RENDICONTI
del
SEMINARIO MATEMATICO
della
UNIVERSITÀ DI PADOVA

BENEDETTO SCIMEMI

Homogeneous verbal functions on groups

Rendiconti del Seminario Matematico della Università di Padova, tome 49 (1973), p. 299-321

<http://www.numdam.org/item?id=RSMUP_1973__49__299_0>

REND. SEM. MAT. UNIV. PADOVA, Vol. 49 (1973)

Homogeneous Verbal Functions on Groups.

BENEDETTO SCIMEMI (*)

1. – This research was originated by our previous paper [4], whose main results will be shortly recalled: let p be a prime number, P a finite p-group of exponent p^m, d a divisor of $p-1$, a a primitive d-th root of unity, mod p^m, φ an automorphism of P of order d; then every element $h \in P$ can be uniquely written as

$$h = h_1 h_2 \dots h_d \quad \text{with} \quad h_j \in P\,, \quad h_j^{\varphi} = h_j^{a^j} \qquad (j = 1, 2, \dots, d)\,.$$

The set $P_1 = \{h_1;\ h \in P\}$ need not be a subgroup of P (we could take any other $P_j = \{h_j;\ h \in P\}$ with $j \neq d$ to avoid trivialities), but a loop operation $\circ$ can be introduced on P_1 by letting for all $x, y \in P_1$: $x \circ y = (xy)_1$. If this element is expanded in terms of basic commutators in x, y

$$x \circ y = x^{e_1} y^{e_2} [y, x]^{e_3} [y, x, x]^{e_4} \dots$$

then a recursive formula naturally yields for the exponents e_u some rational (non-integer) values; all examples show evidence that these numbers are independent of x, y, P, φ and only depend on d.

The motivation for the present research was to prove this independance, thus showing a more natural origin for the loop structures we studied in [4]. After we noticed that we could assume without loss $P = \langle P_1 \rangle$, it seemed natural to look for a group F^{**} admitting

---

(*) Indirizzo dell'A.: Seminario Matematico dell'Università - Via Belzoni 3, 35100 Padova.

Lavoro eseguito nell'ambito dei Gruppi di Ricerca Matematica del C.N.R.

an automorphism Φ such that: if P is any finite p-group with n generators, and φ is an automorphism of P inducing the a-th power on these generators, then P is a homomorphic image of F^{**} and φ is induced by Φ.

By using a recent theorem of R. H. Bruck [1], a satisfactory answer was found. The main theorem of the present paper (theor. 1, par. 5) states the following:

Let F be a free group of finite rank n, generated by the free generators $X, Y, \ldots$. For each positive number d there exist groups F^* and F^{**} with the following properties:

1) $F \leqslant F^* \leqslant F^{**}$.

2) The elements of F^* may be uniquely represented as infinite ordered products in terms of basic commutators in $X, Y, \ldots$

$$X^{e_1} Y^{e_2} \ldots [Y, X]^{e_w} \ldots [Y, X, X]^{e_v} \ldots$$

where the exponents e_u lie in the ring $\mathbb{Z}_{[d]}$ of those rational numbers r/s such that no prime dividing s is $\equiv 1 \bmod d$.

3) The element of F^{**} are similar, with e_u in $\mathbb{Z}_{[d]}[\alpha]$, the ring obtained from $\mathbb{Z}_{[d]}$ by adjunction of a primitive (complex) d-th root of unity α.

4) In F^{**} the « α-th–power » g^α is defined (for each $g \in F^{**}$) and there exists an automorphism Φ of F^{**} such that

$$X^\Phi = X^\alpha, \quad Y^\Phi = Y^\alpha, \ \ldots .$$

5) Every element $g \in F^*$ (in particular, every word in $X, Y, \ldots$) can be uniquely written as

$$g = g_1 g_2 \ldots g_d \quad \text{with} \quad g_j \in F^*, \quad g_j^\Phi = g_j^{\alpha^j} \qquad (j = 1, 2, \ldots, d) .$$

Now let p be a prime number, P a finite p-group of exponent p^m with n generators $x, y, \ldots$, d a divisor of $p-1$, a a primitive d-th root of unity, mod p^m. Then there exists a unique homomorphism ν of F^{**} onto P such that

$$X^\nu = x , \quad Y^\nu = y , \quad \ldots ; \quad (g^\alpha)^\nu = (g^\nu)^a \qquad \text{for every } g \in F^{**}.$$

If φ is an automorphism of P such that $x^\varphi = x^a$, $y^\varphi = y^a$, ... it is clear

that $x^{\varphi} = x^{\alpha} = (X^{\nu})^{\alpha} = (X^{\alpha})^{\nu} = (X^{\Phi})^{\nu}$. etc. Hence it is easily seen that for every $h \in P$, $h = g^{\nu}$ we have $h^{\varphi} = (g^{\Phi})^{\nu}$, as we wanted.

The consequences of 5) are derived in terms of « verbal functions ». A verbal function on a group is the analog of a polynomial function on a ring. Let H be a group, F the free group with free generators $X_1, X_2, \ldots, X_n$; to each word $f = f(X_1, X_2, \ldots, X_n) \in F$ we associate the « verbal function in n variables on H », say $\hat{f}$, mapping the n-ple $(h_1, h_2, \ldots, h_n)$ of elements $h_i \in H$ into the element $\hat{f}(h_1, h_2, \ldots, h_n) \in H$ which is obtained from f by replacing each X_i by h_i and taking inverses and products in H. For $n = 1$, a verbal function is simply a power; for $n = 2$ among the verbal functions (or verbal operations) we find the usual group-multiplication and conjugation, associated to the words $X_1 X_2$ and $X_1^{-1} X_2 X_1$, etc. Clearly, the verbal functions in n variables on H form a group $\hat{F}$ (with respect to multiplication of images), an image of F under the homomorphism $f \mapsto \hat{f}$. If H is a finite p-group, $p \equiv 1 \bmod d$, then there is a natural way to extend the homomorphism $f \mapsto \hat{f}$ to the group F^{**}. If we apply this homomorphism to the word g, factorized as in 5) above, we derive the following (Cor. 1, par. 7):

Let P be a finite p-group of exponent p^m, d a divisor of $p-1$, a a primitive d-th root of unity, $\bmod p^m$. Then every verbal function $\hat{g}$ on P can be uniquely written as $\hat{g} = \hat{g}_1 \hat{g}_2 \ldots \hat{g}_d$ with

$$\hat{g}_j(h_1^a, h_2^a, \ldots, h_n^a) = \left(\hat{g}_j(h_1, h_2, \ldots, h_n)\right)^{a^j} \qquad \text{for all } h_j \in P,\ j = 1, 2, \ldots, d\,.$$

By analogy with Analysis, a verbal function satisfying the above condition for $\hat{g}_j$ is said to be « a-homogeneous of degree j ». Since $g_j \in F^*$ (but in general $g_j \notin F$), the homogeneous factor $\hat{g}_j$ is obtained from a basic commutator expansion which is uniquely defined by the word g and the number d, through a substitution of elements of P.

If we apply this to the group multiplication on P, thus letting $g = XY = g_1 g_2 \ldots g_d$, we find for $\hat{g}_1$ a loop-operation on P (Theor. 2, par. 7). In particular, for $d = 2$, we find, within isomorphisms, the loop operation which has been extensively studied by G. Glauberman (see ref. in [4]). When P admits an automorphism of order d, this operation is easily proved to induce on the « eigensubset » P_1 the same multiplication we defined above, i.e. $x \circ y = \hat{g}_1(x, y)$.

Apart from loops, the whole subject in the present broader context is strictly connected with the work of M. Lazard [3] on nilpotent groups and Lie-algebras; the relation between his « suites typiques »

and our homogeneous verbal functions is explained in par. 8: roughly speaking, some of his results can be obtained from ours by letting d tend to infinity.

2. – In this paragraph we consider the « binomial » properties of some rings; some of the following elementary remarks may be well-known, but we do not know a complete source to refer to.

Let R be an integral domain of characteristic zero. We shall denote by $\mathbf{N}^{-1}R = \{r/n;\ r \in R,\ 0 \neq n \in \mathbf{Z}\}$ its ring of fractions with integer denominators. If $r \in R$, $0 \leqslant k \in \mathbf{Z}$, the element $\binom{r}{k} \in \mathbf{N}^{-1}R$ is defined as follows:

$$\binom{r}{0} = 1; \qquad \binom{r}{k} = \frac{r(r-1)\ldots(r-k+1)}{k!} \qquad \text{if } k > 0\,.$$

DEFINITION. A « binomial ring » is an integral domain C of characteristic zero, such that $\binom{c}{k}$ is in C for every c in C and every non-negative integer k.

Of course, $\mathbf{Z}$ is a binomial ring (the formula $\binom{-r}{k} = (-1)^k \binom{r+k-1}{k}$ accounts for negatives). However, if x is an indeterminate over $\mathbf{Z}$, then the polynomial ring $\mathbf{Z}[x]$ is not binomial. Therefore we introduce the set

$$\mathbf{Z}\{x\} = \left\{\varrho \in \mathbf{Q}[x];\ \varrho = \sum a_k \binom{x}{k},\ a_k \in \mathbf{Z}\right\}.$$

(Polya's « ganzwertige Polynomen »). It is well-known that $\mathbf{Z}\{x\}$ consists precisely of those polynomials in $\mathbf{Q}[x]$ which assume integer values whenever x is replaced by an integer. This characterization has the immediate consequence that $\mathbf{Z}\{x\}$ is a binomial ring. More generally, if $\mathbf{Z}$ is replaced by any binomial ring C, we define

$$C\{x\} = \left\{\varrho \in \mathbf{N}^{-1}C[x];\ \varrho = \sum c_k \binom{x}{k},\ c_k \in C\right\}$$

and easily check that $C\{x\}$ is a binomial ring. Clearly, if u is an element of a ring containing C, then $C\{u\} = \{\varrho(u);\ \varrho \in C\{x\}\}$ is a minimal

binomial ring containing both C and u (thus $C\{x\}$ is the « binomial closure » of $C[x]$). If $x_1, x_2, \ldots, x_n$ are algebraically independent elements over C, it is natural to define by induction

$$C\{x_1, x_2, \ldots, x_{n-1}, x_n\} = C\{x_1, x_2, \ldots, x_{n-1}\}\{x_n\} .$$

An element ϱ of this ring can be expressed as a linear combination with coefficients in C of products $\binom{x_1}{k_1}\binom{x_2}{k_2}\ldots\binom{x_n}{k_n}$, where the k_i's are non-negative integers; ϱ is characterized by the properties:

$$\varrho \in \mathbf{N}^{-1}C[x_1, x_2, \ldots, x_n]; \qquad \varrho(c_1, c_2, \ldots, c_n) \in C$$

for all $c_i \in C$. In [1], an element of $\mathbf{Z}\{x_1, x_2, \ldots, x_n\}$ is called an « integer-producing polynomial ». In particular, since $\mathbf{Z}\{x, y\} = \mathbf{Z}\{x\}\{y\}$, we must have « binomial identities » as

$$\binom{x+y}{k} = \sum a_{ij}\binom{x}{i}\binom{y}{j}; \qquad \binom{xy}{k} = \sum b_{ij}\binom{x}{i}\binom{y}{j}$$

for some $a_{ij}, b_{ij} \in \mathbf{Z}$.

LEMMA 1. *Any subring (with* 1*) of* $\mathbf{Q}$ *is binomial.*

PROOF. Such a ring consists of all the fractions r/s such that the prime factors of s belong to a fixed set of primes. Then, by the binomial identities above, it suffices to prove that for any prime p we have $\binom{1/p}{k} \in \mathbf{Z}[1/p]$, the subring generated by $1/p$. To this aim, we write $k! = p^m r$ with $p \nmid r$; then $1/p = a + rc$ for some $a \in \mathbf{Z}$, $c \in \mathbf{Z}[1/p]$ hence, by the binomial expansion for $\binom{x+y}{k}$, it suffices to prove $\binom{rc}{j} \in \mathbf{Z}[1/p]$ when $0 \leqslant j \leqslant k$. In fact we compute

$$\binom{rc}{j} = \frac{rc(rc-1)\ldots(rc-j+1)}{j!} = \frac{k!}{j!}\,\frac{c(rc-1)\ldots(rc-j+1)}{p^m} \in \mathbf{Z}[1/p] .$$

If d denotes a positive integer, we shall denote by $\mathbf{Z}_{[d]}$ the ring of the rational numbers r/s such that no prime dividing s is $\equiv 1 \bmod d$ (e.g. $\mathbf{Z}_{[2]} = \mathbf{Z}[\frac{1}{2}]$; $\mathbf{Z}_{[4]} = \mathbf{Z}[\frac{1}{2}, \frac{1}{3}, \frac{1}{7}, \ldots]$).

LEMMA 2. *Let α be a primitive (complex) d-th root of unity. For every non-negative integer k there exists a polynomial $\varrho_k \in \mathbb{Z}_{[d]}[x]$ such that $\binom{\alpha^i}{k} = \varrho_k(\alpha^i)$ for all $i \in \mathbb{Z}$.*

PROOF. Let us write $k! = ts$, where the prime factors of t and s are $\equiv 1$ and respectively $\not\equiv 1 \bmod d$. In the factor ring $\mathbb{Z}/t\mathbb{Z}$ the d-th roots of unity are exactly d, say $a + t\mathbb{Z}, a^2 + t\mathbb{Z}, \ldots, a^d + t\mathbb{Z}$, where $a^i - a^j + t\mathbb{Z}$ is a unit if $i \not\equiv j \bmod d$ (for $t = p^m$ this is in Lemma 1 of [4]; then the Chinese remainder theorem applies). In $\mathbb{Z}[x]$ let us divide $k!\binom{x}{k}$ by $x^d - 1$ and write

$$k!\binom{x}{k} = x(x-1)(x-2)\ldots(x-k+1) = (x^d-1)\beta_k(x) + \gamma_k(x)$$

where $\gamma_k \in \mathbb{Z}[x]$ is a polynomial of degree smaller than d. By substituting $x = a^i$ we obtain

$$k!\binom{a^i}{k} = (a^{id}-1)\beta_k(a^i) + \gamma_k(a^i)\,.$$

Since $(a^{id}-1) \in t\mathbb{Z}$, $\binom{a^i}{k} \in \mathbb{Z}$, we deduce $\gamma_k(a^i) \in t\mathbb{Z}$ for $i = 1, 2, \ldots, d$. From this we shall deduce $\gamma_k \in t\mathbb{Z}[x]$ and

$$\varrho_k = \frac{1}{k!}\gamma_k \in \mathbb{Z}_d[x]; \qquad \varrho_k(\alpha^i) = \binom{\alpha^i}{k}$$

as we wanted. In fact, let us denote by $\bar{\gamma}_k$ the image of γ_k under the natural homomorphism of $\mathbb{Z}[x]$ onto $(\mathbb{Z}/t\mathbb{Z})[x]$. We know that $\bar{\gamma}_k(\bar{a}^i) = \bar{0}$ for $i = 1, 2, \ldots, d$; therefore $\bar{\gamma}_k$ is a polynomial having d distinct roots in $\mathbb{Z}/t\mathbb{Z}$ and degree smaller than d; moreover, the difference of any two such roots is a unit in $\mathbb{Z}/t\mathbb{Z}$, thus $\bar{\gamma}_k = 0$ i.e. $\gamma_k \in t\mathbb{Z}[x]$.

LEMMA 3. $\mathbb{Z}\{\alpha, 1/d\} = \mathbb{Z}_{[d]}[\alpha]$.

PROOF. By Lemma 1, $\mathbb{Z}_{[d]}$ is binomial; by Lemma 2, $\mathbb{Z}_{[d]}[\alpha]$ contains $\binom{\alpha}{k}$ for every k. Since $1/d$ lies in $\mathbb{Z}_{[d]}$, we have $\mathbb{Z}_{[d]}[\alpha] \supseteq \mathbb{Z}\{\alpha, 1/d\}$. As for the inverse inclusion, we must only prove $\mathbb{Z}_{[d]} \subseteq \mathbb{Z}\{\alpha, 1/d\}$ or, equivalently, $1/p \in \mathbb{Z}\{\alpha, 1/d\}$ whenever p is a prime, $p \equiv 1 \bmod d$.

Since this is trivial when $p = d$, we can assume $p = dq + h$, $1 < h < d$. Since all the elements of the field $\mathbb{Z}/p\mathbb{Z}$ are roots of $x^p - x$, we have

$$p!\binom{x}{p} = x(x-1)\dots(x-p+1) \in x^p - x + p\mathbb{Z}[x].$$

Then from $x^p - x = (x^{dp} - 1)x^h + x^h - x$ we derive that the remainder of the division of $p!\binom{x}{p}$ by $x^d - 1$ is

$$\gamma_p(x) = x^h - x + p\sigma(x) \qquad \text{for some } \sigma \in \mathbb{Z}[x].$$

Replacing x by α^i yields

$$\alpha^{-i}\gamma_p(\alpha^i) = -1 + \alpha^{i(h-1)} + p\sigma(\alpha^i)\alpha^{-i}.$$

We now sum over i and take into account that $\sum_{i=1}^{d} \alpha^{ij} = 0$ whenever $\alpha^j \neq 1$. Then Lemma 2 yields

$$\sum \alpha^{-i}\binom{\alpha^i}{p} = \frac{1}{p!}\sum \alpha^{-i}\gamma_p(\alpha^i) = \frac{1}{p!}(-d + pz) \qquad \text{for some } z \in \mathbb{Z}.$$

As a binomial ring containing α, $\mathbb{Z}\{\alpha, 1/d\}$ contains the left hand term, thus also $1/p$, since $p \nmid d$.

Let us notice that $\alpha^i - \alpha^j$ is a unit in $\mathbb{Z}_{[d]}[\alpha]$ whenever $i \not\equiv j \bmod d$. This is easily proved by letting $r = i - j$ in the following relation

$$(1-\alpha^r)\left(\alpha^{r(d-2)} + 2\alpha^{r(d-3)} + \dots + (d-2)\alpha^r + d - 1\right) = d.$$

LEMMA 4. *Let p be a prime integer, $p \equiv 1 \bmod d$. Let m be any natural number, a a primitive d-th root of $1 \bmod p^m$. Then there is a unique ring homomorphism of $\mathbb{Z}_{[d]}[\alpha]$ onto $\mathbb{Z}/p^m\mathbb{Z}$ mapping α into $a + p^m\mathbb{Z}$.*

PROOF. Any element of $\mathbb{Z}_{[d]}$ is written as a fraction r/s, with $p \nmid s$; therefore s is a unit $\bmod p^m$ and hence the natural homomorphism of $\mathbb{Z}$ onto $\mathbb{Z}/p^m\mathbb{Z}$ is uniquely extended to the ring of fractions $\mathbb{Z}_{[d]}$. Since $\mathbb{Z}_{[d]}[\alpha]$ is isomorphic to the factor ring $\mathbb{Z}_{[d]}[x]/(\Phi_d)$ where Φ_d is the cyclotomic polynomial, the statement will hold if we prove $\Phi_d(a) \equiv 0 \bmod p^m$. From $x^d - 1 = \prod_{d' \mid d} \Phi_{d'}$ we derive that $\Phi_d(a) \not\equiv 0 \bmod p^m$ implies $\Phi_{d'}(a) \equiv 0 \bmod p^{m'}$ for some $d' < d$, $0 < m' \leqslant m$.

Since $\Phi_{d'}$ divides $x^{d'}-1$, this implies $a^{d'} \equiv 1 \bmod p^{m'}$, which is impossible, as a is a primitive d-th root of 1 mod $p^{m'}$ (see [4], Lemma 1). Thus $\Phi_d(a) \equiv 0 \bmod p^m$.

3. – We shall operate within a group whose existence and properties are the subject of a recent paper by R. H. Bruck [1]; from it we borrow definitions and symbols, and refer to it for details. Here is the statement of Theor. 1.1 of [1], in a slightly simplified form:

Let $(A, \leqslant)$ be a simply ordered set, consisting of a finite number $n > 0$ of elements; $(A_\infty, \leqslant)$ a universe of basic symbols, based on A; A_m the subset consisting of the elements $u \in A_\infty$ of length $L(u) = m$.

Let $(F, \cdot)$ be a free group of rank n on a free set of generators $\{g_a;\ a \in A\}$; $\{g_u;\ u \in A_\infty\}$ the corresponding set of basic commutators; $\{g_u;\ u \in A_m\}$ the subset of commutators whose total weight equals m.

If C denotes a binomial ring, then there exists a group F^C whose elements may be uniquely represented as ordered infinite products

$$g = \prod_{u \in A_\infty} g_u^{e_u} \qquad (e_u \in C);$$

if $\left(\prod_{u \in A_\infty} g_u^{e_u}\right)\left(\prod_{u \in A_\infty} g_u^{f_u}\right) = \prod_{u \in A_\infty} g_u^{h_u}$, then for each $u \in A_\infty$ we have

$$h_u = e_u + f_u + P_u(e_{u_1}, \ldots, e_{u_k};\ f_{u_1}, \ldots, f_{u_k})$$

where $u_1 < u_2 < \ldots < u_k$ are the elements of A_∞ of length smaller then $L(u)$ and P_u is a uniquely defined element of $\mathbf{Z}\{x_1, \ldots, x_k;\ y_1, \ldots, y_k\}$, i.e. an integer-producing polynomial.

F^C is an extension of F, which is in fact represented by elements $\prod_{u \in A_\infty} g_u^{e_u}$ with all exponents e_u in $\mathbf{Z}$ (as in [2], theor. 11.2.4).

In F^C the « c-th–power » g^c exists for every $g \in F^C$, $c \in C$; if $g^c = \left(\prod_{u \in A_\infty} g_u^{e_u}\right)^c = \prod_{u \in A_\infty} g_u^{f_u}$, then

$$f_u = e_u c + R_u(c;\ e_{u_1}, \ldots, e_{u_k}), \qquad \text{with } R_u \in \mathbf{Z}\{y;\ x_1, \ldots, x_k\}.$$

The fact that P_u and R_u do not depend upon C implies that for their determination one can assume $C = \mathbf{Z}$ and operate within the free nilpotent group F/F_m (here F_m denotes the m-th term of the lower central series of F) by the « collecting process ».

Let us point out some conseguences of this theorem (not all explicitly stated in [1]):

The c-th power enjoys the basic properties of integer powers, i.e.

$$g^{c_1+c_2} + g^{c_1}g^{c_2}; \qquad g^{c_1c_2} = (g^{c_1})^{c_2}; \qquad (g_1g_2)^c = g_1^c g_2^c [g_2, g_1]^{\binom{c}{2}} \dots$$

the last formula being a generalization of P. Hall's ([2], 12.3.1).

By analogy with the language of C-modules, one can introduce the concepts of C-groups (i.e. groups with c-th power for $c \in C$), C-subgroups, C-homomorphisms etc. by requiring the compatibility with taking c-th powers. If one does so, some basic properties of F are naturally generalized to F^C; for example: the lower central series of F^C consists of C-subgroups, each term F_C^m consisting of those elements $\prod_{u \in A_\infty} g_u^{e_u}$ for which $e_u = 0$ when $L(u) < m$; the factor-group F_m^C / F_{m+1}^C is a free C-module; since $\bigcap_m F_m^C = \{1\}$, a statement holding on F^C / F_m^C may be proved to hold on F^C, by induction on m. These and others similar statements can be proved by a common procedure, as follows: a property of F is reduced to a set of relations among the (integer) exponents involved in the infinite-product representation. Because of their polynomial nature, the same relation must hold when $\mathbb{Z}$ is replaced by C, thus yielding the analogous property for F^C. In par. 4 we shall exhibit some examples of this procedure.

F^C is called a « completion of F » with respect to the ring C. Here « completeness » means substantially that if $h_1, h_2, \dots, h_j, \dots$ is a sequence of elements of F^C such that $h_j \in F_j^C$ for every j, then the sequence of partial products

$$k_1 = h_1, \quad k_2 = h_1h_2, \quad \dots, \quad k_j = h_1h_2 \dots h_j, \quad \dots$$

converges to a unique element $k \in F^C$; in other words $k \equiv k_j \bmod F_j^C$ for every j. Therefore some infinite products are meaningful in F^C; for example, the ordered product $\prod_{u \in A_\infty} h_u$ is a well-defined element of F^C, provided the following condition holds: if $L(u) = m$, then $h_u \in F_m^C$. In fact, the finiteness of A implies that only a finite number of basic commutators have weight m.

4. – One of the basic properties of the free group F implies that for any integer c there exists a unique endomorphism of F mapping every free generator g_a $(a \in A)$ into its c-th power.

The purpose of this paragraph is to extend in the natural way this endomorphism to F^c, letting c assume any value in C. To this aim, we start with the basic commutators and define, for any $c \in C$, $v \in A_\infty$

$$g_v^{[c]} = g_v^c \qquad \text{if } L(v) = 1\,,$$
$$g_v^{[c]} = [g_t^{[c]}, g_s^{[c]}] \qquad \text{if } g_v = [g_t, g_s];\ s < t;\ L(s), L(t) < L(v)\,.$$

LEMMA 5:

(a) $g_v^{[c]} = \prod_{u \in A_\infty} g_u^{\varepsilon_{v,u}(c)}$ *for some* $\varepsilon_{v,u} \in \mathbb{Z}\{x\}$;

(b) $\varepsilon_{v,v} = x^m$ *if* $L(v) = m$;

$\varepsilon_{v,u} = 0$ *if* $L(v) > L(u)$, *or* $L(u) = L(v)$ *and* $u \neq v$.

PROOF. Since (a) is true by definition if $L(v) = 1$, we shall induce on $m = L(v)$. Then we can assume

$$g_s^{[c]} = \prod_{u \in A_\infty} g_u^{\varepsilon_{s,u}(c)}; \qquad g_t^{[c]} = \prod_{u \in A_\infty} g_u^{\varepsilon_{t,u}(c)}; \qquad \varepsilon_{s,u}, \varepsilon_{t,u} \in \mathbb{Z}\{x\}\,.$$

Therefore we calculate (compare par. 3)

$$g_t^{[c]} g_s^{[c]} = \prod_{u \in A_\infty} g_u^{\eta_u(c)}$$

where

$$\eta_u(x) = \varepsilon_{t,u}(x) + \varepsilon_{s,u}(x) + P_u\big(\varepsilon_{t,u_1}(x), \ldots, \varepsilon_{t,u_k}(x);\ \varepsilon_{s,u_1}(x), \ldots, \varepsilon_{s,u_k}(x)\big) \in \mathbb{Z}\{x\};$$

$$(g_t^{[c]})^{-1} = \prod_{u \in A_\infty} g_u^{\theta_u(c)}$$

where

$$\theta_u(x) = -\varepsilon_{t,u}(x) + R_u\big(-1;\ \varepsilon_{t,u_1}(x), \ldots, \varepsilon_{t,v_k}(x)\big) \in \mathbb{Z}\{x\}\,.$$

Similarly we calculate the commutator $(g_t^{[c]})^{-1}(g_s^{[c]})^{-1} g_t^{[c]} g_s^{[c]}$ and prove statement (a).

b) It is a consequence of well-known commutator-relations ([2], 18.4.10 and foll.) that in the group F we have $g_v^{[c]} \equiv g_v^{c^m} \bmod F_{m+1}$ whenever $c \in \mathbb{Z}$, $m = L(v)$. This is equivalent to $\varepsilon_{v,v}(c) = c^m$, $\varepsilon_{v,u}(c) = 0$ for $L(u) < L(v)$ or $L(u) = L(v)$, $u \neq v$ for any c integer. Since $\varepsilon_{v,u}$ is a polynomial, the same must hold when c assumes any value in the ring C. q.e.d.

Now let $g = \prod_{u \in A_\infty} g_v^{e_v}$ be any element of F^c. We define

$$g^{[c]} = \prod_{v \in A_\infty} (g_v^{[c]})^{e_v}.$$

First of all, we must prove that there is no problem involved with the infinite number of factors. According to the final remarks in par. 3, it will suffice to show that $(g_v^{[c]})^{e_v} \in F_m^c$ if $m = L(v)$. In fact we claim

$$(g_v^{[c]})^{e_v} = \prod_{u \in A_\infty} g_u^{\varrho_{v,u}(c, e_v)}, \qquad \varrho_{v,u} \in \mathbb{Z}\{x, y\},$$

$$\varrho_{v,v} = x^m y; \qquad \varrho_{v,u} = 0 \qquad \text{whenever } L(u) < m \text{ or } L(u) = m,\ u \neq v.$$

This follows from Lemma 5, if we set

$$\varrho_{v,u}(x, y) = \varepsilon_{v,u}(x)\, y + R_u\big(y;\ \varepsilon_{v,u_1}(x), \ldots, \varepsilon_{v,u_k}(x)\big).$$

LEMMA 6. *Let*

$$g = \prod_{u \in A_\infty} g_u^{e_u}, \qquad g^{[c]} = \prod_{u \in A_\infty} g_u^{f_u} \quad (e_u, f_u \in C).$$

Then $f_u = c^m e_u + Q_u(c;\ e_{u_1}, \ldots, e_{u_k})$, *where* $u_1 < u_2 < \ldots < u_k$ *are the elements of* A_∞ *whose length is smaller than* m, *and* $Q_u \in \mathbb{Z}\{y;\ x_1, \ldots, x_k\}$

PROOF. In order to calculate f_u we only have to consider the finite product $\prod_{L(v) \leqslant m} (g_v^{[c]})^{e_v}$. Since we have just seen that $(g_v^{[c]})^{e_v} = \prod_{u \in A_\infty} g_u^{\varrho_{v,u}(c, e_v)}$, a repeated use of the product formula (involving the polynomial P_u) combined with Lemma 5 yields (*b*).

LEMMA 7. *Let* $c \in C$. *Then the mapping* $g \mapsto g^{[c]}$ *is a* C*-endomorphism of* F^c. *If* $e \in C$, *then* $(g^{[c]})^{[e]} = g^{[ce]}$.

PROOF. Let $g = \prod_{u \in A_\infty} g_u^{e_u}$, $g' = \prod_{u \in A_\infty} g_u^{e'_u}$ be elements of F^c. We write $(gg')^{[c]} = \prod_{u \in A_\infty} g_u^{s_u}$, $(g^{[c]})(g'^{[c]}) = \prod_{u \in A_\infty} g_u^{t_u}$ and use Lemma 6 to show that

$$s_u = (e_u + e'_u)\, c^m + S_u(c;\ e_{u_1}, \ldots, e_{u_k};\ e'_{u_1}, \ldots, e'_{u_k})$$

$$t_u = e_u c^m + e'_u c^m + T_u(c;\ e_{u_1}, \ldots, e_{u_k};\ e'_{u_1}, \ldots, e'_{u_k})$$

where

$$L(u_1), \ldots, L(u_k) < L(u) = m; \qquad S_u, T_u \in \mathbb{Z}\{y;\ x_1, \ldots, x_k;\ y_1, \ldots, y_k\}.$$

But when $g \in F$ and $c \in \mathbf{Z}$, by construction, the mapping $g \mapsto g^{[c]}$ induces an endomorphism of F. Therefore $s_u = t_u$ in this case, hence also $S_u = T_u$ by the familiar argument, and $(gg')^{[c]} = (g^{[c]})(g'^{[c]})$.

The proofs that $(g^{[c]})^e = (g^e)^{[c]}$ and $(g^{[c]})^{[e]} = g^{[ce]}$ are similar, involving polynomials in $c, e, e_{u_1}, \ldots, e_{u_k}$.

We conclude this paragraph with a definition and some remarks which will simplify the proof of our main theorem in par. 5.

DEFINITION. A mapping $\varepsilon: C \to F^C$ will be called a $C\{x\}$-mapping if for each $u \in A_\infty$ there exists an element $\varepsilon_u \in C\{x\}$ such that

$$\varepsilon: c \mapsto \prod_{u \in A_\infty} g_u^{\varepsilon_u(c)} \qquad \text{for every } c \in C .$$

For example, if g is a fixed element in F^C, then the « exponential function » $c \mapsto g^c$ is a $C\{x\}$-mapping; by Lemma 6, the same holds for $c \mapsto g^{[c]}$. More generally, our previous remarks show that products and powers of $C\{x\}$-mappings are still such.

5. – Let c be an element of the binomial ring C, $g \mapsto g^{[c]}$ the endomorphism of F^C of Lemma 7, j a natural number. The element $g_0 \in F^C$ will be defined to be « c-homogeneous of degree j » if $g_0^{[c]} = g_0^{c^j}$ (i.e. g_0 is an « eigen-element » belonging to the « eigenvalue » c^j). The term is suggested by the fact that such an element will produce « c-homogeneous functions » in the sense of par. 1.

Let d be a positive number, $\mathbf{Z}_{[d]}$ and $\mathbf{Z}_{[d]}[\alpha]$ the rings defined in par. 2; we apply the construction of par. 3 with these rings in the role of C (by Lemma 1 and 4 both are binomial) and consider the groups $F^{\mathbf{Z}_{[d]}}$, $F^{\mathbf{Z}_{[d]}}[\alpha]$. Then F is naturally embedded in $F^{\mathbf{Z}_{[d]}}$ and the latter in $F^{\mathbf{Z}_{[d]}}[\alpha]$.

The main result of this paper is

THEOREM 1. *Every element $g \in F^{\mathbf{Z}_{[d]}}$ can be uniquely written as*

$$g = g_1 g_2 \ldots g_d \qquad \textit{with} \qquad g_j \in F^{\mathbf{Z}_{[d]}}, \qquad g_j^{[\alpha]} = g_j^{\alpha^j}$$

i.e. a product of α-homogeneous elements of degree $j = 1, 2, \ldots, d$.

PROOF. Let us write for short $F^* = F^{\mathbf{Z}_{[d]}}$, $F^{**} = F^{\mathbf{Z}_{[d]}}[\alpha]$. It may be worth to point out that g_j is to be found in F^* although $g_j^{[\alpha]}$ is

only defined in F^{**}. By Lemma 7, a α-homogeneous element of degree j is also α^i-homogeneous of degree j for all integers i.

We shall operate mod F_m^{**}, and induce on m.

For $m = 1$ we define:

$$g_{1,1} = g; \qquad g_{1,2} = \ldots = g_{1,d} = 1 .$$

It follows from Lemma 5 (or directly from the definition of $g \mapsto g^{[\alpha]}$) that any element of F^{**} is α-homogeneous of degree 1, mod F_2^{**}. Therefore we have

$$g = g_{1,1} g_{1,2} \cdots g_{1,d}; \qquad g_{1,j}^{[\alpha]} \equiv (g_{1,j})^{\alpha^j} \mod F_2^{**}$$

the last congruence being trivial for $j = 2, \ldots, d$. The elements $g_{1,j}$ are in F^* and they are unique mod F_2^{**}, since for $j = 2, \ldots, d$ the condition $(g_{1,j})^{\alpha} \equiv g_{1,j}^{[\alpha]} \equiv (g_{1,j})^{\alpha^j}$ implies $(g_{1,j})^{\alpha - \alpha^j} \equiv 1$, thus $g_{1,j} \equiv 1$. Then the other condition implies also $g_{1,1} \equiv g$.

Let us assume that we have proved the existence of d elements $g_{m-1,j} \in F^*$ which are unique mod F_m^{**} with respect to the following conditions

$$g \equiv g_{m-1,1} g_{m-1,2} \cdots g_{m-1,d}; \qquad g_{m-1,j}^{[\alpha]} \equiv (g_{m-1,j})^{\alpha^j} \mod F_m^{**} .$$

We must construct d elements $g_{m,j} \in F^*$ satisfying similar congruences and prove their unicity mod F_{m+1}^{**}. To this aim, we shall compute the « mean value » of $(g_{m-1,j}^{[c]})^{c^{-j}}$ for c running over the d-th roots of unity. Thus let us define

$$g_{m,j}^* = \left((g_{m-1,j}^{[\alpha]})^{\alpha^{-j}} (g_{m-1,j}^{[\alpha^2]})^{\alpha^{-2j}} \cdots (g_{m-1,j}^{[\alpha^d]})^{\alpha^{-dj}}\right)^{1/d}.$$

We now consider the mapping $\zeta_{m,j}$ of $\mathbf{Z}_{[d]}$ into F^{**} defined by

$$\zeta_{m,j} \colon c \mapsto (g_{m-1,j})^{-1} (g_{m-1,j}^{[c]})^{c^{-j}} \qquad \text{for every } c \in \mathbf{Z}_{[d]} .$$

Since $g_{m-1,j}$ lies in F^*, the final remarks in par. 4 show that $\zeta_{m,j}$ is a $\mathbf{Z}_{[d]}[x]$-mapping, i.e.

$$\zeta_{m,j}(c) = \prod_{u \in A_\infty} g_u^{\varepsilon_u(c)} \qquad \text{with} \qquad \varepsilon_u \in \mathbf{Z}_{[d]}[x] .$$

By letting $c = \alpha^i$ $(i = 1, 2, \ldots, d)$, the inductive assumption implies $\zeta_{m,j}(\alpha^i) \equiv 1 \bmod F_m^{**}$, therefore $\varepsilon_u(\alpha^i) \equiv 0$ if $L(u) < m$. Thus we have $\zeta_{m,j}(\alpha^i) \equiv \prod_{u \in A_m} g_u^{e_u(\alpha^i)} \bmod F_{m+1}^{**}$. If we take into account that these elements are central $\bmod F_{m+1}^{**}$ we can compute:

$$g_{m,j}^* = \Big(\prod_{i=1}^{d} (g_{m-1,j}^{[\alpha^i]})^{\alpha^{-ij}}\Big)^{1/d} \equiv g_{m-1,j}\Big(\prod_{i=1}^{d} \zeta_{m,j}(\alpha^i)\Big)^{1/d} \equiv$$
$$\equiv g_{m-1,j} \prod_{u \in A_m} g_u^{1/d \sum_{i=1}^{d} e_u(\alpha^i)} \bmod F_{m+1}^{**}.$$

We want to prove that the exponent of g_u lies in $\mathbb{Z}_{[d]}$.

In fact, by Lemma 2 for each positive integer k there exists a polynomial $\varrho_k \in \mathbb{Z}_{[d]}[x]$ such that $\binom{\alpha^i}{k} = \varrho_k(\alpha^i)$; it follows that for every $\varepsilon_u \in \mathbb{Z}_{[d]}[x]$ there is a polynomial

$$\eta_u = c_{u,0} + c_{u,1}x + \ldots + c_{u,d-1}x^{d-1} \in \mathbb{Z}_{[d]}[x]$$

such that $\varepsilon_u(\alpha^i) = \eta_u(\alpha^i)$. Since for $j = 1, 2, \ldots, d-1$ we have $\sum_{i=1}^{d} \alpha^{ij} = 0$ we get $1/d \sum_{i=1}^{d} \varepsilon_u(\alpha^i) = c_{u,0} \in \mathbb{Z}_{[d]}$ as we wanted. Therefore we have proved $g_{m,j}^* \in F^* \bmod F_{m+1}^{**}$. For $j \not\equiv m \bmod d$ let us define $g_{m,j} \in F^*$ from $g_{m,j}^*$ by simply cancelling all factors of weight greater than m in its infinite-product representation; for $\bar{j} \equiv m \bmod d$ let us define

$$g_{m,\bar{j}} = (g_{m,\bar{j}-1})^{-1}(g_{m,\bar{j}-2})^{-1} \ldots (g_{m,1})^{-1} g (g_{m,d})^{-1} \ldots (g_{m,\bar{j}+1})^{-1}.$$

We must now prove the congruences $g_{m,j}^{[\alpha]} \equiv (g_{m,j})^{\alpha^j} \bmod F_{m+1}^{**}$.

We have by definition

$$g_{m,j} \equiv g_{m,j}^* \equiv \Big(\prod_{i=1}^{d} (g_{m-1,j}^{[\alpha^i]})^{\alpha^{-ij}}\Big)^{1/d}.$$

Hence by Lemma 7 we compute

$$g_{m,j}^{[\alpha]} \equiv \Big(\prod_{i=1}^{d} (g_{m-1,j}^{[\alpha^{i+1}]})^{\alpha^{-ij}}\Big)^{1/d} \equiv \Big(\Big(\prod_{i=1}^{d} (g_{m-1,j}^{[\alpha^{i+1}]})^{\alpha^{-(i+1)j}}\Big)^{\alpha^j}\Big)^{1/d} \equiv$$
$$\equiv \Big(\Big(\prod_{s=1}^{d} (g_{m-1,j}^{[\alpha^s]})^{\alpha^{-sj}}\Big)^{1/d}\Big)^{\alpha^j} \equiv (g_{m,j})^{\alpha^j}.$$

Here we have used the fact that for all j we have

$$(g_{m-1,j}^{[\alpha^s]})^{\alpha^{-sj}} = g_{m-1,j}\zeta_{m,j}(\alpha^s), \qquad \zeta_{m,j}(\alpha^s) \in F_m^{**}$$

so that $(\mathrm{mod}\, F_{m+1}^{**})$ the order of the factors in the product $\prod_{i=1}^{d}$ is irrelevant, and the exponent α^j may be taken out of the parenthesis. We still have to consider the value $\bar{j} \equiv m \bmod d$. First we notice that for any $j \not\equiv m$ the construction above has given $g_{m,j} \equiv g_{m-1,j} \bmod F_m^*$; then the inductive assumption $g \equiv g_{m-1,1} \dots g_{m-1,d}$ combined with the definition of $g_{m,\bar{j}}$ yields also $g_{m,\bar{j}} \equiv g_{m-1,\bar{j}} \bmod F_m^*$. Since we have proved the congruence $g_{m,\bar{j}}^* \equiv g_{m-1,\bar{j}} \bmod F_m^*$, we deduce that we can write

$$g_{m,\bar{j}} \equiv g_{m,\bar{j}}^* z_m \bmod F_{m+1}^*$$

where z_m is a product of powers of basic commutators g_u of weight $L(u) = m$. From Lemma 5 we know that for such commutators we have

$$g_u^{[\alpha]} \equiv (g_u)^{\alpha^m} \bmod F_{m+1}^{**}.$$

This gives immediately $z_m^{[\alpha]} \equiv z_m^{\alpha^m} = z_m^{\alpha^{\bar{j}}}$ and finally

$$g_{m,\bar{j}}^{[\alpha]} = (g_{m,\bar{j}}^*)^{[\alpha]} z_m^{[\alpha]} \equiv (g)^{\alpha^{\bar{j}}} (z_m)^{\alpha^{\bar{j}}} \equiv (g_{m,j})^{\alpha^{\bar{j}}} \bmod F_{m+1}^{**}.$$

As for unicity, let us assume that $h_{m,j} \in F^*$ $(j = 1, 2, \dots, d)$ satisfy the same requirements for $g_{m,j}$:

$$g \equiv h_{m,1} h_{m,2} \dots h_{m,d}; \qquad h_{m,j}^{[\alpha]} \equiv (h_{m,j})^{\alpha^j}.$$

By the inductive assumption we can write, $\bmod F_{m+1}^{**}$:

$$g_{m,j} \equiv h_{m,j} w_{m,j} \qquad \text{for some } w_{m,j} \in F_m^*.$$

Since the previous argument gives $w_{m,j}^{[\alpha]} \equiv (w_{m,j})^{\alpha^m} \bmod F_{m+1}^{**}$ we can compute $g_{m,j}^{[\alpha]}$ in two different ways, namely:

$$g_{m,j}^{[\alpha]} \equiv (g_{m,j})^{\alpha^j} \equiv (h_{m,j} w_{m,j})^{\alpha^j} \equiv (h_{m,j})^{\alpha^j} (w_{m,j})^{\alpha^j};$$

$$\equiv (h_{m,j} w_{m,j})^{[\alpha]} \equiv h_{m,j}^{[\alpha]} w_{m,j}^{[\alpha]} \equiv (h_{m,j})^{\alpha^j} (w_{m,j})^{\alpha^m}$$

$\bmod F^{**}_{m+1}$. By comparison we get $(w_{m,j})^{\alpha^j-\alpha^m} \equiv 1$, hence $w_{m,j} \equiv 1$, whenever $j \not\equiv m \bmod d$. As for $\bar{j} \equiv m$, the first condition $g \equiv h_{m,1} \dots h_{m,d}$ implies $w_{m,1} \dots w_{m,d} \equiv 1$, thus $w_{m,j} \equiv 1$. Thus the theorem is completely proved.

Let us remark that along the proof the power mappings $g \mapsto g^\alpha$, $g \mapsto g^{1/d}$ have both been used. By Lemma 3, $\mathbb{Z}_{[d]}[\alpha]$ is a minimal binomial ring containing α and $1/d$. Therefore, if this proof has to be carried on in a group of type F^C, we cannot choose for C a smaller ring than $\mathbb{Z}_{[d]}[\alpha]$. For the same reason we cannot expect to find the homogeneous factors g_j in a proper subgroup of $F^* = F^{\mathbb{Z}_{[d]}}$, even if g lies in F.

6. The proof of theorem 1 gives a recursive method to compute $g_{m,j}$ starting with $g_{m-1,j}$, so that g_j can be determined $\bmod F^*_m$ for arbitrary m. We shall apply the first steps of this procedure to the element XY of the free group $F = \langle X, Y \rangle$, whose elements are represented by ordered infinite products as

$$X^{e_1} Y^{e_2} [Y, X]^{e_3} [Y, X, X]^{e_4} [Y, X, Y]^{e_5} \dots .$$

We first choose $d = 2$ ($d = 1$ is uninteresting). Then $\alpha = -1$ and $\mathbb{Z}_{[2]}[\alpha] = \mathbb{Z}_{[2]} = \mathbb{Z}[\frac{1}{2}]$. We compute:

$$\left.\begin{aligned} g_{1,1} &\equiv XY \\ g_{1,2} &\equiv 1 \end{aligned}\right\} \bmod F^*_2; \qquad (\text{here } F^* = F^{\mathbb{Z}_{[2]}})$$

$$\left.\begin{aligned} g_{2,1} &\equiv \big((X^{-1}Y^{-1})^{-1} XY\big)^{\frac{1}{2}} \equiv XY[Y, X]^{\frac{1}{2}} \\ g_{2,2} &\equiv (g_{2,1})^{-1} XY \equiv [Y, X]^{-\frac{1}{2}} \end{aligned}\right\} \bmod F^*_3;$$

$$\left.\begin{aligned} g_{3,1} &\equiv XY(g_{2,2})^{-1} \equiv XY[Y, X]^{\frac{1}{2}} [Y, X, X]^{-\frac{1}{4}} [Y, X, Y]^{-\frac{1}{4}} \\ g_{3,2} &\equiv \big([Y^{-1}, X^{-1}]^{-\frac{1}{2}} [Y, X]^{-\frac{1}{2}}\big)^{\frac{1}{2}} \equiv [Y, X]^{-\frac{1}{2}} [Y, X, X]^{\frac{1}{4}} [Y, X, Y]^{\frac{1}{4}} \\ &\text{etc.} \end{aligned}\right\} \bmod F^*_4$$

Let us now choose $d = 3$. We compute

$$\left.\begin{aligned} g_{1,1} &\equiv XY \\ g_{1,2} &\equiv 1 \\ g_{1,3} &\equiv 1 \end{aligned}\right\} \bmod F^*_2 \qquad (\text{here } F^* = F^{\mathbb{Z}_{[3]}})$$

$$\left.\begin{aligned} g_{2,1} &\equiv \left((X^{\alpha}Y^{\alpha})^{\alpha^{-1}}(X^{\alpha^2}Y^{\alpha^2})^{\alpha^{-2}}XY\right)^{\frac{1}{2}} \equiv XY[Y,X]^{\frac{1}{2}} \\ g_{2,2} &\equiv (g_{2,1})^{-1}XY(g_{2,3})^{-1} \equiv [Y,X]^{-\frac{1}{2}} \\ g_{2,3} &\equiv 1 \end{aligned}\right| \bmod F_3^*$$

$$\left.\begin{aligned} g_{3,1} &\equiv \left(\left(X^{\alpha}Y^{\alpha}[Y^{\alpha},X^{\alpha}]^{\frac{1}{2}}\right)^{\alpha^{-1}}\left(X^{\alpha^2}Y^{\alpha^2}[Y^{\alpha^2},X^{\alpha^2}]^{\frac{1}{2}}\right)^{\alpha^{-2}}\left(XY[Y,X]^{\frac{1}{2}}\right)\right)^{\frac{1}{2}} \equiv \\ &\equiv XY[Y,X]^{\frac{1}{2}}[Y,X,X]^{-\frac{1}{12}}[Y,X,Y]^{\frac{1}{12}} \\ g_{3,2} &\equiv \left(\left([Y^{\alpha},X^{\alpha}]^{-\frac{1}{2}}\right)^{\alpha^{-2}}\left([Y^{\alpha^2},X^{\alpha^2}]^{-\frac{1}{2}}\right)^{\alpha^{-1}}[Y,X]^{-\frac{1}{2}}\right)^{\frac{1}{2}} \equiv \\ &\equiv [Y,X]^{-\frac{1}{2}}[Y,X,X]^{\frac{1}{6}}[Y,X,Y]^{\frac{1}{6}} \\ g_{3,3} &\equiv (g_{3,2})^{-1}(g_{3,1})^{-1}XY \equiv [Y,X,X]^{-\frac{1}{6}}[Y,X,Y]^{-\frac{1}{6}} \\ &\text{etc.} \end{aligned}\right| \bmod F_4^*$$

For $d = 2, 3, 4$ and within weight 4 (i.e. mod F_5^*) we find the same exponents appearing in [4], p. 215. The reason for this coincidence (the computing method was there fairly different) will be explained in par. 7. From theor. 3 it will also be clear why two different values $d < d'$ yield the same elements $g_{i,j}$ for $i, j \leqslant d$.

The case $d = 2$ is special: if we start from a word $g \in F$ we can avoid recursive formulas and basic commutators expansions, since the « mean value » of $(g^{[c]})^{c^{-1}}$ over the two roots ± 1 gives directly the exact formula for g_1. In fact let us write

$$f_1 = \left(g(g^{[-1]})^{-1}\right)^{\frac{1}{2}}; \qquad f_2 = (f_1)^{-1}g; .$$

We claim: $f_1 = g_1$, $f_2 = g_2$. We easily compute:

$$f_1^{[-1]} = \left(g^{[-1]}(g^{[-1][-1]})^{-1}\right)^{\frac{1}{2}} = (g^{[-1]}g^{-1})^{\frac{1}{2}} = (f_1)^{-1},$$

$$f_2^{[-1]} = (f_1^{[-1]})^{-1}g^{[-1]} = f_1 g^{[-1]} = (f_1)^{-1}f_1^2 g^{[-1]} =$$

$$= (f_1)^{-1}g(g^{[-1]})^{-1}g^{[-1]} = (f_1)^{-1}g = f_2 .$$

By unicity we must have $f_1 = g_1$, $f_2 = g_2$ as we wanted.

In particular, if $g = XY$ we find

$$g_1 = (XY^2X)^{\frac{1}{2}}; \qquad g_2 = (XY^2X)^{-\frac{1}{2}}XY = (XY^2X)^{\frac{1}{2}}X^{-1}Y^{-1}.$$

7. We shall apply theor. 1 to finite p-groups; possible generalizations will be discussed later. In this paragraph P will always denote

a finite p-group of exponent p^m, d a divisor of $p-1$, a a primitive d-th root of unity, mod p^m.

There is a unique way to assign to P a structure of $\mathbb{Z}_{[d]}$-group, i.e. for any $h \in P$, $c = r/s \in \mathbb{Z}_{[d]}$ we define h^c to be the unique element $k \in P$ such that $k^s = h^r$. Equivalently, we may consider the canonical ring-homomorphism of $\mathbb{Z}$ onto $\mathbb{Z}/p^m\mathbb{Z}$, extend it to the ring of fractions $\mathbb{Z}_{[d]}$ by letting $c = r/s \mapsto (r + p^m\mathbb{Z})(s + p^m\mathbb{Z})^{-1} = b + p^m\mathbb{Z}$ and define $h^c = h^b$. P becomes also (although not canonically) a $\mathbb{Z}_{[d]}[\alpha]$-group if we define $h^\alpha = h^a$ i.e. we use the homomorphism of Lemma 4.

We now choose n generators $x_1, x_2, \ldots, x_n$ for P and denote by F the free group with free generators $g_1, g_2, \ldots, g_n$. Then we see that there is a unique $\mathbb{Z}_{[d]}[\alpha]$-homomorphism ν of $F^{\mathbb{Z}_{[d]}}[\alpha] = F^{**}$ onto P such that

$$g_i^\nu = x_i \quad (i = 1, 2, \ldots, n); \qquad (g^\alpha)^\nu = (g^\nu)^a \quad \text{for every } g \in F^{**}.$$

If ν is such a homomorphism, it is clear how it must act on a basic commutator g_u; as ν is also $\mathbb{Z}_{[d]}[\alpha]$-admissible, then we must have for any

$$g = \prod_{u \in A_\infty} g_u^{e_u} \quad \left(e_u \in \mathbb{Z}_{[d]}[\alpha]\right), \qquad g^\nu = \prod_{u \in A_\infty} (g_u^\nu)^{e_u}$$

where only finite factors are non trivial, as P is nilpotent. This accounts for unicity. As for existence, we may define g^ν by the last equation above; the proof that ν is a $\mathbb{Z}_{[d]}[\alpha]$-homomorphism follows easily, once the exponents e_u have been replaced by proper integers, i.e. by the ring homomorphism of $\mathbb{Z}_{[d]}[\alpha]$ on $\mathbb{Z}/p^m\mathbb{Z}$ we described in Lemma 4.

As we have already seen in par. 1, this implies in particular that if φ is an automorphism of $P = \langle x_1, x_2, \ldots, x_n \rangle$ such that $x_i^\varphi = x_i^a$ for $i = 1, 2, \ldots, d$ then φ is induced on $P \simeq F^{**}/\mathrm{Ker}\,\nu$ by the automorphism $\Phi: g \mapsto g^{(\alpha)}$ of F^{**}.

Now we reconsider the homomorphism $g \mapsto \hat{g}$ described in par. 1, mapping the free group F onto the group $\hat{P}$ of the verbal functions in n variables on the p-group P. As before, there is the possibility to extend this mapping to a $\mathbb{Z}_{[d]}[\alpha]$-homomorphism of F^{**} (the finite p-group $\hat{P}$ plays now the role of P above): if $g = \prod_{u \in A_\infty} g_u^{e_u}$ $(e_u \in \mathbb{Z}_{[d]}[\alpha])$, for any n-ple $(h_1, h_2, \ldots, h_n)$ of elements $h_i \in P$ we define

$$\hat{g}(h_1, h_2, \ldots, h_n) = \prod_{u \in A_\infty} \hat{g}_u(h_1, h_2, \ldots, h_n)^{e_u}.$$

Clearly, if $g_j^{[\alpha]} = g_j^{\alpha^j}$ in F^{**}, then $\hat{g}_j$ is a-homogeneous of degree j, i.e.

$$\hat{g}_j(h_1^a, h_2^a, \ldots, h_n^a) = (\hat{g}_j(h_1, h_2, \ldots, h_n))^{a^j} \qquad \text{for all } h_i \in P .$$

Then from Theor. 1 it follows

COROLLARY 1. *Let P be a finite p-group of exponent p^m, d a divisor of $p-1$, a a primitive d-th root of $1 \bmod p^m$. Then every verbal function (in n variables) on P can be uniquely written as a product of d a-homogeneous verbal functions of degree $1, 2, \ldots, d$.*

PROOF. Let $\hat{g}$ be a verbal function on P, corresponding to the word $g \in F$. We embed F in F^{**} and write $g = g_1 g_2 \ldots g_d$, $g_j \in F^*$ as in Theor 1. Then g_j may be not in F, but $\hat{g}_j$ is a verbal function on P (i.e. there is a word $g_j' \in F$, although depending on P, such that $\hat{g}_j' = \hat{g}_j$) and clearly $\hat{g} = \hat{g}_1 \hat{g}_2 \ldots \hat{g}_d$, $\hat{g}_j$ being a-homogeneous of degree j. As for unicity, let us assume also $\hat{g} = \hat{f}_1 \hat{f}_2 \ldots \hat{f}_d$, $\hat{f}_j \in F$, $\hat{f}_j$ a-homogeneous of degree j. We shall induce on the class c of P (or $\hat{P}$), thus assuming $\hat{f}_j \equiv \hat{g}_j \bmod P_c$. Then if we set $z_j = f_j^{-1} g_j$, the element $\hat{z}_j(h_1, \ldots, h_n)$ lies in the center of P for any $h_i \in P$, hence:

$$\hat{z}_j(h_1^a, \ldots, h_n^a) = (\hat{f}_j(h_1^a, \ldots, h_n^a))^{-1} \hat{g}_j(h_1^a, \ldots, h_n^a) =$$
$$= (\hat{f}_j(h_1, \ldots, h_n))^{-a^j} \cdot (\hat{g}_j(h_1, \ldots, h_n))^{a^j} = (\hat{z}_j(h_1, \ldots, h_n))^{a^j}.$$

Moreover, the assumption $\hat{f}_1 \ldots \hat{f}_d = \hat{g}_1 \ldots \hat{g}_d$ implies $\hat{z}_1(h_1, \ldots, h_n) \ldots \ldots \hat{z}_d(h_1, \ldots, h_n) = 1$. If we replace each h_j by its power $h_j^{a^j}$ we get for the elements $k_j = \hat{z}_j(h_1, \ldots, h_n)$ the following relations:

$$k_1^a k_2^{a^2} \ldots k_d^{a^d} = k_1^{a^2} k_2^{a^4} \ldots k_d^{a^{2d}} = \ldots = k_1 k_2 \ldots k_d = 1 .$$

These are equivalent to a set of d homogeneous linear equations in the $\mathbb{Z}/p^m\mathbb{Z}$-module P_c, whose coefficients have the (Vandermonde) determinant $\prod_{i<j} (a^i - a^j)$. Since $a^i - a^j$ is a unit $\bmod p^m$, there is only the trivial solutions $k_1 = k_2 = \ldots = k_d = 1$. Therefore $\hat{z}_j = 1$ and $\hat{f}_j = \hat{g}_j$, as we wanted.

When the word-operation $\hat{g}$ is the usual group product, associated to the element $g = XY$ of the free group $F = \langle X, Y \rangle$, then Cor. 1 applies to the situation we studied in [4], and unicity forces $\hat{g}_1$ to be the same operation which was there denoted by the circle $\circ$; in fact, if φ is an automorphism of P and $x, y \in P$; $x^\varphi = x^a$; $y^\varphi = y^a$, then

$xy = \hat{g}_1(x, y) \dots \hat{g}_d(x, y)$ yields

$$(\hat{g}_j(x, y))^\varphi = \hat{g}_j(x^\varphi, y^\varphi) = \hat{g}_j(x^a, y^a) = (\hat{g}_j(x, y))^{a^j}$$

where the fact that $\hat{g}_j$ is a verbal function has been used to write the first equality. Therefore the definition in [4] was: $x \circ y = \hat{g}_1(x, y)$. This settles a question which arose in [4], in connection with the independence (upon P, a etc.) of the rational numbers listed in the table of [4], p. 215; actually these exponents must be independent, as they are uniquely defined by the factorization

$$XY = g_1(X, Y)\, g_2(X, Y) \dots g_d(X, Y)$$

of Theor. 1, and this is uniquely determined by the choice of d. Since this factorization is possible in $F^{\mathbf{Z}_{[d]}}$ but not in F, it is also clear why the independence of the formulas requires the use of rational non-integer exponents.

Once this coincidence has been recognized, many arguments of [4] may be repeated without substantial changes; in fact, the automorphism φ is no longer available, but the first steps of the proof in Theor. 1 imply $x \circ y \equiv xy \bmod \langle x, y\rangle_2$, hence $x \circ z = xz$, $x \circ (yz) = (x \circ y)z$ whenever z commutes with x, y; on these relations most of the proofs in [4] are based. The result is the following.

THEOREM 2. *Let P be a finite p-group. If we choose a divisor d of $p-1$, write $XY = g_1 g_2 \dots g_d$ as in Theor. 1 and define $x \circ y = \hat{g}_1(x, y)$ for each $x, y \in P$, then we obtain a loop $P, \circ$ with the following properties:*

a) $P, \circ$ is power-associative; the order of an element is the same as in the group.

b) If the 3-generators subgroups of P have nilpotency class $\leqslant c$ then $P, \circ$ is centrally nilpotent of class $\leqslant [(c + d - 1)/d]$ ($[\dots]$ = integer part of ...).

c) If a is a d-th root of $1 \bmod p^m$, the exponent of P, then the power mapping: $x \mapsto x^a$ is a loop-automorphism of $P, \circ$.

Here are some particular cases: if $d = 2$, we find $x \circ y = (xy^2x)^{\frac{1}{2}}$, the loop of Glauberman (see ref. in [4]); if $d = p - 1$ and $c < p$, then $P, \circ$ is an abelian group (as we shall see, this is the additive group

of the Lie-algebra associated to P, according to Lazard [3]). Since $x \circ y \in \langle x, y \rangle$, any subgroup of P is a subloop of $P, \circ$,but the converse is not true; for example, the set P_i of the « eigenelements » for an automorphism φ of order d (see par. 1) is a subloop but need not be a subgroup. Since $x \circ y$ is a verbal operation on P, a group-automorphism of P is a loop-automorphism of $P, \circ$; again, the converse is not true, the mapping $x \mapsto x^a$ being a counterexample. The following application may deserve some attention: if the 3-generators subgroups of the p-group P have class $< p$, then the group of the automorphisms of P is isomorphically embedded in the group of the automorphisms of the abelian group $P, \circ$.

The assumptions of Cor. 1 can be weakened, but some caution is needed; for example, we may remark that the finiteness of P was only used to ensure both the finite exponent and the nilpotency of P. The former is not required to define a structure of $\mathbb{Z}_{[d]}[\alpha]$-group on a p-group, since the ring $\mathbb{Z}/p^m\mathbb{Z}$ can be replaced by the ring of p-adic integers; but in this case, if $g_j \in F^{\mathbf{Z}_{[d]}}$, $g_j \notin F$, then $\hat{g}_j$ may not be a verbal function on P. However, a more substantial obstacle to generalizations is met if one wants to omit the nilpotency assumption for P, as the homomorphism $g \to \hat{g}$ is defined only if the infinite products involved converge in P. On the other hand, there is no difficulty in formulating Cor. 1 for any finite nilpotent group such that $p \equiv 1 \bmod d$ for every prime p dividing the order of P.

8. In this paragraph we shall explain the connection between the preceeding theorems and the results of M. Lazard ([3]).

THEOREM 3. *Let C be a binomial ring containing $\mathbb{Z}_{[d]}$; let g be an element of $F^{\mathbf{Z}_{[d]}}$, $g = g_1 g_2 \dots g_d$ the factorization of Theor* 1. *Then for every $c \in C$ we have*

$$g_j^{[c]} \equiv (g_j)^{c^j} \bmod F^c_{d+1} .$$

We only give an outline of the proof, whose details would require first to prove an improvement of Theor. 1.1 of [1], in order to take into account the degrees of the polynomials P_u, R_u (see par. 2) in the single variables. One finds that the $C\{x\}$-mapping of C into F^c defined by

$$c \mapsto (g^{[c]})^{-c} = \prod_{u \in A_\infty} g_u^{\varrho_u(c)} \qquad \varrho_u \in C\{x\}$$

is such that the degree of ϱ_u in x does not exceed $L(u)$. On the other hand, the conditions $g_1^{[\alpha^i]} = (g_1)^{\alpha^i}$ for $i = 1, 2, \ldots, d$ implies that each ϱ_u vanishes for $x = \alpha, \alpha^2, \ldots, \alpha^d = 1$; since clearly ϱ vanishes also for the $(d+1)$-th value $x = 0$, one deduces $\varrho_u = 0$ whenever $L(u) \leqslant d$. Then $(g_1^{[c]})^{-c} \equiv 1 \bmod F_{d+1}^c$, as we wanted. For $j = 2, \ldots, d$ the proof is similar.

COROLLARY 2. *Let P be a p-group whose n-generators subgroups have nilpotency class not exceeding d. Then every verbal function in n variables on P can be uniquely written as $\hat{g} = \hat{g}_1 \hat{g}_2 \ldots \hat{g}_d$, where $\hat{g}_j$ is c-homogeneous of degree j for every integer c.*

The proof is immediate, by Theor. 3 and the usual homomorphism.

There is a connection between these statements and some results of M. Lazard ([3]); he introduced the concept of « suite tipique » and proved that such a sequence can be uniquely represented as an infinite product ([3], p. 143)

$$g(t) = b_1^t b_2^{t^2} \ldots b_j^{t^j} \ldots ; \qquad (b_j \in E_j)$$

where t is a parameter assuming non-negative integer values and b_j lies in a suitable extension, say E, of the free group F. Roughly speaking, this is the factorization of our Theor. 3 for $g = g(1)$ if we let d tend to infinity, thus $\mathbb{Z}_{[d]}$ tend to the field of rationals $\mathbb{Q}$ and $F^* = F^{\mathbb{Z}_{[d]}}$ to $F^{\mathbb{Q}}$, in the role of E. In the following example this connection will appear more precise: let

$$g(t) = X^t Y^t \equiv b_1^t b_2^{t^2} \ldots b_d^{t^d} \bmod E_{d+1}$$

as in [3], theor. 2.4. Now let us apply Theor. 3 to the word $g = XY = g_1 g_2 \ldots g_d$. We have $g^{[c]} = g_1^{[c]} g_2^{[c]} \ldots g_d^{[c]} \equiv g_1^c g_2^{c^2} \ldots g_d^{c^d} \bmod F_{d+1}^*$ for every c. In particular, if we let c assume integer values t and embed F^* in E we obtain

$$g^{[t]} = X^t Y^t \equiv g_1^t g_2^{t^2} \ldots g_d^{t^d} \bmod E_{d+1} .$$

By comparison it is easily seen that $g_1 \equiv b_1, g_2 \equiv b_2, \ldots, g_d \equiv b_d \bmod E_{d+1}$. Likewise, if P is a p-group of class not exceeding $p-1$, then our Cor. 2 applied to $g = XY$ for $d = p-1$ yields substantially Lemma 4.5 of [3]; by letting

$$x + y = \hat{b}_1(x, y); \qquad [\![x, y]\!] = (\hat{b}_2(x, y))^2$$

we assign to P a structure of Lie-algebra from which the original group-multiplication is obtained through the Hausdorff formula. The following (open) questions naturally arise:

Under the assumptions of Cor. 1 (i.e. without any bound for the class of P) let us still write $g = XY$, $\hat{g}_1(x, y) = x + y$, $(\hat{g}(x, y))^2 = [\![x, y]\!]$. Then P, $+$ is a loop (Theorem 2), but what kind of structure is $(P, +, [\![,]\!])$? Does there exist a formula enabling one to reconstruct the group multiplication starting with the two new operations?

REFERENCES

[1] R. H. Bruck: *Completion of free groups by means of infinite product representation*, Math. Zeit., 118 (1970), 9-29.

[2] M. Hall jr.: *The Theory of Groups*, Mac Millan Co., New York, 1959.

[3] M. Lazard: *Sur les groupes nilpotents et les anneaux de Lie*, Ann. E.N.S., 71 (1954), 101-190.

[4] B. Scimemi: *p-groups, diagonalizable automorphisms and loops*, Rend. Sem. Mat. Padova, 45 (1971), 199-221.

Manoscritto pervenuto in redazione il 9 novembre 1972.