RENDICONTI
del
SEMINARIO MATEMATICO
della
UNIVERSITÀ DI PADOVA

BENEDETTO SCIMEMI

p-groups, diagonalizable automorphisms and loops

Rendiconti del Seminario Matematico della Università di Padova, tome 45 (1971), p. 199-221

<http://www.numdam.org/item?id=RSMUP_1971__45__199_0>

p-GROUPS, DIAGONALIZABLE AUTOMORPHISMS AND LOOPS

BENEDETTO SCIMEMI *)

Let φ be an involutory automorphism acting on the group G of odd order. Consider in G the subgroup $F=\{g\in G;\ g^{\varphi}=g\}$ and the subset $I=\{g\in G;\ g^{\varphi}=g^{-1}\}$. Then it is well-known ([4]) that any element $g\in G$ can be uniquely written as $g=fi$, where $f\in F$, $i\in I$. The set I needs not be a subgroup; however it has been noticed ([1], page 120) that I is a loop under the new composition $\circ$ defined by $x\circ y=x^{1/2}xy^{1/2}$ (here $x^{1/2}$ denotes the unique element of G whose square is x). G. Glauberman has extensively studied the structure of these loops ([2], [3]).

In this paper we prove some results of the same type, considering an automorphism φ of order d operating on a p-group P, when $p\equiv 1 \pmod{d}$.

In § 1 we show that P splits into the product of « eigensubsets » for φ: by this we mean that φ induces a specific power on each of these subsets. By analogy with linear algebra, we have called such automorphisms « diagonalizable ». In § 2 we show how a new composition can be naturally defined on each eigensubset, yielding a loop-structure in general, and specializing (within automorphisms) into the composition $\circ$ above, when the « eigenvalue » is -1. These loops are proved to be centrally nilpotent, their class being bounded by the class of P. In § 3 we derive a recurrence method to write explicit formulas for the loop composition, in terms of basic commutators of increasing

*) Indirizzo dell'A.: Seminario Matematico dell'Università di Padova.

Lavoro eseguito nell'ambito dell'attività dei gruppi di ricerca matematici del C.N.R.

weight. A glance at the final formulas suggests a possible connection with the Hausdorff formula for Lie Algebras. This connection is actually proved, by using a theorem of Lazard ([8]). Following his method in § 4 we construct an example which, apart from the loop-problem by which it was originated, may deserve some interest in itself (see e.g. [6]): a 3-generators p-group of class 4, whose 2-generators subgroups have class ≤ 3.

§ 1. If φ is an automorphism of the group G, we call $g \in G$ an « eigenelement » for φ if $g^{\varphi} = g^{r}$ for some integer r. For a set of integers $r_1, r_2, ..., r_s$ we denote by $G_i = \{g \in G;\ g^{\varphi} = g^{r_i}\}$ the « eigensubset » relative to r_i. We say that φ is « diagonalizable » (with respect to an ordered set of « eigenvalues » $r_1, r_2, ..., r_s$) if G splits into the product $G_1 G_2 \dots G_s$, i.e. every $g \in G$ can be uniquely written as $g = g_1 g_2 \dots g_s$, where $g_i \in G_i$. In this § we shall prove the following

THEOREM 1. *Let P be a nilpotent group of exponent p^n. Let d be a divisor of $p-1$, φ an automorphism of P, of order d. Then φ is diagonalizable with respect to the set of the (incongruent) roots of $x^d \equiv 1$ (mod p^n) taken in any order.*

Our first Lemma collects some elementary number-theoretical results:

LEMMA 1. Let $p \neq 2$ be a prime number, d a divisor of $p-1$, n any positive integer. Then

(i) The congruence $x^d \equiv 1$ (mod p^n) has exactly d incongruent solutions, which can be written as the first d powers of a « primitive root » a : $a, a^2, ..., a^{d-1}, a^d \equiv 1$.

Let $J = \{1, 2, ..., d-1, d\}$. Let m be any positive integer not exceeding n. Then

(ii) The same set of integers $\{a^i\}_{i \in J}$ gives all the incongruent solutions of $x^d \equiv 1$ (mod p^m).

(iii) Let x be an indeterminate over the ring of integers. Then $x^d - 1 \equiv (x-a)(x-a^2) \dots (x-a^d)$ (mod p^m).

(iv) For any $i \in J$, $i \neq d$, $\sum_{j \in J} (a^i)^j \equiv 0$ (mod p^m).

(v) For any $i\in J$ define $f_i(x)=\prod_{j\in J,\, j\neq i}(x-a^j)$. Then $f_i(a^i)\equiv da^{-i}$ (mod p^m).

(vi) $\sum_{i\in J}(f_i(x)/f_i(a^i))\equiv 1 \pmod{p^m}$.

PROOF. It is well-known that the group of units in the ring $R_m=Z/p^mZ$ is cyclic of order $(p-1)p^{m-1}$, its subgroup U_m of order $p-1$ being generated by $b_m\equiv b_1p^{m-1}$ (mod p^m), where b_1 is a primitive root of the congruence $x^{p-1}\equiv 1$ (mod p). Thus, if $p-1=dr$, we let $a_m=b_m{}^r$ and obtain the set a_m, $a_m{}^2$, ..., $a_m{}^d$ as incongruent roots of $x^d\equiv 1$ (mod p^m). This yields (i), with $m=n$, $a=a_n$. Since $u^p=u$ for each $u\in U_m$, we have $(a_m{}^i)^p\equiv a_m{}^i$ (mod p^m). Hence $a_m{}^i\equiv a_n{}^i$ (mod p^m). This implies (ii). In particular, if $1\leq i<j\leq d$, then a^i-a^j is a unit in R_m. Then the division algorythm yields easily (iii) to (vi) in chain.

LEMMA 2. Let p, d, n, a be as in Lemma 1. Assume P is an abelian group of exponent p^n and φ is an automorphism of P, of order d. Define $P_i=\{x\in P \mid x^\varphi=x^{a^i}\}$, $i=1, 2, ..., d$. Then P is a direct product

$$P=P_1\times P_2\times \dots \times P_d\,.$$

PROOF. We operate in the ring of the endomorphisms of P, and indicate by $\varphi-a^i$ the mapping $x\to x^\varphi x^{-a^i}$. More generally, the meaning of the symbol $f(\varphi)$ will be understood if $f(x)$ is a polynomial with integer coefficients. We recall the definition of $f_i(x)$ in Lemma 1, (v) and prove that the endomorphisms $e_i(\varphi)=d^{-1}a^if_i(\varphi)$ $(i\in J)$ are projections for P, i.e.

$$e_i(\varphi)^2=e_i(\varphi); \qquad \sum_{i\in J}e_i(\varphi)=1; \qquad e_i(\varphi)e_j(\varphi)=0 \qquad \text{if } i\neq j.$$

In fact, by Lemma 1 (iii), $x\in P^{f_i(\varphi)}$ implies $x^{\varphi-a^i}=1$. On the other hand, if $x^\varphi=x^{a^i}$, then $x^{f_i(\varphi)}=x^{f_i(a^i)}$. Thus $P^{e_i(\varphi)}=P_i$ and by Lemma 1, (v) $e_i(\varphi)$ is idempotent. Moreover, $P^{e_i(\varphi)e_j(\varphi)}=P_i\cap P_j=1$ if $i\neq j$, and finally $\sum_{i\in J}e_i(\varphi)=1$ by Lemma 1, (vi).

The following Lemma was suggested by a well-known result of H. Wielandt ([9], H. satz 4.1).

LEMMA 3. Let p, d, n, a be as in Lemma 1. Let P be a nilpotent group of exponent p^n, φ an automorphism of P, of order d. Assume N is a normal subgroup of P such that

$$(Nx)^\varphi=(Nx)^{a^i} \text{ for some } a^i \text{ and some } x\in P.$$

Then N is φ-invariant, and $(n^*x)^\varphi=(n^*x)^{a^i}$ for some $n^*\in N$.

PROOF. Here $(Nx)^\varphi=Nx^{a^i}$ implies $x^\varphi=n_0x^{a^i}$ for some $n_0\in N$. Then for any $n\in N$, we have $n^\varphi=(nx)^\varphi(x^{-1})^\varphi\in Nx^{a^i}(n_0x^{a^i})^{-1}=N$. Thus N is φ-invariant. To prove the other statement, assume first that P is abelian. As in Lemma 2, we consider the endomorphism $e_i(\varphi)$ and write $y=x^{e_i(\varphi)}$. Then $y^\varphi=y^{a^i}$. On the other hand $x^\varphi=n_0x^{a^i}$ implies $y=x^{e_i(\varphi)}\equiv x^{e_i(a^i)}\equiv x$ (mod N). Hence $y=n_1x$ for some $n_1\in N$ and $y^\varphi=(n_1x)^\varphi=y^{a^i}=(n_1x)^{a^i}$ as we wanted. Then we can induce on the nilpotency class of P. Assume P is not abelian and let $Z=Z(P)$ be the center of P. The factor group $\overline{P}=P/Z$ has exponent p^m $(m\leq n)$ and φ induces on $\overline{P}$ an automorphism $\overline{\varphi}$ of order $\overline{d}$, a divisor of d. Set $d=\overline{d}s$. Then, by Lemma 1, a^s, a^{2s}, ..., $a^{(\overline{d}-1)s}$, $a^{\overline{d}s}$ is a set of incongruent solutions of $x^{\overline{d}}\equiv 1$ (mod p^m). Let the bar denote images under the natural homomorphism of P onto $\overline{P}$. Then $(Nx)^\varphi=(Nx)^{a^i}$ implies $(\overline{N}\overline{x})^{\overline{\varphi}}=(\overline{N}\overline{x})^{a^i}$; therefore $\overline{N}\overline{x}=(\overline{N}\overline{x})^{\overline{\varphi}^{\overline{d}}}=$ $=(\overline{N}\overline{x})^{a^{i\overline{d}}}$ and $\overline{x}^{a^{i\overline{d}}-1}\in\overline{N}$. If $\overline{x}\notin\overline{N}$, this implies that p divides $a^{i\overline{d}}-1$, hence, by Lemma 1 (ii) $a^{i\overline{d}}\equiv 1$ (mod p^m). Then for some j we have $a^i=(a^s)^j$. Now the assumptions of the Lemma hold on $\overline{P}$, with respect to $\overline{d}$, m, a^s, $\overline{\varphi}$. Since $\overline{P}$ is nilpotent of class smaller than P, by induction the Lemma holds on $\overline{P}$, yielding $(\overline{n}\overline{x})^{\overline{\varphi}}=(\overline{n}\overline{x})^{a^i}$ for some $\overline{n}\in\overline{N}$. On the other hand, the last conclusion is trivial if $\overline{x}\in\overline{N}$. Then for some $n\in N$ we have $(Znx)^\varphi=Z(nx)^{a^i}$, i.e. for some $z\in Z$ we have $(nx)^\varphi=z(nx)^{a^i}$. Now consider the two subgroups $P_*=\langle Z, nx\rangle$ and $N_*=Z\cap N$. P_* is abelian and φ-invariant, for $P_*^\varphi=\langle Z^\varphi, (nx)^\varphi\rangle=\langle Z, (nx)^{a^i}\rangle=\langle Z, nx\rangle=P_*$. If we now prove that $(N_*nx)^\varphi=N_*(nx)^{a^i}$, then we can conclude that for some $n_*\in N_1$ we have $(n_*nx)^\varphi=(n_*nx)^{a^i}$ and the element $n^*=n_*n\in N$ will satisfy our requirements. In fact

$$(N_*nx)^\varphi=(Nnx\cap Znx)^\varphi=(Nx)^\varphi\cap(Znx)^\varphi=Nx^{a^i}\cap Z(nx)^\varphi=$$

$$=N(nx)^{a^i}\cap Z(nx)^{a^i}=(N\cap Z)(nx)^{a^i}=N_*(nx)^{a^i}.$$

PROOF OF THEOREM 1. If P is abelian, this is just our Lemma 2. Otherwise, let $\overline{P}=P/Z$, m, $\overline{d}$, $\overline{\varphi}$, a^s as in the last proof. Then by induction we can assume that any $\overline{g}\in\overline{P}$ can be uniquely written as

$$\overline{g}=\overline{g}_s\overline{g}_{2s}\ \dots\ \overline{g}_{(\overline{d}-1)s}\overline{g}_{\overline{d}s}\quad\text{where } (\overline{g}_{js})^{\overline{\varphi}}=(\overline{g}_{js})^{a^{js}}$$

We will now make a remark, which will often be useful in what follows. If $1\leq i<d$, but s does not divide i, then in $\overline{P}$ the equation $\overline{g}^{\overline{\varphi}}=\overline{g}^{a^i}$ implies $\overline{g}=1$, because, as in the proof of Lemma 3, $\overline{g}\neq\overline{1}$ and $\overline{g}^{a^{i\overline{d}}}=\overline{g}$ would imply $a^{i\overline{d}}\equiv 1 \pmod{p^n}$, hence $i\overline{d}=kd=ks\overline{d}$, and $i=ks$ for some k, a contradiction. Therefore, even if $s>1$, we can write $\overline{g}$ as a product of d (instead of $\overline{d}$) eigenelements

$$\overline{g}=\overline{g}_1\overline{g}_2\ \dots\ \overline{g}_s\overline{g}_{s+1}\ \dots\ \overline{g}_d\,,\quad\text{where } (\overline{g}_i)^{\overline{\varphi}}=(\overline{g}_i)^{a^i}$$

and this decomposition will still be unique. Now we write $\overline{g}_i=g^*_iZ$, and by Lemma 3 we can assume that the g^*_i are eigenelements $(g^*_i)^{\varphi}=(g^*_i)^{a^i}$. Therefore, any $g\in P$ can be written as $g=zg^*_1g^*_2\ \dots\ g^*_d$ for some $z\in Z$. By Lemma 2 φ induces on the subgroup Z a diagonalizable automorphism with respect to the same eigenvalues $\{a^i\}_{i\in J}$ (see the remark above). Then z can be written as $z=z_1z_2\ \dots\ z_d$, $z_i\in Z$, $z_i^{\varphi}=z_i^{a^i}$. Therefore we have $g=(z_1g^*_1)(z_2g^*_2)\ \dots\ (z_dg^*_d)$. Since $(z_ig^*_i)^{\varphi}=z_i^{a^i}g_i^{*a}=(z_ig^*_i)^{a^i}$, the decomposition of the theorem is proved, by letting $g_i=zg^*_i$. As for unicity, we know by induction (and the remark above) that $g_1g_2\dots g_d=h_1h_2\dots h_d$ (where $(h_i)^{\varphi}=(h_i)^{a^i}$) implies $g_i\equiv h_i \pmod Z$, i.e. $h_i=g_iz_i$ for some $z_i\in Z$. Since g_i and h_i commute, we have $z_i^{\varphi}=z_i^{a^i}$. Thus z_i is an eigenelement for the automorphism induced by φ on the group Z. Going back to the former equations we find $1=z_1z_2\ \dots\ z_d$, hence $z_1=z_2=\dots=z_d=1$ by Lemma 2 and the remark above.

Throughout the proof we maintained the natural order for the eigenvalues: a, a^2, ..., a^d. However, we could have fixed any other ordering of the set J without affecting any step.

As an illustration of Theorem 1, rather then a test of its power (Lie-rings methods are generally more powerful in this field), we shall apply it to prove quite elementarly a small result on groups admitting fixed-point-free automorphisms (f.p.f.a.) of order 4. A construction in [4] shows that there exists a finite p-group ($p\equiv 1$ mod 4) of arbitrarily high nilpotency class, admitting such an automorphism. However we shall see that, under these assumptions, its commutator subgroup must have class not exceeding 3 [1]).

We first prove a Lemma, which will be often used in the following paragraphs. We use the following standard notation: $\langle S\rangle$ is the subgroup generated by the subset S in the group R; $R=R^{(1)}>R^{(2)}> \dots R^{(c)}>R^{(c+1)}=1$ is the descending central series for the group R, of class c.

LEMMA 4. Let P, φ, d, a be as in Theorem 1; $P_i=\{g\in P;\ g^\varphi=g^{a^i}\}$ $(i=1, 2, \dots, d)$. Then φ induces the power a^{ij} on the factor $\langle P_i\rangle^{(j)}/\langle P_i\rangle^{(j+1)}$.

PROOF. To simplify notations, we assume $i=1$ and write R for $\langle P_1\rangle$. Other cases are treated similarly, by replacing a with a^i. Since the statement is trivial if R is abelian, we induce on c, the class of R. Thus the Lemma holds on $\overline{R}=R/R^{(c)}$, and φ induces the power a^j on $\overline{R}^{(j)}/\overline{R}^{(j+1)}$, hence on $R^{(j)}/R^{(j+1)}$ for $j=1, 2, \dots, c-1$. Then we only have to prove that φ induces the power a^c on any element of $R^{(c)}$. Now if $g\in R^{(c-1)}$, we know by the previous argument that $g^\varphi=g^{a^{c-1}}\cdot z$, for for some $z\in R^{(c)}$. Let $h\in P_1$. Since $R^{(c)}$ is in the center of R, we have

$$[g, h]^\varphi=[g^\varphi, h^\varphi]=[g^{a^{c-1}}z, h^a]=[g^{a^{c-1}}, h^a]=[g, h]^{a^c}.$$

Since $R=\langle P_1\rangle$, $R^{(c)}$ is generated by elements as $[g, h]$. But $R^{(c)}$ is abelian, and the Lemma is proved.

Now assume φ is a f.p.f.a. Then $P_d=1$, and we can write the factorization of Theorem 1 as $P=P_1P_2 \dots P_{d-1}$. Here $R=\langle P_1\rangle$ has class $<d$. In fact, by Lemma 4, φ fixes every element of $R^{(d)}/R^{(d+1)}$, hence (by Lemma 3 or otherwise) $R^{(d+1)}=R^{(d)}=1$. More generally, $\langle P_i\rangle$ has class $<d_i$, the order of a^i, by the same argument. Moreover, P_i and P_{d-i} commute elementwise, as one can easily see by an induction argument, as in Lemma 4. Now let us consider the following cases:

(i) $d=2$. Then $P=P_1$ is trivially an abelian group.

(ii) $d=3$. Then $P=P_1P_2=\langle P_1\rangle\langle P_2\rangle$. By the previous remarks, $\langle P_1\rangle$ and $\langle P_2\rangle$ have both class <3, and commute elementwise. Then P has class <3, a well-known result.

[1]) *Added in proof*: One can actually prove that this class may be 2 but not more.

(iii) $d=4$. Let a, $a^2 \equiv -1$, $a^3 \equiv -a$, $a^4 \equiv 1$ be the « eigenvalues ». Here $\langle P_2 \rangle = P_2$ is abelian, whereas $\langle P_1 \rangle$ and $\langle P_3 \rangle$ commute elementwise and have class <4, hence the same holds for $\langle P_1P_3 \rangle$. We claim that P_2 normalizes the subset P_1P_3. In fact, for any $x_i \in P_i$ $(i=1, 2, 3)$ we know from Theorem 1 that $x_3x_1x_2 = y_2y_3y_1$ for some $y_i \in P_i$. Applying φ^2 yields $x_3^{-1}x_1^{-1}x_2 = y_2y_3^{-1}y_1^{-1}$. Replacing y_2 from the former equation, and taking into account that P_1 and P_3 commute elementwise, we obtain $x_2^{-1}x_1^2x_3^2x_2 = y_1^2y_3^2$. But x^2 runs over P_i when x does, hence our claim is proved. Thus the subgroup $\langle P_1P_3 \rangle$ is normal in P and $P/\langle P_1P_3 \rangle$ is abelian, hence $P^{(2)}$ has class <4, as we wanted.

§ 2. Let P, φ, d, a be as in Theorem 1. For $i=1, 2, ..., d$ we consider the eigensubsets $P_i = \{x \in P;\ x^\varphi = x^{a^i}\}$ and we order them once and for all [2]) by their indexes, thus writing Theorem 1 as $P = P_1P_2 \dots P_d$. For each index i we define a mapping β_i of P onto P_i by letting, for every $x \in P$

$$x = x^{\beta_1}x^{\beta_2} \dots x^{\beta_d} \qquad x^{\beta_i} \in P_i .$$

As a consequence of Theorem 1, the mappings β_i are well defined and behave like « projections »:

$$x^{\beta_i^2} = x^{\beta_i}\ ; \qquad x^{\beta_i\beta_j} = 1$$

for any $x \in P$, and any $i \neq j$.

THEOREM 2. *Define on P_i a new composition $+$ by letting, for any x, $y \in P_i$*

$$x + y = (xy)^{\beta_i}.$$

Then P_i, $+$ is a power-associative loop [3]). *The identity, the n-th power of an element and hence the order of an element are the same in the loop as they were in the group.*

---

[2]) For a different ordering, see the remark at the end of § 3.

[3]) For the sake of simplicity, we are here denoting by the same symbol $+$ all the different operations on the various P_i.

PROOF. Let Z be the center of P. We first remark that for any $x \in P_i$, $z \in P_i \cap Z$ we have $xz \in P_i$ and therefore $x+z=xz=zx=z+x$. In particular, $1+x=x=x+1$. We now claim that for any a, $b \in P_i$ the two equations

$$x+a=b; \qquad a+y=b$$

have unique solutions x, $y \in P_i$. Since the statement is trivial if P is abelian (the loop and group compositions being then coincident), we shall induce on the nilpotency class of P. Let the bar denote images under the canonical homomorphism of P onto $\overline{P}=P/Z$.

If $\overline{\beta}_i$ denotes the projection of $\overline{P}$ onto $\overline{P}_i$ (which is naturally induced to β_i) then we know by induction that the equations

$$(\overline{xa})^{\overline{\beta}_i}=\overline{b}=(\overline{ay})^{\overline{\beta}_i}$$

have unique solutions $\overline{x}$, $\overline{y} \in \overline{P}_i$.

By Lemma 3, we can write $\overline{x}=cZ$, $\overline{y}=dZ$, where c, $d \in P_i$. Therefore, for some $r_j \in P_j$ we can write

$$(cZ)(aZ)=(r_1Z)(r_2Z) \ \dots \ (r_{i-1}Z)(bZ)(r_{i+1}Z) \ \dots \ (r_dZ)$$

yielding $ca=r_1r_2 \dots r_{i-1}br_{i+1} \dots r_dz$ for some $z \in Z$. We write $z_i=z^{\beta_i}$, $z=z_1z_2 \dots z_d$ and find

$$ca=r_1z_1r_2z_2 \ \dots \ bz_i \ \dots \ r_dz_d$$

and hence $(ca)^{\beta_i}=bz_i$.

If we now define $x=cz_i^{-1}$, we can check that $x+a=b$. As for unicity suppose $x^*+a=b$, $x^* \in P_i$. Then by similar arguments we find $x=xz^*_i$ for some $z^*_i \in P_i \cap Z$. Thus

$$(xa)^{\beta_i}=b=(x^*a)^{\beta_i}=(xz^*_ia)^{\beta_i}=(xa)^{\beta_i}z^*_i$$

yielding $z^*_i=1$. An identical argument would show the existence and unicity of y. Thus the loop-structure is proved. Since for any integer n we have $x^n \in P_i$ if $x \in P_i$, then powers (and inverses) of an element in P_i, $+$ are exactly the same as in the group P. Thus the power-associativity is trivially proved and we can introduce the notion of order of an element. Since P is a p-group, P_i, $+$ is a p-loop.

We shall now derive a few properties of the loop P_i, $+$ which are direct consequences of the definition.

LEMMA 5. Assume N is a normal φ-invariant subgroup of P. Then $N_i = N \cap P_i$ is a normal subloop of P_i and the loops P_i/N_i, $(P/N)_i$ are isomorphic under the mapping $x + N_i \rightarrow xN$.

PROOF. For the concepts of loop-homomorphism, normal subloop and relative theorems we refer to [1]. For our purpose, it will suffice to show that the mapping $y \rightarrow yN$ of P_i onto $(P/N)_i$ is a loop-homomorphism whose kernel is $N_i = N \cap P_i$. In fact, by applying the natural group homomorphism of P onto P/N to both sides of the equation

$$yw = (yw)^{\beta_1}(yw)^{\beta_2} \ldots (yw)^{\beta_d} \qquad (y,\ w \in P_i)$$

we write

$$(yN)(wN) = ((yw)^{\beta_1}N)((yw)^{\beta_2}N) \ \ldots \ ((yw)^{\beta_d}N).$$

Here $(yw)^{\beta_j}N \in (P/N)^{\bar{\beta}_j}$, where $\bar{\beta}_j$ is the projection induced on P/N by β_j. By the properties of projections

$$(yN) + (wN) = ((yN)(wN))^{\bar{\beta}_i} = (yw)^{\beta_i}N = (y + w)N$$

so that our mapping is a loop-homomorphism. Moreover, $yN = N$ if and only if $y \in P_i \cap N = N_i$, as we wanted.

LEMMA 6. The mapping $x \rightarrow x^{a^i}$ is an automorphism of the loop P_i, $+$.

PROOF. We have to prove that for any $x,\ y \in P_i$ one has $(x+y)^{a^i} = x^{a^i} + a^{a^i}$. Since p does not divide a^i, this homomorphism will be clearly an automorphism. To this aim, we first notice that φ commutes with all the projections β_j. In fact $g = x_1x_2 \ldots x_d$ $(x_j \in P_j)$ implies $g^\varphi = x_1^\varphi x_2^\varphi \ldots x_d^\varphi$, and since $(x_j)^\varphi \in P_j$ we have $g^{\varphi\beta_j} = g^{\beta_j\varphi}$. Then for any $x,\ y \in P_i$ we have

$$(x+y)^{a^i} = (x+y)^\varphi = ((xy)^{\beta_i})^\varphi = (xy)^{\varphi\beta_i} =$$
$$= (x^{a^i}y^{a^i})^{\beta_i} = x^{a^i} + y^{a^i}.$$

In the following theorems we shall use the concepts of « nucleus », « center », « nuclear- » and « central-nilpotency » of a loop. Again, we refer to [1] for the definitions and the basic properties.

THEOREM 3. *If $i \neq d$, in the loop P_i, $+$ the nucleus and the center coincide.*

PROOF. For the sake of simplicity, we shall assume $i=1$. (For $i \neq 1$ we only have to replace a by a^i).

Let $x \in \mathrm{Nuc}\,(P_1)$; y, $z \in P_1$. Then by definition

$$x+(y+z)=(x+y)+z; \quad y+(x+z)=(y+x)+z; \quad y+(z+x)=(y+z)+x.$$

From this we derive, by induction, that for any integer n we have $(x^{-1}+y+x)^n=x^{-1}+y^n+x$. Then we use Lemma 6 to calculate

$$(x^{-1}+y+x^a)^\varphi=x^{-a}+y^a+x^{a^2}=x^{-a}+y^a+x^{a(a-1)}+x^a.$$

But we also have

$$(x^{-1}+y+x^a)^\varphi=(x^{-a}+{}^{a-1}+y+x^a)^\varphi=$$
$$=(x^{-a}+(x^{a-1}+y)+x^a)^a=x^{-a}+(x^{a-1}+y)^a+x^a=$$
$$=x^{-a}+(x^{a(a-1)}+y^a)+x^a.$$

By cancellation, the two equations yield

$$x^{a(a-1)}+y^a=y^a+x^{a(a-1)}$$

for any $y \in P_1$, $x \in \mathrm{Nuc}\,(P_1)$. However, since P_1 and $\mathrm{Nuc}\,(P_1)$ are p-loops, and p does not divide $a(a-1)$, we conclude that for any $y \in P_1$, $x \in \mathrm{Nuc}\,(P_1)$ we have $x+y=y+x$, i.e. x is in the center of P_1, $+$.

COROLLARY 3. If $i \neq d$, and P_i, $+$ is a group, then it is abelian.

Before going further, we shall make an important remark. Since the subgroup $\langle P_i \rangle$, generated by P_i, is φ-invariant, we can apply Theorem 1 to $\langle P_i \rangle$ to decompose any $g \in \langle P_i \rangle$ into eigenelements belonging to $\langle P_i \rangle$. However, by the unicity of the decomposition, the components we obtain must be the same. Thus if x, $y \in P_i$, then $(xy)^{\beta_j} \in \langle P_i \rangle$ for all j;

in particular, $(xy)^{\beta_i}=x+y$ is still the loop-composition « induced » on $\langle P_i\rangle$. Therefore, in order to study the properties of the loop P_i, $+$, we can assume without loss $P=\langle P_i\rangle$.

LEMMA 7. Let $x\in P_i$, and assume $xy=yx$ for any $y\in P_i$. Then x is in the center of the loop P_i, $+$.

PROOF. According to the previous remark, assume $P=\langle P_i\rangle$. Then $x\in Z(P)$ and $x+y=xy=yx=y+x$, a property which was often used before. Thus we are left with the associative laws. Let $z\in P_i$ and write

$$yz=(yz)^{\beta_1}\ \dots\ (yz)^{\beta_i}\ \dots\ (yz)^{\beta_d}\,.$$

Then

$$yzx=(yz)^{\beta_1}\ \dots\ (yz)^{\beta_i}x\ \dots\ (yz)^{\beta_d}\,.$$

Since $(yz)^{\beta_i}x\in P_i$, by the unicity of the decomposition we have

$$(y+z)+x=(yz)^{\beta_i}x=(yzx)^{\beta_i}=(y(zx))^{\beta_i}=y+(z+x).$$

Likewise (or more easily) $(x+y)+z=x+(y+z)$; $(y+x)+z=y+(x+z)$. Thus x belongs to the center of P_i, $+$.

We are now ready to prove the main result of this paragraph, which was suggested by Theorem 4 of [2].

THEOREM 4. *Let d_i be the order of a^i (mod p^n), c_i the nilpotency class of the group $\langle P_i\rangle$. Then the loop P_i, $+$ is centrally nilpotent of class not exceeding*

$$c'_i=[(c_i+d_i-1)/d_i]\ ^{4)}.$$

PROOF. We can assume without loss $i=1$, $P=\langle P_1\rangle$, according to the previous remarks, and write for simplicity c, d, c' instead of c_1, d_1, c'_1. Assume first $c\leq d$. Then Lemma 4 implies the inclusion $P^{(c)}\subseteq P_c$

[4]) Here the square brackets denote the function « integer part of ». We shall see in § 4 that c'_i may actually exceed the class of the loop P_i.

and by an easy induction $P^{(2)} \subseteq P_2 P_3 \ldots P_d$. Thus $P^{(2)} \cap P_1 = 1$ and by Lemma 5 $P_1, +$ is isomorphic to the abelian group $P/P^{(2)}$. In this case $c' = 1$, and the statement is proved. Then we induce on c. Let $c > d$ (thus $c' > 1$) and consider the group $\overline{P} = P/P^{((c'-1)d+1)}$ whose class is $(c'-1)d < c$. Since all the assumptions hold on $\overline{P}$, by the inductive assumption we know that $\overline{P}_1, +$ is centrally nilpotent of class not exceeding $[((c'-1)d+d-1)/d] = c'-1$. Since by Lemma 5 $\overline{P}_1$ is isomorphic to the loop $P_1/P_1 \cap P^{((c'-1)d+1)}$ the theorem will be proved if we show that the center of the loop $P_1, +$ contains any $x \in P_1 \cap P^{((c'-1)d+1)}$. Let y, $w \in P_1$ and define $z_r \in P_1$ $(r = 0, 1, 2, 3)$ by the relations

$$x + y = (y + x) + z_0 ; \qquad (x + y) + w = (x + (y + w)) + z_1 ;$$

$$(y + x) + w = (y + (x + w)) + z_2 ; \qquad (y + w) + x = (y + (w + x) + z_3 .$$

We must prove $z_r = 1$ for all r. In fact, consider the factor group $\widehat{P} = P/P^{((c'-1)d+2)}$ and denote by ^ images under the homomorphism of P onto $\widehat{P}$. Then $\widehat{x} \in \widehat{P}_1 \cap Z(\widehat{P})$, hence by Lemma 7 $\widehat{z}_r = 1$ for any r. Therefore $z_r \in P^{((c'-1)d+2)}$. However, if we consider the definition of c' and apply Lemma 4 as in the first argument of this proof, we find $P^{((c'-1)d+2)} \cap P_1 = 1$. Thus $z_r = 1$ $(r = 0, 1, 2, 3)$ and the Theorem is proved.

§ 3. Let p be an odd prime, and φ an involutory automorphism operating on the p-group P. Since $a = -1$, $a^2 = 1$ are incongruent roots of the congruence $x^2 \equiv 1$ modulo any power of p, the decomposition $P = P_1 P_2$ of Theorem 1 is equivalent to $P = IF$ of [4]. Then for any $x, y \in P_i$ we write $xy = (xy)^{\beta_1}(xy)^{\beta_2}$, and applying φ to both sides

$$x^{-1}y^{-1} = ((xy)^{\beta_1})^{-1}(xy)^{\beta_2} = ((xy)^{\beta_1})^{-2}xy.$$

Hence we derive:

$$(xy)^{\beta_1} = (xy^2x)^{+1/2}, \qquad (xy)^{\beta_2} = (xy^2x)^{-1/2}xy.$$

We promptly realize that the loop composition $x + y = (xy^2x)^{1/2}$ defined by our Theorem 2 is isomorphic to the loop composition $x \circ y = x^{1/2}yx^{1/2}$

investigated by G. Glauberman in [2]. In fact, as $(x+y)^2 = xy^2x = x^2 \circ y^2$, the mapping $x \to x^2$ is an isomorphism between P_1, $+$ and P_1, $\circ$. More generally, by applying the operation $x+y=(xy^2x)^{1/2}$ to any group G whose elements have odd order, one can repeat all the arguments and calculations of [2]; indeed, owing to the more natural definition of $+$, in doing so one often gains in symmetry and neatness.

At this point the following remark should be made: although the action of φ was used to define the loop on P_1, we end up with a formula which is independent of φ and which can be used to define a loop on the whole P. By a reasonable analogy, also in the case $d>2$ one should be able to elaborate some « word » $f(x, y)$ in the symbols x, y, possibly involving rational exponents, independent of the automorphism and the particular group (hence, somehow « canonically » defined by the choice of d), defining a loop on the whole P and inducing our composition $+$ on P_1.

We wish to publish in a different paper, within a broader context, a full description of how this can be properly accomplished. Our next theorems give only a partial answer to this problem.

We first introduce some definitions and recall some results from the literature:

1) Let r/s be a rational number whose denominator s is not divisible by the prime p. If P is a p-group, then for any $g \in P$ we can define a unique element $g^{r/s}$ by the equation $(g^{r/s})^s = g^r$. Moreover, if P has exponent p^n, then there is an integer h such that $g^{r/s} = g^h$ for every $g \in G$. The use of such rational exponents will simplify our notation.

2) Let $F = F(\bar{x}, \bar{y})$ be the free group on two generators $\bar{x}$, $\bar{y}$. Then any word $f \in F$ can be « approximated » by a product of « basic commutators » in $\bar{x}$, $\bar{y}$, by the « collecting process » of P. Hall (cf. e.g. [7], Ch. 11). More precisely, for any positive integer w, we have

$$f = c_1^{n_1} c_2^{n_2} \ldots c_t^{n_t} f'$$

where f' has weight $\geq w$ (i.e. $f' \in F^{(w)}$), $n_i \in Z$ and the c_i are basic commutators of weight smaller than w. If we order these commutators according to the convention $\bar{x} < \bar{y}$, ([7], p. 178) the first c_i are the following:

$$c_1=\bar{x}; \quad c_2=\bar{y}; \quad c_3=[\bar{y}, \bar{x}]; \quad c_4=[\bar{y}, \bar{x}, \bar{x}];$$

$$c_5=[\bar{y}, \bar{x}, \bar{y}]; \quad c_6=[\bar{y}, \bar{x}, \bar{x}, \bar{x}] \dots$$

3) An operation $*$ on the group G will be called a « word-operation » if there exists an element $f \in F$ such that $x * y = f(x, y)$ for any $x, y \in G$. Here $f(x, y)$ is the element of G which is obtained from the word f by replacing $\bar{x}, \bar{y}$ by x, y and performing products in G.

From 2) and 3) we see that any word-operation on a nilpotent group P of exponent p^n can be written as

$$x * y = x^{n_1}y^{n_2}[y, x]^{n_3}[y, x, x]^{n_4} \dots = \prod_{i=1}^{t} c_i^{n_i}$$

where the last commutator c_t has weight w, if w is the class of P. According to 1), we can also replace the integers n_i by some rationals r_i/s_i, if we find it convenient.

THEOREM 5. *The loop-composition $+$ defined by Theorem 2 is a word operation on P_i : $x+y=f(x, y)$, for any $x, y \in P_i$. The word f is independent of φ and can be calculated by a recurrence algorythm as a function of the eigenvalue a^i.*

PROOF. As in Theorem 4, we assume $i=1$, $P=\langle P_1 \rangle$. Let c denote the class of P and consider the projections β_j of Theorem 2. We shall prove that there exist d words $f_{j,c} \in F$ ($j=1, 2, \dots, d$) such that $(xy)^{\beta_j} = f_{j,c}(x, y)$ for any $x, y \in P_1$. If $c=1$, then $x+y=xy=(xy)^{\beta_1}$ and we can trivially set $f_{1,1}=xy$, $f_{j,1}=1$ for $j \neq 1$. Thus we can induce on c. Since all the assumptions are inherited by the factor group $P^*=P/P^{(c)}$, we know that there exist words $f_{j,c-1} \in F$ such that $(x^*y^*)^{\beta^*_j}=f_{j,c-1}(x^*, y^*)$ for all $x^*, y^* \in P^*_1$ and $j=1, \dots, d$. Therefore for any $x, y \in P_1$ and any j there exists an element $g_{j,c}(x, y) \in P^{(c)}$ such that

$$(xy)^{\beta_j}=f_{j,c-1}(x, y)g_{j,c}(x, y).$$

So far, we do not know whether $g_{j,c}(x, y)$ is a word-operation. However we know that, for any x, y, $g_{j,c}(x, y)$ belongs to the center of P and, by Lemma 4,

$$(g_{j,c}(x, y))^{\varphi}=(g_{j,c}(x, y))^{a^c} .$$

Then we apply φ to the former equation and calculate $(xy)^{\beta_j\varphi}$ in two different ways:

$$(xy)^{\beta_j\varphi}=((xy)^{\beta_j})^{a^j}=(f_{j,c-1}(x, y)g_{j,c}(x, y))^{a^j}=(f_{j,c-1}(x, y))^{a^j}(g_{j,c}(x, y))^{a^j}.$$

$$(xy)^{\beta_j\varphi}=(f_{j,c-1}(x, y))^{\varphi}(g_{j,c}(x, y))^{\varphi}=f_{j,c-1}(x^a, y^a)((g_{j,c}(x, y))^{a^c},$$

where we have used the fact that $f_{j,c-1}$ is a word, so that

$$(f_{j,c-1}(x, y))^{\varphi}=f_{j,c-1}(x^{\varphi}, y^{\varphi}).$$

By comparison we find

$$(g_{j,c}(x, y))^{a^j-a^c}=f_{j,c-1}(x^a, y^a)(f_{j,c-1}(x, y))^{-a^j}$$

By Lemma 1, there are $d-1$ values of j such that p does not divide a^j-a^c. For these j's we can take the power $1/(a^j-a^c)$ of the last equation and substitute for $g_{j,c}$ in its defining relation to find $(xy)^{\beta_j}$ as

$$(*)\qquad f_{j,c}(x, y)=f_{j,c-1}(x, y)(f_{j,c-1}(x^a, y^a)(f_{j,c-1}(x, y))^{-a^j})^{1/(a^j-a^c)}.$$

Therefore, if we know the word $f_{j,c-1}$ and the eigenvalue a, we can construct by the last formula a word $f_{j,c}$ such that $(xy)^{\beta_j}=f_{j,c}(x, y)$. Since by induction $f_{j,c-1}$ is independent of φ, the same will remain true for $f_{j,c}$. As for the unique value $\bar{j}$ for which $a^{\bar{j}}=a^c$, we write $xy=$ $=(xy)^{\beta_1} \dots (xy)^{\beta_{\bar{j}}} \dots (xy)^{\beta_d}$ and again we calculate $(xy)^{\beta_{\bar{j}}}$ as a product of words

$$(**)\qquad f_{\bar{j},c}(x, y)=(f_{\bar{j}-1,c}(x, y))^{-1} \dots$$
$$\dots (f_{1,c}(x, y))^{-1}(xy)(f_{d,c}(x, y))^{-1} \dots (f_{\bar{j}+1,c}(x, y))^{-1}.$$

Thus the theorem is completely proved.

We can use (*), (**) as recurrence formulas to « approximate » the elements $(xy)^{\beta_j}$ within commutators of arbitrarily high weight, beginning with the trivial relations

$$f_{1,1}=xy; \qquad f_{2,1}=f_{3,1}= \dots =f_{d,1}=1 \qquad (\text{mod } P^{(2)}).$$

Along the computation we shall make use of commutation-identities as [5])

$$(xy)^n=x^ny^n[y,\ x]^{\binom{n}{2}}[y,\ 2x]^{\binom{n}{3}}[y,\ x,\ y]^{2\binom{n}{3}+\binom{n}{2}} \dots$$

$$[y^n,\ x^m]=[y,\ x]^{mn}[y,\ 2x]^{\binom{m}{2}n}[y,\ x,\ y]^{\binom{n}{2}m} \dots$$

$$[y^n,\ x^m,\ x^t]=[y,\ 2x]^{nmt} \dots \text{ etc.}$$

which will permit us to write all the results in their « collected form », a particularly suitable one for comparisons. Since we apply these formulas to p-groups, we may let m, n ... assume also rational values whenever p does not divide the denominators, implying only a natural extension of the binomial coefficients.

Of course, we must separately perform the calculations for the different values of d. Since $d=1$ is uninteresting and for $d=2$ we already have explicit formulas for $(xy)^{\beta_j}$, we shall start with $d=3$.

We want to find $f_{j,2}$ $(j=1,\ 2,\ 3)$. Here $j=2$, hence we must first apply the formula (*) to calculate $f_{1,2}$ and $f_{3,2}$ as follows:

$$f_{1,2}=xy(x^ay^a(xy)^{-a})^{(a-a^2)^{-1}}; \qquad f_{3,2}=1.$$

Then we apply (**) to find (mod $P^{(3)}$)

$$f_{2,2}=(f_{1,2})^{-1}(xy)=(xy(x^ay^a(xy)^{-a})^{(a-a^2)^{-1}})^{-1}xy.$$

By the commutator-identities, arrested to weight 2, we compute:

$$f_{1,2}=xy[y,\ x]^{1/2}; \qquad f_{2,2}=[y,\ x]^{-1/2}; \qquad f_{3,2}=1.$$

Now we want to find $f_{j,3}$ $(j=1,\ 2,\ 3)$. Here $j=3$, and we must use (*) for $f_{1,3}$ and $f_{2,3}$, then (**) for $f_{3,3}$. By the commutator-identities,

[5]) Here we write $[y,\ 2x]$ for $[y,\ x,\ x]$ etc.

arrested to weight 3, we compute (mod $P^{(4)}$):

$$f_{1,3}=xy[y,\ x]^{1/2}(x^a y^a[y^a,\ x^a]^{1/2}(xy[y,\ x]^{1/2})^{-a})^{(a-a^3)^{-1}}$$
$$=xy[y,\ x]^{1/2}[y,\ 2x]^{-1/12}[y,\ x,\ y]^{1/12}$$
$$f_{2,3}=[y,\ x]^{-1/2}([y^a,\ x^a]^{-1/2}[y,\ x]^{-a^2/2})^{(a^2-1)^{-1}}$$
$$f_{3,3}=(f_{2,3})^{-1}(f_{1,3})^{-1}xy=[y,\ 2x]^{-1/6}[y,\ x,\ y]^{-1/3} \text{ etc.}$$

Consider now the case $d=4$. Since for $j>c$ we have $f_{j,c}=1$ (a direct consequence of Lemma 4), the preceding formulas for $d=3$ are easily seen to hold as well for $d=4$, within $c=3$. As for $c=4$, since now $a^4 \neq a$, we must apply (*) to compute $f_{1,4}$, $f_{2,4}$, $f_{3,4}$, then (**) for $f_{4,4}$ etc.

We have actually performed all the calculations modulo $P^{(5)}$ and collected the results in the following exponent-table, whose intepretation should now be clear. For the sake of completeness, the case $d=2$ has also been included.

		x	y	$[y,\ x]$	$[y,\ 2x]$	$[y,\ x,\ y]$	$[y,\ 3x]$	$[y,\ 2x,\ y]$	$[y,\ x,\ 2y]$
$d=2$	β_1	1	1	1/2	−1/4	−1/4	1/8	0	1/8
	β_2	0	0	−1/2	1/4	1/4	−1/8	0	−1/8
$d=3$	β_1	1	1	1/2	−1/12	1/12	0	−1/8	−1/6
	β_2	0	0	−1/2	1/4	1/4	−1/6	−1/8	−1/6
	β_3	0	0	0	−1/6	−1/3	1/6	1/4	1/3
$d=4$	β_1	1	1	1/2	−1/12	1/12	1/24	0	−1/24
	β_2	0	0	−1/2	1/4	1/4	−1/6	−1/8	−1/6
	β_3	0	0	0	−1/6	−1/3	1/6	1/4	1/3
	β_4	0	0	0	0	0	−1/24	−1/8	−1/8

A remarkable property of the table above is its complete independance of the eigenvalue a (the computations in the proof of Theorem 5 make this final disappearance of a quite unexpected). That this is no casual coincidence, modulo $P^{(d)}$, will be seen below.

A second remark, which was already used before, is that for any value of d we obtain the same formulas for $f_{j,c}(x,\ y)$ if $c \leq d$. In particular, this implies that whenever the nilpotency class of $\langle P_1 \rangle$ is smaller or equal to d, then the same formula (arrested to the proper « weight » d)

$$x+y=xy[y, x]^{1/2}[y, 2x]^{-1/12}[y, x, y]^{1/12}[y, 3x]^{1/24}[y, x, 2y]^{-1/24} \dots$$

defines an abelian group on P_1, as a consequence of Theorem 4. This remark, as well as the particular form of the exponents, suggests a possible connection with the classical formula of (Baker-) Hausdorff (-Campbell) in the theory of Lie-Algebras (cf. [8] and references there):

$$x \cdot y = x+y-(1/2)[y, x]+(1/12)[y, 2x]-$$
$$-(1/12)[y, x, y]+(1/24)[y, 2x, y]+ \dots$$

In fact this formula defines a multiplicative (non abelian) group on a Lie-albegra $L, +, [\ ,\ ]$. We have found in a wellknown paper of M. Lazard [8] the proof that the two formulas are actually connected, by playing exactly inverse roles. The next statement is comprehensive of two results of M. Lazard (Lemma 4.5 and Theorem 4.3 of [8], pag. 176-178), arranged as required by our situation:

THEOREM (Lazard). Let P be a p-group of class $c<p$. Then for any $x, y \in P$ there exist elements $b_1 \in P^{(1)}$, $b_2 \in P^{(2)}$, ..., $b_c \in P^{(c)}$ such that for any integer t

$$x^t y^t = b_1{}^t b_2^{t^2} b_3^{t^3} \dots b_c^{t^c}$$

By letting $x+y=b_1$, $[x, y]=b_2{}^2$, a structure of Lie-ring is defined on P. The group structure $P, \cdot$ is reobtained by applying to $P, +, [\ ,\ ]$ the Hausdorff formula.

Now in order to establish the connection between our loop-operation and the Hausdorff formula we only have to prove the following

THEOREM 6. *Let $\langle P_1 \rangle$ have class $c \leq d$. Then the theorem of Lazard applies and for any $x, y \in P_1$ we have*

$$b_j = (xy)^{\beta_j} \qquad j=1, 2, \dots, c.$$

PROOF. Since d divides $p-1$, the assumption $c<p$ of Lazard is satisfied. Since for $c=1$ we have trivially $b_1=xy=(xy)^{\beta_1}$ we shall induce on c. Thus, by the familiar procedure, we can assume $b_j \equiv (xy)^{\beta_j}$ (mod $P^{(c)}$) for $j=1, 2, \dots, c-1$. Therefore $b_j=(xy)^{\beta_j} z_j$ for some $z_j \in P^{(c)}$, for $j=1, 2, \dots, c$; the last equation (for $j=c$) being a consequence of

Lemma 4. If we now apply the automorphism φ^j to the equation $xy=(xy)^{\beta_1} \dots (xy)^{\beta_c}$ (clearly, $\beta_j=1$ for $j>c$), we find

$$x^{a^j}y^{a^j}=((xy)^{\beta_1})^{a^j}((xy)^{\beta_2})^{a^{2j}} \dots ((xy)^{\beta_c})^{a^{cj}}.$$

On the other hand, by the definition of b_j, we also have

$$x^{a^j}y^{a^j}=b_1^{a^j}b_2^{a^{2j}} \dots b_c^{a^{cj}}.$$

By comparison, since z_j is in the center of P, we find the c equations

$$z_1^{a^j}z_2^{a^{2j}} \dots z_c^{a^{cj}}=1, \qquad j=1, 2, \dots, c.$$

Rewriting in additive notation, this is equivalent to a system of c linear equations for the z_j, considered as elements of the Z/p^nZ-module $P^{(c)}$. Now the matrix associated with this system has a Vandermonde determinant, equal to $\prod_{1\leq i<j\leq c} (a^j-a^i)$. Since $c\leq d$, by Lemma 1 this is a unit of the ring Z/p^nZ, hence the system has only the trivial solution. Thus $z_1=z_2= \dots =z_c=1$, and the Theorem is proved.

At p. 157 of [8] one can also find an algorythm for the computation of the first terms of c_1 and c_2 in their basic commutators expansion, starting from the knowledge of the first terms of the Hausdorff formula (this is reported there as « the constructive inversion-formula »). We notice that this gives an indirect and partial solution to the problem indicated above, i.e. the independance of the formulas of the eigenvalue a. However, as the whole theory of Lazard cannot be applied when $c\geq p$, the general case cannot be settled in this way.

We finally mention another problem, which naturally arises at the beginning of § 2, when we chose the natural order for the eigensubsets P_i. With different choices, we would have obtained different projections β^*_j, in particular $d!$ different loops on P_1. For example, when $d=2$ the factorization $P=P_2P_1$ yields $(xy)^{\beta^*_1}=(yx)^{\beta_1}$, i.e. a loop anti-isomorphic to the loop we previously had. Now it is clear that the statements of Theorems 2 to 5 remain true for any chosen order. But can one « nicely » describe an algebraic relation between these different loops? Our only contribution will be the following: all these loops are isomorphic modulo $P^{(d)}$. This is implied in the proof of Theorem 5, because the ordering enters the computation only through the formula (**), so that $f_{1,d}$ is not affected.

§ 4. In Theorem 4 we have found the upper bound $c'=$ $=[(c+d-1)/d]$ for the central nilpotency of the loop P_1, $+$, in terms of the class c of $\langle P_1\rangle$. As Theorem 4 in [2] states that $[(c+1)/2]$ is exactly the class of P_1 when φ is involutory, it is natural to ask whether more generally c' is exactly the class of P_1, $+$ when $d>2$. That this is not the case will be proved by a counterexample. We shall construct a p-group P ($p\equiv 1$ mod 3) admitting an automorphism φ of order 3 such that $P=\langle P_1\rangle$ has class 4, but P_1, $+$ is an abelian group. This construction was suggested by the last section of [8], and we refer to it for the details.

A COUNTEREXAMPLE. Let $p\equiv 1$ (mod. 3). Let L_0 be the free Lee-algebra generated over the Galois field Z/pZ by the three independent generators x_1, x_2, x_3. By the Witt formula ([7], 11, 2.2) we can compute the dimension of the submodule of the elements of « weight » s. For $s=1, 2, 3, 4$ we find resp. 3, 3, 8, 18.

In L_0 consider the ideal I generated by:

1) all the elements of weight $s\geq 5$.

2) all elements of weight $s=4$ which have the following form:

$$2[x_i, x_j, x_k, x_k]-[[x_k, x_i], [x_k, x_j]]$$

$$4[x_i, x_j, x_k, x_i]-[[x_i, x_k], [x_i, x_j]].$$

Consider the quotient algebra $L=L_0/I$ and omit, for simplicity, the bar over the homomorphic images from L_0 to L. Then L is a nilpotent algebra of class 4, generated by x_1, x_2, x_3.

Taking into account the defining relations in 2) and the obvious identities

$$[x_i, x_j, x_k, x_r]=-[x_j, x_i, x_k, x_r]$$

$$[x_i, x_j, x_r, x_k]=[x_i, x_j, x_k, x_r][[x_i, x_j], [x_r, x_k]]$$

one finds that the submodule of L whose elements have weight 4 has dimension 3 and the following is a basis for it:

$$z_1=[[x_1, x_2], [x_1, x_3]]; \qquad z_2=[[x_2, x_3], [x_2, x_1]];$$
$$z_3=[[x_3, x_1], [x_3, x_2]].$$

Now we claim that for any choice of $y_j \in L$ the following relations hold:

$$2[y_1, y_2, y_3, y_3]=[[y_3, y_1], [y_3, y_2]]$$
$$4[y_1, y_2, y_3, y_1]=[[y_1, y_3], [y_1, y_2]].$$

To verify this, it will suffice to replace the y_j by the corresponding homogeneous component of weight 1. Thus we write

$$y_j=\sum_{l=1}^{3} a_{jl}x_l \qquad j=1, 2, 3.$$

A tedious but straightforward calculation shows that

$$[y_1, y_2, y_3, y_3]=(D/2)(a_{31}z_1+a_{32}z_2+a_{33}z_3)$$
$$[y_1, y_2, y_3, y_1]=-(D/4)(a_{11}z_1+a_{12}z_2+a_{13}z_3)$$

where D is the determinant of the matrix (a_{jl}). On the other hand we can calculate

$$[[y_1, y_3], [y_1, y_2]]=-D(a_{11}z_1+a_{12}z_2+a_{13}z_3)$$
$$[[y_3, y_1], [y_3, y_2]]=D(a_{31}z_1+a_{32}z_2+a_{33}z_3)$$

and we easily see that our statement is proved. In particular, we remark that any element of the form $[y_1, y_2, y_2, y_2]$ or $[y_1, y_2, y_2, y_1]$ is zero. In fact $D=0$ in this case. This suffices to conclude that any 2-generators subalgebra is nilpotent of class not exceeding 3.

According to the previous remark, the dimension of L as a Z/pZ-algebra is easily calculated: $3+3+8+3=17$.

Now let a be a primitive root of $x^3\equiv 1 \pmod p$. Consider the mapping $\varphi: x_i \rightarrow ax_i$ $(i=1, 2, 3)$ and extend φ to the whole L. Then φ is an automorphism of L, of order 3.

We now apply to L the Hausdorff formula, according to Theorem 4.6 of [8]. This is clearly possible, as the assumption $p\equiv 1 \pmod 3$

implies $4<p$. Then $L, \cdot = P$ is a nilpotent group of class 4, generated by x_1, x_2, x_3. Moreover, we see that for any $y_1, y_2, y_3 \in P$ the following relations hold:

$$[y_1, y_2, 2y_3]=[[y_3, y_1], [y_3, y_2]]^{1/2}$$

$$[y_1, y_2, y_3, y_1]=[[y_1, y_3], [y_1, y_2]]^{1/4}.$$

In particular, all 2-generators subgroups of P have class ≤ 3.

Also, φ induces on P a (group-) automorphism of order 3. Since $x_i^{\varphi}=(x_i)^a$ for $i=1, 2, 3$, we have $P=\langle P_1 \rangle$. According to the table of § 3, we have for the loop operation in P_1

$$x+y=xy[y, x]^{1/2}[y, 2x]^{-1/12}[y, x, y]^{1/12}$$

as $[y, 3x]=[y, 2x, y]=[y, x, 2y]=1$. However, by Theorem 6 the operation $+$ gives back the group structure of the Lie-algebra L. In particular, $P_1, +$ is an abelian group.

In some recent literature ([6]), n-generators p-groups of class c, whose $(n-1)$-generators subgroups have class $<c$ have deserved particular attention. For $n=3$, $c=4$ the only concrete available example seems to be Ex. 4.1 in [5], a group whose properties are derived with some difficulty from the rather complicated defining relations. Thus our construction may have some interest, apart from the problem by which it was originated. Indeed, by ignoring automorphisms and loops, for any prime $p \geq 5$ we have constructed a 3-generators p-group of class 4 (exponent p and order p^{17}) whose 2-generators subgroups have class ≤ 3. Of course, the main point of such constructions consists in the proper choice of the generators for the ideal I in the Lie-algebra. In our case, this choice was greatly facilitated by the loop-theoretical problem. In fact, if one makes use of the exponent-table in § 2 to write down explicitely the associative laws $x+(y+z)=(x+y)+z$ etc., one ends up with a set of necessary conditions as

$$[z, x, 2y]^2[[z, y], [y, x]] \equiv 1 \qquad (\text{mod } P^{(5)})$$

etc., which strongly suggest the form of the generators, as in 1) and 2) above.

AKNOWLEDGEMENTS

The author is grateful to Prof. H. Wielandt, for suggesting and encouraging this investigation. He also wishes to thank the NATO for its support during the writing of this paper at the University of Tübingen.

REFERENCES

[1] BRUCK, R. H.: *A survey of binary systems*, Springer, Berlin, 1958.

[2] GLAUBERMAN, G.: *On loops of odd order*, J. Algebra, *1*, 374-396 (1964).

[3] GLAUBERMAN, G.: *On loops of odd order II*, J. Algebra, *8*, 393-414 (1968).

[4] GORENSTEIN, D., HERSTEIN, I. N.: *Finite groups admitting a fixed-point-free automorphism of order 4*, Amer. Jour. Math., *83*, 71-78 (1961).

[5] GUPTA, C. K.: *A bound for the class of certain nilpotent groups*, J. Austr. M.S., *5*, 506-511 (1965).

[6] GUPTA, C. K., GUPTA, N. D., NEWMAN, M. F.: *Some finite nilpotent p-groups*, J. Austr. M.S., *9*, 287-288 (1969).

[7] HALL, M.: *The theory of groups*, Mc Millan Co., New York, 1959.

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

[9] WIELANDT, H.: *Beziehungen zwischen den Fixpunktzahlen von Automorphismengruppe einer endlichen Gruppe*, Math. Zeit., *73*, 146-158 (1960).

Manoscritto pervenuto in redazione il 15 novembre 1970.