BULLETIN DE LA S. M. F.

J.P. LABUTE

Demuškin groups of rank $\aleph_0$

Bulletin de la S. M. F., tome 94 (1966), p. 211-244
<http://www.numdam.org/item?id=BSMF_1966__94__211_0>

Bull. Soc. math. France,
94, 1966, p. 211 à 244.

DEMUŠKIN GROUPS OF RANK $\aleph_0$

BY

JOHN P. LABUTE (*).

In this paper, we extend the notion of a Demuškin group to pro-p-groups of denumerable rank, *cf.* Definition 1. The classification of Demuškin groups of finite rank is complete (*cf.* [1], [2], [3], [7], [8], [11]), and the purpose of this paper is to extend this classification to Demuškin groups of rank $\aleph_0$ (*cf.* [9]). This is accomplished in Theorems 3 and 4, leaving aside an exceptional case when $p=2$. We then apply our results (*cf.* Theorem 5) and determine for all p, the structure of the p-Sylow subgroup of the Galois group of the extension $\overline{K}/K$, where K is a finite extension of the field $\mathbf{Q}_p$ of p-adic rationals and $\overline{K}$ is its algebraic closure. This answers a question posed to the author by J.-P. SERRE.

1. Definitions and Results.

1.1. **Demuškin Groups.** — Let p be a prime number, and let G be a pro-p-group (i. e., a projective limit of finite p-groups, *cf.* [4], [12]). Throughout this paper $H^q(G)$ will denote the cohomology group $H^q(G, \mathbf{Z}/p\mathbf{Z})$, the action of G on the discrete group $\mathbf{Z}/p\mathbf{Z}$ being the trivial one. ($\mathbf{Z}$ is the ring of rational integers.) The dimension of $H^1(G)$ over the field $\mathbf{Z}/p\mathbf{Z}$ is called the *rank* of G and is denoted by $n(G)$.

(*) The author is the recipient of a post-doctorate overseas fellowship given by the National Research Council of Canada.

DEFINITION 1. — *A pro-p-group G of rank* $\leq \aleph_0$ *is said to be a Demuškin group if the following two conditions are satisfied :*

(i) $H^2(G)$ *is one-dimensional over the field* $\mathbf{Z}/p\mathbf{Z}$;

(ii) *The cup product :* $H^1(G) \times H^1(G) \to H^2(G)$ *is a non-degenerate bilinear form,* i. e., $a \cup b = 0$ *for all* b *in* $H^1(G)$ *implies* $a = 0$.

Remark. — The definition of non-degeneracy given above is equivalent to the one we gave in [9], thanks to results obtained by KAPLANSKY in [6], *cf.* § 2.4.

Our first result relates Demuškin groups of rank $\aleph_0$ to Demuškin groups of finite rank.

THEOREM 1. — *If G is a Demuškin group of rank* $\aleph_0$, *there is a decreasing sequence* (H_i) *of closed normal subgroups of G with* $\bigcap_i H_i = 1$ *and with each quotient* G/H_i *a Demuškin group of finite rank.*

Conversely, if G is a pro-p-group of rank $\aleph_0$ *having such a family of closed normal subgroups, then G is either a free pro-p-group or a Demuškin group.*

If G is a pro-p-group, we let $cd(G)$ denote the cohomological dimension of G in the sense of TATE; recall (*cf.* [4], p. 189-207, or [12], p. I-17) that $cd(G)$ is the supremum, finite or infinite, of the integers n such that there exists a discrete torsion G-module A with $H^n(G, A) \neq 0$. Since G is a pro-p-group, $cd(G)$ is also equal to the supremum of the integers n with $H^n(G) \neq 0$ (*cf.* [12], p. I-32). We then have the following result :

COROLLARY. — *If G is a Demuškin group of rank* $\aleph_0$, *then* $cd(G) = 2$.

Indeed, by Theorem 1, G is the projective limit of Demuskin groups G_i of finite rank. Moreover, since G is of rank $\aleph_0$, we may assume that $n(G_i) \neq 1$ for all i, and hence that $cd(G_i) = 2$ for all i (*cf.* [11], p. 252-609). Since $H^q(G) = \varinjlim H^q(G_i)$ (*cf.* [12], p. I-9), it follows that $cd(G) \leq 2$. But $H^2(G) \neq 0$ by the definition of a Demuskin group. Hence $cd(G) = 2$.

Our next result gives the structure of the closed subgroups of a Demuskin group.

THEOREM 2. — *If G is a Demuškin group of rank* $\neq 1$, *then*

(i) *every open subgroup is a Demuškin group;*

(ii) *every closed subgroup of infinite index is a free pro-p-group.*

The proof of these two theorems can be found in paragraph 3.

1.2. **Demuškin Relations.** — As in the case of Demuškin groups of finite rank, we work with relations. Let G be a Demuškin group, and let F be a free pro-p-group of rank $n(G)$. Then there is a continuous homomorphism f of F onto G such that the homomorphism $H^1(f)$: $H^1(G) \to H^1(F)$ is an isomorphism (*cf.* [12], p. I-36). If $R = \text{Ker}(f)$, we identify G with F/R by means of f. Making use of the exact sequence

$$0 \to H^1(G) \xrightarrow{\text{Inf}} H^1(F) \xrightarrow{\text{Res}} H^1(R)^G \xrightarrow{\text{tg}} H^2(G) \xrightarrow{\text{Inf}} H^2(F)$$

(*cf.* [12], p. I-15), we see that the transgression homomorphism tg is injective since the first inflation homomorphism is bijective. Since $H^2(F) = 0$ (*cf.* [12], p. I-25) it follows that $H^1(R)^G \cong H^2(G) \cong \mathbf{Z}/p\mathbf{Z}$. Hence R is the closed normal subgroup of F generated by a single element r (*cf.* [12], p. I-40). Moreover, since $\chi(r) = 0$ for every $\chi \in H^1(F)$, we have $r \in F^p(F, F)$. [If H, K are closed subgroups of a pro-p-group F, we let (H, K) denote the closed subgroup of F generated by the commutators $(h, k) = h^{-1}k^{-1}hk$ with $h \in H$, $k \in K$.] The purpose of this paper is to find a canonical form for the *Demuškin relation r.*

1.3. **The invariants.** — In order to state our classification theorem we have to define certain invariants of a Demuškin group.

1.3.1. *The invariants* $s(G)$, $\text{Im}(\chi)$. — Let G be a Demuškin group of rank $\neq 1$. Since $H^2(G, \mathbf{Z}/p\mathbf{Z})$ is finite, it follows, by « dévissage », that $H^2(G, M)$ is finite for any finite p-primary G-module M (*cf.* [12], p. I-32). Since $cd(G) = 2$, it follows that G has a dualizing module I, that is, the functor $T(M) = \text{Hom}(H^2(G, M), \mathbf{Q}/\mathbf{Z})$, defined on the category of p-primary G-modules M, is representable (*cf.* [12], p. I-27). If $n(G) < \aleph_0$, then I is isomorphic, as an abelian group, to $\mathbf{Q}_p/\mathbf{Z}_p$ (*cf.* [12], p. I-48). If $n(G) = \aleph_0$, then I is isomorphic, as an abelian group, to either $\mathbf{Q}_p/\mathbf{Z}_p$ or $\mathbf{Z}/p^e\mathbf{Z}$. Indeed, it suffices to show that the group $I_p = \text{Hom}(\mathbf{Z}/p\mathbf{Z}, I)$ is cyclic of order p. But I_p is the inductive limit of the groups $\text{Hom}(H^2(U), \mathbf{Q}/\mathbf{Z})$, where U runs over the open subgroups of G, the maps being induced by the corestriction homomorphisms (*cf.* [12], p. I-30). Moreover, if U is an open subgroup of G, we have $H^2(U) \cong \mathbf{Z}/p\mathbf{Z}$ by Theorem 2. Hence I_p is cyclic of order $\leq p$. Since $I_p \neq 0$, the result follows. *The s-invariant of G is defined by setting $s(G) = 0$ if I is infinite, and letting $s(G)$ be the order of I if I is a finite group.*

The ring $\mathbf{E}$ of endomorphisms of I is canonically isomorphic to $\mathbf{Z}_p$ if $s(G) = 0$, and to $\mathbf{Z}/p^e\mathbf{Z}$ if $s(G) = p^e$. Hence, if $\mathbf{U}$ is the compact group of units of $\mathbf{E}$, we have a *canonical homomorphism* $\chi : G \to \mathbf{U}$. Since χ is continuous, it follows that the *invariant* $\text{Im}(\chi)$ is a closed subgroup of the pro-p-group $\mathbf{U}^{(1)} = 1 + p\mathbf{E}$.

We shall need a list of the closed subgroups of $\mathbf{U}^{(1)}$. Consider first the case where $s(G)=0$. Then we have

$$\mathbf{U}^{(1)}=\mathbf{U}_p^{(1)}=1+p\mathbf{Z}_p.$$

If $p\neq 2$, then $\mathbf{U}_p^{(1)}$ is a free pro-p-group of rank 1 generated by any element u with $v_p(u-1)=1$, and the closed subgroups of $\mathbf{U}_p^{(1)}$ are the subgroups

$$\mathbf{U}_p^{(f)}=1+p^f\mathbf{Z}_p \qquad \text{with} \quad f\in\overline{\mathbf{N}}=\mathbf{N}\cup\{\infty\}.$$

(We let $\mathbf{N}$ denote the set of integers ≥ 1; by convention $\infty\geq a$ for any $a\in\overline{\mathbf{N}}$ and $a^\infty=0$ for any $a\in\mathbf{N}$.) If $p=2$, we have $\mathbf{U}_2^{(1)}=\{\pm 1\}\times\mathbf{U}_2^{(2)}$, and $\mathbf{U}_2^{(2)}$ is a free 2-group of rank 1 generated by any element u with $v_2(u-1)=2$. The closed subgroups of $\mathbf{U}_2^{(1)}$ are therefore of three distinct types :

(i) the groups $\mathbf{U}_2^{(f)}$ with $f\in\overline{\mathbf{N}}$, $f\geq 2$;

(ii) the groups $\{\pm 1\}\times\mathbf{U}_2^{(f)}$ with $f\in\overline{\mathbf{N}}$, $f\geq 2$;

(iii) the groups $\mathbf{U}_2^{[f]}$, where for $f\in\mathbf{N}$, $f\geq 2$, $\mathbf{U}_2^{[f]}$ is the closed subgroup of $\mathbf{U}_2^{(1)}$ generated by $-u$, where u is a generator of $\mathbf{U}_2^{(f)}$.

If $s(G)=p^e\neq 0$, then $\mathbf{U}^{(1)}=\mathbf{U}_p^{(1)}/\mathbf{U}_p^{(e)}$, and the closed subgroups of $\mathbf{U}^{(1)}$ are in one-to-one correspondence with the closed subgroups of $\mathbf{U}_p^{(1)}$ which contain $\mathbf{U}_p^{(e)}$.

1.3.2. *The invariant* $t(G)$. — Suppose that the Demuškin group G is of rank $\aleph_0$, and let $\varphi : H^1(G)\times H^1(G)\to H^2(G)$ be the cup product. Then φ is a non-degenerate skew-symmetric bilinear form on the vector space $V=H^1(G)$. Let β be the linear form on V defined by $\beta(v)=v\cup v$, and let $A=\operatorname{Ker}(\beta)$. *If* $A=V$, i. e., *if* φ *is alternate, we set* $t(G)=1$. If $A\neq V$, which can happen only if $p=2$, the vector space V/A is one-dimensional, and hence A', the orthogonal complement of A in V, is at most one-dimensional. *In this case, we define* $t(G)$ *as follows : set* $t(G)=1$ *if* $\dim(A')=1$ *and* $A'\subset A$; *set* $t(G)=-1$ *if* $\dim(A')=1$ *and* $A'\not\subset A$; *set* $t(G)=0$ *if* $A'=0$.

Remark. — We shall see (*cf.* § 2.4) that the definition of $t(G)$ given above is equivalent to the one we gave in [9].

1.3.3. *The invariants* $h(G)$, $q(G)$. — Let G be a Demuskin group and let $G_a=G/(G, G)$. Representing G as a quotient $F/(r)$, where F is a free pro-p-group and $r\in F^p(F, F)$, we see that *either* G_a is torsion-free *or* the torsion subgroup of G_a is cyclic of order p^h. *The h-invariant of G is defined by setting* $h(G)=\infty$ *in the first case and* $h(G)=h$ *in the second. The q-invariant is defined by setting* $q(G)=p^{h(G)}$. If r is the above relation, then $q=q(G)$ is the highest power of p such that $r\in F^q(F, F)$.

1.4. The Classification Theorem. — Recall (*cf.* [12], p. I-5) that if F is the free pro-p-group generated by the elements x_i, $i \in I$, then $x_i \to 1$ in the sense of the filter formed by the complements of the finite subsets of I. If $(g_i)_{i \in I}$ is a family of elements in a pro-p-group G with $g_i \to 1$, we call (g_i) a *generating system* of G if the continuous homomorphism $f : F \to G$ sending x_i into g_i is surjective. The homomorphism f is surjective if and only if $H^1(f) : H^1(G) \to H^1(F)$ is injective (*cf.* [12], p. I-35). Hence (g_i) is a *minimal* generating system if and only if $H^1(f)$ is bijective. If G is a free pro-p-group and (g_i) is a minimal generating system of G, then f is bijective, i. e. (g_i) is a *basis* of G (*cf.* [12], p. I-36).

The main results of this paper are contained in the following two theorems :

THEOREM 3. — *Let $r \in F^p(F, F)$, where F is a free pro-p-group of rank $\aleph_0$. Suppose that $G = F/(r)$ is a Demuškin group, and let $q = q(G)$, $h = h(G)$, $t = t(G)$. Then :*

(i) *If $q \neq 2$, there is a basis $(x_i)_{i \in \mathbf{N}}$ of F such that r is equal to*

$$(1) \qquad x_1^q (x_1, x_2) \prod_{i \geq 2} x_{2i-1}^s (x_{2i-1}, x_{2i}),$$

with $s = p^e$, $e \in \overline{\mathbf{N}}$, $e \geq h$.

(ii) *If $q = 2$, $t = 1$, there is a basis $(x_i)_{i \in \mathbf{N}}$ of F such that, either r is equal to*

$$(2) \qquad x_1^{2+2^f} (x_1, x_2)(x_3, x_4) \prod_{i \geq 3} x_{2i-1}^s (x_{2i-1}, x_{2i}),$$

with $s = 2^e$, $e \in \overline{\mathbf{N}}$, $f \in \mathbf{N}$, $e > f \geq 2$, or r is equal to

$$(3) \qquad x_1^2 (x_1, x_2) x_2^{2^f} (x_3, x_4) \prod_{i \geq 3} x_{2i-1}^s (x_{2i-1}, x_{2i}),$$

with $s = 2^e$, $e, f \in \overline{\mathbf{N}}$, $e \geq f \geq 2$.

(iii) *If $q = 2$, $t = -1$, there is a basis $(x_i)_{i \in \mathbf{N}}$ of F such that r is equal to*

$$(4) \qquad x_1^2 x_2^{2^f} (x_2, x_3) \prod_{i \geq 2} x_{2i}^s (x_{2i}, x_{2i+1}),$$

with $s = 2^e$, $e, f \in \overline{\mathbf{N}}$, $e \geq f \geq 2$.

(iv) *If $q = 2$, $t = 0$, there is a basis $(x_i)_{i \in \mathbf{N}}$ of F such that r is equa to*

$$(5) \qquad \prod_{i \geq 1} x_{2i-1}^2 (x_{2i-1}, x_{2i}) \prod_{i < j} (x_i, x_j)^{b_{ij}},$$

with $b_{ij} \in 2\mathbf{Z}_2$. (*The product* $\prod_{i<j}$ *is taken with respect to an arbitrarily given linear order of* $\mathbf{N} \times \mathbf{N}$.)

THEOREM 4. — *Let* F *be a free pro-p-group with basis* $(x_i)_{i \in \mathbf{N}}$, *and let* $G = F/(r)$. *Then* :

(i) *If* r *is a relation of the form* (1) *with* $q = p^h$, $s = p^e$, $e, h \in \overline{\mathbf{N}}$, $e \geqq h$, *then* G *is a Demuškin group with* $q(G) = q$, $s(G) = s$, $\chi(x_2) = (1 - q)^{-1}$, $\chi(x_i) = 1$ *for* $i \neq 2$. (χ *is the character associated to the dualizing module of* G.)

(ii) *If* $p = 2$ *and* r *is a relation of the form*

$$x_1^{2+2^f}(x_1, x_2)\, x_3^{2^g}(x_3, x_4) \prod_{i \geqq 3} x_{2i-1}^s (x_{2i-1}, x_{2i}), \tag{6}$$

with $s = 2^e$, $e, f, g \in \overline{\mathbf{N}}$, $e \geqq f \geqq 2$, $e \geqq g \geqq 2$, *then* G *is a Demuškin group with* $q(G) = 2$, $t(G) = 1$, $s(G) = s$, $\chi(x_2) = -(1 + 2^f)^{-1}$, $\chi(x_4) = (1 - 2^g)^{-1}$, $\chi(x_i) = 1$ *for* $i \neq 2, 4$.

(iii) *If* $p = 2$ *and* r *is a relation of the form* (4) *with* $s = 2^e$, $e, f \in \overline{\mathbf{N}}$, $e \geqq f \geqq 2$, *then* G *is a Demuškin group with* $q(G) = 2$, $t(G) = -1$, $s(G) = s$, $\chi(x_1) = -1$, $\chi(x_3) = (1 - 2^f)^{-1}$, $\chi(x_i) = 1$ *for* $i \neq 1, 3$.

(iv) *If* $p = 2$ *and* r *is a relation of the form* (5) *with* $b_{ij} \in 2\mathbf{Z}_2$, *then* G *is a Demuškin group with* $q(G) = 2$, $t(G) = 0$, $s(G) = 2$.

COROLLARY 1. — *Let* G, G' *be Demuškin groups of rank* $\aleph_0$ *with* $q(G) \neq 2$. *Then* $G \cong G'$ *if and only if* $q(G) = q(G')$, $s(G) = s(G')$.

COROLLARY 2. — *Let* G, G' *be Demuškin groups of rank* $\aleph_0$ *with* $t(G) \neq 0$. *Then* $G \cong G'$ *if and only if* $t(G) = t(G')$, $s(G) = s(G')$, $\mathrm{Im}(\chi) = \mathrm{Im}(\chi')$.

COROLLARY 3. — *Let* $r, r' \in F^p(F, F)$, *where* F *is a free pro-p-group of rank* $\aleph_0$. *Suppose that* $G = F/(r)$, $G' = F/(r')$ *are Demuškin groups with* $t(G) \neq 0$. *Then* $G \cong G'$ *if and only if there is an automorphism* σ *of* F *with* $\sigma(r) = r'$.

COROLLARY 4. — *For each* $e \in \mathbf{N}$ *there is a Demuškin group* G *with* $s(G) = p^e$. *If* G *is such a group and* M *is a torsion* G*-module, then* $p^e \alpha = 0$ *for any* $\alpha \in H^2(G, M)$.

Remark. — The invariant $q(G)$ can be determined from the invariants $s(G)$, $\mathrm{Im}(\chi)$. In fact, if $s(G) = p^e$ and $E = \mathbf{Z}_p/p^e\mathbf{Z}_p$, then $h(G)$ is the largest $h \in \overline{\mathbf{N}}$ with $h \leqq e$ and $\mathrm{Im}(\chi) \subset 1 + p^h E$.

1.5. **Application to Galois Theory.** — If Γ is a profinite group, i. e. a projective limit of finite groups, then a Sylow p-subgroup of Γ is a closed subgroup G which is a pro-p-group with $(\Gamma : U)$ prime to p

for any open sub-group U containing G. Every profinite group has Sylow p-subgroups and any two are conjugate (*cf.* [12], p. I-4).

Now let K be a finite extension of $\mathbf{Q}_p$ and let Γ be the Galois group of the extension $\overline{K}/K$, where $\overline{K}$ is an algebraic closure of K. Given the Krull topology, the group Γ is a profinite group. If G is a Sylow p-sub-group of Γ, we have the following result :

THEOREM 5. — *The group G is a Demuškin group of rank $\aleph_0$ and its dualizing module is $\mu_{p^\infty} = \bigcup_{n \geq 1} \mu_{p^n}$, where μ_{p^n} is the group of p^n-th roots of unity. If ζ_p is a primitive p-th root of unity and $K' = K(\zeta_p)$, then $t(G) = (-1)^a$, where $a = [K' : \mathbf{Q}_p]$.*

COROLLARY 1. — *If $K' = K(\zeta_p)$, then $q = q(G)$ is the highest power of p such that K' contains a primitive q-th root of unity.*

Indeed, if $\sigma \in G$, then $\chi(\sigma)$ is the unique p-adic unit such that $\sigma(\zeta) = \zeta^{\chi(\sigma)}$ for any $\zeta \in \mu_{p^\infty}$. If ζ_q is a primitive q-th root of unity, it follows that ζ_q is left fixed by σ if and only if $\chi(\sigma) \in 1 + q\mathbf{Z}_p$. If L is the fixed field of G, it follows that $\zeta_q \in L$ if and only if $\mathrm{Im}(\chi) \subset 1 + q\mathbf{Z}_p$. But $\zeta_q \in L$ if and only if $\zeta_q \in K'$ since L and $K'(\zeta_q)$ are linearly disjoint over K'.

COROLLARY 2. — *If $K = \mathbf{Q}_p$ with $p \neq 2$, there exists a generating system $(\sigma_i)_{i \in \mathbf{N}}$ of G having the single relation*

$$\sigma_1^p(\sigma_1, \sigma_2) \prod_{i \geq 2} (\sigma_{2i-1}, \sigma_{2i}) = 1.$$

In fact, $q(G) = p \neq 2$ (*cf.* [10], p. 85).

COROLLARY 3. — *If $K = \mathbf{Q}_2$, there exists a generating system $(\sigma_i)_{i \in \mathbf{N}}$ of G having the single relation*

$$\sigma_1^2 \sigma_2^4 (\sigma_2, \sigma_3) \prod_{i \geq 2} (\sigma_{2i}, \sigma_{2i+1}) = 1.$$

Indeed, $t(G) = -1$ and $\mathrm{Im}(\chi) = \mathbf{U}_2$.

2. Preliminaries.

2.1. **The Descending Central Series.** — The *descending central series* of a pro-p-group F is defined inductively as follows : $F_1 = F$, $F_{n+1} = (F_n, F)$. The sequence of closed subgroups F_n of F have the following properties :

(i) $F_1 = F$;
(ii) $F_{n+1} \subset F_n$;
(iii) $(F_n, F_m) \subset F_{n+m}$.

The first two properties are obvious, and the third is proved by induction. Such a sequence of subgroups is called a *filtration* of F. Let $\mathrm{gr}(F)$ be the direct sum of the $\mathbf{Z}_p$-modules $\mathrm{gr}_n(F) = F_n/F_{n+1}$. Then $\mathrm{gr}(F)$ is, in a natural way, a Lie algebra over $\mathbf{Z}_p$ (*cf.* [13], page LA 2.3) the bracket operation for homogeneous elements being defined as follows : If $i_n : F_n \to \mathrm{gr}_n(F)$ is the canonical homomorphism and $u \in F_n$, $v \in F_m$, then

$$[i_n(u), i_m(v)] = i_{n+m}((u, v)).$$

Suppose now that F is the *free* pro-p-group of rank n generated by the elements $x_1, \ldots, x_n$. If ξ_i is the image of x_i in $\mathrm{gr}_1(F)$, we have the following proposition :

Proposition 1. — *The Lie algebra* $\mathrm{gr}(F)$ *is a free Lie algebra (over* $\mathbf{Z}_p$*) with basis* $\xi_1, \ldots, \xi_n$.

Proof. — Let L be the free Lie algebra (over $\mathbf{Z}_p$) on the letters $\xi_1, \ldots, \xi_n$, and let $\varphi : L \to \mathrm{gr}(F)$ be the Lie algebra homomorphism sending ξ_i into ξ_i. Using the fact that the x_i form a generating system of F, one shows by induction that the elements $\xi_i \in \mathrm{gr}_1(F)$ generate the Lie algebra $\mathrm{gr}(F)$. Hence φ is surjective.

To show that φ is injective, let A be the ring of associative but non-commutative formal power series on the letters $t_1, \ldots, t_n$, with coefficients in $\mathbf{Z}_p$. Let $\mathfrak{m}^i$ be the ideal of A consisting of those formal power series whose homogeneous components are of degree $\geq i$. The ring $A/\mathfrak{m}^i$ is a compact topological ring if we give it the p-adic topology, and, as a ring, A is the projective limit of the rings $A/\mathfrak{m}^i$. We give A the unique topology which makes it the projective limit of the compact topological rings $A/\mathfrak{m}^i$. Let U^1 be the multiplicative group of formal power series with constant term equal to 1. Then, with the induced topology, U^1 is a pro-p-group containing the elements $1 + t_i$. Since (x_i) is a basis of the free pro-p-group F, there is a continuous homomorphism ε of F into U^1 sending x_i into $1 + t_i$. If

$$\varepsilon(x) = 1 + u, \qquad \varepsilon(y) = 1 + v, \qquad \text{with } u \in \mathfrak{m}^i, \qquad v \in \mathfrak{m}^j,$$

then using the fact that $\varepsilon(xy) = \varepsilon(yx)\,\varepsilon((x, y))$, an easy calculation with formal power series shows that

$$\varepsilon((x, y)) = 1 + (uv - vu) + \text{higher terms.} \tag{7}$$

If $\theta_0 : F \to \mathfrak{m}^1$ is defined by $\theta_0(x) = \varepsilon(x) - 1$, then, applying (7) inductively, we see that $\theta_0(F_i) \subset \mathfrak{m}^i$. If $x \in F_i$, $y \in F_{i+1}$, then $\theta_0(xy) \equiv \theta_0(x)$ (mod $\mathfrak{m}^{i+1}$), and if $x, y \in F_i$, we have

$$\theta_0(xy) \equiv \theta_0(x) + \theta_0(y) \qquad (\mathrm{mod}\, \mathfrak{m}^{i+1}).$$

Hence θ_0 induces an additive homomorphism θ of $\mathrm{gr}(F)$ into $\mathrm{gr}(A)$, where $\mathrm{gr}(A)$ is the graded algebra defined by the $\mathfrak{m}$-adic filtration of A. Moreover, (7) shows that θ is a Lie algebra homomorphism. If τ_i is the image of t_i in $\mathrm{gr}_1(A)$, then $\mathrm{gr}(A)$ is a free associative algebra with basis (τ_i). By the theorem of Birkhoff-Witt (*cf.* [13], page LA 4.4) the Lie algebra homomorphism $\psi : L \to \mathrm{gr}\,(A)$ sending ξ_i into τ_i is injective. Since $\psi = \theta \circ \varphi$, we see that φ is injective, and hence bijective,

Q. E. D.

If F is a free pro-p-group of infinite rank, then F is the projective limit of free pro-p-groups $F\,(i)$ of finite rank, and $\mathrm{gr}_n(F)$ is the projective limit of the groups $\mathrm{gr}_n(F\,(i))$. In particular, this gives the following result :

PROPOSITION 2. — *If* (F_n) *is the descending central series of a free pro-p-group F, then* $\mathrm{gr}_n(F) = F_n/F_{n+1}$ *is a torsion-free* $\mathbf{Z}_p$*-module.*

We shall need the following result on free Lie algebras, the proof of which was communicated to me by J.-P. SERRE :

PROPOSITION 3. — *Let L be the free Lie algebra (over k) on the letters* $\xi_1, \ldots, \xi_n$. *Then $[L, L]$ is generated, as a k-module, by the elements* $\mathrm{ad}\,(\xi_{i_1})\ldots\mathrm{ad}\,(\xi_{i_k})\,\xi_{i_{k+1}}$ *with* $i_{k+1} \geqq i_1, \ldots, i_k$.

Proof. — For $1 \leqq m \leqq n$, let L_m be the subalgebra generated by $\xi_1, \ldots, \xi_m$, and let A_m be the ideal of L_m generated by ξ_m. Then, as a k-module, A_m is generated by ξ_m and the elements $\mathrm{ad}(\xi_{i_1})\ldots\mathrm{ad}\,(\xi_{i_k})\,\xi_m$ with $i_1, \ldots, i_k \leqq m$. Indeed, the ideal A_m contains these elements, and the submodule they generate is invariant under the $\mathrm{ad}(\xi_i)$ for $i \leqq m$. We now show that L is the direct sum of the submodules A_m, from which the proposition immediately follows. It suffices to show that $L_m = L_{m-1} \oplus A_m$ for $2 \leqq m \leqq n$. To do this let $\varphi_m : L_m \to L_{m-1}$ be the Lie algebra homomorphism such that $\varphi_m(\xi_m) = 0$, $\varphi_m(\xi_i) = \xi_i$ if $i < m$. Since L_m/A_m is the free Lie algebra generated by the images of $\xi_1, \ldots, \xi_{m-1}$ and $\mathrm{Ker}\,(\varphi_m) \supset A_m$, it follows that φ_m induces an isomorphism of L_m/A_m onto L_{m-1}. Hence $\mathrm{Ker}(\varphi_m) = A_m$. Since φ_m is the identity on L_{m-1}, the result follows.

Now let F be a free pro-p-group of rank $\aleph_0$ with basis $(x_i)_{i \in \mathbf{N}}$. Let (F_n) be the descending central series of F, and let ξ_i be the image of x_i in $\mathrm{gr}_1(F)$. If N_i is the closed normal subgroup of F generated by the x_j with $j \geqq i$, let $F_{ni} = F_n \cap N_i$, and let B_{ni} be the image of F_{ni} in $\mathrm{gr}_n(F)$. We then have the following result :

PROPOSITION 4. — *If T_n is the closed subgroup of* $\mathrm{gr}_{n+1}(F)$ *generated by the subgroups* $\mathrm{ad}\,(\xi_i)\,B_{ni}$, *then* $T_n = \mathrm{gr}_{n+1}(F)$ *for* $n \geqq 1$.

Proof. — The pro-p-group $\mathrm{gr}_{n+1}(F)$ is generated by the elements of the form $\mathrm{ad}(\xi_{i_1})\ldots\mathrm{ad}(\xi_{i_n})\,\xi_{i_{n+1}}$. However, by Proposition 3, each such element is a linear combination of elements of the same form but with $i_{n+1} \geqq i_1$. Since each of these latter elements belongs to T_n, it follows that T_n contains a generating system of $\mathrm{gr}_{n+1}(F)$. Since T_n is closed, the result follows.

COROLLARY. — *Every element of* $\mathrm{gr}_{n+1}(F)$ *can be written in the form* $\sum_{i \geqq 1} [\xi_i, \tau_i]$ *with* $\tau_i \in \mathrm{gr}_n(F)$, $\tau_i \to 0$.

2.2. **The Descending q-Central Series.** — We shall need the following group-theoretical result :

PROPOSITION 5. — *Let* (F_n) *be a filtration of a group* F. *If* $x \in F_i$, $y \in F_j$, $a \in \mathbf{N}$, $b = \binom{a}{2}$, *then :*

(i) $(xy)^a \equiv x^a y^a (y, x)^b \pmod{F_{i+j+1}}$;

(ii) $(x^a, y) \equiv (x, y)^a ((x, y), x)^b \pmod{F_{i+j+2}}$;

(iii) $(x, y^a) \equiv (x, y)^a ((x, y), y)^b \pmod{F_{i+j+2}}$.

Proof. — Assertion (iii) follows easily form (ii). We now prove (i) and (ii) by induction on a using the following formulae (*cf.* [13], page LA 2.1) :

$$(8) \qquad \begin{cases} (xy, z) = (x, z)\,((x, z), y)\,(y, z), \\ (x, yz) = (x, z)\,(x, y)\,((x, y), z). \end{cases}$$

For $a = 1$, the proposition is obvious.

(i) Working modulo F_{i+j+1}, we have

$$(xy)^{a+1} = xy\,(xy)^a \equiv xyx^a y^a (y, x)^b = x^{a+1} y\,(y, x^a)\,y^a (y, x)^b,$$

which in turn is congruent to $x^{a+1} y^{a+1} (y, x)^{a+b}$, and $a + b = \binom{a+1}{2}$.

(ii) Modulo F_{i+j+2}, we have

$$\begin{aligned}(x^{a+1}, y) &= (xx^a, y) \equiv (x, y)\,((x, y), x^a)\,(x^a, y) \\ &\equiv (x, y)\,((x, y), x)^a (x, y)^a ((x, y), x)^b \equiv (x, y)^{a+1}\,((x, y), x)^{a+b}.\end{aligned}$$

Now let F be a pro-p-group, and let $q = p^h$ with $h \in \mathbf{N}$. The *descending q-central series of* F is defined inductively by $F_1 = F$, $F_{n+1} = F_n^q(F, F_n)$. The groups F_n define a filtration of F. If $\mathrm{gr}(F)$ is the associated Lie algebra, then $\mathrm{gr}(F)$ is a Lie algebra over $\mathbf{Z}/q\mathbf{Z}$. If $P : F \to F$ is the mapping $x \mapsto x^q$, we have $P(F_n) \subset F_{n+1}$ for $n \geqq 1$. Using Proposition 5, we see that P induces a map $\pi : \mathrm{gr}_n(F) \to \mathrm{gr}_{n+1}(F)$ for $n \geqq 1$. The following result is an immediate consequence of Proposition 5 :

PROPOSITION 6. — *Let (F_n) be the descending q-central series of a pro-p-group F. If $\xi \in \mathrm{gr}_i(F)$, $\eta \in \mathrm{gr}_j(F)$, then :*

(i) $\pi(\xi + \eta) = \pi\xi + \pi\eta$ *if* $i = j \neq 1$;

(ii) $\pi(\xi + \eta) = \pi\xi + \pi\eta + \binom{q}{2}[\xi, \eta]$ *if* $i = j = 1$;

(iii) $[\pi\xi, \eta] = \pi[\xi, \eta]$ *if* $i \neq 1$;

(iv) $[\pi\xi, \eta] = \pi[\xi, \eta] + \binom{q}{2}[[\xi, \eta], \xi]$ *if* $i = 1$.

Remarks. — Using the fact that $\binom{q}{2} \equiv 0 \pmod{q}$ if $p \neq 2$, we see that $\mathrm{gr}(F)$ is a Lie algebra over $\mathbf{Z}/q\mathbf{Z}[\pi]$ for $p \neq 2$. If $q = 2^h$, then $\binom{q}{2} \equiv 2^{h-1} \pmod{q}$. Hence in this case $\mathrm{gr}(F)$ is not a Lie algebra over $\mathbf{Z}/q\mathbf{Z}[\pi]$. However, if $\mathrm{gr}'(F) = \sum_{n \geqq 2} \mathrm{gr}_n(F)$, then $\mathrm{gr}'(F)$ is a Lie algebra over $\mathbf{Z}/q\mathbf{Z}[\pi]$. Also, $\mathrm{gr}(F) \otimes \mathbf{Z}/p\mathbf{Z}$ is a Lie algebra over $\mathbf{Z}/q\mathbf{Z}[\pi] \otimes \mathbf{Z}/p\mathbf{Z}$ if $q \neq 2$.

Now let F be a free pro-p-group of rank $\aleph_0$ with basis $(x_i)_{i \in \mathbf{N}}$, and let (F_n) be the descending q-central series of F. Let ξ_i be the image of x_i in $\mathrm{gr}_1(F)$. Let N_i be the closed normal subgroup of F generated by the x_j with $j \geqq i$, let $F_{ni} = F_n \cap N_i$, and let B_{ni} be the image of F_{ni} in $\mathrm{gr}_n(F)$. We then have the following result :

PROPOSITION 7. — *Let T_n be the closed subgroup of $\mathrm{gr}_{n+1}(F)$ generated by the subgroups $\mathrm{ad}(\xi_i) B_{ni}$, and let D be the closed subgroup of $\mathrm{gr}_2(F)$ generated by the elements $\pi\xi_i$. Then the group $\mathrm{gr}_{n+1}(F)$ is generated by T_n and $\pi^{n-1}D$.*

Proof. — Using Proposition 6, we see that $\mathrm{gr}_{n+1}(F)$ is generated by elements of the form

$$\pi^n \xi_i, \quad \pi^{n-k}\mathrm{ad}(\xi_{i_1}) \ldots \mathrm{ad}(\xi_{i_k}) \xi_{i_{k+1}}. \tag{9}$$

It follows, by Proposition 3, that $\mathrm{gr}_{n+1}(F)$ is generated by elements of the form (9) with $i_{k+1} \geqq i_1$. Since

$$\pi^{n-k}[\xi_i, \eta] = [\xi_i, \pi^{n-k}\eta] \quad \text{if } \eta \in \mathrm{gr}_m(F), \quad \text{with} \quad m \geqq 2,$$

and

$$\pi^{n-1}[\xi_i, \xi_j] = [\xi_i, \pi^{n-1}\xi_j] + \left[\xi_j, \binom{q}{2}\pi^{n-2}[\xi_i, \xi_j]\right] \quad \text{for} \quad n \geqq 2,$$

it follows that each of the elements in (9) is in the closed subgroup $T_n + \pi^{n-1}D$.

Q. E. D.

COROLLARY. — *Every element of* $\mathrm{gr}_{n+1}(F)$ *can be written in the form*

$$\sum_{i \geq 1} a_i \pi^n \xi_i + \sum_{i \geq 1} [\xi_i, \tau_i],$$

where $a_i \in \mathbf{Z}/q\mathbf{Z}$, $\tau_i \in \mathrm{gr}_n(F)$, $\tau_i \to 0$.

2.3. **Cohomology and Filtrations.** — Let F be a free pro-p-group, and let $q = p^h$ with $h \in \mathbf{N}$. Let $r \in F^q(F, F)$ with $r \neq 1$, and let R be the closed normal subgroup of F generated by r. If $G = F/R$ and $\mathbf{k} = \mathbf{Z}/q\mathbf{Z}$, we have the exact sequence

$$0 \to H^1(G, \mathbf{k}) \xrightarrow{\text{Inf}} H^1(F, \mathbf{k}) \xrightarrow{\text{Res}} H^1(R, \mathbf{k})^G \xrightarrow{\text{tg}} H^2(G, \mathbf{k}) \xrightarrow{\text{Inf}} H^2(F, \mathbf{k}).$$

Since $R \subset F^q(F, F)$, the first inflation homomorphism is bijective, and we use this homomorphism to identify $H^1(G, \mathbf{k})$ with $H^1(F, \mathbf{k})$. Hence tg is injective. But tg is also surjective since $H^2(F, \mathbf{k}) = 0$. Now let $g \in G$, $\varphi \in H^1(R, \mathbf{k})$. If $x \in R$, then $(g\varphi)(x) = \varphi(g^{-1}xg)$. Hence $g\varphi = \varphi$ if and only if $\varphi((x, g)) = 0$ for all $x \in R$. Thus $\varphi \in H^1(R, \mathbf{k})^G$ if and only if φ vanishes on $R^q(R, F)$. We may therefore identify $H^1(R, \mathbf{k})^G$ with the dual of the pro-p-group $R/R^q(R, F)$. We now show that $R/R^q(R, F)$ is cyclic of order q. This follows immediately form the following lemma :

LEMMA. — *The* $\mathbf{Z}_p$*-module* $N = R/(R, F)$ *is free of rank* 1.

Proof. — Let (F_n) be the descending central series of F. Since the F_n intersect in the identity and $r \neq 1$, there is an $n \in \mathbf{N}$ with $r \in F_n$, $r \notin F_{n+1}$. Hence $R \subset F_n$ and $(R, F) \subset F_{n+1}$. Passing to quotients, we obtain a homomorphism f of N into $\mathrm{gr}_n(F)$ sending the generator $\rho = r(R, F)$ of N into a non-zero element τ of $\mathrm{gr}_n(F)$. Since $\mathrm{gr}_n(F)$ is a torsion-free $\mathbf{Z}_p$-module (*cf.* Proposition 2), it follows that $f(N)$ is free of rank 1 generated by τ, and hence that N is free of rank 1 generated by ρ.

Using the above results, we see that the homomorphism $\rho : H^2(G, \mathbf{k}) \to \mathbf{k}$, defined by $\rho(\alpha) = -\, \mathrm{tg}^{-1}(\alpha)(r)$, is an isomorphism. Given the relation r, we always use this isomorphism to identify $H^2(G, \mathbf{k})$ with $\mathbf{k}$.

Now let (F_n) be the descending q-central series of F. If $(x_i)_{i \in \mathbf{N}}$ is a basis of F, then

$$r \equiv \prod_{i \geq 1} x_i^{q a_i} \prod_{i < j} (x_i, x_j)^{a_{ij}} \qquad (\mathrm{mod}\ F_3)$$

with $a_i, a_{ij} \in \mathbf{k}$. If (χ_i) is the basis of $H^1(G, \mathbf{k})$ defined by $\chi_i(x_j) = \delta_{ij}$, we have the following proposition :

PROPOSITION 8.

(*a*) *If* $\chi_i \cup \chi_j \in H^2(G, \mathbf{k}) = \mathbf{k}$ *is the cup product of* χ_i, χ_j, *then* $\chi_i \cup \chi_j = a_{ij}$ *if* $i < j$, *and* $\chi_i \cup \chi_i = \binom{q}{2} a_i$.

(*b*) *If* $\beta : H^1(G, \mathbf{k}) \rightarrow H^2(G, \mathbf{k}) = \mathbf{k}$ *is the homomorphism defined by the exact sequence*

$$0 \rightarrow \mathbf{Z}/q\mathbf{Z} \rightarrow \mathbf{Z}/q^2\mathbf{Z} \rightarrow \mathbf{Z}/q\mathbf{Z} \rightarrow 0,$$

then : (i) $\beta(\chi_i) = a_i$, *and* (ii) $\chi \cup \chi = \binom{q}{2} \beta(\chi)$ *for any* $\chi \in H^1(G, \mathbf{k})$.

Proof. — The proof of (*a*) when F is of finite rank can be found in [8] (p. 15). The proof given there applies immediately to the case F is of infinite rank. We now prove (*b*).

(i) Let $\chi = \chi_i$ and let $s : \mathbf{Z}/q\mathbf{Z} \rightarrow \mathbf{Z}/q^2\mathbf{Z}$ be defined by

$$s(n + q\mathbf{Z}) = n + q^2\mathbf{Z} \qquad \text{for} \quad 0 \leq n \leq q - 1.$$

Let $\chi' = s \circ \chi$, and let $c'(g, h) = \chi'(g) + \chi'(h) - \chi'(gh)$ for $g, h \in G$. Then $c'(g, h) = qc(g, h)$ for a unique element $c(g, h) \in \mathbf{Z}/q\mathbf{Z}$. The 2-cochain c is a cocycle whose cohomology class α is $\beta(\chi)$. Let $\varphi = \mathrm{tg}^{-1}(\alpha)$. Then by the definition of the transgression, the homomorphism φ is the restriction of a continuous function $f : F \rightarrow \mathbf{Z}/q\mathbf{Z}$ such that (in $\mathbf{Z}/q^2\mathbf{Z}$)

$$q(f(x) + f(y) - f(xy)) = \chi'(x) + \chi'(y) - \chi'(xy)$$

for any $x, y \in F$. Moreover, after subtracting from f a suitable homomorphism, we can suppose that $f(x_j) = 0$ for all j. An easy calculation then shows that $f(x_j^q) = -\delta_{ij}$ and $f((x_h, x_k)) = 0$ for all $h, j, k \in \mathbf{N}$. It follows that $\varphi(r) = -a_i$, and hence that $\beta(\chi_i) = a_i$.

(ii) Using (*a*) and (i) above, we see that

$$\chi_i \cup \chi_i = \binom{q}{2} \beta(\chi_i).$$

If $\chi = \sum u_i \chi_i$, then

$$\chi \cup \chi = \sum u_i^2 \chi_i \cup \chi_i = \sum u_i^2 \binom{q}{2} \beta(\chi_i) = \sum u_i \binom{q}{2} \beta(\chi_i) = \binom{q}{2} \beta(\chi)$$

since $u_i^2 \binom{q}{2} = u_i \binom{q}{2}$ in $\mathbf{Z}/q\mathbf{Z}$.

Q. E. D.

2.4. **Bilinear Forms on $(\mathbf{Z}/q\mathbf{Z})^{(\mathbf{N})}$.** — We begin with a proposition which is due to KAPLANSKY [6].

PROPOSITION 9. — *Let V be a vector space of dimension $\aleph_0$, and let φ be a non-degenerate alternate bilinear form on V. Then V has a symplectic basis, i. e. a basis $(v_i)_{i\in\mathbf{N}}$ with $\varphi(v_{2i-1}, v_{2i}) = -\varphi(v_{2i}, v_{2i-1}) = 1$ for $i \geq 1$, and $\varphi(v_i, v_j) = 0$ for all other i, j.*

Proof. — Let $(u_i)_{i\in\mathbf{N}}$ be an arbitrary basis of V, and suppose that we have already chosen $v_1, \ldots, v_{2n}$. If X is the subspace generated by $v_1, \ldots, v_{2n}$, let u_m be the first of the u_i such that $u_i \notin X$. Since φ is non-degenerate on X, the space V is the direct sum of X and its orthogonal complement X'. Let w be the X'-component of u_m, and choose $w \in X'$ with $\varphi(w, z) = 1$. We may then choose $v_{2n+1} = w$, $v_{n+2} = z$. Proceeding in this way, we eventually pick up all the u_i.

Q. E. D.

The following proposition generalizes a result of KAPLANSKY [6] :

PROPOSITION 10. — *Let V be a free $\mathbf{Z}/q\mathbf{Z}$-module of rank $\aleph_0$, where $q = p^h$, with $h \in \mathbf{N}$, and let φ be a skew-symmetric bilinear form on V whose reduction modulo p is non-degenerate. Let β be a linear form on V, and suppose that either φ is alternate, or $q \neq 2$ and $\varphi(v, v) = \binom{q}{2}\beta(v)$ for any $v \in V$. Then there exist integers c, d with $0 \leq c \leq d \leq h$ and a basis $(v_i)_{i\in\mathbf{N}}$ of V such that*

(a) $\beta(v_1) = p^c$, $\beta(v_2) = 0$, and $\beta(v_{2i-1}) = p^d$, $\beta(v_{2i}) = 0$ for $i \geq 2$;

(b) $\varphi(v_{2i-1}, v_{2i}) = 1$ for $i \geq 1$, and $\varphi(v_i, v_j) = 0$ for all other v_i, v_j with $i < j$.

Proof. — Since the reduction of φ modulo p is non-degenerate and alternate, there exists by Proposition 9 a symplectic basis (v'_i) of V/pV. If (v_i) is a family of elements of V lifting the v'_i, then it is easy to see that the v_i form a basis of V. Moreover, suitably choosing the basis (v'_i), we can choose v_1 to be a given element $v \notin pV$. In particular, we can choose v_1 so that $\beta(v_1) = p^c$, where c is the unique integer with $0 \leq c \leq h$ such that p^c generates $\mathrm{Im}(\beta)$.

Now (*b*) holds modulo p, and, replacing v_{2i} by $\varphi(v_{2i-1}, v_{2i})^{-1} v_{2i}$, we may assume that $\varphi(v_{2i-1}, v_{2i}) = 1$ for all $i \geq 1$. Then, replacing v_i by

$$v_i + \sum_{j<i/2} (\varphi(v_i, v_{2j-1})\, v_{2j} + \varphi(v_{2j}, v_i)\, v_{2j-1}),$$

we obtain a basis (v_i) such that condition (*b*) is satisfied and such that $\beta(v_1) = p^c$. Let d be the smallest integer with $c \leq d \leq h$ such that there is an infinite subset S_d of $\mathbf{N}$ with the property that for $i \in S_d$ we have $\beta(v_i) = p^d u_i$ with $u_i \not\equiv 0 \pmod p$, and let N be the smallest even integer ≥ 2 such that $\beta(v_i) \equiv 0 \pmod{p^d}$ for all $i > N$. Then it is possible to choose a strictly increasing sequence $(n_i)_{i \in \mathbf{N}}$ of even integers with $n_1 = N$ so that, for $i \neq 1$, we have $j \in S_d$ for at least one j with $n_{i-1} < j \leq n_i$. Let W_1 be the submodule generated by $v_1, \ldots, v_N$, and for $i > 1$ let W_i be the submodule generated by the v_j with $n_{i-1} < j \leq n_i$. The following lemma applied to W_1 shows that we may assume $N = 2$, and another application to the W_i yields the result.

LEMMA. — *Let W be a free $\mathbf{Z}/q\mathbf{Z}$-module of rank $2n$, $n \geq 1$, and let φ, β be forms on W as in Proposition* 10. *If $u_1, \ldots, u_{2n}$ generate* $\operatorname{Im}(\beta)$, *there exists a basis (w_i) of W such that : (a) $\beta(w_i) = u_i$; (b) $\varphi(w_{2i-1}, w_{2i}) = 1$ for $1 \leq i \leq n$, and $\varphi(w_i, w_j) = 0$ for all other i, j with $i < j$.*

Proof. — We first prove the lemma for the case $u_1 = u$ is a generator of $\operatorname{Im}(\beta)$ and $u_i = 0$ otherwise. Let (w_i) be a basis of W such that $\beta(w_1) = u$ and $\beta(w_i) = 0$ for $i \neq 1$. Since the reduction of φ modulo p is non-degenerate and alternate, there is an $i \geq 2$ and a unit t in $\mathbf{Z}/q\mathbf{Z}$ such that $\varphi(w_1, w_i) = t$. After a permutation, we may assume that $i = 2$, and, after multiplying w_2 by t^{-1}, we may even assume that $\varphi(w_1, w_2) = 1$. If $\varphi(w_1, w_i) = a_i \neq 0$ for some $i > 2$, replace w_i by $w_i - a_i w_2$. In this way we may also assume that $\varphi(w_1, w_i) = 0$ for $i > 2$.

If N is the submodule generated by $w_3, \ldots, w_{2n}$, then, on N, the form φ is alternate and its reduction modulo p is non-degenerate. Hence we may choose $w_3, \ldots, w_{2n} \in N$ so that (*b*) is satisfied for $i, j > 2$. Condition (*a*) still holds, and (*b*) is true for all i, j except possibly we may have $\varphi(w_2, w_i) \neq 0$ for some $i > 2$. If this is so, replace w_2 by $w_2 + a_3 w_3 + \ldots + a_{2n} w_{2n}$, where $a_{2i} = \varphi(w_2, w_{2i-1})$ and $a_{2i-1} = \varphi(w_{2i}, w_2)$. Then the resulting basis is the one required.

For the general case, let $v_1, \ldots, v_{2n}$ be an arbitrary basis of W. Let β' be the linear form on W such that $\beta'(v_i) = u_i$, and let φ' be the bilinear form on W defined by

$$\varphi'(v_i, v_i) = \binom{q}{2} \beta'(v_i), \qquad \varphi'(v_{2i-1}, v_{2i}) = - \varphi'(v_{2i}, v_{2i-1}) = 1,$$

and

$$\varphi'(v_i, v_j) = 0 \quad \text{for all other } i, j.$$

Then the pair (φ', β') satisfies the hypotheses of the lemma, and, by what we have shown above, there is an automorphism σ of W (as a module) such that

$$\varphi(x, y) = \varphi'(\sigma(x), \sigma(y)), \qquad \beta(x) = \beta'(\sigma(x))$$

for all $x, y \in W$. If $w_i = \sigma^{-1}(v_i)$, then (w_i) is a basis of W, and

$$\varphi(w_i, w_j) = \varphi'(v_i, v_j), \qquad \beta(w_i) = \beta'(v_i).$$

Hence (w_i) is the required basis.

Q. E. D.

Remark. — The integer d in Proposition 10 can be invariantly described as follows : For $0 \leq e \leq h$, let $V_e = V/p^e V$, and let φ_e, β_e be the forms obtained from φ, β on reducing modulo p^e. Let ψ_e be the homomorphism of V_e into its dual defined by the bilinear form ψ_e, and let $\psi = \psi_h$. Then $\beta \in \mathrm{Im}(\psi)$ if and only if $d = h$. If $\beta \notin \mathrm{Im}(\psi)$, then d is the smallest integer ≥ 0 such that $\beta_{d+1} \notin \mathrm{Im}(\psi_{d+1})$.

The last proposition of this section, and which again is due to KAPLANSKY [6], classifies non-alternate symmetric bilinear forms on vector spaces of dimension $\aleph_0$ over a perfect field k of characteristic 2. Recently (*cf.* Notices of the A. M. S., 66 T-4, January 1966), H. GROSS and R. D. ENGLE have classified such forms replacing the condition $[k : k^2] = 1$ by the condition $[k : k^2] < \infty$. In this paper, we are interested in the case $k = \mathbf{Z}/2\mathbf{Z}$.

PROPOSITION 11. — *Let k be a perfect field of characteristic 2, and let V be a vector space over k of dimension $\aleph_0$. If φ is a non-degenerate non-alternate symmetric bilinear form on V, then precisely one of following three possibilities holds :*

(i) *V is the orthogonal direct sum of subspaces W, Z with W one-dimensional and φ alternate on Z;*

(ii) *V is the orthogonal direct sum of subspaces W, Z with W two-dimensional, φ non-alternate on W, and φ alternate on Z;*

(iii) *V has an orthonormal basis.*

Proof. — Let A be the subspace formed by the elements v with $\varphi(v, v) = 0$. Then V/A is one-dimensional, and A', the orthogonal complement of A, is at most one-dimensional.

Case I. — *A' is one-dimensional and is not in A.* Then $V = A \oplus A'$, and φ is of type (i). Conversely, any form of type (i) falls in this category.

Case II. — *A' is one-dimensional an is contained in A.* Let z be any element not in A, and let Z be the subspace of A annihilated by z. Then $\dim(A/Z) = 1$, and A' is not contained in Z. Thus $A = Z \oplus A'$, and $V = Z \oplus W$, where W is the subspace spanned by A' and z. Hence φ is of type (ii). Moreover, any form of type (ii) falls in Case II.

Case III. — $A' = 0$. In this case, we shall show that V has an orthonormal basis $(v_i)_{i \in \mathbf{N}}$. Let $(u_i)_{i \in \mathbf{N}}$ be any basis of V with $\varphi(u_1, u_1) = 1$, and suppose that $v_1, \ldots, v_n$ have already been chosen. If X is the subspace they span, let u_m be the first of the u_i with $u_i \notin X$, and let z be the X'-component of u_m. If $\varphi(z, z) = a^2 \neq 0$, we choose $v_{n+1} = az$. If $\varphi(z, z) = 0$, find $w \in X'$ with $\varphi(z, w) = 1$. If $\varphi(w, w) = b^2 \neq 0$, choose $v_{n+1} = b^{-1}w$, $v_{n+2} = bz + b^{-1}w$. If $\varphi(w, w) = 0$, choose $v_{n+1} = v + w$, $v_{n+2} = v_n + z + w$, and replace v_n by $v_n + z$. Proceeding in this way, we eventually pick up all the u_i. Conversely, it is easy to see that a form with an orthonormal basis falls under Case III.

COROLLARY. — *Let φ be of type* (i) *or* (ii), *and let V be the union of an increasing family (V_i) of finite-dimensional subspaces on which φ is non-degenerate. If φ is of type* (i) [*resp.* (ii)], *then* dim (V_i) *is odd* (*resp. even*) *for i sufficiently large.*

Proof. — If W is the subspace found in the Proposition, then V is the direct sum of W and its orthogonal complement W', and φ is alternate on W'. Now let X be a finite-dimensional subspace of V on which φ is non-degenerate. If $W \subset X$, then X is the orthogonal direct sum of W and another subspace $Y \subset W'$. Since φ is non-degenerate and alternate on Y, it follows that $\dim(Y)$ is even, and hence that $\dim(X)$ has the same parity as $\dim(W)$. The corollary now follows from the fact that W is contained in V_i for i sufficiently large.

3. Proof of Theorems 1 and 2.

3.1. **Proof of Theorem** 1. — If G is a Demuškin group of rank $\aleph_0$, then, by Propositions 9 and 11, the vector space $H^1(G)$ is the union of an increasing family (V_i) of finite-dimensional non-zero subspaces such that the cup product

$$\varphi : \quad H^1(G) \times H^1(G) \to H^2(G)$$

is non-degenerate on each V_i. Choose a basis (χ_i) of $H^1(G)$ such that $\chi_1, \ldots, \chi_{n_i}$ is a basis of V_i. This choice of basis gives an isomorphism $\theta : H^1(G) \to (Z/pZ)^{(\mathbf{N})}$. Let F be a free pro-p-group of rank $\aleph_0$, and let f be a continuous homomorphism of F onto G such that $\theta = H^1(f)$ (*cf.* [12], p. I-36). If $R = \mathrm{Ker}(f)$, then $R = (r)$ with $r \in F^p(F, F)$. We identify G with F/R by means of f. Using the duality between the compact group $F/F^p(F, F) = G/G^p(G, G)$ and the discrete group $H^1(G)$, we obtain a generating system (ξ_i) of $F/F^p(F, F)$ such that $\chi_i(\xi_j) = \delta_{ij}$. Now let $\sigma : F/F^p(F, F) \to F$ be a continuous section, sending 0 into 1 (*cf.* [12], p. I-2, prop. 1). If $x_i = \sigma(\xi_i)$, then (x_i) is a basis of F. Now let $f_n : F \to F$ be the continuous homomorphism defined by $f_n(x_i) = x_i$ if $1 \leq i \leq n$, $f_n(x_i) = 1$ if $i > n$. If $n_i = \dim(V_i)$, let $F_i = \mathrm{Im}(f_{n_i})$, $r_i = f_{n_i}(r)$, $G_i = F_i/(r_i)$, and let $\psi_i : G \to G_i$ be the homomorphism induced by f_{n_i}. We shall show that the closed normal subgroups $H_i = \text{Ker}(\psi_i)$ are the ones required. If g_i is the image of x_i in G, then $\text{Ker}(\psi_i)$ is the closed normal subgroup of G generated by the g_j with $j > n_i$. Hence $H_{i+1} \subset H_i$. Since $g_i \to 1$ as $i \to \infty$, it also follows that the H_i intersect in the identity. It remains to show that $G_i = G/H_i$ is a Demuškin group of finite rank. To do this, we use the commutative diagram

$$\begin{array}{ccccc} H^1(G) & \times & H^1(G) & \longrightarrow & H^2(G) \\ \uparrow & & \uparrow & & \uparrow \\ H^1(G_i) & \times & H^1(G_i) & \longrightarrow & H^2(G_i) \end{array}$$

where the vertical arrows are the inflation homomorphisms. The homomorphism $\text{Inf} : H^1(G_i) \to H^1(G)$ maps $H^1(G_i)$ isomorphically onto V_i. Since the cup product φ is non-degenerate on V_i, the above diagram shows that $\text{Inf} : H^2(G_i) \to H^2(G)$ is not the zero homomorphism. Since $\dim H^2(G_i) \leq 1$ and $\dim H^2(G) = 1$, it follows that this homomorphism must be bijective. This implies that $H^2(G_i)$ is one-dimensional and that the cup product :

$$H^1(G_i) \times H^1(G_i) \to H^2(G_i)$$

is non-degenerate. Hence G_i is a Demuškin group of rank n_i.

Conversely, assume that we are given such a family of quotients $G_i = G/H_i$ of the pro-p-group G, the group G being of rank $\aleph_0$. Then $cd(G) \leq 2$. If $cd(G) < 2$, then G is a free pro-p-group (*cf.* [12], p. I-37). So assume that $cd(G) = 2$. Since $H^2(G)$ is the direct limit of the one-dimensional subspaces $H^2(G_i)$, it follows that $\text{Inf} : H^2(G_i) \to H^2(G)$ is an isomorphism for i sufficiently large. We assume that we have chosen the H_i so that this is true for all i. If V_i is the image of $H^1(G_i)$ in $H^1(G)$ under the inflation map, the commutative diagram then shows that the cup product $\varphi : H^1(G) \times H^1(G) \to H^2(G)$ is non-degenerate on V_i. Since $H^1(G)$ is the union of the V_i, it follows that φ is non-degenerate. Hence G is a Demuškin group.

3.2. **Proof of Theorem** 2. — To prove (i), it suffices to consider the case G is of rank $\aleph_0$ (*cf.* [11], p. 252-309). Let U be an open subgroup of the Demuškin group G and let (H_i) be a decreasing family of closed normal subgroups of G with $\bigcap_i H_i = 1$ and each quotient G/H_i a Demuškin group of finite rank $\neq 1$. If $U_i = U \cap H_i$, then $U/U_i = UH_i/H_i$ is an open subgroup of the Demuškin group G/H_i. Since G/H_i is of finite rank $\neq 1$, it follows that U/U_i is a Demuškin group of finite rank.

Since $\bigcap_i U_i = 1$, it follows, by Theorem 1, that U is either a free pro-p-group or a Demuškin group. But, since U is open in G and $cd(G) = 2$, we have $cd(U) = 2$ (*cf.* [12], p. I-20, Prop. 14). Hence U is a Demuškin group.

For the proof of (ii), let K be a closed subgroup of the Demuškin group G with $(G : K) = \infty$. This implies, in particular, that $n(G) \neq 1$. If U, V are open subgroups of G with $U \subset V$, the corestriction homomorphism

$$\text{Cor} : \; H^2(U) \to H^2(V)$$

is surjective since $cd(V) = 2$ (*cf.* [12], p. I-20, lemme 4) and hence is bijective since $H^2(U) \simeq H^2(V) \simeq \mathbf{Z}/p\mathbf{Z}$. But, if $U \neq V$ and

$$\text{Res} : \; H^2(V) \to H^2(U)$$

is the restriction homomorphism, we have

$$\text{Cor} \circ \text{Res} = 0 \qquad \text{since} \quad \text{Cor} \circ \text{Res} = (V : U) = p^n.$$

It follows that Res is the zero homomorphism if $U \neq V$. Since K is the intersection of the open subgroups containing it, $H^2(K)$ is the direct limit of the groups $H^2(U)$, where U runs over the open subgroups of G containing K, the homomorphisms being the restriction homomorphisms. Since $(G : K) = \infty$, it follows that $H^2(K) = 0$. Hence K is a free pro-p-group.

4. Proof of Theorem 3.

In this section, F is a free pro-p-group of rank $\aleph_0$; $r \in F^p(F, F)$; $G = F/(r)$ is a Demuškin group; $q = q(G)$; $h = h(G)$: $t = t(G)$. We divide the proof of theorem 3 into cases.

4.1. **The Case** $q = 0$. — If $x = (x_i)_{i \in \mathbf{N}}$ is a basis of F, let

$$r_0(x) = \prod_{i \geq 1} (x_{2i-1}, x_{2i}).$$

Let (F_n) be the descending central series of F. We first show that we can choose the basis (x_i) so that $r \equiv r_0(x)$ modulo F_3.

Let $H^i(G, \mathbf{Z}_p) = \varprojlim_m H^i(G, \mathbf{Z}/p^m\mathbf{Z})$. Then $V = H^1(G, \mathbf{Z}_p)$ can be identified with the set of continuous homomophisms of G into $\mathbf{Z}_p$, where $\mathbf{Z}_p$ is given the p-adic topology. If $(\chi_i)_{i \in \mathbf{N}}$ is a family of elements of V such that the χ_i (mod p) form a basis of $V/pV = H^1(G)$, then every element of V can be uniquely written in the form $\sum_{i \geq 1} a_i \chi_i$ with $a_i \in \mathbf{Z}_p$ and $a_i \to 0$. We call such a family of elements a *basis* of V. Using the cup product :

$$H^1(G, \mathbf{Z}/p^m\mathbf{Z}) \times H^1(G, \mathbf{Z}/p^m\mathbf{Z}) \to H^2(G, \mathbf{Z}/p^m\mathbf{Z})$$

and passing to the limit we obtain a cup product :

$$H^1(G, \mathbf{Z}_p) \times H^1(G, \mathbf{Z}_p) \to H^2(G, \mathbf{Z}_p)$$

which is $\mathbf{Z}_p$-bilinear (and continuous). Moreover, under the identification of $H^2(G, \mathbf{Z}/p^m\mathbf{Z})$ with $\mathbf{Z}/p^m\mathbf{Z}$ the map $H^2(G, \mathbf{Z}/p^{m+1}\mathbf{Z}) \to H^2(G, \mathbf{Z}/p^m\mathbf{Z})$ is the canonical homomorphism of $\mathbf{Z}/p^{m+1}\mathbf{Z}$ onto $\mathbf{Z}/p^m\mathbf{Z}$. Hence, passing to the limit, we may identify $H^2(G, \mathbf{Z}_p)$ with $\mathbf{Z}_p$.

If (x_i) is a basis of F, then

$$r \equiv \prod_{i<j} (x_i, x_j)^{a_{ij}} \qquad (\operatorname{mod} F_3),$$

where $a_{ij} \in \mathbf{Z}_p$. Let $\chi_i : F \to \mathbf{Z}_p$ be the continuous homomorphism defined by $\chi_i(x_j) = \delta_{ij}$. Then (χ_i) is a basis of $H^1(G, \mathbf{Z}_p)$. Since each such homomorphism χ_i vanishes on (F, F) and since $r \in (F, F)$, we may view the χ_i as elements of $H^1(G, \mathbf{Z}_p)$. We then have the following lemma :

LEMMA 1. — *The cup product* $H^1(G, \mathbf{Z}_p) \times H^1(G, \mathbf{Z}_p) \to H^2(G, \mathbf{Z}_p) = \mathbf{Z}_p$ *is alternating and* $\chi_i \cup \chi_j = a_{ij}$ if $i < j$.

Proof. — If ε_m is the canonical homomorphism of $\mathbf{Z}_p$ onto $\mathbf{Z}_p/p^m\mathbf{Z}_p = \mathbf{Z}/p^m\mathbf{Z}$, let $\chi_i^{(m)} = \varepsilon_m \circ \chi_i$, $a_{ij}^{(m)} = \varepsilon_m(a_{ij})$. Then, by Proposition 8, $\chi_i^{(m)} \cup \chi_i^{(m)} = 0$ and $\chi_i^{(m)} \cup \chi_j^{(m)} = a_{ij}^{(m)}$ if $i < j$. It follows that $\chi_i \cup \chi_i = 0$ and $\chi_i \cup \chi_j = a_{ij}$ for $i < j$.

Q. E. D.

The basis (χ_i) of $H^1(G, \mathbf{Z}_p)$ is said to be a symplectic basis if $\chi_{2i-1} \cup \chi_{2i} = -\chi_{2i} \cup \chi_{2i-1} = 1$ and $\chi_i \cup \chi_j = 0$ for all other i, j. The existence of a symplectic basis of $V = H^1(G, \mathbf{Z}_p)$ follows from the following lemma together with the existence of a symplectic basis on $V/pV = H^1(G)$ (*cf.* Proposition 9).

LEMMA 2. — *Let* M *be a free* $\mathbf{Z}/p^m\mathbf{Z}$*-module of rank* $\aleph_0$ *with an alternating form* φ. *If* $(\bar{\chi}_i)$ *is a symplectic basis of* $M/p^{m-1}M$, *there exists a symplectic basis of* F *lifting* $(\bar{\chi}_i)$.

Proof. — Let (χ_i') be a basis of M lifting the symplectic basis (χ_i). Then $\varphi(\chi_{2i-1}', \chi_{2i}') = 1 + p^{m-1}u_i$ for $i \geq 1$ and $\varphi(\chi_i', \chi_j') = p^{m-1}u_{ij}$

for all other i, j with $i \leqq j$. Replacing χ'_{2i-1} by $(1+p^{m-1}u_i)^{-1}\chi'_{2i-1}$, we may assume that $\varphi(\chi'_{2i-1}, \chi'_{2i}) = 1$ for all $i \geqq 1$. Then the basis (χ_i), where

$$\chi_i = \chi'_i + \sum_{j<i/2} (\varphi(\chi'_i, \chi'_{2j-1})\chi'_{2j} + \varphi(\chi'_{2j}, \chi'_i)\chi'_{2j-1})$$

is the required symplectic basis of M.

Q. E. D.

The existence of a basis $x = (x_i)$ of F such that $r = r_0(x)$ (mod F_3) now follows from lemmas 1 and 2 and the following lemma :

LEMMA 3. — *If* $(\chi_i)_{i\in\mathbf{N}}$ *is a basis of* $H^1(G, \mathbf{Z}_p)$, *there exists a basis* (x_i) *of* F *such that* $\chi_i(x_j) = \delta_{ij}$.

Proof. — If ε_m is the canonical homomorphism of $\mathbf{Z}_p$ onto $\mathbf{Z}/p^m\mathbf{Z}$, let $\chi_i^{(m)} = \varepsilon_m \circ \chi_i$. Using the duality between the compact groups $F/F^{p^m}(F, F)$ and the discrete group $H^1(F, \mathbf{Z}/p^m\mathbf{Z})$, we obtain a generating system $(\xi_i^{(m)})$ of $F/F^{p^m}(F, F)$ such that $\chi_i^{(m)}(\xi_j^{(m)}) = \delta_{ij}$. Since $F/(F, F) = \varprojlim_m F/F^{p^m}(F, F)$ and the image of $\xi_i^{(m+1)}$ in $F/F^{p^m}(F, F)$ is $\xi_i^{(m)}$, there exists $\xi_i \in F/(F, F)$ such that, for all m, $\xi_i^{(m)}$ is the image of ξ_i in $F/F^{p^m}(F, F)$. Moreover, it is easy to see that (ξ_i) is a basis of $F/(F, F)$. If $\sigma : F/(F, F) \to F$ is a continuous section such that $\sigma(0) = 1$ and if $x_i = \sigma(\xi_i)$, then (x_i) is the required basis of F.

Q. E. D.

Suppose now that we have found a basis (x_i) of F such that $r \equiv r_0(x)$ modulo F_{n+1} for some $n \geqq 2$. If $(t_i)_{i\in\mathbf{N}}$ is a family of elements of F_n with $t_i \to 1$, and if $y_i = x_i t_i^{-1}$, then $y = (y_i)$ is a basis of F and $r_0(x) = r_0(y)\, d_n$ with $d_n \in F_{n+1}$. If τ_i (resp. ξ_i) is the image of t_i(resp. x_i) in $\mathrm{gr}_n(F)$ [resp. $\mathrm{gr}_1(F)$], then, using (8), we see that the image of d_n in $\mathrm{gr}_{n+1}(F)$ is

$$\partial_n(\tau) = \sum_{i\geqq 1}([\xi_{2i-1}, \tau_{2i}] + [\tau_{2i-1}, \xi_{2i}]),$$

where $\tau = (\tau_i)$. If W_n is the submodule of $V_n = \mathrm{gr}_n(F)^{\mathbf{N}}$ consisting of those families $\tau = (\tau_i)$ with $\tau_i \to 0$, we obtain a homomorphism $\partial_n : W_n \to \mathrm{gr}_{n+1}(F)$. If $\Delta_n : V_n \to \mathrm{gr}_n(F)$ is defined by

$$\Delta_n(\tau) = \sum_{i\geqq 1}[\xi_i, \tau_i],$$

then $\Delta_n(W_n) = \mathrm{Im}(\partial_n)$, and, by the corollary to Proposition 4, we have $\Delta_n(W_n) = \mathrm{gr}_{n+1}(F)$. Consequently ∂_n is surjective. Hence if

$r = r_0(x)\,e_{n+1}$ with $e_{n+1} \in F_{n+1}$, we may choose $\tau = (\tau_i) \in W_n$ so that $-\varepsilon_{n+1} = \delta_n(\tau)$, where ε_{n+1} is the image of e_{n+1} in $\mathrm{gr}_{n+1}(F)$. If $\sigma : \mathrm{gr}_n(F) \to F_n$ is a continuous section with $\sigma(0) = 1$, let $t_i = \sigma(\tau_i)$. If $y_i = x_i t_i^{-1}$, then $y = (y_i)$ is a basis of F and $r \equiv r_0(y) \pmod{F_{n+2}}$.

Proceeding in this way, we obtain for each $n \geq 2$ a basis $x^{(n)} = (x_i^{(n)})$ of F such that $r \equiv r_0(x^{(n)}) \pmod{F_{n+1}}$ and such that $x_i^{(n+1)} \equiv x_i^{(n)} \pmod{F_n}$. If $x_i = \lim x_i^{(n)}$, $n \to \infty$, then (x_i) is a basis of F and $r = r_0(x)$.

Q. E. D.

4.2. **The Case** $q \neq 0, 2$. — If $V = H^1(G, \mathbf{Z}/q\mathbf{Z})$, then V is free $\mathbf{Z}/q\mathbf{Z}$-module of rank $\aleph_0$, and the cup product

$$H^1(G, \mathbf{Z}/q\mathbf{Z}) \times H^1(G, \mathbf{Z}/q\mathbf{Z}) \to H^2(G, \mathbf{Z}/q\mathbf{Z}) = \mathbf{Z}/q\mathbf{Z}$$

is a bilinear form on V whose reduction modulo p is non-degenerate. If β is the linear form on V defined in Proposition 8, then $\chi \cup \chi = \binom{q}{2}\beta(\chi)$ for any $\chi \in V$. Moreover, $\beta(V) = \mathbf{Z}/q\mathbf{Z}$ since $r \notin F^{p^{h+1}}(F, F)$. Since $q \neq 2$, we may apply Proposition 10 to obtain a basis (χ_i) of V and an integer d with $0 \leq d \leq h$ such that

(*a*) $\beta(\chi_1) = 1$, $\beta(\chi_2) = 0$, and $\beta(\chi_{2i-1}) = p^d$, $\beta(\chi_{2i}) = 0$ for $i \geq 2$.

(*b*) $\chi_{2i-1} \cup \chi_{2i} = 1$ for $i \geq 1$, and $\chi_i \cup \chi_j = 0$ for all other i, j with $i < j$.

Let (x_i) be a basis of F such that $\chi_i(x_j) = \delta_{ij}$ and let (F_n) be the descending q-central series of F. Then by Proposition 8 we have

$$r \equiv x_1^q\,(x_1, x_2) \prod_{i \geq 2} x_{2i-1}^{qp^d}\,(x_{2i-1}, x_{2i}) \qquad \pmod{F_3}.$$

Now suppose that for some $n \geq 2$, we have found a basis (x_i) of F and integers a_i with $q \mid a_{2i-1}$, $q^2 \mid a_{2i}$ such that

$$r = x_1^q\,(x_1, x_2) \prod_{i \geq 2} x_{2i-1}^{a_{2i-1}} x_{2i}^{a_{2i}}\,(x_{2i-1}, x_{2i})\, e_{n+1},$$

where $e_{n+1} \in F_{n+1}$, and where either all a_i are equal to zero, or there exists an infinite number of i with $v_p(a_i) < nh$. If $(t_i)_{i\in\mathbf{N}}$ is a family of elements $t_i \in F_n$ with $t_i \to 1$, then (y_i), where $y_i = x_i t_i^{-1}$, is a basis of F and

$$(10) \qquad r = y_1^q\,(y_1, y_2) \prod_{i \geq 2} x_{2i-1}^{a_{2i-1}} x_{2i}^{a_{2i}}\,(x_{2i-1}, x_{2i})\, d_n e_{n+1},$$

where $d_n \in F_{n+1}$. If τ_i (resp. ξ_i) is the image of t_i (resp. x_i) in $\mathrm{gr}_n(F)$ [resp. $\mathrm{gr}_1(F)$], then, using (8) together with Proposition 6, we see that the image of d_n in $\mathrm{gr}_{n+1}(F)$ is

$$\begin{aligned}\partial_n(\tau) = \pi\tau_1 + \binom{q}{2}[\tau_1, \xi_1] + [\tau_1, \xi_2] + [\xi_1, \tau_2] \\ + \sum_{i\geq 2}(p^d \pi\tau_{2i-1} + p^d\binom{q}{2}[\tau_{2i-1}, \xi_{2i-1}]) \\ + \sum_{i\geq 2}([\tau_{2i-1}, \xi_{2i}] + [\xi_{2i-1}, \tau_{2i}]).\end{aligned}$$

If W_n is the subgroup of $V_n = \mathrm{gr}_n(F)^{\mathbf{N}}$ consisting of those families (τ_i) with $\tau_i \to 0$, we obtain a homomorphism $\partial_n : W_n \to \mathrm{gr}_{n+1}(F)$.

LEMMA. — *If E is the closed subgroup of $\mathrm{gr}_2(F)$ generated by the elements $\pi\xi_j$ with $j \neq 1, 2$, then*

(11) $$\mathrm{gr}_{n+1}(F) = \mathrm{Im}(\partial_n) + \pi^{n-1}E.$$

Moreover, if $p^d = q$, then $\pi^n\xi_j \in \mathrm{Im}(\partial_n)$ for all j.

Proof. — If $\Delta_n : V_n \to \mathrm{gr}_{n-1}(F)$ is the homomorphism defined by

$$\Delta_n(\tau) = \sum_{i\geq 1}[\xi_i, \tau_i],$$

we have $\mathrm{Im}(\partial_n) = \Delta_n(W_n) + \pi\,\mathrm{gr}_n(F)$. By the Corollary to Proposition 7 we have

$$\mathrm{gr}_{n+1}(F) = \Delta_n(W_n) + \pi\,\mathrm{gr}_n(F).$$

Hence, $\mathrm{gr}_{n+1}(F) = \mathrm{Im}(\partial_n) + \pi\,\mathrm{gr}_n(F)$. Since $\pi\,\mathrm{Im}(\partial_{m-1})$ is contained in $\mathrm{Im}(\partial_m)$ for $m \geq 3$, it follows that

$$\mathrm{gr}_{n+1}(F) = \mathrm{Im}(\partial_n) + \pi^{n-1}\mathrm{gr}_2(F).$$

But, using Proposition 6 and the fact that $q \neq 2$, we see that

$$\pi\,\mathrm{gr}_2(F) = \pi D + \Delta_2(W_2) + p\,\mathrm{gr}_3(F),$$

where D is the closed subgroup of $\mathrm{gr}_2(F)$ generated by the elements $\pi\xi_j$. Hence,

$$\mathrm{gr}_{n+1}(F) = \mathrm{Im}(\partial_n) + \pi^{n-1}D + p\,\mathrm{gr}_{n+1}(F).$$

Since $\pi^n\xi_2 = \partial_n(\tau)$, where $\tau_1 = \pi^{n-1}\xi_2$, $\tau_2 = \binom{q}{2}\tau_1$, $\tau_i = 0$ otherwise, and $\pi^n\xi_1 = \partial_n(\tau)$, where

$$\tau_1 = \pi^{n-1}\xi_1 + \binom{q}{2}\pi^{n-2}[\xi_1, \xi_2],$$

$$\tau_2 = \binom{q}{2}\tau_1 + \binom{q}{2}\pi^{n-2}[\xi_1, \xi_2] - \pi^{n-1}\xi_2 + \binom{q}{2}\pi^{n-1}\xi_2,$$

$$\tau_i = 0 \quad \text{for} \quad i \neq 1, 2,$$

we see that (11) is true modulo p. Since $\operatorname{Im}(\partial_n) + \pi^{n-1}E$ is a subgroup of $\operatorname{gr}_{n+1}(F)$, it follows that (10) is true modulo p^i for any $i \in \mathbf{N}$. Since $p^h \operatorname{gr}_{n+1}(F) = 0$, the result follows.

Now suppose that $p^d = q$. If $\Delta'_n : V_n \to \operatorname{gr}_{n+1}(F)$ is defined by

$$\Delta'_n(\tau) = \pi\tau_2 + \sum_{i \geq 1} [\xi_i, \tau_i],$$

then $\operatorname{Im}(\partial_n) = \Delta'_n(W_n)$. If $j \geq 3$, then $\pi^n \xi_j = \Delta'_n(\tau)$, where

$$\tau_2 = \pi^{n-1}\xi_j + \binom{q}{2}\pi^{n-2}[\xi_j, \xi_2],$$

$$\tau_j = \binom{q}{2}\pi^{n-2}[\xi_j, \xi_2] + \binom{q}{2}\pi^{n-1}\xi_2 + \pi^{n-1}\xi_2,$$

$$\tau_i = 0 \qquad \text{for} \quad i \neq 2, j.$$

This completes the proof of the lemma.

Returning to (10), the above lemma allows us to choose the t_i so that

$$d_n e_{n+1} \equiv \prod_{i \geq 3} y_i^{q^n a'_i} \qquad (\operatorname{mod} F_{n+2}).$$

Moreover, if all the a_i in (10) are equal to zero, in which case $q = p^h$, then, by the second part of the lemma, we can choose the t_i so that either all $a'_i = 0$, or $a'_i \notin q\mathbf{Z}$ for an infinite number of i. Then, since $y_i^{q^n}$ is in the center of F, modulo F_{n+2}, we see that

$$r \equiv y_1^q(y_1, y_2)\prod_{i \geq 2} y_{2i-1}^{b_{2i-1}} y_{2i}^{b_{2i}}(y_{2i-1}, y_{2i}) \qquad (\operatorname{mod} F_{n+2}),$$

where $b_i = a_i + q^n a'_i$, and where either all b_i are equal to zero, or there exists an infinity of i with $v_p(b_i) < (n+1)h$.

Proceeding inductively and passing to the limit, we see the we can find a basis (x_i) of F such that

$$r = x_1^q(x_1, x_2)\prod_{i \geq 2} x_{2i-1}^{a_{2i-1}} x_{2i}^{a_{2i}}(x_{2i-1}, x_{2i}),$$

where $a_i \in \mathbf{Z}_p$ and where either all a_i are equal to zero, or there exists an infinite number of i with $v_p(a_i) = e$, where e is the infimum of the $v_p(a_i)$ and $q \leq e < \infty$. In the latter case, there exists a strictly increasing sequence $(n_i)_{i \geq 1}$ of even integers with $n_1 = 2$ such that, for each $i \geq 1$, there is a j with $n_i < j \leq n_{i+1}$ and $v_p(a_j) = e$. If for $i \geq 1$ we set

$$r_i = \prod_{n_i \leq j \leq v_i} x_{2j-1}^{a_{2j-1}} x_{2j}^{a_{2j}}(x_{2j-1}, x_{2j}),$$

where $u_i = (n_i + 2)/2$, $v_i = n_{i+1}/2$, then r_i is a Demuškin relation in the variables x_j, $n_i < j \leq n_{i+1}$. The corresponding Demuškin group G_i is of finite rank with $q(G_i) = p^\nu \neq 2$. If $s = q(G_i)$, then by the theory of Demuškin groups of finite rank (*cf.* [1] or [11]) we can choose the x_j so that

$$r_i = \prod_{u_i \leq j \leq v_i} x_{2j-1}^s (x_{2j-1}, x_{2j}).$$

Since $r = x_1^q (x_1, x_2) \prod_{i \geq 1} r_i$, this completes the proof of case 2.

4.3. **The Case** $q = 2$, $t = 1$. — Let (F_n) be the descending 2-central series of F. By the definition of the invariant $t = t(G)$ together with Propositions 8, 9 and 11, there exists a basis (χ_i) of $H^1(G)$ such that $\chi_1 \cup \chi_1 = 1$, $\chi_{2i-1} \cup \chi_{2i} = 1$ for $i \geq 1$, and $\chi_i \cup \chi_j = 0$ for all other i, j with $i \leq j$. If $x = (x_i)$ is a basis of F with $\chi_i(x_j) = \delta_{ij}$, then, by Proposition 8, we have

$$r \equiv x_1^2 (x_1, x_2)\, r_0(x) \qquad (\operatorname{mod} F_3),$$

where $r_0(x) = \prod_{i \geq 2} (x_{2i-1}, x_{2i})$.

Now assume that for some $n \geq 2$ we have found a basis $x = (x_i)$ of F and integers $a_i \in 4\mathbf{Z}$ such that

$$r = x_1^{2+a_1} (x_1, x_2)\, r_0(x) \prod_{i \geq 3} x_i^{a_i}\, e_{n+1}$$

where $e_{n+1} \in F_{n+1}$. If (t_i) is a family of elements $t_i \in F_n$ with $t_i \to 1$, then $y = (y_i) = (x_i t_i^{-1})$ is a basis of F and

$$r = y_1^{2+a_1} (y_1, y_2)\, r_0(y) \prod_{i \geq 3} y_i^{a_i}\, d_n e_{n+1} \tag{12}$$

with d_n in F_{n+1}. If τ_i (resp. ξ_i) is the image of t_i (resp. x_i) in $\operatorname{gr}_n(F)$ [resp. $\operatorname{gr}_1(F)$], then the image of d_n in $\operatorname{gr}_{n+1}(F)$ is

$$\partial_n(\tau) = \pi\tau_1 + [\tau_1, \xi_1] + \sum_{i \geq 1} ([\tau_{2i-1}, \xi_{2i}] + [\xi_{2i-1}, \tau_{2i}]).$$

If W_n is the subspace of $V_n = \operatorname{gr}_n(F)^{\mathbf{N}}$ consisting of those families $\tau = (\tau_i)$ with $\tau_i \to 0$, then ∂_n is a homomorphism of W_n into $\operatorname{gr}_{n+1}(F)$, and we have the following lemma :

Lemma. — *If E is the closed subgroup of* $\operatorname{gr}_2(F)$ *generated by the elements $\pi\xi_j$ with $j \neq 2$, then* $\operatorname{gr}_{n+1}(F)$ *is generated by* $\operatorname{Im}(\partial_n)$ *and* $\pi^{n-1}E$.

Proof. — Using the Corollary to Proposition 7, we see that

$$\mathrm{gr}_{n+1}(F) = \mathrm{Im}(\partial_n) + \pi\, \mathrm{gr}_n(F).$$

Since $\pi\ \mathrm{Im}(\partial_{m-1}) \subset \mathrm{Im}(\partial_m)$ for $m \geqq 3$, it follows that $\mathrm{gr}_{n+1}(F)$ is generated by $\mathrm{Im}(\partial_n)$ and $\pi^{n-1}\mathrm{gr}_2(F)$. Hence, to prove the lemma, it suffices to show that $\pi^2\xi_2 \in \mathrm{Im}\ (\partial_2)$ and

$$\sum_{i<j} a_{ij}\pi[\xi_i, \xi_j] \in \mathrm{Im}\ (\partial_2) + \pi \mathrm{E}$$

for arbitrary $a_{ij} \in \mathbf{Z}/2\mathbf{Z}$.

If $\tau = (\tau_i)$, where $\tau_1 = \pi\xi_2$, $\tau_2 = \tau_1$, $\tau_i = 0$ for $i \geqq 3$, then $\tau \in W_2$ and $\partial_2(\tau) = \pi^2\xi_2$. Hence $\pi^2\xi_2 \in \mathrm{Im}\ (\partial_2)$. Now let $\Delta : W_2 \to \mathrm{gr}_3(F)$ be defined by

$$\Delta(\tau) = \pi\tau_2 + \sum_{i \geqq 1} [\xi_i, \tau_i].$$

Then clearly $\mathrm{Im}(\partial_2) = \mathrm{Im}(\Delta)$. Let $\tau = (\tau_i)$, where

$$\tau_1 = a_{12}[\xi_1, \xi_2] + \sum_{j \geqq 3} a_{1j}\pi\xi_j,$$

$$\tau_2 = a_{12}\pi\xi_1 + \sum_{j \geqq 3} a_{2j}\pi\xi_j,$$

$$\tau_i = \sum_{j>i} a_{ij}\pi\xi_j + \sum_{j<i} a_{ji}[\xi_j, \xi_i] \qquad \text{for } i \geqq 3.$$

Then $\tau \in W_2$, and a straightforward calculation using Proposition 6 shows that

$$\Delta(\tau) = a_{12}\pi^2\xi_1 + \sum_{j \geqq 3} a_{2j}\pi^2\xi_j + \sum_{i<j} a_{ij}\pi[\xi_i, \xi_j].$$

Hence $\sum_{i<j} a_{ij}\pi\,[\xi_i, \xi_j] \in \mathrm{Im}(\Delta) + \pi \mathrm{E}$.

Q. E. D.

Returning to (12), the above lemma allows us to choose the $t_i \in F_n$ so that

$$r \equiv y_1^{2+b_1}(y_1, y_2)\, r_0(y) \prod_{i \geqq 3} y_i^{b_i} (\mathrm{mod}\ F_{n+2}),$$

with $b_i \in \mathbf{Z}$, $b_i \equiv a_i\ (\mathrm{mod}\, 2^n)$.

Proceeding inductively and passing to the limit, we see that there exists a basis (x_i) of F and 2-adic integers a_i with $v_2(a_i) \geqq 2$ such that

$$r = x_1^{2+a_1}(x_1, x_2)\ r_0(x) \prod_{i \geqq 3} x_i^{a_i}.$$

The relation $r_1 = r_0(x) \prod_{i \geqq 3} x_i^{a_i}$ is a Demuškin relation in the variables x_i, $i \geqq 3$, and the q-invariant of the corresponding Demuškin group is $\neq 2$. Hence, by what we have shown in sections 4.1 and 4.2, we may choose the x_i, $i \geqq 3$, so that

$$r_1 = x_3^{2^f}(x_3, x_4) \prod_{i \geqq 3} x_{2i-1}^s (x_{2i-1}, x_{2i}),$$

where $s = 2^e$, $e, f \in \mathbf{N}$, $2 \leqq f \leqq e$. If

$$r_2 = x_1^{2+a_1}(x_1, x_2)\, x_3^{2^f}(x_3, x_4),$$

then r_2 is a Demuškin relation in the variables $x_1, \ldots, x_4$ and the q-invariant of the corresponding Demuškin group is 2. We now appeal to the theory of such relations (*cf.* [3] or [8]). If $f \leqq v_2(a_1)$, we can choose $x_1, \ldots, x_4$ so that

$$r_1 = x_1^2(x_1, x_2)\, x_3^{2^f}(x_3, x_4).$$

If $f > v_2(a_1) = g$, then we can choose $x_1, \ldots, x_4$ so that

$$r_1 = x_1^{2-2^g}(x_1, x_2)\ (x_3, x_4).$$

Since $r = r_1 \prod_{i \geqq 3} x_{2i-1}^s (x_{2i-1}, x_{2i})$, the proof of Theorem 3 for the case $q = 2$, $t = 1$ is complete.

4.4. **The Case** $q = 2$, $t = -1$. — Let (F_n) be the descending 2-central series of F. Since $t = -1$, then by the definition of t, together with Propositions 9 and 11, there exists a basis (χ_i) of $H^1(G)$ such that $\chi_1 \cup \chi_1 = 1$, $\chi_{2i} \cup \chi_{2i+1} = 1$ for $i \geqq 1$, and $\chi_i \cup \chi_j = 0$ for all other i, j with $i \leqq j$. If (x_i) is a basis of F with $\chi_i(x_j) = \delta_{ij}$, then, by Proposition 8, we have $r \equiv r_0(x)$ modulo F_3, where

$$r_0(x) = x_1^2 \prod_{i \geqq 1} (x_{2i}, x_{2i+1}).$$

Now assume that, for some $n \geqq 2$, we have found a basis $x = (x_i)$ of F and integers a_i with $a_i \in 4\mathbf{Z}$ such that

$$r \equiv r_0(x) \prod_{i \geqq 2} x_i^{a_i} \pmod{F_{n+1}}.$$

Then, proceeding exactly as in the previous section, we obtain a homomorphism $\partial_n : W_n \to \mathrm{gr}_{n+1}(F)$, where

$$\partial_n(\tau) = \pi\tau_1 + [\tau_1, \xi_1] + \sum_{i \geq 1}([\tau_{2i}, \xi_{2i+1}] + [\xi_{2i}, \tau_{2i+1}]).$$

LEMMA. — *If E is the closed subgroup of $\mathrm{gr}_2(F)$ generated by the elements $\pi\xi_j$ with $j \neq 1$, then $\mathrm{gr}_{n+1}(F)$ is generated by $\mathrm{Im}(\partial_n)$ and $\pi^{n-1}E$.*

Proof. — The proof is exactly the same as the proof of the corresponding lemma in the previous section except for the following changes : $\pi^2\xi_1 = \partial_2(\tau)$, where $\tau_1 = \pi\xi_1$ and $\tau_i = 0$ for $i \geq 2$; the homomorphism Δ is defined by

$$\Delta(\tau) = \pi\tau_1 + \sum_{i \geq 1}[\xi_i, \tau_i],$$

and we have

$$\Delta(\tau) = \sum_{j \geq 2} a_{1j}\pi^2\xi_j + \sum_{i<j} a_{ij}\pi[\xi_i, \xi_j]$$

if we let

$$\tau_1 = \sum_{j \geq 2} a_{1j}\pi\xi_j,$$

$$\tau_i = \sum_{j>i} a_{ij}\pi\xi_j + \sum_{j<i} a_{ji}[\xi_i, \xi_j] \qquad \text{for} \quad i \geq 2.$$

This completes the proof of the lemma.

Hence, using the above lemma, we see that there is a basis $y = (y_i)$ of F such that

$$r \equiv r_0(y)\prod_{i \geq 2} y_i^{b_i} \qquad (\mathrm{mod}\ F_{n+2}),$$

where $y_i \equiv x_i \pmod{F_n}$, and $b_i \equiv a_i \pmod{2^n}$. Proceeding inductively and passing to the limit, we see that there exists a basis (x_i) of F and 2-adic integers $a_i \in 4\mathbf{Z}_2$ such that $r = x_1^2 r_1$, where

$$r_1 = \prod_{i \geq 1}(x_{2i}, x_{2i+1})\prod_{i \geq 2} x_i^{a_i}.$$

The relation r_1 is a Demuškin relation in the variables x_i, $i \geq 2$, and the q-invariant of the corresponding Demuškin group is $\neq 2$. Hence we can choose the x_i so that

$$r_1 = x_2^{2^f}(x_2, x_3)\prod_{i \geq 2} x_{2i}^{s}(x_{2i}, x_{2i+1}),$$

where $s = p^e$, $e, f \in \bar{\mathbf{N}}$, $e \geq f \geq 2$. Since $r = x_1^2 r_1$, we have found the required basis of F.

4.5. **The Case** $q = 2$, $t = 0$. — Let (F_n) be the descending 2-central series of F. Since $t(G) = 0$, the definition of the invariant $t(G)$ together with Proposition 11 shows that there is an orthonormal basis (χ_i) of $H^1(G)$. Replacing χ_{2i} by $\chi_{2i} + \chi_{2i-1}$, we obtain a basis (χ_i) of $H^1(G)$ such that

$$\chi_{2i-1} \cup \chi_{2i-1} = \chi_{2i-1} \cup \chi_{2i} = 1 \qquad \text{and} \qquad \chi_i \cup \chi_j = 0$$

for all other i, j with $i \leq j$. If $x = (x_i)$ is a basis of F with $\chi_i(x_j) = \delta_{ij}$, then, by Proposition 8, we have $r \equiv r_0(x)$ modulo F_3, where

$$r_0(x) = \prod_{i \geq 1} x_{2i-1}^2 (x_{2i-1}, x_{2i}).$$

Now assume that, for some $n \geq 2$, we have found a basis $x = (x_i)$ of F and integers $a_{ij} \in 2\mathbf{Z}$ such that

$$r \equiv r_0(x) \prod_{i<j} (x_i, x_j)^{a_{ij}} \qquad (\text{mod } F_{n+1}).$$

Then, proceeding as in the previous sections, we obtain a homomorphism $\delta_n : W_n \to \mathrm{gr}_{n+1}(F)$, where $\delta_n(\tau)$ is given by

$$\sum_{i \geq 1} (\pi \xi_{2i-1} + [\tau_{2i-1}, \xi_{2i-1}] + [\tau_{2i-1}, \xi_{2i}] + [\xi_{2i-1}, \tau_{2i}]).$$

Lemma. — *If E is the closed subgroup of $\mathrm{gr}_2(F)$ generated by the elements $[\xi_i, \xi_j]$, then $\mathrm{gr}_{n+1}(F)$ is generated by $\mathrm{Im}(\delta_n)$ and $\pi^{n-1}E$.*

Proof. — Since $\mathrm{gr}_{n+1}(F) = \mathrm{Im}(\delta_n) + \pi\, \mathrm{gr}_n(F)$ by the Corollary to Proposition 7, it follows that $\mathrm{gr}_{n+1}(F)$ is generated by $\mathrm{Im}(\delta_n)$ and $\pi^{n-1}\mathrm{gr}_2(F)$. Hence, it suffices to show that any element of the form $\sum_{i \geq 1} a_i \pi^2 \xi_i$ belongs to $\mathrm{Im}(\delta_2) + \pi E$. If $\Delta : W_2 \to \mathrm{gr}_3(F)$ is defined by

$$\Delta(\tau) = \sum_{i \geq 1} \pi \tau_{2i-1} + \sum_{i \geq 1} [\xi_i, \tau_i],$$

then $\mathrm{Im}(\Delta) = \mathrm{Im}(\delta_2)$. Now let $\tau = (\tau_i)$, where

$$\tau_{2i-1} = a_{2i-1} \pi \xi_{2i-1} + a_{2i} \pi \xi_{2i}, \qquad \tau_{2i} = a_{2i} [\xi_{2i-1}, \xi_{2i}].$$

Then $\tau \in W_2$, and a simple calculation using Proposition 6 shows that

$$\Delta(\tau) = \sum_{i \geq 1} a_i \pi^2 \xi_i + \sum_{i \geq 1} a_{2i} \pi [\xi_{2i-1}, \xi_{2i}].$$

Hence $\sum_{i \geq 1} a_i \pi^2 \xi_i \in \operatorname{Im}(\partial_2) + \pi E.$

Q. E. D.

Using the above lemma, we find a basis $y = (y_i)$ of F such that

$$r \equiv r_0(y) \prod_{i<j} (y_i, y_j)^{b_{ij}} \qquad (\text{mod } F_{n+2}),$$

where $y_i \equiv x_i$ (mod F_n), and $b_{ij} \equiv a_{ij}$ (mod 2^{n-1}). Proceeding inductively and passing to the limit, we see that there exists a basis (x_i) of F and 2-adic integers $b_{ij} \in 2\mathbf{Z}_2$ such that r is of the form (5).

This completes the proof of Theorem 3.

5. Proof of Theorem 4.

5.1. **The Properties** P_n, Q_n. — If χ is a continuous homomorphism of a pro-p-group G into the group of units of the compact ring $\mathbf{Z}_p/p^n\mathbf{Z}_p$, let $J = J(\chi)$ be the compact G-module obtained from $\mathbf{Z}_p/p^n\mathbf{Z}_p$ by letting G act on this group by means of χ. If $n < \infty$, then G is said to have *the property* P_n *with respect to* χ if the canonical homomorphism

$$(13) \qquad \varphi: \; H^1(G, J) \rightarrow H^1(G, J/pJ) = H^1(G)$$

is *surjective*. If $n = \infty$, then G is said to have *the property* P_n *with respect to* χ if the canonical homomorphism

$$(14) \qquad \varphi: \; H^1(G, J/p^m J) \rightarrow H^1(G, J/pJ) = H^1(G)$$

is *surjective for* $m \geq 1$. The pro-p-group G is said to have *the property* Q_n if there exists a *unique* continuous homomorphism $\chi : G \rightarrow (\mathbf{Z}_p/p^n\mathbf{Z}_p)^*$ such that G has the property P_n with respect to χ.

Remark. — If G is a free pro-p-group, then G has the property P_n with respect to any continuous homomorphism $\chi : G \rightarrow (\mathbf{Z}_p/p^n\mathbf{Z}_p)^*$ since $cd(G) \leq 1$.

PROPOSITION 12. — *Let G be a pro-p-group of rank $\aleph_0$, and let $\chi : G \rightarrow (\mathbf{Z}_p/p^n\mathbf{Z}_p)^*$ be a continuous homomorphism. Then the following statements are equivalent :*

(*a*) *The group G has the property P_n with respect to χ.*

(*b*) *If* (g_i) *is a minimal generating system of* G *and* (a_i) *is a family of elements of* $J = J(\chi)$ *with* $a_i \to 0$, *there exists a continuous crossed homomorphism* D *of* G *into* J *such that* $D(g_i) = a_i$.

Proof. — Clearly (*b*) implies (*a*). Now assume that (*a*) is true and let g_i, a_i be given as in (*b*).

If $n < \infty$, the surjectivity of (13) shows that there is a continuous crossed homomorphism D_1 of G into J such that $D_1(g_i) \equiv a_i \pmod p$. Suppose that we have found a continuous crossed homomorphism D_j $(1 \leq j < n)$ of G into J such that $D_j(g_i) = a_i + p^j b_i$. Then, as above, there is a continuous crossed homomorphism D' of G into J, such that $D'(g_i) \equiv b_i \pmod p$. If $D_{j+1} = D_j - p^j D'$, then D_{j+1} is a continuous crossed homomorphism of G into J such that $D_{j+1}(g_i) \equiv a_i \pmod{p^{j+1}}$. Proceeding inductively, we see that D_n is the required crossed homomorphism.

If $n = \infty$, let $\chi_m = \varepsilon_m \circ \chi$, where ε_m is the canonical homomorphism of $\mathbf{Z}_p$ onto $\mathbf{Z}_p/p^m\mathbf{Z}_p$. Then G has the property P_m with respect to χ_m, and $J/p^m J = J(\chi_m)$ where $J = J(\chi)$. If $a_i^{(m)} = \varepsilon_m(a_i)$, then by what we have shown above, there exists a continuous crossed homomorphism $D^{(m)}$ of G into $J/p^m J$ such that $D^{(m)}(g_i) = a_i^{(m)}$. Passing to the limit, we obtain the required crossed homomorphism D.

PROPOSITION 13. — *Let* G *be a Demuškin group of rank* $\aleph_0$ *with* $s(G) = p^e$, *and let* $\chi : G \to (\mathbf{Z}_p/p^e\mathbf{Z}_p)^*$ *be the character associated to the dualizing module of* G. *Then* G *has the property* P_e *with respect to* χ.

Proof. — If $J = J(\chi)$, then $I = \mathrm{Hom}(J, Q_p/\mathbf{Z}_p)$ is the dualizing module of G. It follows that $H^2(G, J/p^n J)$ is cyclic of order p^n if $1 \leq n < e$, or if $n = e < \infty$. This, together with the fact that $cd(G) = 2$, shows that the sequence

$$(15) \qquad 0 \to H^2(G, J/p^{n-1}J) \xrightarrow{\alpha} H^2(G, J/p^n J) \to H^2(G, J/pJ) \to 0$$

is exact for any integer n with $1 \leq n \leq e$. But

$$\mathrm{Ker}(\alpha) = \mathrm{Coker}\,(H^1(G, J/p^n J) \to H^1(G, J/pJ)),$$

which proves the proposition.

5.2. **Proof of Theorem** 4. — Let F be a free pro-p-group of rank $\aleph_0$ with basis $(x_i)_{i \in \mathbf{N}}$, and let r be a relation satisfying the hypotheses of the theorem. The fact that $G = F/(r)$ is a Demuskin group follows from Proposition 8, as does the assertion concerning the invariant $t(G)$. The rest of the proof deals with the computation of $s(G)$ and χ, where χ is the character associated to the dualizing module of G. We do this for a relation of the form (1), the same method applying, with obvious modifications, to relations of the form (2), ..., (5).

If g_i is the image of x_i in G, then (g_i) is a minimal generating system of G and we have

$$(16) \qquad g_1^q(g_1, g_2)\prod_{i\geq 2} g_s^{2i-1}(g_{2i-1}, g_{2i}) = 1,$$

where $q = p^f$, $s = p^e$, $e, f \in \overline{\mathbf{N}}$. Suppose that G has the property P_n with respect to some homomorphism θ. Then, by Proposition 12, there exists a continuous crossed homomorphism D_i of G into $J(\theta)$ such that $D_i(g_j) = \delta_{ij}$. Applying D_2 to both sides of (16), we obtain

$$\theta(g_1)^{q-1}\theta(g_2)^{-1}(\theta(g_1) - 1) = 0,$$

which implies that $\theta(g_1) = 1$. Similarly, $\theta(g_{2i-1}) = 1$ for $i \geq 2$. Applying D_1 to both sides of (16), we obtain $q + \theta(g_2)^{-1} - 1 = 0$, which implies that

$$\theta(g_2) = (1 - q)^{-1}.$$

Similarly, $\theta(g_{2i}) = (1 - s)^{-1}$ for $i \geq 2$. But, since θ is continuous and $g_i \to 1$, we have $\theta(g_i) \to 0$. In view of what we have shown above, this is possible if and only if $n \leq e$. If $s(G) = p^{e'}$, it follows that $e' \leq e$ since G has the property $P_{e'}$ with respect to χ. It also follows that G has the property $Q_{e'}$, and that

$$\chi(x_2) = (1 - q)^{-1}, \qquad \chi(x_i) = 1 \quad \text{for } i \neq 2.$$

All that remains to be shown is that $e' = e$. To do this, let $\theta_0 : F \to (\mathbf{Z}_p/p^e\mathbf{Z}_p)^*$ be the continuous homomorphism defined by

$$\theta_0(x_2) = (1 - q)^{-1}, \qquad \theta_0(x_i) = 1 \quad \text{otherwise.}$$

Then $\theta_0(r) = 1$, and θ_0 induces a homomorphism θ of G into $(\mathbf{Z}_p/p^e\mathbf{Z}_p)^*$. A simple calculation shows that $D(r) = 0$ for any continuous crossed homomorphism D of F into $J(\theta)$. In view of Proposition 12, it follows that G has the property P_e with respect to θ. If n is an integer with $1 \leq n \leq e$, then an inductive argument using the sequence (15) with $J = J(\theta)$ shows that $H^2(G, J/p^n J)$ is cyclic of order p^n. It follows immediately that $e' = e$, which completes the proof of Theorem 4.

6. Proof of Theorem 5.

Let K, Γ, G be as in the statement of the theorem. Let $(U_i)_{i\in\mathbf{N}}$ be a decreasing sequence of open subgroups of Γ containing G such that $\bigcap_i U_i = G$. Let $G_i = U_i/V_i$ be the largest quotient of U_i which is a pro-p-group; if K_i is the fixed field of U_i, then G_i is the Galois group of $K_i(p)/K_i$, where $K_i(p)$ is the maximal p-extension of K_i. Composing the inclusion $G \to U_i$ with the canonical homomorphism of U_i onto G_i, we obtain a homomorphism $\psi_i : G \to G_i$. It is easy to see that ψ_i is surjective and that the subgroups $H_i = \operatorname{Ker}(\psi_i)$ form a decreasing sequence of closed normal subgroups of G which intersect in the identity.

If K does not contain a primitive p-th root of unity ζ_p, let $K' = K(\zeta_p)$, and let Γ' be the Galois group of $\overline{K}/K'$. Then G is a Sylow p-subgroup of Γ' since $(\Gamma : \Gamma') = [K' : K]$ is prime to p. Hence, we are reduced to proving the theorem for the case K contains a primitive p-th root of unity. In this case G_i is a Demuškin group of rank $[K_i : \mathbf{Q}_p] + 2$, and its dualizing module is μ_{p^∞} (*cf.* [12], p. II-30). Since $H^1(G)$ is the union of the $H^1(G_i)$, it follows that G is of rank $\aleph_0$. By Theorem 1, we see that G is either a Demuškin group, or a free pro-p-group. But, by a theorem of J. Tate, we have $cd(G) = 2$ (*cf.* [12], p. II-16). Hence, G is a Demuškin group. To show that μ_{p^∞} is the dualizing module, it suffices to show that the canonical homomorphism

$$\varphi : \quad H^1(G, \mu_{p^n}) \to H^1(G, \mu_p) = H^1(G)$$

is surjective for $n \geqq 1$ (*cf.* § 5.1). But since μ_{p^∞} is the dualizing module of G_i, we have a commutative diagram

$$\begin{array}{ccc} H^1(G, \mu_{p^n}) & \xrightarrow{\varphi} & H^1(G) \\ \uparrow & & \uparrow \\ H^1(G_i, \mu_{p^n}) & \xrightarrow{\varphi_i} & H^1(G_i) \end{array}$$

in which φ_i is surjective for $n \geqq 1$. Passing to the limit, we obtain the surjectivity of φ.

To prove the assertion concerning $t(G)$, it suffices to consider the case $q(G) = 2$, for otherwise $t(G) = 1$ and $[K(\zeta_p) : \mathbf{Q}_p]$ is even. Let $V = H^1(G)$, and let V_i be the image of $H^1(G_i)$ in V under the homomorphism $H^1(\psi_i)$. Since $\dim(V_i) = [K_i : \mathbf{Q}_2] + 2$ and $[K_i : K]$ is odd, we have

$$(-1)^{\dim(V_i)} = (-1)^{[K : \mathbf{Q}_2]}.$$

Moreover, as we have seen in the proof of Proposition 1, the cup-product : $H^1(G) \times H^1(G) \to H^2(G)$ is non-degenerate on V_i for i sufficiently large. [Actually, the cup-product is non-degenerate on each V_i since $H^2(\psi_i) : H^2(G_i) \to H^2(G)$ is bijective.] Also, the cup-product is non-alternate since $q(G) = 2$, and $t(G) = 1$ or -1 since $s(G) = 0$. Hence, since V is the union of the V_i, it follows from the definition of $t(G)$ together with the proof of Proposition 11 and its Corollary that

$$t(G) = (-1)^{\dim(V_i)}$$

for i sufficiently large.

Q. E. D.

BIBLIOGRAPHY.

[1] DEMUŠKIN (S. P.). — On the maximal p-extensions of a local field [in Russian], *Izv. Akad. Nauk S. S. S. R., Math. Series*, t. 25, 1961, p. 329-346.

[2] DEMUŠKIN (S. P.). — On 2-extensions of a local field [in Russian], *Mat. Sibirsk. Ž.*, t. 4, 1963, p. 951-955.

[3] DEMUŠKIN (S. P.). — Topological 2-groups with an even number of generators and one defining relation [in Russian], *Izv. Akad. Nauk S. S. S. R.*, t. 29, 1965, p. 3-10.

[4] DOUADY (A.). — Cohomologie des groupes compacts totalement discontinus, *Séminaire Bourbaki*, t. 12, 1959-1960, nº 189, 12 pages.

[5] HOCHSCHILD (G.) and SERRE (J.-P.). — Cohomology of group extensions, *Trans. Amer. math. Soc.*, t. 74, 1953, p. 110-134.

[6] KAPLANSKY (I.). — Forms in infinite-dimensional spaces, *Ann. Acad. Bras. Cienc.*, t. 22, 1950, p. 1-17.

[7] LABUTE (J.). — Classification des groupes de Demuškin, *C. R. Acad. Sc.*, t. 260, 1965, p. 1043-1046.

[8] LABUTE (J.). — Classification of Demuškin groups, Thesis, Harvard Univ., 1965; *Canadian J. Math.* (to appear).

[9] LABUTE (J.). — Les groupes de Demuškin de rang dénombrable, *C. R. Acad. Sc.*, t. 262, 1966, p. 4-7.

[10] SERRE (J.-P.). — *Corps locaux*. — Paris, Hermann, 1962 (*Act. scient. et ind.*, 1296; *Publ. Inst. Math. Univ. Nancago*, 7).

[11] SERRE (J.-P.). — Structures de certains pro-p-groupes, *Séminaire Bourbaki*, t. 15, 1962-1963, nº 252, 11 pages.

[12] SERRE (J.-P.). — *Cohomologie galoisienne*. — Berlin, Springer-Verlag, 1964 (*Lecture Notes in Mathematics*, 5).

[13] SERRE (J.-P.). — *Lie algebras and Lie groups*. 1964 Lectures given at Harvard University. — New York, W. A. Benjamin, 1965.

(Manuscrit reçu le 13 juin 1966.)

John P. LABUTE,
9 *bis*, parc de Montretout,
92, Saint-Cloud (Hauts-de-Seine).