], p. 104). Lazard then extended the Mal'cev correspondence in the following way.

By Theorem 4.2, F is a free nilpotent group of class c with free generators $f_1, \ldots, f_n$. Recall that F is a subgroup of the $\mathbb{Q}$-powered group $F^\star$. For every set of primes π, we define

$$F_\pi = \sqrt[\pi]{F} = \{g \in F^\star \mid g^k \in F \text{ for some } \pi\text{-number } k\}.$$

Note that $F^\star$ is a $\mathbb{Q}_\pi$-powered subgroup. By Lemma 2.2 above and Theorem 10.20 of [13], we obtain:

Theorem 4.7. *Let π be a set of primes. Then F_π is a subgroup of $F^\star$, and is the free nilpotent $\mathbb{Q}_\pi$-powered group of class c freely generated by $f_1, \ldots, f_n$.*

Now let σ be the set of all primes not exceeding c and π be a set of primes containing σ. Because the coefficients in the BCH formula (Theorem 3.4) lie in $\mathbb{Q}_\sigma$ (and hence in $\mathbb{Q}_\pi$), the Lie $\mathbb{Q}_\pi$-algebra $\mathbb{Q}_\pi L$ is closed under the group operation $\star$. By [13], Theorem 10.22,

$$F_\pi = \{e^x \mid x \in \mathbb{Q}_\pi L\}. \tag{4.8}$$

Recall from (4.3)

$$e^{x_1+x_2} = h_1(f_1, f_2) \quad \text{and} \quad e^{[x_1,x_2]} = h_2(f_1, f_2).$$

Since $x_1 + x_2$ and $[x_1, x_2]$ lie in L, hence in $\mathbb{Q}_\pi L$,

$$h_1(f_1, f_2) \text{ and } h_2(f_1, f_2) \text{ lie in } e^{\mathbb{Q}_\pi L}.$$

Now we may apply our previous arguments to $\mathbb{Q}_\pi$-powered groups and Lie algebras over $\mathbb{Q}_\pi$ instead of $\mathbb{Q}$-powered groups and Lie algebras over $\mathbb{Q}$. We obtain (Results 10.11 and 10.13 and p. 124 of [13])

Theorem 4.8 (Lazard correspondence). *Let c be a positive integer and π be a set of primes containing every prime not exceeding c. For every nilpotent $\mathbb{Q}_\pi$-powered group G of class at most c, the corresponding nilpotent Lie $\mathbb{Q}_\pi$-algebra L_G of class at most c is defined on the same underlying set $L_G = G$, with Lie $\mathbb{Q}_\pi$-algebra operations*

$$a + b = h_1(a, b), \quad [a, b] = h_2(a, b), \quad ra = a^r$$

for $r \in \mathbb{Q}_\pi$.

Conversely, for every nilpotent Lie $\mathbb{Q}_\pi$-algebra M of class at most c, the corresponding nilpotent $\mathbb{Q}_\pi$-powered group G_M of class at most c is defined on the same underlying set $G_M = M$, with group operations

$$a \cdot b = H(a, b) \quad \textit{and} \quad a^r = ra \textit{ for } r \in \mathbb{Q}.$$

These transformations are inverses of one another: $L_{G_M} = M$ as Lie $\mathbb{Q}_\pi$-algebras (that is, not only sets, but all operations coincide), and, similarly, $G_{L_G} = G$ as $\mathbb{Q}_\pi$-powered groups.

Corollary 4.9. *Let π be a set of primes containing every prime not exceeding c. Let $A^\star$ be a nilpotent algebra over $\mathbb{Q}_\pi$ of class at most c contained in an algebra $B^\star$ with 1 over $\mathbb{Q}_\pi$. Let $1 + A^\star$ be the set $\{1 + a \mid a \in A^\star\}$. Then*

(a) $1 + A^\star = \{e^a \mid a \in A^\star\}$,

(b) $1 + A^\star$ *is a nilpotent* $\mathbb{Q}_\pi$*-powered group of class at most* c *under multiplication, and*

(c) *for every* a, a' *in* $A^\star$ *and* r *in* $\mathbb{Q}_\pi$,

$$h_1(e^a, e^{a'}) = e^{a+a'}, \quad h_2(e^a, e^{a'}) = e^{aa'-a'a}, \quad \textit{and} \quad (e^a)^r = e^{ra}.$$

Proof. Let $R = \mathbb{Q}_\pi$. Note that Hypothesis 3.1 is satisfied with $A^\star$ and $R1 \oplus A^\star$ in place of A and B. Our discussion after Lemma 3.3 shows that $1 + A^\star$ is a group under multiplication and that (a) is valid.

Let us consider $A^\star$ as a Lie R-algebra under the bracket multiplication given by $[a, a'] = aa' - a'a$. Since $A^\star$ is nilpotent of class at most c, $A^\star$ is a nilpotent Lie R-algebra of class at most c. By the Lazard correspondence, $A^\star$ becomes a nilpotent R-powered group $G_{A^\star}$ of class at most c under the operation $\star$ (given by the BCH-formula), and then for a, a' in $A^\star$ (regarded as elements of the group $G_{A^\star}$) and r in $\mathbb{Q}_0$,

$$h_1(a, a') = a + a', \quad h_2(a, a') = [a, a'] = aa' - a'a, \quad \text{and} \quad a^r = ra. \tag{4.9}$$

By our discussion after Lemma 3.3, the group operation $\star$ is also given by

$$\operatorname{Exp}(a \star b) = (\operatorname{Exp} a)(\operatorname{Exp} b),$$

and the exponential mapping defines a group isomorphism of $A^\star$ under $\star$ onto the group $1 + A^\star$ under its usual multiplication. Therefore, (b) is valid by the previous paragraph, and in the group $1 + A^\star$ under multiplication, (4.9) gives

$$h_1(e^a, e^{a'}) = e^{a+a'}, \quad h_2(e^a, e^{a'}) = e^{aa'-a'a}, \quad \text{and} \quad (e^a)^r = e^{ra},$$

which then gives (c). □

Let S be the set of all basic commutators $\kappa_j = \kappa_j(x, y)$ of weight at least two and at most c in two variables of a group. We order S linearly so that commutators of smaller weight precede those of larger weight. Let σ be the set of primes not exceeding c.

By Lemma 10.12, Remark 10.15, and p. 124 of [13], there exist unique elements r_j and s_j of $\mathbb{Q}_\sigma$ such that, for any elements a, b of a nilpotent $\mathbb{Q}_\sigma$-powered group of class at most c,

$$h_1(a, b) = ab \prod_{\kappa_j \in S} \kappa_j(a, b)^{r_j} \tag{4.10}$$

and

$$h_2(a, b) = \prod_{\kappa_j \in S} \kappa_j(a, b)^{s_j}. \tag{4.11}$$

Note that h_1 and h_2 may be defined by (4.10) and (4.11) for every $\mathbb{Q}_\sigma$-powered group, regardless of whether it is nilpotent. Moreover, by p. 116 of [13], for any positive integer d less than c, the analogous formulas hold with the same exponents, but with the product taken over only those κ_j in S of weight at most d. For such κ_j, the previous paragraph asserts that the exponents r_j and s_j lie in $\mathbb{Q}_\tau$, for τ being the set of primes not exceeding d.

Note that every $\mathbb{Q}_\sigma$-powered group is a $\mathbb{Q}_\tau$-powered group. By the discussion above, we obtain:

Proposition 4.10. *Suppose d is a positive integer less than c. Let σ be the set of primes not exceeding c and τ be the set of primes not exceeding d. Take functions h_1 and h_2 on $\mathbb{Q}_\sigma$-powered groups as above, and let h_1' and h_2' be the analogous functions on $\mathbb{Q}_\tau$-powered groups, where κ_j ranges over only the elements of S of weight at most d.*

Then, for all elements u, v in a $\mathbb{Q}_\sigma$-powered group G,

$$(h_j'(u,v))^{-1}h_j(u,v) \in \gamma_{d+1}(G), \quad \text{for } j = 1,2.$$

Now we obtain a further relation between the group structure and Lie algebra structure.

Proposition 4.11. *Suppose $\pi, A^\star$, and $B^\star$ satisfy the hypothesis of Corollary* 4.9*, and $g \in (1 + A^\star)$, $u = \operatorname{Log} g$, and d is a positive integer. Assume that*

$$d \le c \quad \text{and} \quad u^i b u^{d+1-i} = 0, \text{ for all } b \text{ in } B^\star \text{ and } i = 1, 2, \ldots, d.$$

Define operations $\hat{+}$ and $\hat{[\,,\,]}$ on $1 + A^\star$ and scalar multiplication on $1 + A^\star$ by

$$x \mathbin{\hat{+}} y = h_1(x,y), \quad \hat{[}x,y\hat{]} = h_2(x,y), \quad \text{and} \quad rx = x^r,$$

for $r \in \mathbb{Q}_\pi$.

Define mappings γ and δ on $1 + A^\star$ by

$$\gamma(h) = g^{-1}hg \quad \text{and} \quad \delta(h) = \gamma(h) \mathbin{\hat{+}} (h^{-1}).$$

Define powers of δ by composition.

Then $\delta^{d+1} = 0$ and, for all h in $1 + A^\star$,

$$\hat{[}h, g\hat{]} = \{\delta(h)\}^{e(1)} \mathbin{\hat{+}} \{\delta^2(h)\}^{e(2)} \mathbin{\hat{+}} \cdots \mathbin{\hat{+}} \{\delta^d(h)^d\}^{e(d)},$$

where $e(i) = (-1)^{i+1}/i$, for each i.

Proof. Recall from the proof of Corollary 4.9 that the exponential mapping is a bijection of $A^\star$ into $1 + A^\star$ and that the logarithm mapping is the inverse bijection.

Let $L(h) = \operatorname{Log} h$ for every h in $1 + A^\star$. For all x, y in $A^\star$ and r in $\mathbb{Q}_\pi$, Corollary 4.9 asserts that

$$e^x \hat{+} e^y = e^{x+y}, \quad \hat{[}e^x, e^y\hat{]} = e^{[x,y]}, \quad \text{and} \quad r \cdot e^x = e^{rx}.$$

Therefore, for all g_1, g_2 in $1 + A^\star$ and r in $\mathbb{Q}$,

$$L(g_1 \hat{+} g_2) = L(g_1) + L(g_2), \tag{4.12}$$

$$L(\hat{[}g_1, g_2\hat{]}) = [L(g_1), L(g_2)], \tag{4.13}$$

and

$$L(g_1^r) = rL(g_1) \tag{4.14}$$

Since $u = L(g)$, $g = e^u$. Let $R = \mathbb{Q}_\pi$. Note that Hypothesis 3.1′ is satisfied. Extend the definition of γ to all of B by defining

$$\gamma(b) = g^{-1}bg.$$

Since $c!$ is invertible in R, part (c) of Lemma 3.3 applies with c in place of d. Hence $\gamma(e^x) = e^{\gamma(x)}$ for all x in $A^\star$, and

$$L(\gamma(h)) = \gamma(L(h)), \quad \text{for all } h \text{ in } 1 + A^\star.$$

By (4.12) and (4.14),

$$L(\delta(h)) = L(\gamma(h) \hat{+} h^{-1}) = L(\gamma(h)) + L(h^{-1}) = \gamma(L(h)) - L(h).$$

We have defined δ on $1 + A^\star$. We define δ on the set $A^\star$ (which is disjoint from $1 + A^\star$) by

$$\delta(h) = \gamma(x) - x.$$

Then, for h in $1 + A^\star$,

$$L(\delta(h)) = \gamma(L(h)) - L(h) = \delta(L(h)). \tag{4.15}$$

Since δ is an endomorphism of $A^\star$ under addition, so are its powers under composition, and (4.15) gives

$$L(\delta^i(h)) = \delta^i(L(h)), \quad \text{for all positive integers } i. \tag{4.16}$$

As before, take h in $1 + A^\star$. Let $v = L(h)$. By Proposition 3.5,

$$[v, u] = e(1)\delta(v) + e(2)\delta^2(v) + \cdots + e(d)\delta^d(v).$$

So, by (4.16),

$$[v, u] = e(1)L(\delta(h)) + e(2)L(\delta^2(h)) + \cdots + e(d)L(\delta^d(h)).$$

By (4.12), (4.13), and (4.14), this says

$$\begin{aligned} L(\hat{[}h, g\hat{]}) &= [L(h), L(g)] = [v, u] \\ &= L\big(\{\delta(h)\}^{e(1)}\big) + L\big(\{\delta^2(h)\}^{e(2)}\big) + \cdots + L\big(\{\delta^d(h)\}^{e(d)}\big) \\ &= L\big(\{\delta(h)\}^{e(1)} \mathbin{\hat{+}} \{\delta^2(h)\}^{e(2)} \mathbin{\hat{+}} \cdots \mathbin{\hat{+}} \{\delta^d(h)\}^{e(d)}\big). \end{aligned}$$

Since L is an injective function from $1 + A^\star$ to $A^\star$, this gives the conclusion. □

5. A new definition for the Lie product $[u, v]$

In Section 4, we used the free associative $\mathbb{Q}$-algebra A of nilpotency class c on n generators to construct the free nilpotent $\mathbb{Q}$-powered group $F^\star$ of class c on n generators, and to obtain the operations $+$ and $[\ ,\ ]$ for the Mal'cev correspondence. In a similar way, we used a subgroup F_π of $F^\star$ to obtain the Lazard correspondence. In this section, we define an ideal I_d of A and a normal subgroup K_d of $F^\star$ so that A/I_d, $F^\star/K_d$ and $F_\pi K_d/K_d$ will play similar roles for defining a "word" $h_2'(u, v)$ for u and v in a $\mathbb{Q}_\pi$-powered group (for suitable π). In Section 6, we will show that $h_2'(u, v)$ can be used to extend the definition of the Lie product $[u, v]$ given in the Lazard correspondence to suitable elements in a wider class of groups.

We continue to assume the hypothesis and notation of Section 4. We also let π be an arbitrary set of primes, d be a positive integer such that $d \le c$, and τ be the set of all primes p such that $p \le d$.

Recall that

$$f_i = e^{x_i} = 1 + x_1 + \frac{x_i^2}{2!} + \cdots + \frac{x_i^d}{d!}, \quad \text{for } i = 1, 2, \ldots, n, \tag{5.1}$$

$1 + A$ is a group under multiplication, and F is the subgroup $\langle f_1, f_2, \ldots, f_n\rangle$ of $1 + A$. For each $i = 1, 2, \ldots, n$ and each positive integer k, let

$$N_i = \langle f_i^{\,g} \mid g \in F\rangle = \text{normal closure of } f_i \text{ in } F \tag{5.2}$$

and let C_{ik} be the $\mathbb{Q}$-subgroup of A spanned by all monomials of degree at least k in x_i. It is easy to see that C_{ik} is an ideal of A and of B.

Let I_d be the $\mathbb{Q}$-subspace of A spanned by all the monomials in $x_1, \ldots, x_d$ that have degree at least $d + 1$ in x_i for some i $(1 \le i \le n)$. Thus,

$$I_d = C_{1,d+1} + C_{2,d+1} + \cdots + C_{n,d+1}.$$

Let

$$K_d = \{g \in F^\star \mid g \equiv 1 \pmod{I_d}\}.$$

Lemma 5.1. *Suppose I is an ideal of B contained in A. Let*

$$K_I = \{g \in F^\star \mid g \equiv 1 \pmod{I}\}$$

Then

(a) *K_I is a normal subgroup of $F^\star$, and*

(b) *K_I and $F^\star/K_I$ are $\mathbb{Q}$-powered groups.*

Remark. Note that since B contains a copy of the rational field $\mathbb{Q}$, every ring ideal of B is a $\mathbb{Q}$-algebra ideal of B. By taking $I = I_d$, we obtain $K_d = K_{I_d}$.

Proof. (a) Since I is an ideal of B, there is a canonical algebra homomorphism of B onto B/I that induces a group homomorphism of $F^\star$. Then K_I is the kernel of this homomorphism and is, therefore, a normal subgroup of $F^\star$.

(b) Recall that

> the mapping Log is a group isomorphism of $1 + A$ (under multiplication) onto A under $\star$, and Exp is the inverse isomorphism. (5.3)

From the definition of g^r for a rational number r and an element g of a $\mathbb{Q}$-powered group and from (4.6), we obtain

$$\mathrm{Log}(g^r) = r\,\mathrm{Log}(g), \quad \mathrm{Exp}(rx) = (\mathrm{Exp}(x))^r, \tag{5.4}$$

for g in $1 + A$ and r in $\mathbb{Q}$.

Recall from Proposition 4.4 that $F^\star = e^{\mathbb{Q}L}$. For g in K_I, $\mathrm{Log}(g)$ lies in I because it is a linear combination over $\mathbb{Q}$ of positive powers of $g - 1$. Similarly, for x in $\mathbb{Q}L \cap I$, $\mathrm{Exp}(x)$ lies in K_I because it is a polynomial in x over $\mathbb{Q}$ with constant term 1. Thus, by (5.3),

> the mapping Log induces a group isomorphism of K_I (under multiplication) onto $\mathbb{Q}L \cap I$ under $\star$. (5.5)

Since I is a $\mathbb{Q}$-algebra ideal of B, $\mathbb{Q}L \cap I$ is closed under multiplication from $\mathbb{Q}$. By (5.3), (5.4), and (5.5), $\mathbb{Q}L \cap I$ is a $\mathbb{Q}$-powered group under $\star$ and K_I is a $\mathbb{Q}$-powered group under multiplication.

A similar argument shows that the factor groups $\mathbb{Q}L/(\mathbb{Q}L \cap I)$ under $\star$ and $F^\star/K_I$ (under multiplication) are isomorphic $\mathbb{Q}$-powered groups. □

Suppose $1 \le i \le n$. Recall that $f_i = e^{x_i}$ is a polynomial in x_i with constant term 1, and that, for every k, C_{ik} is an ideal of A and of B.

Lemma 5.2. *Suppose $1 \leq i \leq n$, k is a positive integer, g is an element of the set $1 + C_{ik}$, and f is an element of the set $1 + C_{i1}$. Let*

$$h = (g, f) = g^{-1} f^{-1} g f.$$

Then $h - 1$ lies in $C_{i,k+1}$.

Proof. Let $u = g - 1$, and $v = h - 1$. Then u lies in C_{ik} and

$$fg + fgv = fgh = fgg^{-1} f^{-1} gf = gf.$$

So

$$fgv = gf - fg = f + uf - f - fu = uf - fu = u(f-1) - (f-1)u. \quad (5.6)$$

Since $f - 1$ lies in C_{i1} and u lies in C_{ik}, (5.6) shows that fgv lies in $C_{i,k+1}$. Since $C_{i,k+1}$ is an ideal of B and $v = g^{-1} f^{-1}(fgv)$, it follows that v in $C_{i,k+1}$, as desired. □

Proposition 5.3. *Suppose $1 \leq i \leq n$, k is a positive integer, and g lies in $\gamma_k(N_i)$. Then $g - 1$ lies in C_{ik}.*

Proof. For each positive integer k, let

$$H_k = F \cap K_{C_{ik}} = \{g \in F \mid g - 1 \in C_{ik}\}.$$

By Lemma 5.1, $K_{C_{ik}}$ is a normal subgroup of $F^\star$. Hence H_k is a normal subgroup of F.

We prove the conclusion by induction on k.

By (5.1), f_i lies in H_1. Since N_i is the normal closure of f_i in F (by (5.2)) and H_1 is normal in F, it follows that H_1 contains N_i. This proves the conclusion for $k = 1$.

Now, assume $k \geq 1$ and $\gamma_k(N_i) \leq H_k$. Let $M = H_{k+1}$. Since $N_i \leq H_1$, Lemma 5.2 gives

$$\gamma_{k+1}(N_i) = (\gamma_k(N_i), N_i) \leq H_{k+1}.$$

This proves the result by induction. □

Proposition 5.4. *We have $\gamma_{nd+1}(F^\star) \leq K_d$.*

Proof. Let $b = nd$. Recall that $F^\star / K_d$ is isomorphic to the image of the multiplicative subgroup $F^\star$ of $1 + A$ under the algebra homomorphism of B onto B/I_d. Clearly, each monomial in $x_1, \ldots, x_n$ of degree at least $b+1$ must have degree at least $d + 1$ in x_i for some i, and hence must lie in I_d. Therefore, B/I_d is a homomorphic image of the $\mathbb{Q}$-algebra $\mathbb{Q}1 \oplus \hat{A}$ for the free nilpotent associative algebra $\hat{A}$ of class b

over $\mathbb{Q}$ on n generators $z_1, \ldots, z_n$, with z_i mapping to $x_i + I_d$ for each i. This shows that $F^\star/K_d$ is a homomorphic image of the corresponding multiplicative subgroup

$$\sqrt{\langle e^{z_1}, \ldots, e^{z_n}\rangle}$$

of $1 + \hat{A}$.

By Remark 4.3 with b in place of c, this subgroup has class at most b. Therefore, $F^\star/K_d$ is nilpotent of class at most b, and $\gamma_{b+1}(F^\star/K_d) = 1$. Hence,

$$\gamma_{nd+1}(F^\star) = \gamma_{b+1}(F^\star) \leq K_d,$$

as desired. □

Lemma 5.5. *We have*

(a) $F^\star/K_d$ *is a* $\mathbb{Q}$*-powered group, and*

(b) $F_\pi/(F_\pi \cap K_d)$ *is a* $\mathbb{Q}_\pi$*-powered group.*

Proof. By Theorem 4.7, F_π is a nilpotent $\mathbb{Q}_\pi$-powered, hence π-divisible, group. Therefore,

$$F_\pi/(F_\pi \cap K_d) \text{ is } \pi\text{-divisible.} \tag{5.7}$$

By definition, I_d is an ideal of B contained in A. Therefore, (a) follows from Lemma 5.1. In particular, $F^\star/K_d$ is torsion-free.

Since

$$F_\pi/(F_\pi \cap K_d) \simeq F_\pi K_d/K_d \leq F^\star/K_d,$$

$F_\pi/(F_\pi \cap K_d)$ is also torsion-free and hence π-torsion-free. Therefore, by (5.7), $F_\pi/(F_\pi \cap K_d)$ is $\mathbb{Q}_\pi$-powered. □

Theorem 5.6. *Suppose* $nd \leq c$. *Let*

$$M_0 = \langle \gamma_{d+1}(N_i) \mid i = 1, \ldots, n\rangle$$

and

$$M = {}_{F_\pi}\sqrt[\pi]{M_0} = \{g \in F_\pi \mid g^k \in M_0 \text{ for some } \pi\text{-number } k\}.$$

Then:

(a) M *is a normal subgroup of* F_π,

(b) $M = F_\pi \cap K_d$, *and*

(c) F_π/M *has nilpotence class exactly* nd.

Proof. Recall from Section 4 that A was defined to be the free non-associative $\mathbb{Q}$-algebra of nilpotency class c with free (non-commuting) generators $x_1, \ldots, x_n$. Thus, we can calculate in A by setting every monomial of total degree at least $c+1$ to zero. Since $c+1 \geq nd+1$, each such monomial has degree at least $d+1$ in x_i for some i, and hence lies in I_d. Therefore, up to isomorphism; A/I_d is independent of the choice of c, as long as $c \geq nd$. Moreover,

> the distinct monomials in $x_1, \ldots, x_n$ having degree at most d in x_i for every $i = 1, \ldots, n$ form a basis of A, modulo I_d, i.e., map to a basis of A/I_d in the canonical homomorphism of A onto A/I_d. (5.8)

We defined F_π just before Theorem 4.7 by

$$F_\pi = {}_{F^\star}\sqrt[\pi]{F} = \{g \in F^\star \mid g^k \in F \text{ for some } \pi\text{-number } k\}. \tag{5.9}$$

Let $G = F_\pi$.

(a) For each i, N_i is a normal subgroup of F, and $\gamma_{d+1}(N_i)$ is a characteristic subgroup of N_i and hence a normal subgroup of F. Therefore, M_0 is normal in F. By (5.9) and Lemma 2.3,

$$M = {}_G\sqrt[\pi]{M_0} \lhd_G \sqrt[\pi]{F} = F_\pi = G.$$

(b) By Proposition 5.3, $g-1$ lies in $C_{i,d+1}$ (hence in I_d) for every $i = 1, \ldots, n$ and every element g of $\gamma_{d+1}(N_i)$. Therefore, $M_0 \leq K_d$, and since $M = {}_G\sqrt[\pi]{M_0}$,

$$MK_d/K_d \text{ is a } \pi\text{-group.}$$

However, $F^\star/K_d$ is a $\mathbb{Q}$-powered group by Lemma 5.5, and hence is torsion-free. Consequently,

$$MK_d/K_d = 1, \quad M \leq K_d, \quad \text{and}$$

$$M \text{ is contained in } G \cap K_d. \tag{5.10}$$

We wish to show that $M = G \cap K_d$. We will show first that $F \cap K_d \leq M_0$.

Take any element h of F that lies outside M_0. We must show that h lies outside K_d, i.e., $h \not\equiv 1 \pmod{I_d}$. By Theorem 4.2, F is a free nilpotent group of class c with free generators $f_1, \ldots, f_n$. Therefore, by [10], Theorem 11.2.4, p. 175, h may be uniquely expressed in the form

$$h = c_1^{e_1} c_2^{e_2} \ldots c_r^{e_r},$$

where $c_1, c_2, \ldots, c_r$ are the basic commutators of weight at most c in $f_1, \ldots, f_n$, and $e_1, e_2, \ldots, e_r$ are integers.

Any basic commutator in $f_1, \ldots, f_n$ of weight at least $d+1$ in f_i for some i must lie in $\gamma_{d+1}(N_i)$ and thus in M_0. Therefore,

$$h \equiv \prod_{j \in S} c_j^{e_j}, \quad \text{modulo } M_0, \tag{5.11}$$

where j ranges over the set S of all subscripts for which $e_j \neq 0$ and c_j has weight at most d in f_i for $i = 1, \ldots, n$ (and hence has total weight at most nd). Since h lies outside M_0, the set S is not empty.

Let d' be the minimal total weight of c_j for j ranging over S. Then

$$d' \leq nd \leq c. \tag{5.12}$$

We may assume that the basic commutators c_j in S are numbered so that, for some positive integer k,

> $c_1, \ldots, c_k$ have total weight d', and c_j has total weight greater than d' whenever $j \in S$ and $j > k$.

Then, by (5.11), there exists an element h' in $\gamma_{d'+1}(F)$ such that

$$h \equiv c_1^{e_1} c_2^{e_2} \ldots, c_k^{e_k} h', \quad \text{modulo } M_0.$$

Moreover, $e_j \neq 0$ for every $j = 1, \ldots, k$.

By (5.10), $M_0 \leq M \leq K_d$. So $g \equiv 1 \,(\text{mod } I_d)$ for each element g of M_0. Therefore,

$$h \equiv c_1^{e_1} c_2^{e_2} \ldots c_k^{e_k} h', \quad \text{modulo } I_d. \tag{5.13}$$

For each j, let u_j be the Lie ring commutator in $x_1, \ldots, x_n$ (in A^-) that corresponds to the group commutator c_j in F, so that u_j has weight at most d in x_i for every i and total weight d'. By (5.12) and (4.1), $u_1, \ldots, u_k$ are linearly independent elements of degree d' over $\mathbb{Q}$. By Lemma 4.1,

$$c_1^{e_1} \ldots c_k^{e_k} h' = 1 + \sum_{j=1}^{k} e_j u_j + \lambda, \tag{5.14}$$

where λ lies in $A^{d'+1}$.

By (5.13) and (5.14),

$$h \equiv 1 + \sum_{j=1}^{k} e_j u_j + \lambda, \quad \text{modulo } I_d.$$

However, by (5.8), $u_1, \ldots, u_k$ are linearly independent modulo $(A^{d'+1} + I_d)$. Therefore, $h - 1$ does not lie in I_d, and h does not lie in K_d, as desired. This proves $F \cap K_d \leq M_0$.

Suppose $g \in G \cap K_d = F_\pi \cap K_d$. By (5.9), there exists a π-number k such that $g^k \in F$. Then

$$g^k \in F \cap K_d \leq M_0,$$

and $g \in_{F_\pi} \sqrt[\pi]{M_0} = M$. Thus, $G \cap K_d \leq M$. By (5.10), $G \cap K_d = M$, as desired.

(c) By Proposition 5.4, $\gamma_{nd+1}(G) \leq \gamma_{nd+1}(F^\star) \leq K_d$. Hence, $G/(G \cap K_d) = G/M$ has nilpotence class at most nd. We show that the class is exactly nd by exhibiting a commutator g of weight nd that lies outside M.

Let $g = (c_1, c_2, \ldots, c_{nd})$, where $c_1 = f_2$ and

$$c_2 = c_3 = \cdots = c_{d+1} = f_1, \quad c_{d+2} = c_{d+3} = \cdots = c_{2d} = f_2,$$

and, if $n > 2$,

$$c_{kd+1} = c_{kd+2} = \cdots = c_{(k+1)d} = f_{k+1}, \quad \text{for } k = 2, 3, \ldots, n-1.$$

Then g has weight d in each f_i and total weight nd.

By Lemma 4.1,

$$g = 1 + u + \lambda \quad \text{for } u = [y_1, y_2, \ldots, y_{nd}],$$

where λ lies in A^{nd+1} and we have $y_j = x_i$ whenever $c_j = f_i$. Then u is a $\mathbb{Z}$-linear combination of monomials of degree d in each x_i and total degree nd. By (5.8), these monomials are linearly independent over $\mathbb{Q}$ modulo $(A^{nd+1} + I_d)$. Moreover, it is easy to see that the monomial $x_1^d x_2^d \ldots x_n^d$ appears in u with coefficient ± 1. Therefore, modulo $(A^{nd+1} + I_d)$,

$$u \not\equiv 0 \text{ and } g \equiv 1 + u + \lambda \equiv 1 + u \not\equiv 1.$$

Thus, $g - 1$ does not lie in I_d and g does not lie in K_d, as desired. □

In the next result, we show that $F_\pi/(F_\pi \cap K_d)$ is a "free" group with respect to certain constraints.

Theorem 5.7. *Suppose $nd \leq c$. Assume G is a nilpotent $\mathbb{Q}_\pi$-powered group and $g_1, \ldots, g_n$ lie in G. For each i, assume that the normal closure $\langle g_i^G \rangle$ of g_i in G has nilpotence class at most d. Then*

(a) *there exists a unique homomorphism ψ of F_π into G such that $\psi(f_i) = g_i$ for all i,*

(b) *for ψ as in* (a)*, the kernel of ψ contains $F_\pi \cap K_d$, and*

(c) *for ψ as in* (a)*, the image of ψ is nilpotent of class at most nd.*

Proof. For each i, let $H_i = \langle g_i^G \rangle$, and let $H = H_1 H_2 \dots H_n$. Let

$$H_\pi = {}_G\sqrt[\pi]{H} = \{g \in G \mid g^k \in H \text{ for some } \pi\text{-number } k\}.$$

Since H_i is a normal subgroup of G of class at most d for each i, H is a subgroup of class at most nd (from Fitting's Theorem in [11], p. 276, and induction). By Lemma 2.2, H_π is a $\mathbb{Q}_\pi$-powered subgroup of G of nilpotence class at most nd.

By Theorem 4.7, F_π is the free nilpotent $\mathbb{Q}_\pi$-powered group of class c freely generated by $f_1, \dots, f_n$. Since $nd \le c$, there exists a unique homomorphism ψ of F_π into H_π such that $\psi(f_i) = g_i$ for all i. Furthermore, any homomorphism of F_π into G that takes f_i to g_i for all i must take F into H and then (because $F_\pi = {}_{F^\star}\sqrt[\pi]{F}$ by (5.9)) take F_π into H_π, and so must coincide with ψ. This proves (a).

Let K be the kernel of ψ. It is easy to see that, for each i,

$$\psi(N_i) = \psi(\langle f_i^F \rangle) \le \langle (\psi(f_i))^G \rangle = \langle g_i^G \rangle = H_i$$

and

$$\psi(\gamma_{d+1}(N_i)) = \gamma_{d+1}(\psi(N_i)) \le \gamma_{d+1}(H_i) = 1,$$

whence $\gamma_{d+1}(N_i) \le K$. Take M_0 and M as in Theorem 5.6, so that

$$M_0 = \langle \gamma_{d+1}(N_i) \mid i = 1, \dots, n \rangle$$

and $M = {}_{F_\pi}\sqrt[\pi]{M_0}$. Then

$$M_0 \le K \tag{5.15}$$

and by Theorem 5.6,

$$M = F_\pi \cap K_d \text{ and } F_\pi / M \text{ has nilpotence class } nd. \tag{5.16}$$

From (5.15) and the definition of M, it follows that $M/(M \cap K)$ is a π-group. However,

$$M/(M \cap K) \simeq MK/K \le F_\pi/K \simeq \psi(F_\pi) \le G,$$

and G is π-torsion-free. Therefore, $M/(M \cap K) = 1$, and $M = M \cap K \le K$. This proves (b). Then (b) and (5.16) yield (c). □

Recall that τ is the set of all primes p such that $p \le d$.

Theorem 5.8. *Suppose $nd \le c$ and π contains τ. Let $\bar{B} = B/I_d$ and, for every element x and subset T of B, let*

$$\bar{x} = x + I_d \quad \text{and} \quad \bar{T} = \{\bar{x} \mid x \text{ in } T\}.$$

Define operations $+$ and $[\,,]$ on $\bar{F}^\star$ by the Lazard correspondence. Define a mapping δ on $\bar{F}^\star$ by

$$\delta(x) = (\bar{f}_2^{-1} x \bar{f}_2) + (x^{-1}), \quad \text{for all } x \text{ in } \bar{F}^\star.$$

Let $L = {}_{\bar{F}_\pi}\sqrt[\pi]{\bar{N}_1}$ and $e(i) = (-1)^{i+1}/i$ for $i = 1, \dots, d$. Then:

(a) *L is a $\mathbb{Q}_\pi$-powered normal subgroup of $\overline{F}_\pi$ of class at most d;*

(b) *L is closed under $+$ and $[\,,]$;*

(c) *$\delta^{d+1} = 0$ and L contains $[\bar{f}_1, \bar{f}_2]$ and $(\delta^i(\bar{f}_1))^{e(i)}$ for $i = 1, \ldots, d$;*

(d) *$[\bar{f}_1, \bar{f}_2] = (\delta(\bar{f}_1))^{e(1)} + \cdots + (\delta^d(\bar{f}_1))^{e(d)}$; and*

(e) *$h_2(f_1, f_2)$ is equal to $[f_1, f_2]$ and lies in $F_\pi K_d$.*

Remark. The proof shows that $\overline{F}^\star$ is isomorphic to $F^\star/K_d$, which is a $\mathbb{Q}$-powered group by Lemma 5.5. Therefore, we may use the Lazard (or Mal'cev) correspondence to define operations $+$ and $[\,,]$ on $\overline{F}^\star$. We write $+$ and $[\,,]$ instead of $\hat{+}$ and $\hat{[\,,]}$ (used in Remark 4.5) for $\overline{F}^\star$, and likewise for F, because we will not need the natural Lie ring operations on $\overline{B}$ and B.

Proof. Recall that

$$K_d = \{g \in F^\star \mid g \equiv 1 \pmod{I_d}\}.$$

Therefore, the natural algebra homomorphism ψ of B onto $\overline{B}$ given by $x \mapsto \bar{x}$ induces a group homomorphism of $F^\star$ onto $\overline{F}^\star$ with kernel K_d. Thus, $\overline{F}^\star \simeq F^\star/K_d$.

As mentioned in the Remark above (and Remark 4.3), $\overline{F}^\star$ and $F^\star$ are $\mathbb{Q}$-powered groups and hence admit operations defined by the Lazard correspondence, i.e., for u and v both in $\overline{F}^\star$ or both in $F^\star$,

$$u + v = h_1(u, v) \quad \text{and} \quad [u, v] = h_2(u, v). \tag{5.17}$$

For u and v in $F^\star$, ψ takes the "word" $h_j(u, v)$ to the "word" $h_j(\psi(u), \psi(v))$ for $j = 1, 2$. Thus,

$$\text{for } u \text{ and } v \text{ in } F^\star, \overline{u + v} = \bar{u} + \bar{v} \text{ and } \overline{[u, v]} = [\bar{u}, \bar{v}]. \tag{5.18}$$

Let $G = \overline{F}_\pi$. Then $G \simeq F_\pi K_d/K_d \simeq F_\pi/(F_\pi \cap K_d)$. By Lemma 5.5,

$$G \text{ is a } \mathbb{Q}_\pi\text{-powered group.} \tag{5.19}$$

Recall that $N_1 = \langle f_i^F \rangle$, so that $N_1 \lhd F$. For M_0 and M as in Theorem 5.6, $\gamma_{d+1}(N_1) \le M_0 \le M \le K_d$. Therefore,

$$\bar{N}_1 \lhd \overline{F} \text{ and } \bar{N}_1 \text{ has nilpotence class at most } d. \tag{5.20}$$

Since $F_\pi = {}_{F^\star}\sqrt[\pi]{F}$, we have $G = \overline{F}_\pi = {}_G\sqrt[\pi]{\overline{F}}$. Take L as in the statement of the theorem. By (5.20) and Lemma 2.3,

$$L = {}_G\sqrt[\pi]{\overline{N}_1} \lhd {}_G\sqrt[\pi]{\overline{F}} = G.$$

Then by (5.19), (5.20) and Lemma 2.2, we obtain (a).

By (a) and the Lazard correspondence, we may define $+$ and $[\ ,\ ]$ on L by (5.17). Since we used (5.17) to define $+$ and $[\ ,\ ]$ on the entire group $\overline{F}^\star$, we see that L is closed under $+$ and $[\ ,\ ]$, which gives (b).

Since f_1 lies in N_1, we have $\bar{f}_1 \in \overline{N}_1 \leq \overline{L}$. As L is normal in G and is a $\mathbb{Q}_\pi$-powered group, L is closed under δ and all of its powers, and

$$L \text{ contains } (\delta^i(\bar{f}_1))^{e(i)}, \text{ for } i = 1, 2, \ldots, d. \tag{5.21}$$

Now we check the hypothesis of Proposition 4.11 with π chosen to be the set of all primes; $A^\star$ and $B^\star$ to be $\overline{A}$ and $\overline{B}$; and g and u to be $\bar{f}_2$ and $\bar{x}_2$ respectively. Note that the hypothesis of Corollary 4.9 is satisfied, that $u = \operatorname{Log} g$ because $f_2 = e^{x_2}$, and that $d \leq nd \leq c$. Moreover, for all b in B and $i = 1, \ldots, d$,

$$x_2^i b x_2^{d+1-i} \in C_{2,d+1} \subseteq I_d, \text{ so that } u^i \bar{b} u^{d+1-i} = 0.$$

In addition, the definition of δ on $\overline{F}^\star$ in this theorem agrees with the definition in Proposition 4.11. Thus, the hypothesis of the proposition is satisfied, and the proposition, (5.21), and part (b) of this theorem give parts (c) and (d) of this theorem.

By (5.17), (5.18), and (c),

$$\psi(h_2(f_1, f_2)) = h_2(\bar{f}_1, \bar{f}_2) = [\bar{f}_1, \bar{f}_2],$$

which lies in L and thus in G. Since $G = \overline{F_\pi} \simeq F_\pi K_d / K_d$ and K_d is the kernel of the restriction of ψ to $F^\star$, $h_2(f_1, f_2)$ lies in $F_\pi K_d$. As $h_2(f_1, f_2) = [f_1, f_2]$, we obtain (e). This completes the proof of the theorem. □

Remark 5.9. Let $n = 2$. Assume $2d \leq c$. By Theorem 5.8 for the case in which $\pi = \tau$, there exists an element $h_2'(f_1, f_2)$ of F_τ such that

$$h_2'(f_1, f_2) \equiv h_2(f_1, f_2) \pmod{K_d} \tag{5.22}$$

Here, $h_2'(f_1, f_2)$ is a "word" in f_1 and f_2 obtained by taking inverses, products, and rational powers $g^{m/k}$ for which $k = 1$ or k is a product of powers of primes in τ.

Now suppose π is any set of primes containing τ and G is any nilpotent $\mathbb{Q}_\pi$-powered group. Assume g_1 and g_2 are elements of G contained in (possibly different) normal subgroups of G having nilpotence class at most d. By Theorem 5.7 (for $n = 2$), there exists a unique homomorphism ψ of F_π into G such that

$$\psi(f_1) = g_1, \psi(f_2) = g_2, \text{ and } F_\pi \cap K_d \text{ is contained in the kernel of } \psi. \tag{5.23}$$

Since π contains τ, $h_2'(f_1, f_2) \in F_\tau \leq F_\pi$. If we evaluate the "word" h_2' on g_1 and g_2 by replacing f_i by g_i for each i, we obtain

$$h_2'(g_1, g_2) = \psi(h_2'(f_1, f_2)). \tag{5.24}$$

By (5.22), $h_2(f_1, f_2) = h_2'(f_1, f_2)h_2''(f_1, f_2)$ for an element $h_2''(f_1, f_2)$ in K_d. One may show by a proof similar to that of Theorem 5.6 that $h_2''(f_1, f_2)$ is a product of basic commutators in M_0 (and thus in K_d) raised to rational powers c^r. For each such commutator c, $\psi(c) = 1$ by (5.23). The reason that we use the "word" h_2' rather than h_2 is that the exponents r in the rational powers c^r in h_2'' may have denominators divisible by primes outside π, so that $(\psi(c))^r$ may not be defined.

Now we adopt the bar notation of Theorem 5.8, so that the natural homomorphism of B onto $\overline{B}$ induces an isomorphism $\overline{F_\pi} \simeq F_\pi K_d / K_d$. As $F_\pi \cap K_d$ is contained in the kernel of ψ, it follows that ψ induces a well defined homomorphism ϕ from $\overline{F_\pi}$ to G given by

$$\phi(\bar{x}) = \psi(x), \quad \text{for all } x \text{ in } F_\pi.$$

Let $h = h_2'(f_1, f_2)$. By (5.24) and Theorem 5.8, ϕ is the unique homomorphism of $\overline{F_\pi}$ to G taking $\bar{f}_1$ to g_1 and $\bar{f}_2$ to g_2, and

$$h_2'(g_1, g_2) = \psi(h) = \phi(\bar{h}) = \phi([\bar{f}_1, \bar{f}_2]).$$

Thus, $h_2'(g_1, g_2)$ is independent of the original choice of $h_2'(f_1, f_2)$, and we may define unambiguously

$$\begin{aligned} &h_2'(g_1, g_2) = \phi([\bar{f}_1, \bar{f}_2]) \text{ for the unique homomorphism} \\ &\phi \text{ of } \overline{F_\pi} \text{ into } G \text{ such that } \phi(\bar{f}_1) = g_1, \text{ and } \phi(\bar{f}_2) = g_2. \end{aligned} \tag{5.25}$$

In the next section, we will define $[g_1, g_2]$ to be $h_2'(g_1, g_2)$ in this situation.

Lemma 5.10. *Suppose G is a nilpotent $\mathbb{Q}_\pi$-powered group and N is a normal subgroup of G. Then $\sqrt[\pi]{N}$ is a $\mathbb{Q}_\pi$-powered normal subgroup of G that contains N and has the same nilpotence class as N.*

Proof. Obviously, $\sqrt[\pi]{N}$ contains N and has the same or larger nilpotence class. By Lemma 2.2 (with d in place of c), $\sqrt[\pi]{N}$ is a $\mathbb{Q}_\pi$-powered subgroup of G of the same class as N. By Lemma 2.3,

$$\sqrt[\pi]{N} \lhd \sqrt[\pi]{G} = G. \qquad \square$$

6. The main results

In this section, we obtain our main results. We continue to assume the hypothesis and notation of Section 4, except that after Theorem 6.1 we no longer need the algebras A and B, since we deal only with groups. However, here we take d to be an arbitrary positive integer and choose c to be $3d$. As in Section 5, we let π be an arbitrary set of primes and τ be the set of all primes p such that $p \leq d$.

Theorem 6.1. *The function $h_2'(u, v)$ given in Remark* 5.9 *satisfies the following conditions:*

Suppose π contains τ, G is a nilpotent $\mathbb{Q}_\pi$-powered group, and g_1 and g_2 are elements of G lying in normal subgroups G_1 and G_2 of G having nilpotence class at most d. Let $H = {}_G\sqrt[\pi]{G_1}$. Assume the bar notation of Theorem 5.8 *and let $e(i) = (-1)^{i+1}/i$ for $i = 1, \ldots, d$. Then:*

(a) *for $n = 2$ and ψ as in Theorem* 5.7, *ψ induces a homomorphism of $\overline{F_\pi}$ into G that takes $[\bar{f}_1, \bar{f}_2]$ to $h_2'(g_1, g_2)$,*

(b) $h_2'(g_2, g_1) = (h_2'(g_1, g_2))^{-1}$,

(c) $h_2'(g_1, g_2) = h_2(g_1, g_2) = [g_1, g_2]$, *if G has nilpotence class at most d,*

(d) *H is a $\mathbb{Q}_\pi$-powered normal subgroup of G having nilpotence class at most d,*

(e) *H is endowed with an operation $+$ by the Lazard correspondence,*

(f) *there exists a well-defined endomorphism δ of H under $+$ given by $\delta(x) = (g_2^{-1} x g_2) + (x^{-1})$,*

(g) $\delta^{d+1} = 0$,

(h) *H contains $h_2'(g_1, g_2)$ and $(\delta^i(g_1))^{e(i)}$ for $i = 1, \ldots, d$, and*

(i) $h_2'(g_1, g_2) = (\delta(g_1))^{e(1)} + \cdots + (\delta^d(g_1))^{e(d)}$.

Proof. For every element x and subset T of B, the bar notation of Theorem 5.8 gives

$$\bar{x} = x + I_d \quad \text{and} \quad \overline{T} = \{\bar{x} \mid x \in T\}.$$

Then $\overline{F_\pi} \cong F_\pi K_d / K_d$.

Assume $n = 2$ and take ψ as in Theorem 5.7. By Theorem 5.7 (b), the kernel of ψ contains $F_\pi \cap K_d$. Therefore ψ induces a well-defined homomorphism ϕ from $\overline{F_\pi}$ into G given by

$$\phi(\bar{x}) = \psi(x), \quad \text{for all } x \text{ in } F_\pi.$$

Let $h = h_2'(f_1, f_2)$. By (5.25) (in Remark 5.9),

$$\begin{aligned} &\phi \text{ is the unique homomorphism of } \overline{F_\pi} \text{ taking } \bar{f}_1 \text{ to } g_1 \text{ and} \\ &\bar{f}_2 \text{ to } g_2, \text{ and } h_2'(g_1, g_2) = \psi(h) = \phi(\bar{h}) = \phi([\bar{f}_1, \bar{f}_2]). \end{aligned} \tag{6.1}$$

This proves (a) and shows that, for g_1 and g_2 as in the hypothesis, $h_2'(g_1, g_2)$ is independent of the original choice of $h_2'(f_1, f_2)$.

Since the roles of f_1 and f_2 are symmetric, as are those of g_1 and g_2, we have

$$h_2'(g_2, g_1) = \psi([\bar{f}_2, \bar{f}_1])$$

because by (6.1), ϕ is the unique homomorphism of $\overline{F_\pi}$ taking $\bar{f}_2$ to g_2 and $\bar{f}_1$ to g_1.

However, $[\bar{f}_2, \bar{f}_1]$ and $[\bar{f}_1, \bar{f}_2]$ are negatives of each other as Lie ring elements of $\overline{F^\star}$. Therefore, by (6.1),

$$h_2'(g_1, g_2) = \phi([\bar{f}_1, \bar{f}_2]) = \phi([\bar{f}_2, \bar{f}_1]^{-1}) = \phi([\bar{f}_2, \bar{f}_1])^{-1} = (h_2'(g_2, g_1))^{-1}.$$

This proves (b).

By Lemma 5.10 we obtain (d). Then (e) follows from the Lazard correspondence.

Since H is a normal subgroup of G, it is closed under conjugation and under inverses. Hence, (f) follows from (e) and (g) follows from Theorem 5.8 (c).

Now consider the subgroup L of $\overline{F_\pi}$ given in Theorem 5.8; recall that

$$N_1 = \langle f_1^x \mid x \in F \rangle \leq F \leq F_\pi$$

and $L = {}_{F_\pi}\sqrt[\pi]{\bar{N}_1}$. Then

$$\phi(\bar{N}_1) = \langle (\phi(\bar{f}_1))^{\phi(y)} \mid y \in \bar{F} \rangle \leq \langle g_1^z \mid z \in G \rangle \leq G_1$$

and

$$\phi(L) \leq_G \sqrt[\pi]{G_1} = H \tag{6.2}$$

Let D be the mapping on $\overline{F^\star}$ that was denoted by δ in Theorem 5.8:

$$D(x) = (\bar{f}_2^{-1} x \bar{f}_2) + (x^{-1}) \quad \text{for all } x \text{ in } \overline{F^\star}.$$

Recall that $\bar{f}_2$ lies in $\overline{F_\pi}$ and $\phi(\bar{f}_2) = g_2$. As L is a $\mathbb{Q}_\pi$-powered normal subgroup of $\overline{F_\pi}$ of class at most d, addition on L is given by the Lazard correspondence by

$$x + y = h_1(x, y),$$

and L is closed under conjugation and under D, and under taking powers in $\mathbb{Q}_\pi$; likewise for H, with g_2 and δ in place of $\bar{f}_2$ and D. Thus, by (6.2),

$$\phi(x + y) = \phi(h_1(x, y)) = h_1(\phi(x), \phi(y)) = \phi(x) + \phi(y).$$

for all x, y in L. Similarly, for all x in L,

$$\begin{aligned} \phi(D(x)) &= \phi(\bar{f}_2^{-1} x \bar{f}_2) + \phi(x^{-1}) = \phi(\bar{f}_2)^{-1} \phi(x) \phi(\bar{f}_2) + \phi(x)^{-1} \\ &= (g_2^{-1} \phi(x) g_2) + \phi(x)^{-1} = \delta(\phi(x)). \end{aligned} \tag{6.3}$$

By Theorem 5.8, L contains $[\bar{f}_1, \bar{f}_2]$ and $(D^i(\bar{f}_1))^{e(i)}$, for $i = 1, \ldots, d$, and

$$[\bar{f}_1, \bar{f}_2] = (D^1(\bar{f}_1))^{e(1)} + \cdots + (D^d(\bar{f}_1))^{e(d)}. \tag{6.4}$$

Clearly, $\phi(x^r) = (\phi(x))^r$ for all x in L and r in $\mathbb{Q}_\pi$. Therefore, by (6.3),

$$\phi((D^i(\bar{f}_1))^{e(i)}) = (\delta^i(\phi(\bar{f}_1)))^{e(i)} = (\delta^i(g_1))^{e(i)}, \quad \text{for } i = 1, \ldots, d.$$

Now (h) and (i) follow from (6.1), (6.2), (6.4), and Theorem 5.8 (c).

To prove part (c), suppose G has nilpotence class at most d. Then we may define $+$ and $[\,,]$ on G by the functions h_1 and h_2 in Lazard's correspondence, and (6.1) gives

$$\begin{aligned} h_2'(g_1, g_2) &= \phi([\bar{f}_1, \bar{f}_2]) = \phi(h_2(\bar{f}_1, \bar{f}_2)) = h_2(\phi(\bar{f}_1), \phi(\bar{f}_2)) \\ &= h_2(g_1, g_2) = [g_1, g_2]. \end{aligned}$$ □

Corollary 6.2. *Suppose π contains τ and G is a nilpotent $\mathbb{Q}_\pi$-powered subgroup of class at most d. Define operations $+$ and $[\,,]$ on G as in the Lazard correspondence.*

Take v in G and define a mapping δ on G by

$$\delta(u) = (v^{-1}uv) + (u^{-1}), \quad \textit{for every } u \textit{ in } G.$$

Define powers of δ by composition. Let $e(i) = (-1)^{i+1}/i$ for $i = 1, 2, \ldots, d$.

Then $\delta^{d+1} = 0$ and, for every u in G,

$$[u, v] = (\delta(u))^{e(1)} + (\delta^2(u))^{e(2)} + \cdots + (\delta^d(u))^{e(d)}.$$

Remark 6.3. This corollary shows that the formula for $h_2'(g_1, g_2)$ in part (i) of Theorem 6.1 also gives $[g_1, g_2]$ in the situation of the Lazard correspondence. Thus, Lazard's definition of bracket multiplication in G is determined by conjugation in G and Lazard's definition of addition in G. For this reason, we often denote $h_2'(g_1, g_2)$ by $[g_1, g_2]$ in the situation of Theorem 6.1.

Recall from Section 1 that we have defined iterated commutators in groups and Lie rings to be left normed, i.e. for $r \geq 2$,

$$(x_1, x_2, \ldots, x_r, x_{r+1}) = ((x_1, x_2, \ldots, x_r), x_{r+1})$$

and

$$[x_1, x_2, \ldots, x_r, x_{r+1}] = [[x_1, x_2, \ldots, x_r], x_{r+1}].$$

Theorem 6.4. *Suppose π contains τ, G is a nilpotent $\mathbb{Q}_\pi$-powered group, and G_1, G_2 and G_3 are normal subgroups of G that have nilpotence class at most d. Define $+$ on every $\mathbb{Q}_\pi$-powered normal subgroup of G of class at most d by the Lazard correspondence. Define $[x, y]$ as in Remark 6.3 whenever x and y lie in normal subgroups of G having nilpotence class at most d.*

Take u in G_1 and v in G_2. Then G satisfies the following conditions (and all terms in the conditions are well defined):

(a) *For u' in G_1 and r in $\mathbb{Q}_\pi$,*

$$[ru, v] = r[u, v], \quad [u + u', v] = [u, v] + [u', v]$$

and

$$[[u, u'], v] = [[u, v], u'] + [u, [u', v]].$$

(b) *For w in G_3,*

$$[u, v, w] + [v, w, u] + [w, u, v] = 1.$$

(c) *If G_1 and G_2 are $\mathbb{Q}_\pi$-powered, then $[u, v] \equiv (u, v)$, modulo (G_1, G_2, G_1G_2), and $[u, v] \in (G_1, G_2)$.*

Remark. For (b), recall that the identity element of G is the zero element of any subgroup of G that forms a Lie algebra under the Lazard correspondence.

Proof. Take u' and w in G as in (a) and (b). As in Theorem 6.1, let $H = {}_G\sqrt[\pi]{G_1}$.

By Theorem 6.1, H is a $\mathbb{Q}_\pi$-powered normal subgroup of G of class at most d (so that we may define $+$ and scalar multiplication from $\mathbb{Q}_\pi$ on H), and $[x, y]$ $(= h_2'(x, y))$ is well defined and lies in H whenever x lies in G_1 (or H) and y lies in a normal subgroup of G of class at most d (e.g., G_2 or G_3). This shows that the elements

$$u + u', \quad [u, v], \quad [u', v], \quad \text{and} \quad [w, u]$$

are well defined and lie in H , as do the elements $[u + u', v]$ and $[u, v, w]$ and $[w, u, v]$.

By the symmetry of G_1, G_2 and G_3, the element $[v, w]$ is well defined and lies in a $\mathbb{Q}_\pi$-powered normal subgroup of G of class at most d. Therefore, $[v, w, u]$ is well defined and lies in H.

Recall that for x in H and r in $\mathbb{Q}_\pi$, the group power h^r coincides with the scalar product $r \cdot h$ for H considered as a $\mathbb{Q}_\pi$-module. Therefore, for g_1 in G_1 and g_2 in G_2 and δ as in Theorem 6.1, part (i) of Theorem 6.1 gives

$$[g_1, g_2] = h_2'(g_1, g_2) = e(1)\delta(g_1) + \cdots + e(d)\delta^d(g_1).$$

Since δ is an endomorphism of H under $+$, this shows that the mapping on H given by $x \mapsto [x, v]$ is a $\mathbb{Q}_\pi$-module endomorphism of H. In particular,

$$[ru, v] = r[u, v] \quad \text{and} \quad [u + u', v] = [u, v] + [u', v]. \tag{6.5}$$

Next we prove (b). The proof is similar to the proof of the corresponding statement (i.e., the Jacobi identity) for the Lazard correspondence, which we summarized in Remark 4.5. We assume $n = 3$ and adopt the notation of Theorem 5.8. It is easy to see that the group L in Theorem 5.8 contains $[f_i, f_j, f_k]$ whenever $\{i, j, k\} = \{1, 2, 3\}$, and satisfies

$$[f_1, f_2, f_3] + [f_2, f_3, f_1] + [f_3, f_1, f_2] = 1. \tag{6.6}$$

By Theorem 5.7, there exists a unique homomorphism ψ of F_π into G such that

$$\psi(f_1) = u, \quad \psi(f_2) = v, \quad \text{and} \quad \psi(f_3) = w,$$

and $F_\pi \cap K_d$ is contained in the kernel of ψ. Therefore, ψ induces an homomorphism ϕ of $\bar{F}_\pi$ into G such that

$$\phi(\bar{f}_1) = u, \quad \phi(\bar{f}_2) = v, \quad \text{and} \quad \phi(\bar{f}_3) = w.$$

By (5.25) (in Remark 5.9) and its proof, we have whenever $\{i, j, k\} = \{1, 2, 3\}$,

$$\phi([f_i, f_j, f_k]) = [\phi([f_i, f_j]), \phi(f_k)] = [\phi(f_i), \phi(f_j), \phi(f_k)].$$

Therefore, (6.6) yields (b).

By (b) and Theorem 6.1 (b),

$$[u, v, w] + [u, [w, v]] = [u, w, v].$$

By considering the special case in which $G_3 = G_1$ and $w = u'$, we obtain

$$[u, u', v] = [u, v, u'] + [u, [u', v]]$$

This and (6.5) yield (a).

To prove (c), assume G_1 and G_2 are $\mathbb{Q}_\pi$-powered. Then $H = {}_G\sqrt[\pi]{G_1} = G_1$. We apply Theorem 6.1 with $g_1 = u$ and $g_2 = v$, so that

$$\delta(x) = (v^{-1}xv) + (x^{-1}) = (x^{-1}) + (v^{-1}xv), \quad \text{for all } x \in G_1. \tag{6.7}$$

Let $L = (G_1, G_2)$ and $M = (L, G_1G_2)$. Since $G_1, G_2 \lhd G$, we have $L, M \lhd G$ and $M \le L \le G_1 \cap G_2$. Moreover, by Lemma 2.4 and Proposition 2.6,

$$L \text{ and } M \text{ are } \pi\text{-divisible.} \tag{6.8}$$

Let $\bar{G} = G/M$ and let $\bar{X} = XM/M$ and $\bar{g} = gM$ for every subgroup X and element g of G. Since $M = (L, G_1G_2)$,

$$\bar{L} \le Z(\bar{G}_1\bar{G}_2). \tag{6.9}$$

Now take an element x in G_1. Let $x' = v^{-1}xv$. Then $(x, v) \in L$ and $x(x, v) = xx^{-1}v^{-1}xv = x'$. Hence,

$$(\bar{x}, \bar{v}) \in \bar{L} \le Z(\bar{G}_1\bar{G}_2) \quad \text{and} \quad \bar{x}(\bar{x}, \bar{v}) = \bar{x'}. \tag{6.10}$$

Therefore, the elements $\bar{x}$ and $\bar{x}'$ commute. By (6.8), L and M are both π-divisible, which forces $\bar{L}$ to be $\mathbb{Q}_\pi$-powered. Thus, by (6.7), (6.10), and (4.10),

$$\overline{\delta(x)} = \overline{(x^{-1}) + x'} = \overline{x^{-1}} + \overline{x'} = \overline{(x^{-1})}\,\overline{x'} = \overline{x^{-1}x'} = \overline{(x, v)}.$$

Similarly, by (6.7) and (6.9), $\overline{\delta(x)} = 1$ for all x in L. Therefore, $\overline{\delta^i(x)} = 1$ for all $i \ge 2$. By Theorem 6.1,

$$\overline{[x, v]} = \overline{\delta(x)} = \overline{(x, v)}.$$

By taking $x = u$, we obtain (c). □

Corollary 6.5. *Assume the hypothesis and notation of Theorem* 6.4.

(a) *Suppose* $u \in \gamma_i(G)$ *and* $v \in \gamma_j(G)$ *for some positive integers* i, j. *Then*

$$[u, v] \in \gamma_{i+j}(G) \quad \textit{and} \quad [u, v] \equiv (u, v) \pmod{\gamma_{i+j+1}(G)}.$$

(b) *Suppose* $u_i \in \gamma_{k_i}(G)$ *for* $i = 1, \ldots, r$ *and some positive integers* k_i. *Let* $k = k_1 + \cdots + k_r$. *Then*

$$[u_1, u_2, \ldots u_r] \in \gamma_k(G) \quad \textit{and}$$
$$[u_1, u_2, \ldots u_r] \equiv (u_1, u_2, \ldots u_r) \pmod{\gamma_{k+1}(G)}.$$

Proof. (a) By Corollary 2.5, $\gamma_k(G)$ is $\mathbb{Q}_\pi$-powered for every positive integer k. By Corollary 3.5 of [13],

$$(\gamma_i(G), \gamma_j(G), \gamma_i(G)\gamma_j(G)) \leq \gamma_{i+j+1}(G) \text{ and } (u, v) \text{ lies in } \gamma_{i+j}(G).$$

Then $[u, v] \equiv (u, v) \pmod{\gamma_{i+j+1}(G)}$ by part (c) of Theorem 6.4. Therefore, $[u, v]$ lies in $\gamma_{i+j}(G)$.

(b) We use induction on r. The result is trivial for $r = 1$, and follows immediately from (a) for $r = 2$.

Now assume $r \geq 3$ and the result is true for $r - 1$. Let

$$u' = [u_1, \ldots u_{r-1}], \quad u'' = (u_1, \ldots u_{r-1}), \quad \text{and} \quad k' = k_1 + k_2 + \cdots + k_{r-1}.$$

Then $k = k' + k_r$. By induction,

$$u' \in \gamma_{k'}(G) \quad \text{and} \quad u' \equiv u'' \pmod{\gamma_{k'+1}(G)}. \tag{6.11}$$

By (a), $[u', u_r] \equiv (u', u_r) \pmod{\gamma_{k+1}(G)}$. By (6.11) and Theorem 6.2 of [13],

$$(u', u_r) \equiv (u'', u_r) \pmod{\gamma_{k+1}(G)}.$$

Therefore, $[u', u_r] \equiv (u'', u_r) \pmod{\gamma_{k+1}(G)}$, as desired. □

Theorem 6.6. *Assume* π *is a set of primes containing* τ, G *is a nilpotent* $\mathbb{Q}_\pi$*-powered group,* $\mathcal{N}$ *is the set of all* $\mathbb{Q}_\pi$*-powered normal subgroups of* G *of nilpotence class at most* d, *and* $\mathcal{S}$ *is a subset of* $\mathcal{N}$. *Let* $U(\mathcal{N})$ *and* $U(\mathcal{S})$ *be the set-theoretic unions of the elements of* $\mathcal{N}$ *and of the elements of* S.

For each N *in* $\mathcal{N}$, *define* $+$ *on* N *by the Lazard correspondence. For each* u, v *in* $U(\mathcal{N})$, *define* $[u, v]$ *as in Remark* 6.3. *Let* $E(\mathcal{S})$ *be the set of all mappings* ϕ *on* $U(\mathcal{S})$ *such that, for each* N *in* S,

ϕ *maps* N *into* N *and induces an endomorphism of* N *under* $+$.

Define addition and multiplication on $E(\mathcal{S})$ *by*

$$(\phi + \phi')(x) = \phi(x) + \phi'(x) \quad \textit{and} \quad \phi\phi'(x) = \phi(\phi'(x)).$$

For each v in $U(\mathcal{N})$, define a mapping $\operatorname{ad} v$ *on* $U(\mathcal{S})$ *by*

$$(\operatorname{ad} v)(u) = [u, v].$$

Then

(a) *$E(\mathcal{S})$ forms an associative algebra over $\mathbb{Q}_\pi$, and also forms a Lie algebra $E(\mathcal{S})^-$ over $\mathbb{Q}_\pi$ under the bracket multiplication given by*

$$[\phi, \phi'] = \phi\phi' - \phi'\phi;$$

(b) *for each v in $U(\mathcal{N})$ and r in $\mathbb{Q}_\pi$,*

$$\operatorname{ad} v \text{ lies in } E(\mathcal{S}) \text{ and } \operatorname{ad}(rv) = r(\operatorname{ad} v);$$

(c) *for each N in $\mathcal{N}$ and each v, w in N,*

$$\operatorname{ad}(v + w) = \operatorname{ad} v + \operatorname{ad} w;$$

(d) *for v, w in $U(\mathcal{N})$,*

$$[\operatorname{ad} v, \operatorname{ad} w] = \operatorname{ad}[w, v] = -\operatorname{ad}[v, w];$$

(e) *the additive subgroup $L(\mathcal{S})$ of $E(\mathcal{S})$ spanned by the mappings* $\operatorname{ad} v$ *for v in $U(\mathcal{S})$ is a Lie $\mathbb{Q}_\pi$-subalgebra of $E(\mathcal{S})^-$; and*

(f) *for $L(\mathcal{S})$ as in* (e)*, each element ϕ of $L(\mathcal{S})$ satisfies*

$$\phi([u, v]) = [\phi(u), v] + [u, \phi(v)], \quad \text{for every } u, v \text{ in } U(S).$$

Remark. Part (a) of Theorem 6.4 shows that, for each v in $U(\mathcal{N})$ and N in $\mathcal{N}$, $\operatorname{ad} v$ induces a derivation of N, for N regarded as a Lie algebra over $\mathbb{Q}_\pi$ by Lazard's correspondence. Part (f) of this theorem extends this.

Proof. Note that, by Theorem 6.1 (b),

$$[v, u] = [v, u]^{-1} = -[u, v], \quad \text{for all } u, v \text{ in } U(\mathcal{S}). \tag{6.12}$$

(a) This follows directly from the definitions of addition, multiplication, bracket multiplication, and scalar multiplication from $\mathbb{Q}_\pi$.

(b) This follows from Theorem 6.4.

(c) Take v and w as in (c) and u in $U(\mathcal{S})$. By (b) and (6.12),

$$[u, v + w] = -[v + w, u] = -[v, u] - [w, u] = [u, v] + [u, w],$$

as desired.

(d) Take u in $U(\mathcal{S})$ and v, w in $U(\mathcal{N})$. Then

$$\begin{aligned}
[\operatorname{ad} v, \operatorname{ad} w](u) &= (\operatorname{ad} v)(\operatorname{ad} w)(u) - (\operatorname{ad} w)(\operatorname{ad} v)(u) \\
&= [[u, w], v] - [[u, v], w] \\
&= -[[w, u], v] - [[u, v], w] \qquad \text{by (6.12)}
\end{aligned}$$

$$= [[v, w], u] \qquad \text{by Theorem 6.4}$$
$$= -[u, [v, w]] = [u, [w, v]] \qquad \text{by (6.12).}$$

(e) This follows from (d) and (b).

(f) First, consider the case in which $\phi = \operatorname{ad} w$ for some w in $U(\mathcal{S})$: by (6.12) and Theorem 6.4,

$$[\phi(u), v] + [u, \phi(v)] = [[u, w], v] + [[u, v], w]$$
$$= -[[w, u], v] - [[v, w], u] = [[u, v], w] = \phi([u, v]).$$

Since this is a linear condition on ϕ, it remains valid for all the elements in the linear span $L(\mathcal{S})$ of all the mappings $\operatorname{ad} w$. □

Theorem 6.7. *Assume the hypothesis and notation of Theorem* 6.6. *Let $G^\star$ be the subgroup of G generated by $\mathcal{S}$ and k be the nilpotence class of $G^\star$. Then:*

(a) *each normal subgroup of G of nilpotence class at most d is contained in some normal $\mathbb{Q}_\pi$-powered subgroup of nilpotence class at most d;*

(b) *$G^\star$ is a normal $\mathbb{Q}_\pi$-powered subgroup of G;*

(c) *for every $v_1, \ldots, v_k$ in $U(\mathcal{S})$,*

$$(\operatorname{ad} v_1)(\operatorname{ad} v_2) \ldots (\operatorname{ad} v_k) = 0;$$

(d) *for v in $U(\mathcal{N})$, $(\operatorname{ad} v)^{d+1} = 0$;*

(e) *the Lie $\mathbb{Q}_\pi$-algebra $L(\mathcal{S})$ is nilpotent of class at most $k - 1$.*

Proof. (a) Apply Lemma 5.10.

(b) Each element of $\mathcal{S}$ is a normal $\mathbb{Q}_\pi$-powered subgroup of G. Therefore, $G^\star \lhd G$, and $G^\star$ is π-divisible by Proposition 2.6. Since $G^\star$ is nilpotent and G (and hence $G^\star$) are π-torsion-free, $G^\star$ is $\mathbb{Q}_\pi$-powered.

(c) Take $u, v_1, v_2, \ldots, v_k$ in $U(\mathcal{S})$. Let

$$w = (\operatorname{ad} v_1)(\operatorname{ad} v_2) \ldots, (\operatorname{ad} v_k)(u) = [u, v_k, v_{k-1}, \ldots, v_1].$$

By Corollary 6.5 applied to $G^\star$ in place of G, we have $w \in \gamma_{k+1}(G^\star) = 1$.

(d) Take u and v in $U(\mathcal{N})$. Take v lies in some element N of $\mathcal{N}$. By Theorem 6.4 and induction,

$$(\operatorname{ad} v)^i(u) \in \gamma_i(N), \quad \text{for every natural number } i.$$

Therefore,

$$(\operatorname{ad} v)^{d+1}(u) \in \gamma_{d+1}(N) = 1.$$

(e) Since $L(\mathcal{S})$ is spanned by the mappings $\operatorname{ad} v$ for all v in $U(\mathcal{S})$, every Lie commutator in $L(\mathcal{S})$ of weight at least k is zero, by (c) and the definition of bracket multiplication in $E(\mathcal{S})^-$. □

Lemma 6.8. *Assume the hypothesis and notation of Theorem* 6.6. *Let $G^\star$ be the subgroup of G generated by $\mathcal{S}$ and H be a subgroup of $G^\star$ generated by a subset T of $U(\mathcal{S})$. Let d' be the nilpotence class of $H/(H \cap Z(G^\star))$.*

Then d' is the nilpotence class of the Lie $\mathbb{Q}_\pi$-subalgebra $L^\star(T)$ of $L(\mathcal{S})$ generated by the elements ad x *for all x in T.*

Proof. Here,

$$Z(G^\star) \text{ contains } \gamma_{d'+1}(H), \text{ but not } \gamma_{d'}(H). \tag{6.13}$$

Take any positive integer r and any elements $x_1, \ldots, x_r$ of T. By Corollary 6.5,

$$[x_1, \ldots, x_r] \equiv (x_1, \ldots, x_r) \pmod{\gamma_{r+1}(H)}. \tag{6.14}$$

By Theorem 6.6 (d) and induction,

$$[\operatorname{ad} x_1, \ldots, \operatorname{ad} x_r] = (-1)^r \operatorname{ad}[x_1, x_2 \ldots, x_r]. \tag{6.15}$$

First, consider the case in which $r = d'+1$. Then, for any choice of $x_1, \ldots, x_{d'+1}$, we see from (6.13), (6.14), and (6.15) that

$$[x_1, \ldots x_{d'+1}] \in H \cap Z(G^\star) \quad \text{and} \quad [\operatorname{ad} x_1, \ldots, \operatorname{ad} x_{d'+1}] = 0.$$

Next, consider the case in which $r = d'$. By (6.13) and Theorem 3.12 of [13] applied to $H/(H \cap Z(G^\star))$, there exists a choice of $x_1, \ldots, x_{d'}$ in T such that $(x_1, \ldots, x_{d'})$ lies outside of $H \cap Z(G^\star)$. By (6.13) and (6.14),

$$[x_1, \ldots, x_{d'}] \equiv (x_1, \ldots, x_{d'}) \not\equiv 1 \pmod{H \cap Z(G^\star)}.$$

Therefore by (6.15), $[\operatorname{ad} x_1, \ldots, \operatorname{ad} x_{d'}] \neq 0$. Consequently, the previous paragraph shows that $L^\star(T)$ has nilpotence class precisely d'. □

Remark 6.9. For the next result, consider an element x of G in the situation of Theorem 6.6. The inner automorphism $i(x)$ of G given by $i(x)(g) = x^{-1}gx$ for each g in G preserves every normal subgroup of G. In particular, for every N in $\mathcal{S}$, $i(x)$ induces a group automorphism on N and hence an automorphism of N as a Lie algebra under Lazard's definition. Thus, $i(x)$ induces an element of $E(\mathcal{S})$ that we will denote by $\gamma(x)$.

Theorem 6.10. *Assume the hypothesis and notation of Theorem* 6.6, *and assume that $\mathcal{S}$ generates G. For each x in G, define $\gamma(x)$ as in Remark* 6.9. *Then:*

(a) *for each x in G, $\gamma(x)$ is an invertible element of $E(\mathcal{S})$;*

(b) *for each v in $U(\mathcal{N})$,*

$$\gamma(v) = \operatorname{Exp}(\operatorname{ad} v) = 1 + (\operatorname{ad} v) + \frac{(\operatorname{ad} v)^2}{2!} + \cdots + \frac{(\operatorname{ad} v)^d}{d!} \quad \textit{and}$$
$$\operatorname{ad} v = \operatorname{Log}(\gamma(v));$$

(c) *for v and w in $U(\mathcal{N})$,* $\operatorname{ad} v = \operatorname{ad} w$ *if and only if* $v \equiv w \pmod{Z(G)}$*;*

(d) *the multiplicative group generated by the elements $\gamma(v)$ for all v in $U(\mathcal{S})$ is the group $\{\gamma(x) \mid x \in G\}$; and*

(e) *the inner automorphism group of G acts faithfully on $U(\mathcal{S})$ by restriction and induces the group $\{\gamma(x) \mid x \in G\}$ on $U(\mathcal{S})$.*

(f) *Moreover, suppose H is a subgroup of G generated by a subset $\mathcal{S}'$ of $\mathcal{S}$, and v is an element of H that lies in $U(\mathcal{N})$. Then* $\operatorname{ad} v$ *is contained in the associative $\mathbb{Q}_\pi$-subalgebra E' of $E(\mathcal{S})$ generated by* 1 *and the elements* $\operatorname{ad} u$ *as u ranges over the elements of the subgroups in $\mathcal{S}'$.*

Proof. Note that for u in $U(\mathcal{S})$ and x, y in G,

$$\gamma(x)\gamma(y)(u) = x^{-1}(y^{-1}uy)x = (yx)^{-1}u(yx),$$

so that

$$\gamma(x)\gamma(y) = \gamma(yx) \quad \text{for } x, y \text{ in } G. \tag{6.16}$$

Part (a) follows from Remark 6.9.

For (b), take any v in $U(\mathcal{N})$ and H in $\mathcal{S}$. Note that $H = \sqrt[\pi]{H}$ because H is $\mathbb{Q}_\pi$-powered. Moreover, the element $\gamma(v) - 1$ of $E(\mathcal{S})$ induces on H (under $+$) the endomorphism δ of Theorem 6.1, with $g_2 = v$. Then Theorem 6.1 yields that $\delta^{d+1} = 0$ and that the mapping β given by

$$\beta = \delta - \delta^2/2 + \cdots + (-1)^{d+1}\delta^d/d$$

coincides with the restriction of $\operatorname{ad} v$ to H.

From Section 3,

$$\beta = \operatorname{Log}(1+\delta),\ \beta^{d+1} = 0, \quad \text{and} \quad 1 + \delta = \operatorname{Exp}(\beta) = 1 + \beta + \frac{\beta}{2} + \cdots + \frac{\beta^d}{d!}.$$

Since this is valid for every H in $\mathcal{S}$,

$$\operatorname{ad} v = \operatorname{Log} \gamma(v) \quad \text{and} \quad \gamma(v) = \operatorname{Exp}(\operatorname{ad} v), \tag{6.17}$$

which gives (b).

Take w in $U(\mathcal{N})$. Then $v \equiv w \pmod{Z(G)}$ if and only if vw^{-1} lies in $Z(G)$. Since $\mathcal{S}$ generates G, this occurs if and only if $\gamma(v) = \gamma(w)$. From (6.17) and the analogous result for w, this occurs if and only if $\operatorname{ad} v = \operatorname{ad} w$. So we obtain (c).

Since $\mathcal{S}$ generates G, (d) and (e) follow from (6.16).

Finally, assume the hypothesis of (f) and define E' as in (f). For each element u in each subgroup in $\mathcal{S}'$, $\gamma(u) = \operatorname{Exp}(\operatorname{ad} u)$ by (6.17), so that $\gamma(u)$ lies in E'. Since these elements u generate H, (6.16) shows that E' contains $\gamma(x)$ for every element x of H, including $\gamma(v)$. By (6.17), $\operatorname{ad} v$ is equal to $\operatorname{Log} \gamma(v)$, and hence lies in E'. This proves (f). □

Remark 6.11. Assume $\mathcal{S}$ generates G in Theorem 6.6. Theorem 6.10 shows that one may determine the structure of the inner automorphism group of G, and thus of $G/Z(G)$, from $\mathcal{S}$ and $L(\mathcal{S})$. We do not know whether one may determine the structure of G. In (f), we do not know whether $\mathrm{ad}\, v$ lies in $L(\mathcal{S})$.

Assume in addition that $\mathcal{S}$ is strictly smaller than $\mathcal{N}$. Then $\mathcal{N}$ generates G and we may define $E(\mathcal{N})$ and $L(\mathcal{N})$ as in Theorem 6.6. They act on all the elements of $\mathcal{N}$, including the elements of $\mathcal{S}$. By taking G to be elementary of order p^2, we can easily see that $E(\mathcal{N})$ need not act faithfully on the set of all elements of $\mathcal{S}$. But we do not know whether $L(\mathcal{N})$ acts faithfully on this set in general.

Lemma 6.12. *Assume the hypothesis and notation of Theorem* 6.6*, and suppose T is a subset of $U(\mathcal{S})$ that generates a normal subgroup M_0 of G of nilpotence class at most d. Let*

$$M = \sqrt[\pi]{M_0}, \quad \mathrm{ad}\, T = \{\mathrm{ad}\, x \mid x \in T\}, \quad \textit{and} \quad \mathrm{ad}\, M = \{\mathrm{ad}\, x \mid x \in M\}.$$

Then

(a) *M is a normal $\mathbb{Q}_\pi$-powered subgroup of G of the same nilpotence class as M_0;*

(b) $\mathrm{ad}\, M$ *is the Lie $\mathbb{Q}_\pi$-subalgebra of $L(\mathcal{S})$ generated by* $\mathrm{ad}\, T$*;*

(c) $\mathrm{ad}\, M$ *is an ideal of $L(\mathcal{S})$; and*

(d) *if $\mathcal{S}$ generates G and T has the form $\{w^g \mid g \in G\}$ for some element w of $\mathcal{S}$, then* $\mathrm{ad}\, M$ *is the smallest ideal of $L(\mathcal{S})$ that contains* $\mathrm{ad}\, w$.

Proof. (a) This follows from Lemma 5.10.

(b) Note that (a) shows that we may define $\mathrm{ad}\, x$ for each x in M and that we may view M as a Lie $\mathbb{Q}_\pi$-algebra. Let $I = \mathrm{ad}\, M$.

From the definitions, M is the smallest $\mathbb{Q}_\pi$-powered subgroup of G containing T. Therefore, by the Lazard correspondence, M is generated by T under the Lie algebra operations on M. Hence, by Theorem 6.6, I is likewise generated by $\mathrm{ad}\, T$, as desired.

(c) Take any x in M and v in $U(\mathcal{S})$. By Theorem 6.6,

$$[\mathrm{ad}\, x, \mathrm{ad}\, v] = -\mathrm{ad}[x, v].$$

By (a) and Theorem 6.4 (c), $[x, v]$ lies in M, so that $\mathrm{ad}[x, v]$ lies in I. As $L(\mathcal{S})$ is spanned by the elements $\mathrm{ad}\, v$ for all v in $U(\mathcal{S})$, I is an ideal of $L(\mathcal{S})$.

(d) Let I' be the smallest ideal of $L(\mathcal{S})$ that contains $\mathrm{ad}\, w$. By (c), I' is contained in $\mathrm{ad}\, M$. Let $T^\star$ be the set of all elements x of M such that $\mathrm{ad}\, x$ lies in I'. Then $T^\star$ contains w. Since I' is a subalgebra of $L(\mathcal{S})$, Theorem 6.6 shows that $T^\star$ is a subgroup of M that contains w.

Suppose t lies in $T^\star$ and u lies in $U(\mathcal{S})$. We claim that t^u lies in $T^\star$. First, by Lemma 10.12 (d) in [13], the group commutator (t, u) can be expressed as a sum of

$[t,u]$ and Lie ring commutators in t and u of weight at least 3. Therefore, by Theorem 6.6, $\mathrm{ad}(t,u)$ is a sum of $[\mathrm{ad}\,u, \mathrm{ad}\,t]$ and other Lie ring commutators in $\mathrm{ad}\,t$ and $\mathrm{ad}\,u$. Hence, $\mathrm{ad}(t,u)$ lies in I' and (t,u) lies in $T^\star$. As $T^\star$ is a subgroup of M and

$$t^u = u^{-1}tu = t(t,u),$$

$T^\star$ contains t^u, as claimed.

This shows that $T^\star$ is closed under conjugation from $U(\mathcal{L})$. As $\mathcal{L}$ generates G and $T^\star$ contains w, $T^\star$ contains w^g for every g in G. Thus, I' contains $\mathrm{ad}\,T$. By (b), I' contains $\mathrm{ad}\,M$. Since I' is contained in $\mathrm{ad}\,M$, they are equal. □

In some applications of the Lazard correspondence, G is a finite p-group and one seeks a subgroup $A^\star$ of G with special properties. Representing G as a Lie algebra helps to find $A^\star$ as a subalgebra, and hence as a subgroup (e.g., in [6], Section 3).

If G is instead a product of normal subgroups of class less than p, one cannot generally represent G as a Lie algebra, but one can associate to G a Lie algebra $L(\mathcal{L})$ as in Theorem 6.6. In this case, a subalgebra may contain elements that are not of the form $\mathrm{ad}\,x$ for x in G, or that may lack other desired properties. The following two results help in this situation. For example, in some cases they show that an abelian subalgebra of $L(\mathcal{L})$ comes from an abelian subgroup of G.

Recall that G' denotes the commutator subgroup of G,

$$G' = (G,G) = \langle (x,y) \mid x, y \text{ in } G \rangle.$$

Theorem 6.13. *Assume the hypothesis and notation of Theorem* 6.6. *Suppose G' has nilpotence class at most d.*

Then G' is a $\mathbb{Q}_\pi$-powered normal subgroup of G and we may regard G' as a Lie $\mathbb{Q}_\pi$-algebra under the Lazard correspondence. Moreover:

(a) *There exists a unique $\mathbb{Q}_\pi$-bilinear mapping ψ of $L(\mathcal{L}) \times L(\mathcal{L})$ into G' such that*

$$\psi(\mathrm{ad}\,v, \mathrm{ad}\,w) = [v,w], \quad \textit{for all } v, w \textit{ in } U(\mathcal{L}).$$

For ψ as in (a),

(b) $\psi(\alpha,\beta) = -\psi(\beta,\alpha)$ *for all α, β in $L(\mathcal{L})$, and*

(c) $[\psi(\mathrm{ad}\,u, \mathrm{ad}\,v), w] + [\psi(\mathrm{ad}\,v, \mathrm{ad}\,w), u] + [\psi(\mathrm{ad}\,w, \mathrm{ad}\,u), v] = 0$, *for all u, v, w in $U(\mathcal{L})$.*

Proof. Let $R = \mathbb{Q}_\pi$. By Corollary 2.5, G' is π-divisible. Since G is nilpotent and π-torsion-free, G' is R-powered (of nilpotence class at most d). Therefore we may view G' as a Lie R-algebra.

Since $(\mathrm{ad}\,v)(w) = [w,v]$ for every v, w in $U(\mathcal{L})$, and $[w,v]$ lies in (G,G) by Corollary 6.5 , we see that $L(\mathcal{L})$ maps $U(\mathcal{L})$ into G'.

For each element v of $U(\mathcal{S})$, define a mapping θ_v from $L(\mathcal{S})$ into G' by

$$\theta_v(\phi) = \phi(v).$$

Then θ_v is an R-module homomorphism of $L(\mathcal{S})$ into G', and, for w in $U(\mathcal{S})$,

$$\theta_v(\operatorname{ad} w) = (\operatorname{ad} w)(v) = [v, w] = -[w, v] = (\operatorname{ad} v)(-w). \tag{6.18}$$

Let $\operatorname{Hom}(L(\mathcal{S}), G')$ be the R-module of all R-module homomorphisms of $L(\mathcal{S})$ into G'.

Suppose we are given elements a_v in R for finitely many elements v of $U(\mathcal{S})$ such that

$$\sum a_v(\operatorname{ad} v) = 0.$$

Then (6.18) shows that $\sum a_v\theta_v$ vanishes on $\operatorname{ad} w$ for every w in $U(\mathcal{S})$. Since the elements $\operatorname{ad} w$ span $L(\mathcal{S})$, it follows that $\sum a_v\theta_v = 0$. Thus we obtain an R-module homomorphism $\psi^\star$ of $L(\mathcal{S})$ into $\operatorname{Hom}(L(\mathcal{S}), G')$ determined by

$$\psi^\star(\operatorname{ad} v) = \theta_v, \quad \text{for each } v \text{ in } U(\mathcal{S}).$$

Let $\psi(\phi, \phi') = \psi^\star(\phi)(\phi')$, for all ϕ, ϕ' in $L(\mathcal{S})$. Then ψ is an R-bilinear mapping of $L(\mathcal{S}) \times L(\mathcal{S})$ into G'. Since the mappings $\operatorname{ad} v$ span $L(\mathcal{S})$ as a R-module, ψ is determined by the condition

$$\psi(\operatorname{ad} v, \operatorname{ad} w) = \psi^\star(\operatorname{ad} v)(\operatorname{ad} w) = \theta_v(\operatorname{ad} w) = (\operatorname{ad} w)(v) = [v, w],$$

for all v, w in $U(\mathcal{S})$, which proves (a).

Now (b) and (c) follow from Theorem 6.1 (b) and Theorem 6.4 (b). □

Theorem 6.14. *Assume the hypothesis and notation of Theorem* 6.6. *Suppose* $\mathcal{S}$ *generates* G, v *and* w *are elements of* $U(\mathcal{S})$,

$$\alpha = \operatorname{ad} v + \operatorname{ad} w,$$

and b *is the nilpotence class of the group* $\langle v^G\rangle Z(G)/Z(G)$. *Assume* $b \leq d - 1$ *and* α *is contained in an ideal of* $L(\mathcal{S})$ *of nilpotence class at most* $d - 1 - b$.

Then there exists y *in* $U(\mathcal{N})$ *such that* $\operatorname{ad} y = \alpha$.

Proof. Let

$$Z = Z(G), \quad N_1 = \langle v^G\rangle, \quad N_2 = \sqrt[\pi]{N_1}, \quad \text{and} \quad I_2 = \{\operatorname{ad} x \mid x \in N_2\}.$$

Then $N_2Z/Z = \sqrt{N_1Z/Z}$. By Lemma 2.2, N_2Z/Z has nilpotence class b. By Lemma 6.12 with $T = \{v^g \mid g \in G\}$, I_2 is an ideal of $L(\mathcal{S})$ and is the Lie subalgebra of $L(\mathcal{S})$ generated by the set

$$\{\operatorname{ad} v^x \mid x \in G\}.$$

Therefore, by Lemma 6.8,

$$I_2 \text{ has nilpotence class at most } b. \tag{6.19}$$

Let I_1 be the smallest ideal of $L(\mathcal{S})$ containing α. By hypothesis, I_1 has class at most $d-1-b$. Moreover, I_1+I_2 is an ideal of $L(\mathcal{S})$. Since $(d-1-b)+b = d-1$, (6.19) and a theorem of Fitting yield

$$I_1 + I_2 \text{ has class at most } d-1. \tag{6.20}$$

(Fitting's Theorem follows from a slight variation in the proof of Proposition I.6 in p. 25 of [12].)

Since $\operatorname{ad} v$ lies in I_2, α lies in I_1, and $\operatorname{ad} w = \alpha - \operatorname{ad} v$, we see that $\operatorname{ad} w$ lies in $I_1 + I_2$. By Lemma 6.12 (d),

$$I_1 + I_2 \text{ contains } \operatorname{ad} w^g \text{ for every } g \text{ in } G. \tag{6.21}$$

Now let T be the subset of G given by

$$T = \{v^g, w^g \mid g \in G\}.$$

Then T generates a normal subgroup M_0 of G. By construction, I_2 contains $\operatorname{ad} v^g$ for every g in G. Hence, by (6.21), $I_1 + I_2$ contains $\operatorname{ad} x$ for every x in T, and contains the subalgebra of $L(\mathcal{S})$ that they generate, which we denote by $L^\star(T)$ as in Lemma 6.8.

By (6.20), $L^\star(T)$ has class at most $d-1$. By Lemma 6.8, $M_0/(M_0 \cap Z(G))$ has class at most $d-1$, so M_0 has class at most d. Let $M = \sqrt[\pi]{M_0}$.

Since $\alpha = \operatorname{ad} v + \operatorname{ad} w$, α lies in $L^\star(T)$. By Lemma 6.12, M is a normal subgroup of G of class at most d, and

$$L^\star(T) = \operatorname{ad} M = \{\operatorname{ad} x \mid x \in M\}.$$

So $\alpha = \operatorname{ad} y$ for some y in M, as desired. □

Acknowledgments. It is a pleasure to dedicate this article to Professor Avinoam Mann for many years of friendship, help, and encouragement.

We also thank the National Security Agency (USA) for its support through a grant.

References

[1] R. Baer, Groups with abelian central quotient group. *Trans. Amer. Math. Soc.* **44** (1938), 357–386. JFM 64.0068.01 Zbl 0020.00802 MR 1501972

[2] J. L. Alperin and G. Glauberman, Limits of abelian subgroups of finite p-groups. *J. Algebra* **203** (1998), 533–566. Zbl 0964.20011 MR 1622791

[3] R. W. Carter, *Simple groups of Lie type*. Pure Appl. Math. 28, John Wiley & Sons, London 1972. Zbl 0248.20015 MR 0407163

[4] J. D. Dixon, M. P. F. du Sautoy, A. Mann, and D. Segal, *Analytic pro−p groups*. 2nd ed., Cambridge Stud. Adv. Math. 61, Cambridge University Press, Cambridge 1999. Zbl 0934.20001 MR 1720368

[5] T. E. Easterfield, The orders of products and commutators in prime-power groups. *Proc. Cambridge Philos. Soc.* **36** (1940), 14–26. Zbl 0024.01703 MR 0000622

[6] G. Glauberman, An extension of Thompson's replacement theorem by algebraic group methods. In *Finite groups 2003*, Walter de Gruyter, Berlin 2004, 105–110. Zbl 1095.20007 MR 2125069

[7] G. Glauberman, Abelian subgroups of small index in finite p-groups. *J. Group Theory* **8** (2005), 539–560. Zbl 1085.20008 MR 2165290

[8] G. Glauberman, Centrally large subgroups of finite p-groups. *J. Algebra* **300** (2006), 480–508. Zbl 1103.20013 MR 2228208

[9] D. Gorenstein, *Finite groups*. 2nd ed., Chelsea Publishing Co., New York 1980. Zbl 0463.20012 MR 0569209

[10] M. Hall, Jr., *The theory of groups*. The Macmillan Co., New York 1959. Zbl 0084.02202 MR 103215

[11] B. Huppert, *Endliche Gruppen I*. Grundlehren Math. Wiss. 134, Springer-Verlag, Berlin 1967. Zbl 0217.07201 MR 0224703

[12] N. Jacobson, *Lie algebras*. Dover, New York 1979. Zbl 0121.27504 MR 0559927

[13] E. I. Khukhro, *p-automorphisms of finite p-groups*. London Math. Soc. Lecture Note Ser. 246, Cambridge University Press, Cambridge 1998. Zbl 0897.20018 MR 1615819

[14] M. Lazard, Sur les groupes nilpotents et les anneaux de Lie. *Ann. Sci. École Norm. Sup.* (3) **71** (1954), 101–190. Zbl 0055.25103 MR 0088496

Received December 24, 2006; revised August 30, 2007

G. Glauberman, Department of Mathematics, University of Chicago, 5734 University Avenue, Chicago, IL 60637-1514, USA

E-mail: gg@math.uchicago.edu