Ulam Quarterly — Volume 1, Number 1, 1992

Magnus' Method in the Theory of Free Groups

N. Jacobson[1]

Department of Mathematics
Yale University
New Haven, CT 06520

Dedicated to Jacques Tits on his Sixtieth Birthday

This paper is largely expository. Most of the results were obtained in the thirties and forties by Magnus, Witt, Zassenhaus and Grün. Their objective was to develop tools that might be used to settle the problem formulated by Burnside in 1902: Is the group $B(m,n)$ presented by m generators with the identical relation $x^n = 1$ finite? Eventually counterexamples were given (e.g. for odd $n \geq 4381$, by Adian and Novikov). A weaker problem than the original Burnside Problem is the Restricted Burnside Problem (RBP): Does the group $B(m,n)$ have only a finite number of finite homomorphic images? This was answered affirmatively by Kostrikin ([86]) for prime exponents n and during the past year for prime power exponents by Zelmanov ([89], [90$_1$], [90$_2$] and [88] by Kostrikin and Zelmanov). This result combined with an earlier result of P. Hall and Higman and the finiteness of sporadic finite groups implies an affirmative answer to RBP for any m and n.

Magnus' method is based on a realization of a finitely generated free group as a group of invertible elements in the ring of formal power series in r non-commuting indeterminates with coefficients in $\mathbf{Z}$. This leads to construction of a graded Lie algebra $L(G)$ for any group G. In this way the RBP for $B(m,p)$, p prime, can be reduced to a problem on Lie algebras. Zassenhaus applied Magnus' method to obtain a realization of the free group with a finite set of generators in the algebra over $\mathbf{Z}_p = \mathbf{Z}/(p)$ of formal power series in non-commuting indeterminates over $\mathbf{Z}_p$. In this way he gave a construction of a restricted Lie algebra $L^{(p)}(G)$ for any G, which is an appropriate tool for studying and eventually giving an affirmative answer, thanks to Zelmanov, of the RBP for prime powers.

We shall give Magnus' and Zassenhaus' method and their applications to the study of the lower central series of any group and Zassenhaus' lower central series (see sec. 3) via corresponding Lie algebras. We shall also

[1]This research was partially supported by National Science Foundation Grant DMS-88-06371.

introduce another lower central series that we call the p-adic lower central series. The results here were derived by the author around 1960 but have not been previously published (see secs. 2 and 5 for the p-adic lower central series).

1. Magnus' Theorem. Let $A = \mathbf{Z}\{\{x_1, \ldots, x_r\}\}$ be the ring of formal power series in the non-commutative but associative indeterminates x_i with coefficients in $\mathbf{Z}$. Let I be the ideal of power series with 0 constant term so $I = \sum_1^r x_i A$. The elements of A that are $\equiv 1 (\mathrm{mod} I)$ form a subgroup U of the multiplicative group of invertible elements of A since if $y, z \in I$ then

$$(1+y)(1+z) = 1 + y \circ z, y \circ z = y + z + yz \tag{1}$$

and

$$(1+y)^{-1} = 1 - y + y^2 - \cdots \tag{2}$$

which is well defined in A.

Let F denote the subgroup of U generated by the elements

$$a_i = 1 + x_i, 1 \leq i \leq r. \tag{3}$$

Then F is the free group on the a_i. To see this we have to show that $a_{i_1}^{k_1} a_{i_2}^{k_2} \cdots a_{i_\ell}^{k_\ell} \neq 1$ if the $i_j \in \mathbf{Z}^* = \mathbf{Z}\backslash\{0\}$ and successive i_j are distinct. Now $a_i^k = (1+x_i)^k = 1 + \binom{k}{1} x_i + \cdots + x_i^k$ and $a_i^{-k} = ((1 + x_i)^k)^{-1} = 1 - \binom{k}{1} x_i + \cdots$ if $k > 0$. Hence, $a_{i_1}^{k_1} \cdots a_{i_\ell}^{k_\ell}$ contains the term $k_1, k_2 \cdots k_\ell x_{i_1} x_{i_2} \cdots x_{i_\ell}$, so $a_{i_1}^{k_1} \cdots a_{i_\ell}^{k_\ell} \neq 1$.

Let $F^{[n]}$ denote the subset of F of elements $a \equiv 1 (\mathrm{mod} I^n), n = 1, 2, \ldots$. The elements of $F^{[n]}$ have the form

$$1 + x \tag{4}$$

where $x \in I^n$. If $b = 1 + y, y \in I^n$ then

$$ab = 1 + x + y + xy \tag{5}$$

and $x + y + xy \in I^n$. Also

$$a^{-1} = 1 - x + x^2 - \cdots \tag{6}$$

and $-x + x^2 - \cdots \in I^n$. Hence, $F^{[n]}$ is a subgroup of F that we shall call the nth *dimensional subgroup*of F.

If $a = 1 + x, x \in I^n$ and $b = 1 + y, y \in I^m$ then a simple calculation shows that

$$(a, b) = a^{-1}, b^{-1}ab \equiv 1 + [x, y] (\mathrm{mod}\ I^{m+n+1}). \tag{7}$$

Since $[x,y] = xy - yx \in I^{m+n}$ this implies that $(a,b) \in F^{[m+n]}$. Hence,

$$(F^{[m]}, F^{[n]}) \subset F^{[m+n]} \tag{8}$$

where for subgroups H, K of a group G, (H,K) denotes the subgroup of G generated by the $(h,k), h \in H, k \in K$. Since $F^{[1]} = F$, (8) implies that $F^{[n]} \lhd F$. We recall that the lower central series of a group G is $G = G, \supset G_2 \supset \cdots$ where $G_k = (G, G_{k-1})$. By (8) we have $F_n \subset F^{[n]}$. Since it is clear that $\cap F^{[n]} = 1$ we have the result, first proved by Magnus, that the free group F is ω-nilpotent in the sense that $\cap F_n = 1$. Now we have

Magnus' Theorem. *The n-th dimensional subgroup $F^{[n]} = F_n$ for $n = 1, 2, \ldots$* (Magnus [37]).

If $a \in F^{[n]}, \notin F^{[n+1]}$ then $a = 1 + d_n(a) + b$ where $d_n(a)$ is a non-zero homogeneous polynomial in the x's (with integral coefficients) of degree n and $b \in I^{n+1}$. The uniquely determined polynomial $d_n(a)$ is called the *leading term*of a. It is a consequence of Magnus' theorem that $d_n(a)$ is in the Lie algebra $L/\mathbf{Z}$ generated by the x's under the composition $[x,y] = xy - yx$ (Witt [37], p. 159). More precisely, $d_n(a) \in L^n$ where $L^1 = L$ and $L^k = [L, L^{k-1}]$. We recall also that the Jacobi identity implies that $L^n \supset [L^k, L^\ell]$ with $k + \ell = n$. Also, if d is any element of L^n then there exists an a whose leading term $d_n(a) = d$. It follows that $F^{[n]}/F^{[n+1]}$ is a free abelian group isomorphic to the additive group of L^n. Witt [37] has given a formula for the rank ψ_n of this group, namely,

$$\psi_n = \frac{1}{n} \sum_{d|n} \mu(d) r^{n/d} \tag{9}$$

where μ is the Möbius function.

2. p-adic Lower Central Series. Let p be a prime. We have a continuous isomorphism π of the ring A into a subring B such that $x_i \sim> px_i, 1 \leq i \leq r$. Then $\pi a_i = \pi(1 + x_i) = 1 + px_i \equiv b_i$. Hence, the b_i generate a subgroup G (or more precisely G_p) of the multiplicative group of units of A that is free on the b_i. We denote the ideal pB of B by (p) and we write (p^n) for $(pB)^n = p^n B$. As in section 1, the subset G_n of G of elements b such that $b \equiv 1 (p^n)$ is a subgroup and $(G_n, G_m) \subset G_{n+m}$ so $G_n \lhd G$. If $b = 1 + p^n x$ then $b^p = 1 + \binom{p}{1} p^n x + \binom{p}{2} (p^n x)^2 + \cdots + (p^n x)^p$. Hence, if for a subgroup H of a group, H^{p^j} dentoes the subgroup generated by the $h^{p^j}, h \in H$, then $G_n^p \subset G_{n+1}$. Thus we have

$$(G_n, G_m) \subset G_{m+n} \qquad G_n^p \subset G_{n+1}. \tag{10}$$

By (10) we have

$$G_n \supset \bar{G}_n = \{G^{[i]p^j} \mid i + j \geq\}. \tag{11}$$

Evidently $\bigcap_{n=1}^{\infty} G_n = \{1\}$. Hence, by (11), $\bigcap_{n=1}^{\infty} \bar{G}_n = \{1\}$

Theorem 1. $G_n = \bar{G}_n, n = 1, 2, 3, \ldots$.

Proof. We shall prove the result by induction. We have $G_1 = \bar{G}_1$, and for the inductive step, we assume $G_n = \bar{G}_n$. Then we have $\bar{G}_n = G_n \supset G_{n+1} \supset \bar{G}_{n+1}$ and we shall show that $G_{n+1} = \bar{G}_{n+1}$ by showing that if $b \in \bar{G}_n, \notin \bar{G}_{n+1}$ then $b \notin G_{n+1}$. Let $a = \pi^{-1}(b)$ and suppose $a \in F^{[i]}, \notin F^{[i+1]}$ and let $d_i(a)$ be the leading term of a so $d_i(a) \in L^i$ and

$$a = 1 + d_i(a) + \cdots \tag{12}$$

where the omitted terms are homogeneous polynomials of degree $> i$. Let p^j be the highest power of p dividing $d_i(a)$. Then applying π to (12) we obtain

$$b = 1 + p^{i+j} e_i + \cdots \tag{13}$$

where e_i is a non-zero homogeneous polynomial in the x's of degree i and the omitted terms are homogeneous of degree $< i$. Since $b \in G_n$ this implies that $i + j \geq n$. We have $d_i(a) = p^j d'_i(a)$. By a result of Magnus' ([3], p. 106), $d'_i(a) \in L^i$, so we have an element $u_i \in F^{[i]}, \notin F^{[i+1]}$ with leading term $d_i(u_i) = d'_i(a)$. Then $u_i = 1 + d'_i(a) + z_i$ where $z_i \in I^{i+1}$ and

$$\begin{aligned} u_i^{p^j} &= (1 + d'_i(a) + z_i)^{p^j} \\ &= 1 + p^j (d'_i(a) + z_i) + \binom{p^j}{2} (d'_i(a) + z_i)^2 + \cdots \\ &= 1 + d_i(a) + w_i \end{aligned} \tag{14}$$

where $w_i \in I^{i+1}$. This implies that $a = u_i^{p^j} a'$ where $a' \in F^{[i']}, i' > i$. Applying π to $a = u_i^{p^j} a'$ we obtain $b = v_i^{p^j} b'$ where $v_i^{p^j} \in \bar{G}_{i+j} \subset \bar{G}_n$. Then $b' = v_i^{-p^j} b \in \bar{G}_n$. We may repeat this process to obtain

$$a = u_{i_1}^{p^{j_1}} u_{i_2}^{p^{j_2}} \cdots u_{i_k}^{p^{j_k}} a^{(k)} \tag{15}$$

where $i_1 < i_2 < \cdots < i_k \leq n, u_{i_\ell} \in F^{[i_\ell]} \notin F^{[i_\ell+1]}$, $1 \leq \ell \leq k, a^{(k)} \in F^{[n+1]}$. Then

$$b = v_{i_1}^{b^{j_1}} v_{i_2}^{p^{j_2}} \cdots v_{i_k}^{p^{j_k}} b^{(k)} \tag{16}$$

where $b^{(k)} \in \bar{G}_{n+1}$. For at least one ℓ we have $i_\ell + j_\ell = n$ since otherwise, $b \in \bar{G}_{n+1}$. Let s be the least ℓ for which this equality holds. Then $b = 1 + p^n(e_{i_s} + \cdots)$ where e_{i_s} is homogeneous of degree i_s in the x's not divisible by p and the other terms in the parenthesis are of degree $> i_s$. Hence, $b \notin G_{n+1}$, so we have shown that if $b \in \bar{G}_n$ and $b \notin \bar{G}_{n+1}$ then $b \notin G_{n+1}$. This implies that $G_n = \bar{G}_n$ for all n. $\square$

We can now write G_n for $\bar{G}_n = \langle G^{[i]p^j} \mid i + j \geq n \rangle$. Then (11) holds for these G_n. We shall call

$$G = G_1 \supset G_2 \supset \cdots \tag{17}$$

the *p-adic lower central series* for the free group G with r generators.

3. mod$p$ Lower Central Series. We now replace the coefficient ring $\mathbf{Z}$ by $\mathbf{Z}_p = \mathbf{Z}/(p)$ and we consider the ring $A_p = \mathbf{Z}_p\{\{x_1, \ldots, x_r\}\}$ of formal power series in $x_1, \ldots, x_r$ with coefficients in $\mathbf{Z}_p$. Put $c_i = 1 + x_i$. These c_i generate a subgroup $H(= H_p)$ of the multiplicative group of units of the ring A_p. It is readily seen, as in Section. 1, that H is free on the c_i. For $n = 1, 2, \ldots$, let H_n be the subset of H of elements $\equiv 1 (\mathrm{mod} I^n)$ where I is the ideal in A_p of power series with 0 constant term. Then H_n is a subgroup of H and

$$(H_n, H_m) \subset H_{n+m}, \qquad H_n^p \subset H_{np} \tag{18}$$

Since $H_1 = H$ and $(H_n, H_1) \subset H_{n+1} \subset H_n$, H_n is normal in H. We have

Zassenhaus' Theorem. $H_n = \langle H^{[i]p^j} \mid ip^j \geq n \rangle$. *(Zassenhaus* [40]*)*

If $c = 1 + d_n(c) + \cdots$ where $d_n(c)$ is a non-zero homogeneous polynomial of degree n in the x's and the omitted terms are of degree $> n$ then it follows from Zassenhaus' theorem that $d_n(c) \in \sum_{ip^j \geq n}^{n} R^{[i]p^j}$ where R is the restricted Lie algebra over $\mathbf{Z}_p$ generated by the x's under $[xy] = xy - yx$ and p-th powers, and $R^{[i]}$ is defined by $R^{[i]} = R$, $R^{[1]} = [R^{[k-1]}, R]$ and S^{p^j} for a subspace S is the subspace spanned by the $s^{p^j}, s \in S$.

4. Some Congruences on Commutators and p-th Powers. We shall now list some congruences that are consequences of the foregoing results.

From Magnus' theorem

(i) If $a_k \in F_k, b_\ell, c_\ell \in F_\ell$, etc. then

$$(a_k, b_\ell c_\ell) \equiv (a_k, b_\ell)(a_k, c_\ell) (\mathrm{mod}\ F_{k+\ell+1},$$
$$(b_\ell c_\ell, a_k) \equiv (b_\ell, a_k)(c_\ell, a_k) (\mathrm{mod}\ F_{k+\ell+1}).$$

(ii) $(a_k, b_\ell, c_m)(b_\ell, c_m, a_k)(c_m, a_k, b_\ell) \equiv 1 \ (\mathrm{mod}\ F_{k+\ell+m+1})$ (Hall [34]) where $(a, b, c, \ldots, f) = (\cdots((a, b), c), \cdots, f)$.

From the theorem on the G-series (the p-adic lower central series):

(iii) If $a_k \in G_k, b_\ell, c_\ell \in G_\ell$ then

$$(a_k, b_\ell c_\ell) \equiv (a_k, b_\ell)(a_k, c_\ell) (\mathrm{\ mod}\ G_{k+\ell+1})$$
$$(b_\ell c_\ell a_k) \equiv (b_\ell, a_k)(c_\ell, a_k) (\mathrm{\ mod}\ G_{k+\ell+1})$$

(iv) $(a_k, b_\ell, c_m)(b_\ell, c_m, a_k)(c_m, a_k, b_\ell) \equiv 1 (\mathrm{\ mod}\ G_{k+\ell+m+1})$.

(v) If $a_k \in G_k, b_\ell \in G_\ell$ then

$$(a_k, b_\ell)^p \equiv (a_k^p, b_\ell) \equiv (a_k, b_\ell^p) (\mathrm{\ mod}\ G_{k+\ell+2})$$

From the H-series (the mod p lower central series):

We have the analogues of (2) and (72) and we have the following congruence:

(vi) If $a_k \in H_k, b_\ell \in H_\ell$ then

$$(a_k, b_\ell^p) \equiv (a_k, \overbrace{b_\ell, \ldots, b_\ell}^{p}) (\text{ mod } H_{k+p\ell+1})$$

(Zassenhaus [40]).

This follows from the following identity in any associative algebra of characteristic p:

$$[xy^p] = [x, \overbrace{y, \ldots, y}^{p}] \tag{19}$$

where $[x, y, \ldots, t] = [\cdots[[xy]z]\cdots t]$. (See Jacobson [62], p. 186.)

(vii) If $a_k, b_k \in H_\ell$ then

$$(a_k b_k)^p \equiv a_k^p b_k^p s(a, b) (\text{ mod } H_{pk+1})$$

where $s(a, b) = \prod_1^{p-1} s_i(a, b)$ and $s_i(a, b) \in H_k^{[p]} \subset H_{pk}$.

The specific form of $s_i(a, b)$ is obtained from the following p power Lie relation in any associative algebra of characteristic p:

$$(x + y)^p = x^p + y^p + \sum_{i=1}^{p-1} s_i(x, y) \tag{20}$$

where $is_i(x, y)$ is the coefficient of λ^{i-1} in

$$[x, \overbrace{\lambda x + y, \lambda x + y, \ldots, \lambda x + y}^{p-1}]$$

(see Jacobson [62], pp. 186-187). Thus, $s_i(x, y)$ is a multiple of a certain p-fold Lie commutator in x and y and $s_i(a, b)$ is the corresponding p-fold group commutator. For example, we have

$$s_1(x, y) = [xy] \text{ if } p = 2$$
$$s_1(x, y) = [[xy]y], 2s_2(x, y) = [[xy]x] \text{ if } p = 3$$

Correspondingly, we have if $a_k, b_k \in H_k$ then

$$(a_k b_k)^2 \equiv a_k^2 b_k^2 (a, b) (\text{ mod } H_{2k+1})$$
$$(a_k b_k)^3 \equiv a_k^3 b_k^3 (a, b, b)(a, b, a)^{-1} (\text{ mod } H_{3k+1})$$

The congruence (vii) is closely related to the following congruence due to P. Hall ([34]):

$$(ab)^p \equiv a^p b^p c_2^p \cdots c_p^p (\bmod F_{p+1}) \tag{21}$$

where $c_i \in F_i$ (see Magnus [37]). A congruence which is in a sense the inverse of (vii) is

(viii) If $a_k, b_k \in H_k$ and $p \neq 2$, then

$$(a_k, \overbrace{b_k, \ldots, b_k}^{p-1})(a_k^p (a_k b_k^{-1})^p \cdots (a_k b_k^{-(p-1)})^p) \equiv 1 (\bmod H_{pk+1})$$

(Grün [40]).

This follows from the relation

$$[x, \overbrace{y, \cdots, y}^{p-1}] = -(x^p + (x-y)^p + \cdots + (x-(p-1)y)^p) \tag{22}$$

for p an odd prime in any associative algebra of characteristic p. This can be proved by applying (20) to the terms on the right hand side of (22). This gives

$$\begin{aligned} & -x^p \\ & -x^p + y^p - \sum_1^{p-1} s_i(x, -y) \\ & \cdots\cdots\cdots \\ & -x^p + ((p-1)y)^p - \sum_1^{p-1} s_i(x, -(p-1)y) \\ = & -\sum s_i(x,-y) - \cdots - \sum s_i(x, -(p-1)y) \end{aligned}$$

for the right hand side of (22). Since $s_i(x, y)$ is homogeneous of degree $(p-i)$ in y,

$$\begin{aligned} & s_i(x,-y) + s_i(x,-2y) + \cdots + s_i(x,-(p-1)y) \\ & = s_i(x,-y)(1 + 2^{p-i-1} + \cdots + (p-1)^{p-i}). \end{aligned} \tag{23}$$

Now we have

$$\begin{aligned} & 1 + 2^k + \cdots + (p-1)^k = 0 \text{ if } 1 \leq k \leq p-2 \\ & 1 + 2^{p-1} + \cdots + (p-1)^{p-1} = -1 \end{aligned} \tag{24}$$

To prove these relations we consider the two matrices

$$s = \begin{bmatrix} 0 & 1 & 0 & & \\ \cdot & 0 & 1 & & 0 \\ \cdot & \cdot & \cdot & & \cdot \\ \cdot & \cdot & \cdot & & \cdot \\ 0 & & & 0 & 1 \\ 1 & & & & 0 \end{bmatrix}, t = \begin{bmatrix} 1 & & & 0 & \\ & 2 & & & \\ & & 0 & \ddots & \\ & & & & p-1 \end{bmatrix}$$

in $M_{p-1}(\mathbf{Z}_p)$. These have the same minimum polynomial $\lambda^{p-1}-1$ of degree $p-1$. Hence, they are similar. We have $tr(s^k)=0, 1\leq k\leq p-2, s^{p-1}=1$ so $tr(s^{p-1})=-1$. Hence, $tr(t^k)=0, 1\leq k\leq p-2$, $tr(t^{p-1})=-1$. Thus (24) holds. Then the right hand side of (22) reduces to $s_1(x,-y)=s_1(x,y)=[x,\overbrace{y,\ldots,y}]^{p-1}$. Hence (22) holds.

Another congruence on higher commutators is the following. If $a_\ell\in H_k, b_\ell\in H_\ell, c_m\in H_m$ then

$$\prod_{i=0}^{p-2}(b,\overbrace{a,\cdots,a}^{p-2-i},c,\overbrace{a,\cdots,a}^{i})\equiv \tag{ix}$$
$$\prod_{i=0}^{p-2}(c,\overbrace{a,\cdots,a}^{p-2-i},b,\overbrace{a,\cdots,a}^{i})(\bmod H_{(p-2)k+\ell+m+1})$$

The proof of this can be based on a characteristic p Lie commutor identity which is stated as exercise 23 in Jacobson [62], p. 197.

The foregoing results have been derived for finitely generated free groups. They have immediate extensions to arbitrary free groups and, hence, by applying homomorphisms they carry over to arbitrary groups. We shall make use of this in the next section.

5. Graded Lie Algebras Defined by Descending Central Series of a Group. We now make a drastic change of notation by letting G denote *any* group. The lower central series of G is $G=G_1\supset G_2\supset\cdots$ where $G_n=[G_{n-1},G]$. As we noted, the results on free groups imply that

$$(G_m,G_n)\subset G_{m+n} \tag{25}$$

and G_n/G_{n+1} is an abelian group. We write this in additive notation and put $L_n=G_n/G_{n+1}$. If $x_m\in L_m$, $y_n\in L_n$ so $x_m=a_mG_{m+1}, y_n=b_nG_{n+1}$, $a_m\in G_m, b_n\in G_n$ then we define

$$[x_m,y_n]=(a_m,b_n)G_{m+n+1}\in L_{m+n}. \tag{26}$$

Using (i) we see that this is independent of the choice of the coset representatives and is $\mathbf{Z}$-bilinear. Moreover, $[x_n,x_n]=0$, and, by (ii), we have $[[x_m,y_n]z_q]+[[y_nz_q]x_m]+[[z_qx_m]y_n]=0$. Hence, if we extend $[\ ,\ ]$ additively to $L=\oplus L_n, L=L(G)$ becomes a Lie algebra over $\mathbf{Z}$ (or Lie ring) that is graded by the L_n. We call this *Magnus' Lie algebra* of G.

Next, let p be a prime and define ${}^{(p)}G_n=\langle G_i^{p^j}\mid i+j\geq n\rangle$. Then the results on free groups imply that $({}^{(p)}G_m,{}^{(p)}G_n)\subset^{(p)}G_{m+n}$, $({}^{(p)}G_n)^p\subset^{(p)}G_{n+1}$. We have the abelian factor group ${}^{(p)}G_n/{}^{(p)}G_{n+1}$ which we can write additively and denote as ${}^{(p)}L_n$. Then, as for the L_n, we can define a Lie algebra over $\mathbf{Z}$, ${}^{(p)}L=^{(p)}L(G)$ which is graded by the ${}^{(p)}L_n$. Since

$({}^{(p)}G_n)^p \subset {}^{(p)}G_{n+1}$, ${}^{(p)}L_n$ is a p-torsion abelian group, so this may be regarded as a vector space over $\mathbf{Z}_p = \mathbf{Z}/(p)$. Then ${}^{(p)}L$ is a Lie algebra over the field $\mathbf{Z}_p$.

We recall that a Lie algebra L over a field F of characteristic p is called restricted if there is a map $x \sim> x^{[p]}$ in L such that

$$(\alpha x)^{[p]} = \alpha^p x^{[p]},\ \alpha \in F \qquad \text{RL1}$$

$$[y, \overbrace{x, \ldots, x}^{p}] = [yx^{[p]}] \qquad \text{RL2}$$

$$(x+y)^{[p]} = x^{[p]} + y^{[p]} + \sum_1^{p-1} s_i(x,y) \qquad \text{RL3}$$

where $(i)s_i(x,y)$ is the coefficient of λ^{i-1} in $[y, \lambda x \overbrace{+y, \ldots, \lambda x+}^{p-1} y]$. We shall now show that we can use the mod p lower central series to construct a restricted Lie algebra, the *Zassenhaus Lie algebra* of G. Here, the n-th term of the mod p lower central series of G is $G_n^{(p)} = \langle G_i^{p^j} \mid ip^j \geq n \rangle$. We have $(G_m^{(p)}, G_n^{(p)}) \subset G_{m+n}^{(p)}, (G_n^{(p)})^p \subset G_{pn}^{(p)}$. Put $L_n^{(p)} = G_n^{(p)}/G_{n+1}^{(p)}$ which, written additively, is a vector space over $\mathbf{Z}_p$. As in the case of the Magnus Lie algebra, we can define a graded Lie algebra structure on $L^{(p)} = \oplus L_n^{(p)}$ in which the $L_n^{(p)}$ give the grading and for $x_m = a_m G_{m+1}^{(p)}, a_m \in G_m^{(p)}$ and $y_n = b_n G_{n+1}^{(p)}$ we have

$$[x_m y_n] = (a_m, b_n) G_{m+n+1}^{(p)}. \qquad (27)$$

Also, if $c_{m+1} \in G_{m+1}^{(p)}$ then, by (vii), $(a_m c_m)^p \equiv a_m^p \pmod{G_{pm+1}^{(p)}}$. Accordingly, we can define

$$x_m^{[p]} = a_m^p G_{pm+1}^{(p)} \qquad (28)$$

in $L^{(p)}$. By (vi) we have $[y, x_m^{[p]}] = [y, \overbrace{x_m, \ldots, x_m}^{p}]$ and from (vii) we have RL3 for $x = x_m, y = y_m$. It follows from this that there exists a unique map $x \sim> x^{[p]}$ on $L^{(p)}$ that satisfies RL1-RL3 and coincides with $x_m \sim> x_m^{[p]}$ (of $L_m^{(p)}$ into $L_{pm}^{(p)}$) on $L_m^{(p)}$ (see Jacobson [62], p. 190).

It has been shown by Witt ([37]) that if a group G is generated by r elements $g_1, \ldots, g_r$ then G_n/G_{N+1} is generated by the cosets.

$$(g_{i_1}, g_{i_2}, \ldots, g_{i_n}) G_{n+1} \qquad (29)$$

$1 \leq i_\alpha \leq r$. It follows that the Magnus Lie algebra $L(G)$ is generated by the cosets $g_1 G_2, \ldots, g_r G_2$. Similarly, ${}^{(p)}L(G)$ is generated by the cosets $g_1^{(p)} G, \ldots, g_r^{(p)} G$ and $L^{(p)}(G)$ is generated by the cosets $g_1 G^{(p)}, \ldots, g_r G^{(p)}$.

References

[02] W. Burnside, *On an unsettled question in the theory of discontinuous groups* , Quart. J. Pure Appl. Math., 1902, 33, 230-238.

[40] O. Grün, *Zusammenhang zwischen Potenzbildung und Kommutatorbildung* , J. reine angew. Math., 182, 1940, 158-177.

[34] P. Hall, *A Contribution to the theory of groups of prime power order,* Proc. London Math. Soc., 35, 1934, 29-95.

[56] P. Hall and G. Higman, *On the p-length of p-solvable groups and reduction theorems for Burnside's problem* , Proc. London Math. Soc., 6, N3, 1956, 1-42.

[58] G. Higman, *Lie ring methods in the theory of finite nilpotent groups,* Proc. Inter. Congress Math., Edinburgh, 1958, 307-312.

[41] N. Jacobson, *Restricted Lie algebras of characteristic p* , Trans. AMS, 50, 1941, 15-25.

[62] N. Jacobson, *Lie Algebras, Interscience Publishers* , Dover reprint, 1979.

[86] A.I. Kostrikin, *Around Burnside,* , Nauka, Moscow, 1986 (Russian), English translation with addenda, Springer-Verlag 1990.

[88] A.I. Kostrikin and E.I. Zelmanov, *A theorem on sandwich algebras* (Russian), Proc. Steklov Math. Inst. of ANSSSR, 183, 1988, 159-167.

[54] M. Lazard, *Sur les groupes nilpotent et les anneaux de Lie* , Ann. Sci. École Norm Supérieure, 71, N3, 1954, 101-190.

[35] W. Magnus, *Beziehungen zwischen Gruppen und Idealen in einem speziellen Ring* , Math. Ann., 111, 1935, 259-280.

[37] W. Magnus, *Über Beziehungen zwischen höheren Kommutatoren,* J. reine angew. Math., 177, 1937, 105-115.

[40] W. Magnus, *Über Gruppen und zugeordnete Liesche Ringe,* J. reine angew. Math, 182, 1940, 142-149.

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

[51] I. N. Sanov, *On a certain system of relations in periodic groups of prime power exponent,* Izvestia AN SSSR (Russian), 15, 1951, 477-502.

[37] E. Witt, *Treu Darstellung Liescher Ringe,* J. reine angew Math., 177, 1937, 152-160.

[40] H. Zassenhaus, *Ein Verfaren, jeder endlichen p-Gruppe einen Lie-Ring mit der Charackteristic p zuzuordnen,* Abh. Math. Sem. Univ. Hamburg, 13, 1940, 200-207.

[89] E. I. Zelmanov, *On some problems in the theory of groups and Lie algebras* (Russian), Mat. Sb., 180, 1989, 159-167.

[90_1] E. I. Zelmanov, *The solution of the restricted Burnside problem for groups of odd exponent* , to appear in Izvestia AN SSSR (Russian).

[90_2] E. I. Zelmanov, *The solution of the restricted Burnside problem for* 2*-groups,* to appear in Mat. Sb (Russian).