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>
DEMUŠKIN GROUPS OF RANK $n_0$

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 $n_0$ (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 $\mathbb{Q}_p$ 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 $H^i(G)$ will denote the cohomology group $H^i(G, \mathbb{Z}/p\mathbb{Z})$, the action of $G$ on the discrete group $\mathbb{Z}/p\mathbb{Z}$ being the trivial one. ($\mathbb{Z}$ is the ring of rational integers.) The dimension of $H^i(G)$ over the field $\mathbb{Z}/p\mathbb{Z}$ 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.
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) $H^1(G)$ is one-dimensional over the field $\mathbb{Z}/p\mathbb{Z}$;

(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 $\bigcap H_i = 1$ 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. 1-17) 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. 1-33). 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 Demuškin 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 $H^2(G) = \lim H^2(G_i)$ (cf. [12], p. 1-9), it follows that $cd(G) \leq 2$. But $H^2(G) \neq 0$ by the definition of a Demuškin group. Hence $cd(G) = 2$.

Our next result gives the structure of the closed subgroups of a Demuškin 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 $R = \ker(f)$, 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 $\text{tg}$ is injective since the first inflation homomorphism is bijective. Since $H^2(F) = 0$ (cf. [12], p. I-25) it follows that $H^1(R)^G \cong H^2(G) \cong \mathbb{Z}/p\mathbb{Z}$. 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 $s(G), \text{Im}(\gamma)$. — Let $G$ be a Demuškin group of rank $\neq 1$. Since $H^2(G, \mathbb{Z}/p\mathbb{Z})$ 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 $\text{cd}(G) = 2$, it follows that $G$ has a dualizing module $I$, that is, the functor $T(M) = \text{Hom}(H^2(G, M), \mathbb{Q}/\mathbb{Z})$, 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 $\mathbb{Q}/\mathbb{Z}$, (cf. [12], p. I-48). If $n(G) = \aleph_0$, then $I$ is isomorphic, as an abelian group, to either $\mathbb{Q}/\mathbb{Z}$ or $\mathbb{Z}/p^\infty \mathbb{Z}$. Indeed, it suffices to show that the group $I_p = \text{Hom}(\mathbb{Z}/p\mathbb{Z}, I)$ is cyclic of order $p$. But $I_p$ is the inductive limit of the groups $\text{Hom}(H^2(U), \mathbb{Q}/\mathbb{Z})$, 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 $H^2(U) \cong \mathbb{Z}/p\mathbb{Z}$ 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 $E$ of endomorphisms of $I$ is canonically isomorphic to $\mathbb{Z}_p$, if $s(G) = 0$, and to $\mathbb{Z}/p\mathbb{Z}$ if $s(G) = p^\infty$. Hence, if $U$ is the compact group of units of $E$, we have a canonical homomorphism $\gamma : G \to U$. Since $\gamma$ is continuous, it follows that the invariant $\text{Im}(\gamma)$ is a closed subgroup of the pro-$p$-group $U^{(1)} = 1 + pE$. 

BULL. SOC. MATH. — T. 94, FASC. 3.
We shall need a list of the closed subgroups of $U^i$. Consider first the case where $s(G) = 0$. Then we have

$$U^i = U^i_p = 1 + p\mathbb{Z}_p.$$  

If $p \neq 2$, then $U^i_p$ 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 $U^i_p$ are the subgroups

$$U^i_p = 1 + p^f\mathbb{Z}_p \quad \text{with} \quad f \in \mathbb{N} = \mathbb{N} \cup \{ \infty \}.$$  

(We let $\mathbb{N}$ denote the set of integers $\geq 1$; by convention $\infty \geq a$ for any $a \in \mathbb{N}$ and $a^\infty = 0$ for any $a \in \mathbb{N}$.) If $p = 2$, we have $U^i_2 = 1 \pm 1 \times U^i_2$, and $U^i_2$ is a free 2-group of rank 1 generated by any element $u$ with $v_2(u - 1) = 2$. The closed subgroups of $U^i_2$ are therefore of three distinct types:

(i) the groups $U^i_2$ with $f \in \mathbb{N}$, $f \geq 2$;
(ii) the groups $1 \pm 1 \times U^i_2$ with $f \in \mathbb{N}$, $f \geq 2$;
(iii) the groups $U^i_2$, for which $f \in \mathbb{N}$, $f \geq 2$. $U^i_2$ is the closed subgroup of $U^i_2$ generated by $-u$, where $u$ is a generator of $U^i_2$.

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

1.3.2. The invariant $l(G)$. — Suppose that the Demuskin group $G$ is of rank $s$, and let $\varphi : H^i(G) \times H^i(G) \to H^i(G)$ be the cup product. Then $\varphi$ is a non-degenerate skew-symmetric bilinear form on the vector space $V = H^i(G)$. Let $\delta$ be the linear form on $V$ defined by $\delta(v) = v \cup v$, and let $A = \ker(\delta)$. If $A = V$, i.e., if $\varphi$ is alternate, we set $l(G) = 1$. 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 $l(G)$ as follows: set $l(G) = 1$ if $\dim(A') = 1$ and $A' \subset A$; set $l(G) = -1$ if $\dim(A') = 1$ and $A' \not\subset A$; set $l(G) = 0$ if $A' = \emptyset$.

Remark. — We shall see (cf. § 2.4) that the definition of $l(G)$ 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 $G_n = G/(G, G)$. Representing $G$ as a quotient $F/(r)$, where $F$ is a free pro-$p$-group and $r \in F'(F, F)$, we see that either $|G_n|$ is torsion-free or the torsion subgroup of $G_n$ is cyclic of order $p^\ell$. 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 $r \in F'(F, F)$. 
1.4. The Classification Theorem. — Recall (cf. [12], p. 1–5) 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. 1–35). 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. 1–36).

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

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

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

$$x^s_1(x_i, x_j) \prod_{i \geq 2} x^s_{i-1}(x_{2i-1}, x_{2i}),$$

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

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

$$x^{s_1}_1(x_i, x_j)(x_i, x_j) \prod_{i \geq 2} x^{s_2}_{i-1}(x_{2i-1}, x_{2i}),$$

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

$$x^{s_3}_1(x_i, x_j, x_k) \prod_{i \geq 3} x^{s_4}_{i-1}(x_{2i-1}, x_{2i}),$$

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

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

$$x^s_1x^s_2(x_i, x_j) \prod_{i \geq 2} x^{s_3}_{i}(x_{2i}, x_{2i+1}),$$

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

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

$$\prod_{i \geq 1} x^{s_1}_{i-1}(x_{2i-1}, x_{2i}) \prod_{i < j} (x_i, x_j)^{s_{ij}},$$

with $s = 2^e$, $e \in \mathbb{N}$, $e \geq f \geq 2$. 
with \( b_{ij} \in 2\mathbb{Z}_2 \). (The product \( \prod_{i<j} \) is taken with respect to an arbitrarily given linear order of \( \mathbb{N} \times \mathbb{N} \).

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

(i) If \( r \) is a relation of the form (1) with \( q = p^e \), \( s = p^e \), \( e, h \in \mathbb{N} \), \( e \geq h \), then \( G \) is a Demuškin group with \( q(G) = q \), \( s(G) = s \), \( \gamma_i(x_i) = (1 - q)^{-1} \), \( \gamma_i(x_i) = 1 \) for \( i \neq 2 \). (\( \gamma_i \) is the character associated to the dualizing module of \( G \).)

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

\[
(x_1^{a_1} x_2^{a_2} (x_1, x_2) x_3^{a_3} (x_3, x_4) \prod_{i \geq 2} x_{2i-1}^{a_{2i-1}} (x_{2i-1}, x_{2i}))
\]

with \( s = 2^e \), \( e, f, g \in \mathbb{N} \), \( e \geq f \geq g \geq 2 \), then \( G \) is a Demuškin group with \( q(G) = 2 \), \( t(G) = 1 \), \( s(G) = s \), \( \gamma_i(x_i) = (1 + 2^e)^{-1} \), \( \gamma_i(x_i) = 1 \) for \( i \neq 2, 4 \).

(iii) If \( p = 2 \) and \( r \) is a relation of the form (4) with \( s = 2^e \), \( e, f \in \mathbb{N} \), \( e \geq f \geq 2 \), then \( G \) is a Demuškin group with \( q(G) = 2 \), \( t(G) = -1 \), \( s(G) = s \), \( \gamma_i(x_i) = (1 - 2^e)^{-1} \), \( \gamma_i(x_i) = 1 \) for \( i \neq 1, 3 \).

(iv) If \( p = 2 \) and \( r \) is a relation of the form (5) with \( b_{ij} \in 2\mathbb{Z}_2 \), 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 \( \mathfrak{s}_0 \) 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 \( \mathfrak{s}_0 \) with \( t(G) \neq 0 \). Then \( G \cong G' \) if and only if \( t(G) = t(G') \), \( s(G) = s(G') \), \( \text{Im}(\gamma) = \text{Im}(\gamma') \).

**Corollary 3.** — Let \( r, r' \in F^p(F, F) \), where \( F \) is a free pro-p-group of rank \( \mathfrak{s}_0 \). 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 \( \sigma \) of \( F \) with \( \sigma(r) = r' \).

**Corollary 4.** — For each \( e \in \mathbb{N} \) 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 \( p^e z = 0 \) for any \( z \in H^1(G, M) \).

**Remark.** — The invariant \( q(G) \) can be determined from the invariants \( s(G), \text{Im}(\gamma) \). In fact, if \( s(G) = p^e \) and \( E = \mathbb{Z}_p/p^e \mathbb{Z}_p \), then \( h(G) \) is the largest \( h \in \mathbb{N} \) with \( h \leq e \) and \( \text{Im}(\gamma) \subseteq 1 + p^h E \).

1.5. **Application to Galois Theory.** — If \( \Gamma \) is a profinite group, i.e. a projective limit of finite groups, then a Sylow \( p \)-subgroup of \( \Gamma \) 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. 1-4).

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

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

**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 $\zeta \in \mu_p^{**}$. If $\zeta_q$ is a primitive $q$-th root of unity, it follows that $\zeta_q$ is left fixed by $\sigma$ if and only if $\chi(\sigma) \in 1 + q\mathbb{Z}_p$. If $L$ is the fixed field of $G$, it follows that $\zeta_q \in L$ if and only if $\text{Im}(\chi) \subseteq 1 + q\mathbb{Z}_p$. 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 $K = \mathbb{Q}_p$ with $p \neq 2$, there exists a generating system $(\sigma_i)_{i \in \mathbb{N}}$ of $G$ having the single relation

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

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

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

$$\sigma_i^2 \sigma_i^2(\sigma_1, \sigma_2) \prod_{l \geq 2} (\sigma_{2l}, \sigma_{2l+1}) = 1.$$ 

Indeed, $t(G) = -1$ and $\text{Im}(\chi) = \mathbb{U}$.

### 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) $F_{n+1} \subseteq F_n$;
(iii) $(F_n, F_m) \subseteq F_{n+m}$.
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 $\text{gr}(F)$ be the direct sum of the $\mathbb{Z}_p$-modules $\text{gr}_n(F) = F_n/F_{n+1}$. Then $\text{gr}(F)$ is, in a natural way, a Lie algebra over $\mathbb{Z}_p$ (cf. [13], page LA 2.3) the bracket operation for homogeneous elements being defined as follows: If $i_n : F_n \rightarrow \text{gr}_n(F)$ 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 $\tilde{z}_i$ is the image of $x_i$ in $\text{gr}_i(F)$, we have the following proposition:

**Proposition 1.** — The Lie algebra $\text{gr}(F)$ is a free Lie algebra (over $\mathbb{Z}_p$) with basis $\tilde{z}_1, \ldots, \tilde{z}_n$.

**Proof.** — Let $L$ be the free Lie algebra (over $\mathbb{Z}_p$) on the letters $\tilde{z}_1, \ldots, \tilde{z}_n$, and let $\varphi : L \rightarrow \text{gr}(F)$ be the Lie algebra homomorphism sending $\tilde{z}_i$ into $\tilde{z}_i$. Using the fact that the $x_i$ form a generating system of $F$, one shows by induction that the elements $\tilde{z}_i \in \text{gr}_i(F)$ generate the Lie algebra $\text{gr}(F)$. Hence $\varphi$ is surjective.

To show that $\varphi$ 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 $\mathbb{Z}_p$. Let $m'$ be the ideal of $A$ consisting of those formal power series whose homogeneous components are of degree $\geq l$. The ring $A/m'$ 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 $A/m^j$. We give $A$ the unique topology which makes it the projective limit of the compact topological rings $A/m^j$. Let $U^i$ be the multiplicative group of formal power series with constant term equal to $1$. Then, with the induced topology, $U^i$ is a pro-$p$-group containing the elements $1 + t^i$. Since $(x)$ is a basis of the free pro-$p$-group $F$, there is a continuous homomorphism $\varepsilon$ of $F$ into $U^i$ sending $x_i$ into $1 + t_i$. If

$$\varepsilon(x) = 1 + u, \quad \varepsilon(y) = 1 + v,$$

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

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

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

$$\theta_0(xy) \equiv \theta_0(x) + \theta_0(y) \pmod{m^{i+1}}.$$
Hence \( \theta_n \) induces an additive homomorphism \( \theta \) of \( \text{gr}(F) \) into \( \text{gr}(A) \), where \( \text{gr}(A) \) is the graded algebra defined by the \( m \)-adic filtration of \( A \). Moreover, (7) shows that \( \theta \) is a Lie algebra homomorphism. If \( \tau \) is the image of \( t \) in \( \text{gr}(A) \), then \( \text{gr}(A) \) is a free associative algebra with basis \( \tau \). By the theorem of Birkhoff-Witt (cf. [13], page LA 4.4) the Lie algebra homomorphism \( \varphi : L \rightarrow \text{gr}(A) \) sending \( \tau \) into \( \tau \) is injective. Since \( \varphi = \theta \circ \varphi \), we see that \( \varphi \) 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 \( \text{gr}_n(F) \) is the projective limit of the groups \( \text{gr}_n(F(i)) \). 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 \( \text{gr}_n(F) = F_n/F_{n+1} \) is a torsion-free \( \mathbb{Z}_p \)-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 \( \tilde{z}_1, \ldots, \tilde{z}_n \). Then \( [L, L] \) is generated, as a \( k \)-module, by the elements

\[
\text{ad}(\tilde{z}_{i_1}) \cdots \text{ad}(\tilde{z}_{i_k}) \tilde{z}_{i_{k+1}}, \text{ with } i_{k+1} \geq i_1, \ldots, i_k.
\]

**Proof.** — For \( 1 \leq m \leq n \), let \( L_m \) be the subalgebra generated by \( \tilde{z}_1, \ldots, \tilde{z}_m \), and let \( A_m \) be the ideal of \( L_m \) generated by \( \tilde{z}_m \). Then, as a \( k \)-module, \( A_m \) is generated by \( \tilde{z}_m \) and the elements \( \text{ad}(\tilde{z}_{i_1}) \cdots \text{ad}(\tilde{z}_{i_k}) \tilde{z}_m \) with \( i_1, \ldots, i_k \leq m \). Indeed, the ideal \( A_m \) contains these elements, and the submodule they generate is invariant under the \( \text{ad}(\tilde{z}) \) for \( i \leq m \). 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 \( 1 \leq m \leq n \). To do this let \( \varphi_m : L_m \rightarrow L_{m-1} \) be the Lie algebra homomorphism such that \( \varphi_m(\tilde{z}_m) = 0 \), \( \varphi_m(\tilde{z}_i) = \tilde{z}_i \) if \( i < m \). Since \( L_m/A_m \) is the free Lie algebra generated by the images of \( \tilde{z}_1, \ldots, \tilde{z}_{m-1} \) and \( \text{Ker}(\varphi_m) \supseteq A_m \), it follows that \( \varphi_m \) induces an isomorphism of \( L_m/A_m \) onto \( L_{m-1} \). Hence \( \text{Ker}(\varphi_m) = A_m \). Since \( \varphi_m \) 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 \( (x_i)_{i \in \mathbb{N}} \). Let \( (F_n) \) be the descending central series of \( F \), and let \( \tilde{z}_i \) be the image of \( x_i \) in \( \text{gr}_1(F) \). If \( N_i \) is the closed normal subgroup of \( F \) generated by the \( x_j \) with \( j \geq i \), then \( F_{n+1} = F_n \cap N_i \), and let \( B_{ni} \) be the image of \( F_{ni} \) in \( \text{gr}_n(F) \). We then have the following result:

**Proposition 4.** — If \( T_n \) is the closed subgroup of \( \text{gr}_{n+1}(F) \) generated by the subgroups \( \text{ad}(\tilde{z}_i)B_{ni} \), then \( T_n = \text{gr}_{n+1}(F) \) for \( n \geq 1 \).
Proof. — The pro-p-group \( \text{gr}_{n+1}(F) \) is generated by the elements of the form \( \text{ad}(z_i) \ldots \text{ad}(z_n) \). However, by Proposition 3, each such element is a linear combination of elements of the same form but with \( i_{n+1} \geq i \). Since each of these latter elements belongs to \( T_n \), it follows that \( T_n \) contains a generating system of \( \text{gr}_{n+1}(F) \). Since \( T_n \) is closed, the result follows.

Corollary. — Every element of \( \text{gr}_{n+1}(F) \) can be written in the form
\[
\sum_{i \geq 1} \left[ z_i, \tau_i \right] \text{ with } \tau_i \in \text{gr}_n(F), \tau_i \to 0.
\]

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 \( x \in F_i, y \in F_j, a \in \mathbb{N}, b = \binom{a}{2} \), then:

(i) \( (xy)^a = x^a y^a (y, x)^b \mod F_{i+j+1} \);

(ii) \( (x^a, y) = (x, y)^a ((x, y), x)^b \mod F_{i+j+2} \);

(iii) \( (x, y^a) = (x, y)^a ((x, y), y)^b \mod F_{i+j+2} \).

Proof. — Assertion (iii) follows easily from (ii). We now prove (i) and (ii) by induction on \( a \) using the following formulae (cf. [13], page LA 2.1):
\[
\begin{align*}
(\text{xy}, z) &= (x, z) ((x, z), y) (y, z), \\
(\text{xz}, y) &= (x, z) (x, y) ((x, y), z).
\end{align*}
\]

For \( a = 1 \), the proposition is obvious.

(i) Working modulo \( F_{i+j+1} \), we have
\[
(xy)^{a+1} = xy(xy)^a = xyx^a y^a (y, x)^b = x^{a+1} y^a (y, x)^b,
\]
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
\[
(x^{a+1}, y) = (xx', y) = (x, y) ((x, y), x') (x', y) = (x, y)^a ((x, y), y)^b = (x, y)^{a+1} ((x, y), x)^{a+b}.
\]

Now let \( F \) be a pro-p-group, and let \( q = p^h \) with \( h \in \mathbb{N} \). 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 \( \text{gr}(F) \) is the associated Lie algebra, then \( \text{gr}(F) \) is a Lie algebra over \( \mathbb{Z}/q\mathbb{Z} \). If \( P : F \to F \) is the mapping \( x \mapsto x^q \), we have \( P(F_n) \subset F_{n+1} \) for \( n \geq 1 \). Using Proposition 5,
we see that \( P \) induces a map \( \pi : \text{gr}_n(F) \to \text{gr}_{n+1}(F) \) for \( n \geq 1 \). The following result is an immediate consequence of Proposition 5:

**Proposition 6.** Let \((F_n)\) be the descending \( q \)-central series of a pro-

\[ \text{group } F. \]  

If \( \xi \in \text{gr}_i(F) \), \( \eta \in \text{gr}_j(F) \), then:

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

(ii) \( \pi(\xi + \eta) = \pi\xi + \pi\eta + \left( \frac{q}{2} \right) [\xi, \eta] \) if \( i = j = 1 \);

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

(iv) \( [\pi\xi, \eta] = \pi[\xi, \eta] + \left( \frac{q}{2} \right) [[\xi, \eta], \xi] \) if \( i = 1 \).

**Remarks.** Using the fact that \( \left( \frac{q}{2} \right) \equiv 0 \pmod{q} \) if \( p \neq 2 \), we see that \( \text{gr}(F) \) is a Lie algebra over \( \mathbb{Z}/q\mathbb{Z}[\pi] \) for \( p \neq 2 \). If \( q = 2 \), then \( \left( \frac{q}{2} \right) \equiv 2^{k-1} \pmod{q} \). Hence in this case \( \text{gr}(F) \) is not a Lie algebra over \( \mathbb{Z}/q\mathbb{Z}[\pi] \). However, if \( \text{gr}'(F) = \sum_{n \geq 2} \text{gr}_n(F) \), then \( \text{gr}'(F) \) is a Lie algebra over \( \mathbb{Z}/q\mathbb{Z}[\pi] \). Also, \( \text{gr}(F) \otimes \mathbb{Z}/p\mathbb{Z} \) is a Lie algebra over \( \mathbb{Z}/q\mathbb{Z}[\pi] \otimes \mathbb{Z}/p\mathbb{Z} \) if \( q \neq 2 \).

Now let \( F \) be a free pro-\( p \)-group of rank \( \aleph_0 \) with basis \( (x_i)_{i \in \mathbb{N}} \) and let \((F_n)\) be the descending \( q \)-central series of \( F \). Let \( \bar{z}_i \) be the image of \( x_i \) in \( \text{gr}_i(F) \). Let \( N_i \) be the closed normal subgroup of \( F \) generated by the \( x_j \) with \( j \geq i \), let \( F_{n_i} = F_n \cap N_i \), and let \( B_{n_i} \) be the image of \( F_{n_i} \) in \( \text{gr}_i(F) \). We then have the following result:

**Proposition 7.** Let \( T_n \) be the closed subgroup of \( \text{gr}_{n+1}(F) \) generated by the subgroups \( \text{ad}(\bar{z}_i) B_{n_i} \), and let \( D \) be the closed subgroup of \( \text{gr}_i(F) \) generated by the elements \( \pi\bar{z}_i \). Then the group \( \text{gr}_{n+1}(F) \) is generated by \( T_n \) and \( \pi^{n-1}D \).

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

\[ \pi^{n-k} \text{ad}(\bar{z}_i) \ldots \text{ad}(\bar{z}_i) \bar{z}_{i+k}, \]

It follows, by Proposition 3, that \( \text{gr}_{n+1}(F) \) is generated by elements of the form \((g) \) with \( i_{k+1} \geq i \). Since

\[ \pi^{n-k}[\bar{z}_i, \eta] = [\bar{z}_i, \pi^{n-k}\eta] \text{ if } \eta \in \text{gr}_m(F), \quad \text{with } m \geq 2, \]

and

\[ \pi^{n-1}[\bar{z}_i, \xi] = [\bar{z}_i, \pi^{n-1}\xi] + \left\{ \bar{z}_j, \left( \frac{q}{2} \right)^n \pi^{n-1}[\bar{z}_i, \xi] \right\} \text{ for } n \geq 2, \]

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

Q. E. D.
Corollary. — Every element of $\text{gr}_{n+1}(F)$ can be written in the form

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

where $a_i \in \mathbb{Z}/q\mathbb{Z}$, $\tau_i \in \text{gr}_{n}(F)$, $\tau_i \rightarrow 0$.

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

$$0 \rightarrow H^1(G, k) \rightarrow H^1(F, k) \rightarrow H^1(R, k) \rightarrow H^2(G, k) \rightarrow H^2(F, k).$$

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

Lemma. — The $\mathbb{Z}/p\mathbb{Z}$-module $N = R^i(R, F)$ 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 $n \in \mathbb{N}$ 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 $\text{gr}_{n}(F)$ sending the generator $\varphi = r(R, F)$ of $N$ into a non-zero element $\tau$ of $\text{gr}_{n}(F)$. Since $\text{gr}_{n}(F)$ is a torsion-free $\mathbb{Z}/p\mathbb{Z}$-module (cf. Proposition 2), it follows that $f(N)$ is free of rank $1$ generated by $\tau$, and hence that $N$ is free of rank $1$ generated by $\tau$.

Using the above results, we see that the homomorphism $\varphi : H^1(G, k) \rightarrow k$, defined by $\varphi(z) = -\tau^{-1}(z)(r)$, is an isomorphism. Given the relation $r$, we always use this isomorphism to identify $H^1(G, k)$ with $k$.

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

$$r = \prod_{i \geq 1} x_i^a_i \prod_{i < j} (x_j x_i)^{a_i} \quad (\text{mod } F_i).$$
with \( a_i, a_j \in k \). If \((\gamma_i)\) is the basis of \( H^1(G, k) \) defined by \( \gamma_i(x_j) = \delta_{ij} \), we have the following proposition:

**Proposition 8.**

(a) If \( \gamma_i \cup \gamma_j \in H^2(G, k) = k \) is the cup product of \( \gamma_i, \gamma_j \), then \( \gamma_i \cup \gamma_j = a_{ij} \) if \( i < j \), and \( \gamma_i \cup \gamma_j = \left( \begin{array}{c} q \\ 2 \end{array} \right) a_i \).

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

\[
o \rightarrow \mathbb{Z}/q\mathbb{Z} \rightarrow \mathbb{Z}/q^i\mathbb{Z} \rightarrow \mathbb{Z}/q\mathbb{Z} \rightarrow o,\]

then : (i) \( \beta(\gamma_i) = a_i \), and (ii) \( \gamma_i \cup \gamma_j = \left( \begin{array}{c} q \\ 2 \end{array} \right) \beta(\gamma) \) for any \( \gamma \in H^1(G, k) \).

**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 \( \gamma = \gamma_i \), and let \( s : \mathbb{Z}/q\mathbb{Z} \rightarrow \mathbb{Z}/q^i\mathbb{Z} \) be defined by

\[
s(n + q\mathbb{Z}) = n + q^i\mathbb{Z} \text{ for } 0 \leq n \leq q - 1.\]

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

\[
q(f(x) + f(y) - f(xy)) = \gamma'(x) + \gamma'(y) - \gamma'(xy)
\]

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

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

\[
\gamma_i \cup \gamma_i = \left( \begin{array}{c} q \\ 2 \end{array} \right) \beta(\gamma_i).
\]

If \( \gamma = \sum u_i \gamma_i \), then

\[
\gamma \cup \gamma = \sum u_i \gamma_i \cup \gamma_i = \sum u_i \left( \begin{array}{c} q \\ 2 \end{array} \right) \beta(\gamma_i) = \sum u_i \left( \begin{array}{c} q \\ 2 \end{array} \right) \beta(\gamma_i) = \left( \begin{array}{c} q \\ 2 \end{array} \right) \beta(\gamma)
\]

since \( u_i \left( \begin{array}{c} q \\ 2 \end{array} \right) = u_i \left( \begin{array}{c} q \\ 2 \end{array} \right) \) in \( \mathbb{Z}/q\mathbb{Z} \).

Q. E. D.
Proposition 9. — Let $V$ be a vector space of dimension $\mathfrak{h}$, and let $\varphi$ be a non-degenerate alternate bilinear form on $V$. Then $V$ has a symplectic basis, i.e., a basis $(v_j)_{j \in \mathbb{N}}$ 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 $(u_i)_{i \in \mathbb{N}}$ be an arbitrary basis of $V$, and suppose that we have already chosen $v_1, \ldots, v_{2\mathfrak{h}}$. If $X$ is the subspace generated by $v_1, \ldots, v_{2\mathfrak{h}}$, let $u_n$ be the first of the $u_i$ such that $u_n \notin X$. Since $\varphi$ 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 $u_n$, and choose $w \in X'$ with $\varphi(w, z) = 1$. We may then choose $v_{2n+1} = w$, $v_{2n+2} = z$.

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 $\mathbb{Z}/q\mathbb{Z}$-module of rank $\mathfrak{h}$, where $q = p^h$, with $h \in \mathbb{N}$, and let $\varphi$ be a skew-symmetric bilinear form on $V$ whose reduction modulo $p$ is non-degenerate. Let $\beta$ be a linear form on $V$, and suppose that either $\varphi$ is alternate, or $q \neq 2$ and $\varphi(v, v) = \left(\begin{smallmatrix} q \\ 2 \end{smallmatrix}\right) \beta(v)$ for any $v \in V$.

Then there exist integers $c$, $d$ with $0 \leq c \leq d \leq h$ and a basis $(v_i)_{i \in \mathbb{N}}$ of $V$ such that

(a) $\beta(v_i) = p^c$, $\beta(v_i) = 0$, and $\beta(v_{2i-1}) = p^d$, $\beta(v_i) = 0$ 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 $v_i, v_j$.

Proof. — Since the reduction of $\varphi$ 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 $v_i$ to be a given element $v \notin pV$. In particular, we can choose $v_i$ so that $\beta(v_i) = p^c$, where $c$ is the unique integer with $0 \leq c \leq h$ such that $p^c$ generates $\text{Im}(\beta)$.

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

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

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

**Lemma.** — Let $W$ be a free $\mathbb{Z}/q\mathbb{Z}$-module of rank $2n$, $n \geq 1$, and let $\varphi, \beta$ be forms on $W$ as in Proposition 10. If $u_1, \ldots, u_{2n}$ generate $\text{Im}(\beta)$, 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 $\text{Im}(\beta)$ and $u_i = 0$ otherwise. Let $(w_i)$ be a basis of $W$ such that $\beta(w_i) = u$ and $\beta(w_i) = 0$ for $i \neq 1$. Since the reduction of $\varphi$ modulo $p$ is non-degenerate and alternate, there is an $i > 2$ and a unit $t$ in $\mathbb{Z}/q\mathbb{Z}$ such that $\varphi(w_i, w_i) = t$. 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 $\varphi(w_i, w_i) = a_i \neq 0$ for some $i > 2$, replace $w_i$ by $w_i - a_i w_2$. In this way we may also assume that $\varphi(w_i, w_i) = 0$ for $i > 2$.

If $N$ is the submodule generated by $w_2, \ldots, w_{2n}$, then, on $N$, the form $\varphi$ is alternate and its reduction modulo $p$ is non-degenerate. Hence we may choose $w_1, \ldots, w_{2n} \in N$ 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 $\varphi(w_i, w_i) \neq 0$ for some $i > 2$. If this is so, replace $w_2$ by $w_2 + a_2 w_1 + \ldots + a_{2n} w_{2n}$, where $a_{2i} = \varphi(w_2, w_{2i-1})$ and $a_{2i-1} = \varphi(w_{2i}, w_i)$. 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 $\beta'$ be the linear form on $W$ such that $\beta'(v_i) = u_i$, and let $\varphi'$ be the bilinear form on $W$ defined by

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

and

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

Then the pair $(\varphi', \beta')$ satisfies the hypotheses of the lemma, and, by what we have shown above, there is an automorphism $\sigma$ of $W$ (as a module) such that

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

for all \( x, y \in W \). If \( w_i = \tau^{-i}(v_i) \), then \((w_i)\) is a basis of \( W \), and
\[
\varphi(w_i, w_j) = \varphi'(v_i, v_j), \quad \varphi'(w_i) = \varphi'(v_i).
\]
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 \( \varphi_e, \beta_e \) be the forms obtained from \( \varphi, \beta \) on reducing modulo \( p^e \). Let \( \psi_e \) be the homomorphism of \( V_e \) into its dual defined by the bilinear form \( \varphi_e \), and let \( \varphi = \psi_h \). Then \( \beta \in \text{Im}(\psi) \) if and only if \( d = h \). If \( \beta \notin \text{Im}(\psi) \), then \( d \) is the smallest integer \( \geq 0 \) such that \( \beta_{d+1} \in \text{Im}(\psi_{d+1}) \).

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 \( k \) 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 \( k = \mathbb{Z}/2\mathbb{Z} \).

Proposition 11. — Let \( k \) be a perfect field of characteristic 2, and let \( V \) be a vector space over \( k \) of dimension \( k \). If \( \varphi \) is a non-degenerate non-alternate symmetric bilinear form on \( V \), then precisely one of the following three possibilities holds:

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

(ii) \( V \) is the orthogonal direct sum of subspaces \( W, Z \) with \( W \) two-dimensional, \( \varphi \) non-alternate on \( W \), and \( \varphi \) 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 \( \varphi \) is of type (i). Conversely, any form of type (i) falls in this category.

Case II. — \( A' \) is one-dimensional and 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 \( \varphi \) 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 \((v_i)_{i \in \mathbb{N}} \). Let \((u_i)_{i \in \mathbb{N}} \) be any basis of \( V \) with \( \varphi(u_i, u_i) = 1 \),
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 \( x_i \) with \( x_i \notin X \), and let \( z \) be the \( X' \)-component of \( u_m \). If \( \phi(z, z) = a^2 \neq 0 \), we choose \( v_{n+1} = az \). If \( \phi(z, w) = 0 \), find \( w \in X' \) with \( \phi(z, w) = 1 \). If \( \phi(w, w) = b^2 \neq 0 \), choose \( v_{n+1} = b^{-1} w, v_{n+2} = bz + b^{-1} w \). If \( \phi(w, w) = 0 \), 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 \( u_n \). Conversely, it is easy to see that a form with an orthonormal basis falls under Case III.

**Corollary.** — Let \( \phi \) be of type (i) or (ii), and let \( V \) be the union of an increasing family \( (V_i) \) of finite-dimensional subspaces on which \( \phi \) is non-degenerate. If \( \phi \) is of type (i) [resp. (ii)], then \( \dim(V) \) 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 \( \phi \) is alternate on \( W' \). Now let \( X \) be a finite-dimensional subspace of \( V \) on which \( \phi \) is non-degenerate. If \( W \subset X \), then \( X \) is the orthogonal direct sum of \( W \) and another subspace \( Y \subset W' \). Since \( \phi \) 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

\[
\phi : H^i(G) \times H^i(G) \to H^i(G)
\]

is non-degenerate on each \( V_i \). Choose a basis \( (\xi_i) \) of \( H^i(G) \) such that \( \xi_1, \ldots, \xi_{\aleph_0} \) is a basis of \( V_i \). This choice of basis gives an isomorphism \( \theta : H^i(G) \to (\mathbb{Z}/p\mathbb{Z})^{\aleph_0} \). Let \( F \) be a free pro-\( p \)-group of rank \( \aleph_0 \), and let \( \delta \) be a continuous homomorphism of \( F \) onto \( G \) such that \( \theta = H^i(f) \) (cf. [12], p. I-36). If \( R = \ker(f) \), then \( R = (r) \) with \( r \in F^\vee(F, F) \). We identify \( G \) with \( F/R \) by means of \( f \). Using the duality between the compact group \( F/F^\vee(F, F) = G/G^\vee(G, G) \) and the discrete group \( H^i(G) \), we obtain a generating system \( (\xi_i) \) of \( F/F^\vee(F, F) \) such that \( \xi_i(\xi_j) = \delta_{ij} \).

Now let \( \sigma : F/F^\vee(F, F) \to F \) be a continuous section, sending \( \sigma \) into \( 1 \) (cf. [12], p. I-2, prop. 1). If \( x = \sigma(\xi_i) \), then \( (x_i) \) is a basis of \( F \). Now let \( f_i : F \to F \) be the continuous homomorphism defined by \( f_i(x_i) = x_i \) if \( 1 \leq i \leq n \), \( f_i(x_i) = 1 \) if \( i > n \). If \( n_i = \dim(V_i) \), let \( F_i = \text{Im}(f_i) \), \( r_i = f_i(r) \), \( G_i = F_i/(r_i) \), and let \( \psi_i : G \to G_i \) be the homomorphism
induced by \( f_n \). We shall show that the closed normal subgroups
\( H_i = \ker(\phi_i) \) are the ones required. If \( g_i \) is the image of \( x_i \) in \( G \), then \( \ker(\phi_i) \) is the closed normal subgroup of \( G \) generated by the \( g_j \) with \( j > n_i \). Hence \( H_{i+1} \subset H_i \). Since \( g_i \rightarrow 1 \) as \( i \rightarrow \infty \), it also follows
that the \( H_i \) intersect in the identity. It remains to show that \( G_i = G/H_i \) is a Demushkin group of finite rank. To do this, we use the commutative diagram

\[
\begin{array}{ccc}
H^1(G) \times H^1(G) & \longrightarrow & H^2(G) \\
\uparrow & & \uparrow \\
H^1(G_i) \times H^1(G_i) & \longrightarrow & H^2(G_i)
\end{array}
\]

where the vertical arrows are the inflation homomorphisms. The homomorphism \( \text{Inf} : H^1(G_i) \rightarrow H^1(G) \) maps \( H^1(G_i) \) isomorphically onto \( V_i \). Since the cup product \( \varphi \) is non-degenerate on \( V_i \), the above diagram shows that \( \text{Inf} : H^2(G_i) \rightarrow H^2(G) \) 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 :

\[
H^1(G_i) \times H^1(G_i) \rightarrow H^2(G_i)
\]

is non-degenerate. Hence \( G_i \) is a Demushkin 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 \( s_0 \). Then \( cd(G) \leq 2 \). If \( cd(G) < 2 \), then \( G \) is a free pro-\( p \)-group (cf. [12], p. 1-37). So assume that \( cd(G) = 2 \). Since \( H^1(G) \) is the direct limit of the one-dimensional subspaces \( H^1(G_i) \), it follows that \( \text{Inf} : H^3(G_i) \rightarrow H^3(G) \) 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 \( H^1(G) \) in \( H^1(G) \) under the inflation map, the commutative diagram then shows that the cup product \( \varphi : H^1(G) \times H^1(G) \rightarrow H^2(G) \) is non-degenerate on \( V_i \). Since \( H^1(G) \) is the union of the \( V_i \), it follows that \( \varphi \) is non-degenerate. Hence \( G \) is a Demushkin group.

3.2. **Proof of Theorem 2.** — To prove (i), it suffices to consider the case \( G \) is of rank \( s_0 \) (cf. [11], p. 252-309). Let \( U \) be an open subgroup
of the Demushkin 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
Demushkin 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 Demushkin group \( G/H_i \). Since \( G/H_i \) is of
finite rank \( \neq 1 \), it follows that \( U/U_i \) is a Demushkin 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 $H^2(U) \cong H^2(V) \cong \mathbb{Z}/p\mathbb{Z}$. But, if $U \neq V$ and

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

is the restriction homomorphism, we have

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

It follows that $\text{Res}$ 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 $\aleph_0$; $r \in F^c(F, F)$; $G = F/(r)$ 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 $x = (x_i)_{i \in \mathbb{N}}$ is a basis of $F$, let

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

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

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

\[
H^1(G, \mathbb{Z}/p^n\mathbb{Z}) \times H^1(G, \mathbb{Z}/p^n\mathbb{Z}) \to H^2(G, \mathbb{Z}/p^n\mathbb{Z})
\]

and passing to the limit we obtain a cup product:

\[
H^1(G, \mathbb{Z}_p) \times H^1(G, \mathbb{Z}_p) \to H^2(G, \mathbb{Z}_p)
\]

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

If \( (x_i) \) is a basis of \( F \), then

\[
r \equiv \prod_{i < j} (x_i, x_j)^{x_{ij}} \quad \text{(mod } F_0)\text{,}
\]

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

**Lemma 1.** — The cup product \( H^1(G, \mathbb{Z}_p) \times H^1(G, \mathbb{Z}_p) \to H^2(G, \mathbb{Z}_p) = \mathbb{Z}_p \) is alternating and \( \gamma^i \cup \gamma^j = a_{ij} \) if \( i < j \).

**Proof.** — If \( z_m \) is the canonical homomorphism of \( \mathbb{Z}_p \) onto \( \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}/p^n\mathbb{Z} \), let \( \gamma^i(z_m) = z_m \circ \gamma^i \), \( a_{ij} = z_m(a_{ij}) \). Then, by Proposition 8, \( \gamma^i(z_m) \cup \gamma^j(z_m) = 0 \) and \( \gamma^i(z_m) \cup \gamma^j(z_m) = a_{ij} \) if \( i < j \). It follows that \( \gamma^i \cup \gamma^j = 0 \) and \( \gamma^i \cup \gamma^j = a_{ij} \) for \( i < j \).

Q. E. D.

The basis \( (\gamma^i) \) of \( H^1(G, \mathbb{Z}_p) \) is said to be a symplectic basis if \( \gamma^i \cup \gamma^j = -\delta_{ij} \) for all \( i, j \). The existence of a symplectic basis of \( V = H^1(G, \mathbb{Z}_p) \) 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 \( \mathbb{Z}/p^n\mathbb{Z} \)-module of rank \( n \) with an alternating form \( \varphi \). If \( (\gamma^i) \) is a symplectic basis of \( M/p^{n+1}M \), there exists a symplectic basis of \( F \) lifting \( (\gamma^i) \).

**Proof.** — Let \( (\gamma^i) \) be a basis of \( M \) lifting the symplectic basis \( (\gamma^i) \). Then \( \varphi(\gamma^i, \gamma^j) = 1 + p^{n-1}u_{ij} \) for \( i \geq 1 \) and \( \varphi(\gamma^i, \gamma^j) = p^{n-1}u_{ij} \)
for all other $i, j$ with $i \leq j$. Replacing $\gamma'_i$ by $(1 + p^{n-1}u)\gamma'_i$, we may assume that $\varphi(\gamma'_i, \gamma'_i) = 1$ for all $i \geq 1$. Then the basis $(\gamma'_i)$, where
\[
\gamma'_i = \gamma'_i + \sum_{j < i/2} \varphi(\gamma'_i, \gamma'_{2j-1}) \gamma'_{2j} + \varphi(\gamma'_i, \gamma'_i) \gamma'_{2j-1}
\]
is the required symplectic basis of $M$.

Q. E. D.

The existence of a basis $x = (x_i)$ of $F$ such that $r = r_n(x) \pmod{F_n}$ now follows from lemmas 1 and 2 and the following lemma:

**Lemma 3.** — If $(x_i) \in \mathbb{Z}$ is a basis of $H^1(G, \mathbb{Z}_p)$, there exists a basis $(x_i)$ of $F$ such that $r_n(x_i) = 0$.

**Proof.** — If $\varepsilon_m$ is the canonical homomorphism of $\mathbb{Z}_p$ onto $\mathbb{Z}/p^n\mathbb{Z}$, let $\gamma^m_i = \varepsilon_m \circ \gamma_i$. Using the duality between the compact groups $F/F_{m+1}(F, F)$ and the discrete group $H^1(F, \mathbb{Z}/p^n\mathbb{Z})$, we obtain a generating system $(\gamma^m_i)$ of $F/F_{m+1}(F, F)$ such that $\gamma^m_i(\gamma^m_j) = 0$. Since $F/F_{m+1}(F, F) = \lim_{m \to \infty} F/F_{m+1}(F, F)$ and the image of $\gamma^m_i$ is $\gamma_i$ in $F/F_{m+1}(F, F)$. Moreover, it is easy to see that $(\varepsilon_m)$ is a basis of $F/F_{m+1}(F, F)$. If $\sigma : F/F_{m+1}(F, F) \to F$ is a continuous section such that $\sigma(0) = 1$ and if $x_i = \sigma(\gamma_i)$, 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 $r = r_n(x)$ modulo $F_{n+1}$ for some $n \geq 2$. If $(l_i) \in \mathbb{N}$ is a family of elements of $F_n$ with $l_i \to 1$, and if $y_i = x_i l_i^{-1}$, then $y = (y_i)$ is a basis of $F$ and $r_n(x) = r_n(y) d_n$ with $d_n \in F_{n+1}$. If $\tau_i$ (resp. $\varepsilon_i$) is the image of $l_i$ (resp. $x_i$) in $\text{gr}_n(F)$ [resp. $\text{gr}_1(F)$], then, using (8), we see that the image of $d_n$ in $\text{gr}_{n+1}(F)$ is
\[
\delta_n(\tau) = \sum_{l \geq 1} \left( [\tau_{2l-1}, \tau_{2l}] + [\tau_{2l-1}, \varepsilon_{2l}] \right),
\]
where $\tau = (\tau_i)$. If $W_n$ is the submodule of $V_n = \text{gr}_n(F) \mathbb{N}$ consisting of those families $\tau = (\tau_i)$ with $\tau_i \to 0$, we obtain a homomorphism $\delta_n : W_n \to \text{gr}_{n+1}(F)$.

If $\Delta_n : V_n \to \text{gr}_n(F)$ is defined by
\[
\Delta_n(\tau) = \sum_{l \geq 1} [\varepsilon_l, \tau_l],
\]
then $\Delta_n(W_n) = \text{Im}(\delta_n)$, and, by the corollary to Proposition 4, we have $\Delta_n(W_n) = \text{gr}_{n+1}(F)$. Consequently $\delta_n$ is surjective. Hence if
\[ r = r_n(x) e_{n+1} \text{ with } e_{n+1} \in F_{n+1}, \] we may choose \( \tau = (\tau_i) \in W_n \) so that
\[ \varepsilon_{n+1} = \delta_n(\tau), \] where \( \varepsilon_{n+1} \) is the image of \( e_{n+1} \) in \( \gr_{n+1}(F) \). If \( \sigma : \gr_n(F) \to F_n \) 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 \( r \equiv r_n(y) \pmod{F_{n+2}} \).

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

Q. E. D.

4.2. The Case \( q \neq 0, 2 \). — If \( V = H^1(G, \mathbb{Z}/q\mathbb{Z}) \), then \( V \) is free \( \mathbb{Z}/q\mathbb{Z} \)-module of rank \( k \), and the cup product
\[ H^1(G, \mathbb{Z}/q\mathbb{Z}) \times H^1(G, \mathbb{Z}/q\mathbb{Z}) \to H^1(G, \mathbb{Z}/q\mathbb{Z}) = \mathbb{Z}/q\mathbb{Z} \]
is a bilinear form on \( V \) whose reduction modulo \( p \) is non-degenerate.

If \( \beta \) is the linear form on \( V \) defined in Proposition 8, then \( \gamma \cup \gamma = \left( \begin{array}{c} q \\ 2 \end{array} \right) \beta(\gamma) \) for any \( \gamma \in V \). Moreover, \( \beta(V) = \mathbb{Z}/q\mathbb{Z} \) since \( r \in F_{0+1}(F, F) \). Since \( q \neq 2 \), we may apply Proposition 10 to obtain a basis \( (\gamma_i) \) of \( V \) and an integer \( d \) with \( 0 \leq d \leq h \) such that
\begin{enumerate}
  \item \( \beta(\gamma_i) = 1 \), \( \beta(\gamma_{2j}) = 0 \), and \( \beta(\gamma_{2j-1}) = p^j \), \( \beta(\gamma_{2i}) = 0 \) for \( i \geq 2 \).
  \item \( \gamma_{2i-1} \cup \gamma_{2i-1} = 1 \) for \( i \geq 1 \), and \( \gamma_i \cup \gamma_j = 0 \) for all other \( i, j \) with \( i < j \).
\end{enumerate}

Let \( (x_i) \) be a basis of \( F \) such that \( \gamma_i(x_j) = \delta_{ij} \) and let \( (F_i) \) be the descending \( q \)-central series of \( F \). Then by Proposition 8 we have
\[ r \equiv x_i^* (x_1, x_2) \prod_{l \geq z} x_{2l-1 \choose 2l} (x_{2l-1}, x_{2l}) \pmod{F_z}. \]

Now suppose that for some \( n \geq 2 \), we have found a basis \( (x_i) \) of \( F \) and integers \( a_i \) with \( q \mid a_{2l-1}, q^2 \mid a_{2l} \) such that
\[ r = x_i^* (x_1, x_2) \prod_{l \geq z} x_{2l-1 \choose 2l} (x_{2l-1}, x_{2l}) e_{2l}, \]
where \( e_{2l} \in F_{2l+1} \), 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 \( (t_i) \in \mathbb{N} \) 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
\[ r = y_i^* (y_1, y_2) \prod_{l \geq z} x_{2l-1 \choose 2l} (x_{2l-1}, x_{2l}) d_n e_{2l-1}, \]
where \( d_n \in F_{n+1} \). If \( \tau_i \) (resp. \( \tilde{\tau}_i \)) is the image of \( t_i \) (resp. \( x_i \)) in \( \text{gr}_n(F) \) [resp. \( \text{gr}_i(F) \)], then, using (8) together with Proposition 6, we see that the image of \( d_n \) in \( \text{gr}_{n+1}(F) \) is

\[
\hat{\delta}_n(\tau) = \pi \tau_1 + \left( \begin{array}{c} q \\ 2 \end{array} \right) [\tau_1, \tilde{\tau}_1] + [\tau_1, \tilde{\tau}_2] + [\tilde{\tau}_1, \tau_2] + \sum_{i \geq 2} (p^i \pi \tau_{2i-1} + p^i \left( \begin{array}{c} q \\ 2 \end{array} \right) [\tau_{2i-1}, \tilde{\tau}_{2i-1}]) + \sum_{i \geq 2} ([\tau_{2i-1}, \tilde{\tau}_{2i}] + [\tilde{\tau}_{2i-1}, \tau_{2i}]).
\]

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

**Lemma.** — If \( E \) is the closed subgroup of \( \text{gr}_i(F) \) generated by the elements \( \pi \tilde{\tau}_j \) with \( j \neq 1, 2 \), then

\[
\text{gr}_{i+1}(F) = \text{Im}(\hat{\delta}_n) + \pi^{n-1} E.
\]

Moreover, if \( p^i = q \), then \( \pi^n \tilde{\tau}_j \in \text{Im}(\hat{\delta}_n) \) for all \( j \).

**Proof.** — If \( \Delta_n : V_n \to \text{gr}_{n+1}(F) \) is the homomorphism defined by

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

we have \( \text{Im}(\hat{\delta}_n) = \Delta_n(W_n) + \pi \text{gr}_n(F) \). By the Corollary to Proposition 7 we have

\[
\text{gr}_{n+1}(F) = \Delta_n(W_n) + \pi \text{gr}_n(F).
\]

Hence, \( \text{gr}_{n+1}(F) = \text{Im}(\hat{\delta}_n) + \pi \text{gr}_n(F) \). Since \( \pi \text{Im}(\hat{\delta}_{m-1}) \) is contained in \( \text{Im}(\hat{\delta}_m) \) for \( m \geq 3 \), it follows that

\[
\text{gr}_{n+1}(F) = \text{Im}(\hat{\delta}_n) + \pi^{n-1} \text{gr}_i(F).
\]

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

\[
\pi \text{gr}_i(F) = \pi D + \Delta_i(W_i) + p \text{gr}_i(F),
\]

where \( D \) is the closed subgroup of \( \text{gr}_i(F) \) generated by the elements \( \pi \tilde{\tau}_j \). Hence,

\[
\text{gr}_{n+1}(F) = \text{Im}(\hat{\delta}_n) + \pi^{n-1} D + p \text{gr}_{n-1}(F).
\]

Since \( \pi^n \tilde{\tau}_2 = \hat{\delta}_n(\tau) \), where \( \tau_1 = \pi^{n-1} \tilde{\tau}_2 \), \( \tau_2 = \left( \begin{array}{c} q \\ 2 \end{array} \right) \tau_1 \), \( \tau_i = 0 \) otherwise, and \( \pi^n \tilde{\tau}_1 = \hat{\delta}_n(\tau) \), where

\[
\tau_1 = \pi^{n-1} \tilde{\tau}_1 + \left( \begin{array}{c} q \\ 2 \end{array} \right) \pi^{n-2} [\tilde{\tau}_1, \tau_1],
\]

\[
\tau_2 = \left( \begin{array}{c} q \\ 2 \end{array} \right) \tau_1 + \left( \begin{array}{c} q \\ 2 \end{array} \right) \pi^{n-2} [\tilde{\tau}_1, \tau_2] - \pi^{n-1} \tilde{\tau}_2 + \left( \begin{array}{c} q \\ 2 \end{array} \right) \pi^{n-1} \tilde{\tau}_2,
\]

\( \tau_i = 0 \) for \( i \neq 1, 2 \),
we see that \((\text{ii})\) is true modulo \(p\). Since \(\text{Im}(\delta_n) + \pi^{n-1} E\) is a subgroup of \(gr_{n+1}(F)\), it follows that \((\text{io})\) is true modulo \(p^i\) for any \(i \in \mathbb{N}\). Since \(p^i gr_{n+1}(F) = 0\), the result follows.

Now suppose that \(p^i = q\). If \(\Delta'_n : V_n \to gr_{n+1}(F)\) is defined by

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

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

\[
\tau_2 = \pi^{n-1} \xi_j + \left(\frac{q}{2}\right) \pi^{n-2} [\xi_j, \xi_j],
\]

\[
\tau_j = \left(\frac{q}{2}\right) \pi^{n-2} [\xi_j, \xi_j] + \left(\frac{q}{2}\right) \pi^{n-3} \xi_j + \pi^{n-1} \xi_j,
\]

\[
\tau_i = 0 \quad \text{for} \quad i \neq 2, j.
\]

This completes the proof of the lemma.

Returning to \((\text{io})\), the above lemma allows us to choose the \(t_i\) so that

\[
d_n e_{n+1} = \prod_{i \geq 2} y_i^{q^i} e_i \pmod{F_{n+2}}.
\]

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

\[
r = y_i^{q_i}(g, y_i) \prod_{i \geq 2} y_i^{b_{i-1}} y_i^{b_i}(y_{2i-1}, y_{2i}) \pmod{F_{n+2}},
\]

where \(b_i = a_i + q^i a_i\), 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

\[
r = x_i^e(x_i, x_i) \prod_{i \geq 2} x_{2i-1}^{a_{2i-1}} x_{2i}^{a_{2i}} (x_{2i-1}, x_{2i}),
\]

where \(a_i \in \mathbb{Z}_p\) 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 \(n_i = 2\) 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

\[
r_i = \prod_{n_i \leq j \leq n_{i+1}} x_j^{a_{2j-1}} x_j^{a_{2j}} (x_{2j-1}, x_{2j}),
\]
where \( u_i = (n_i + \alpha)/2, \) \( v_i = n_i + 1/2, \) then \( r_i \) is a Demuškin relation in the variables \( x_i, \) \( n_i < j \leq n_{i+1}. \) The corresponding Demuškin group \( G_i \) is of finite rank with \( q(G_i) = p^t \neq \alpha. \) 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

\[
    r_i = \prod_{j_i < j \leq v_i} x_j^{r_{j-1}}(x_{j-1}, x_j).
\]

Since \( r = x_r^{r}(x_1, x_2) \prod r_i, \) this completes the proof of case 2.

4.3. The Case \( q = 2, t = 1. \) — Let \( (F, \alpha) \) be the descending 2-central series of \( F. \) By the definition of the invariant \( t = l(G) \) together with Propositions 8, 9 and 11, there exists a basis \( (\gamma_i) \) of \( H^t(G) \) such that \( \gamma_i \cup \gamma_{i+1} = 1, \) \( \gamma_{i-1} \cup \gamma_{i+1} = 1 \) for \( i \geq 1, \) and \( \gamma_i \cup \gamma_j = 0 \) for all other \( i, j \) with \( i \leq j. \) If \( x = (x_i) \) is a basis of \( F \) with \( \gamma_i(x_i) = \delta_i, \) then, by Proposition 8, we have

\[
    r = x^r(x_1, x_2) r_0(x) \quad \text{(mod } F_3),
\]

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 \( a_i \in \mathbb{Q} \) such that

\[
    r = x_{1+a_1}(x_1, x_2) r_0(x) \prod x_i^{a_i} e_{n+1}
\]

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

(12) \[
    r = y_1^{a_1}(y_1, y_2) r_0(y) \prod y_i^{a_i} d_i e_{n+1}
\]

with \( d_i \in F_{n-1}. \) If \( \tau_i \) (resp. \( z_i \)) is the image of \( t_i \) (resp. \( x_i \)) in \( \text{gr}_n(F) \) [resp. \( \text{gr}_i(F) \)], then the image of \( d_i \) in \( \text{gr}_{n+1}(F) \) is

\[
    \delta_i(\tau) = \pi \tau_i + [\tau_i, z_i] + \sum_{i \geq 1} ([\tau_{2i-1}, z_{2i}] + [\zeta_{2i-1}, \tau_{2i}]).
\]

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

**Lemma.** — *If \( E \) is the closed subgroup of \( \text{gr}_n(F) \) generated by the elements \( \pi z_i \) with \( j \neq 2, \) then \( \text{gr}_{n+1}(F) \) is generated by \( \text{Im}(\delta_n) \) and \( \pi^{n-1} E. \)
Proof. — Using the Corollary to Proposition 7, we see that

\[ \text{gr}_{n+1}(F) = \text{Im}(\partial_n) + \pi \text{gr}_n(F). \]

Since \( \pi \text{ Im}(\partial_{m-1}) \subset \text{Im}(\partial_m) \) for \( m \geq 3 \), it follows that \( \text{gr}_{n+1}(F) \) is generated by \( \text{Im}(\partial_n) \) and \( \pi^{n-1} \text{gr}_1(F) \). Hence, to prove the lemma, it suffices to show that \( \pi^n \mathfrak{z}_n \in \text{Im}(\partial_n) \) and

\[ \sum_{i<j} a_{ij} \pi [\mathfrak{z}_i, \mathfrak{z}_j] \in \text{Im}(\partial_n) + \pi E \]

for arbitrary \( a_{ij} \in \mathbb{Z}/2\mathbb{Z} \).

If \( \tau = (\tau_i) \), where \( \tau_1 = \pi \mathfrak{z}_1, \tau_2 = \tau_1, \tau_i = 0 \) for \( i \geq 3 \), then \( \tau \in W_2 \) and \( \partial_2(\tau) = \pi \mathfrak{z}_2 \). Hence \( \pi \mathfrak{z}_2 \in \text{Im}(\partial_2) \). Now let \( \Delta : W_2 \to \text{gr}_2(F) \) be defined by

\[ \Delta(\tau) = \pi \tau_2 + \sum_{i \geq 1} [\mathfrak{z}_i, \tau_i]. \]

Then clearly \( \text{Im}(\partial_n) = \text{Im}(\Delta) \). Let \( \tau = (\tau_i) \), where

\[
\begin{align*}
\tau_1 &= a_{12}[\mathfrak{z}_1, \mathfrak{z}_2] + \sum_{j \geq 3} a_{1j} \pi \mathfrak{z}_j, \\
\tau_2 &= a_{12} \pi \mathfrak{z}_1 + \sum_{j \geq 3} a_{2j} \pi \mathfrak{z}_j, \\
\tau_i &= \sum_{j \geq 1} a_{ij} \pi \mathfrak{z}_j + \sum_{j < i} a_{ji} [\mathfrak{z}_j, \mathfrak{z}_i] \quad \text{for} \quad i \geq 3.
\end{align*}
\]

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

\[ \Delta(\tau) = a_{12} \pi^2 \mathfrak{z}_1 + \sum_{j \geq 3} a_{2j} \pi^2 \mathfrak{z}_j + \sum_{i<j} a_{ij} [\mathfrak{z}_i, \mathfrak{z}_j]. \]

Hence \( \sum_{i<j} a_{ij} [\mathfrak{z}_i, \mathfrak{z}_j] \in \text{Im}(\Delta) + \pi E \).

Q. E. D.

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

\[ r = y_1^{t_1 + b_1}(y_1, y_2) y_2(y) \prod_{i \geq 3} y_i^{b_i}(\text{mod } F_{n+1}), \]

with \( b_i \in \mathbb{Z}, b_i = a_i \pmod{2^n} \).
Proceeding inductively and passing to the limit, we see that there exists a basis \((x_i)\) of \(F\) and \(\mathbb{Z}_2\)-adic integers \(a_i\) with \(v_2(a_i) \geq 2\) such that
\[
r = x_1^{a_1} \otimes (x_2, x_3) r_3(x) \prod_{i \geq i} x_i^{a_i}.
\]

The relation \(r_i = r_3(x) \prod_{i \geq i} x_i^{a_i}\) is a Demuškin relation in the variables \(x_i\), \(i \geq 3\), 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 \(x_i, i \geq 3\), so that
\[
r_i = x_i^f (x_3, x_4) \prod_{i \geq i} x_i^{a_i} (x_{2i-1}, x_{2i}),
\]
where \(s = 2^e, e, f \in \mathbb{N}, 2 \leq f \leq e\). If
\[
r_2 = x_1^{a_1} (x_1, x_2) x_3^f (x_5, x_6),
\]
then \(r_2\) is a Demuškin relation in the variables \(x_1, \ldots, x_6\), 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 \(f \leq v_2(a)\), we can choose \(x_1, \ldots, x_6\), so that
\[
r_1 = x_1^f (x_2, x_3) x_5^f (x_5, x_6).
\]
If \(f > v_2(a) = g\), then we can choose \(x_1, \ldots, x_6\), so that
\[
r_1 = x_1^{-g} (x_2, x_3) (x_5, x_6).
\]
Since \(r = r_1 \prod_{i \geq 3} x_i^{a_i} (x_{2i-1}, x_{2i})\), the proof of Theorem 3 for the case \(q = 2, l = 1\) is complete.

4.4. The Case \(q = 2, l = -1\). — Let \((F_n)\) be the descending \(2\)-central series of \(F\). Since \(l = -1\), then by the definition of \(l\), together with Propositions 9 and 11, there exists a basis \((x_i)\) of \(H'(G)\) such that \(\gamma_i \cup \gamma_{i+1} = 1\), \(\gamma_i \cup \gamma_{2i-1} = 1\) for \(i \geq 1\), and \(\gamma_i \cup \gamma_j = 0\) for all other \(i, j\) with \(i \leq j\). If \((x_i)\) is a basis of \(F\) with \(\gamma_i(x_i) = \delta_{ij}\), then, by Proposition 8, we have \(r = r_0(x)\) modulo \(F_n\), where
\[
r_0(x) = x_1^f (x_{2i}, x_{2i+1}).
\]

Now assume that, for some \(n \geq 2\), we have found a basis \(x = (x_i)\) of \(F\) and integers \(a_i\) with \(a_i \in \mathbb{Z}\) such that
\[
r = r_0(x) \prod_{i \geq 2} x_i^{a_i} \quad (\text{mod } F_{n+1}).
\]
Then, proceeding exactly as in the previous section, we obtain a homomorphism \( \hat{\phi}_n : W_n \rightarrow \text{gr}_{n+1}(F) \), where

\[
\hat{\phi}_n(\tau) = \pi \tau_1 + \sum_{i \geq 1} (\tau_{2i}, \zeta_i) + \sum_{i \geq 1} \left( [\tau_{2i}, \zeta_{2i+1}] + [\zeta_{2i}, \tau_{2i+1}] \right).
\]

**Lemma.** — If \( E \) is the closed subgroup of \( \text{gr}_{n}(F) \) generated by the elements \( \pi \zeta_j \) with \( j \neq 1 \), then \( \text{gr}_{n+1}(F) \) is generated by \( \text{Im}(\hat{\phi}_n) \) 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:

\( \pi^{i-1} \zeta_1 = \hat{o}_i(\tau) \), where \( \tau_1 = \pi \zeta_1 \) and \( \tau_i = 0 \) for \( i \geq 2 \); the homomorphism \( \Delta \) is defined by

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

and we have

\[
\Delta(\tau) = \sum_{i \geq 2} a_i \pi^{i-1} \zeta_i + \sum_{i < j} a_{ij} \pi [\zeta_i, \zeta_j]
\]

if we let

\[
\tau_1 = \sum_{j \geq 2} a_j \pi \zeta_j,
\]

\[
\tau_i = \sum_{j > i} a_i \pi \zeta_j + \sum_{j < i} a_{ij} [\zeta_i, \zeta_j] \quad \text{for} \quad i \geq 2.
\]

This completes the proof of the lemma.

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

\[
r = r_0(y) \prod_{i \geq 2} y_i^{b_i} \quad (\text{mod } F_{n+2}),
\]

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

\[
r_i = \prod_{i \geq 1} (x_{2i}, x_{2i+1}) \prod_{i \geq 2} x_i^{b_i}.
\]

The relation \( r_i \) 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 \( x_1 \) so that

\[
r_1 = x_2^{a_1}(x_2, x_3) \prod_{i \geq 2} x_1^{b_1}(x_{2i}, x_{2i+1}),
\]
where \( s = p^r, \ e, f \in \mathbb{N}, \ e \geq f \geq a. \) 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 \( (\gamma_j) \) of \( H^1(G). \) Replacing \( \gamma_{zi} \) by \( \gamma_{zi} + \gamma_{zi-1}, \) we obtain a basis \( (\gamma_j) \) of \( H^1(G) \) such that

\[
\gamma_{zi-1} \cup \gamma_{zi-1} = \gamma_{zi-1} \cup \gamma_{zi} = 1 \quad \text{and} \quad \gamma_j \cup \gamma_j = 0
\]

for all other \( i, j \) with \( i \leq j. \) If \( x = (x) \) is a basis of \( F \) with \( \gamma_j(x) = \hat{\delta}_j, \) then, by Proposition 8, we have \( r \equiv r_0(x) \) modulo \( F_a, \) where

\[
r_0(x) = \prod_{t \geq 1} x^2_{zi-1} (x_{zi-1}, x_{zi}).
\]

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

\[
r \equiv r_0(x) \prod_{i < j} (x_{ni}, x_j)^{a_{ij}} \pmod {F_{n+1}}.
\]

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

\[
\sum_{t \geq 1} (\zeta_{zi-1} + [\zeta_{zi-1}, \zeta_{zi}] + [\zeta_{zi-1}, \tau_{zi}] + [\zeta_{zi-1}, \zeta_{zi}]).
\]

**Lemma.** — If \( E \) is the closed subgroup of \( \text{gr}_z(F) \) generated by the elements \( [\zeta_i, \zeta_j], \) then \( \text{gr}_{n+1}(F) \) is generated by \( \text{Im}(\delta_n) \) and \( \pi^{n-1} E. \)

**Proof.** — Since \( \text{gr}_{n+1}(F) = \text{Im}(\delta_n) + \pi \text{gr}_z(F) \) by the Corollary to Proposition 7, it follows that \( \text{gr}_{n+1}(F) \) is generated by \( \text{Im}(\delta_n) \) and \( \pi^{n-1} \text{gr}_z(F). \) Hence, it suffices to show that any element of the form \( \sum a_i \pi^z \zeta_i \) belongs to \( \text{Im}(\delta_z) + \pi E. \) If \( \Delta : W_z \to \text{gr}_z(F) \) is defined by

\[
\Delta(\tau) = \sum_{t \geq 1} \pi \tau_{zi-1} + \sum_{t \geq 1} [\zeta_i, \tau],
\]

then \( \text{Im}(\Delta) = \text{Im}(\delta_z). \) Now let \( \tau = (\tau), \) where

\[
\tau_{zi-1} = a_{zi-1} \pi \zeta_{zi-1} + a_{zi} \pi \zeta_{zi}, \quad \tau_{zi} = a_{zi} [\zeta_{zi-1}, \zeta_{zi}].
\]
Then \( \tau \in W_2 \), and a simple calculation using Proposition 6 shows that

\[
\Delta(\tau) = \sum_{i \geq 1} a_i \pi^i \bar{z}_i + \sum_{i \geq 1} a_i \pi [\bar{z}_{i-1}, \bar{z}_i].
\]

Hence \( \sum_{i \geq 1} a_i \pi^i \bar{z}_i \in \text{Im}(\delta_i) + \pi E. \)

Q. E. D.

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

\[
r = r_0(y) \prod_{i < j} (y_i, y_j)^{b_{ij}} \pmod{F_{n+2}},
\]

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

This completes the proof of Theorem 3.


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

\[
\varphi: H^1(G, J) \to H^1(G, J/pJ) = H^1(G)
\]

is surjective. If \( n = \infty \), then \( G \) is said to have the property \( P_n \) with respect to \( \chi \) if the canonical homomorphism

\[
\varphi: H^1(G, J/p^mJ) \to H^1(G, J/pJ) = H^1(G)
\]

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 \( \chi : G \to (\mathbb{Z}_/p^m\mathbb{Z}_p)^* \) such that \( G \) has the property \( P_n \) with respect to \( \chi \).

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

Proposition 12. — Let \( G \) be a pro-p-group of rank \( s \), and let \( \chi : G \to (\mathbb{Z}_/p^m\mathbb{Z}_p)^* \) be a continuous homomorphism. Then the following statements are equivalent:

(a) The group \( G \) has the property \( P_n \) with respect to \( \chi \).
(b) If \((g_i)\) is a minimal generating system of \(G\) and \((a_i)\) is a family of elements of \(J = J(\gamma)\) with \(a_i \rightarrow 0\), 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 \(D_i\) of \(G\) into \(J\) such that \(D_i(g_i) = a_i \mod p\). Suppose that we have found a continuous crossed homomorphism \(D_j\) 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 \(D'(g_i) = b_i \mod p^j\). If \(D_{j+1} = D_j - p^j D'_j\), then \(D_{j+1}\) is a continuous crossed homomorphism of \(G\) into \(J\) such that \(D_{j+1}(g_i) = a_i \mod p^{j+1}\). Proceeding inductively, we see that \(D_n\) is the required crossed homomorphism.

If \(n = \infty\), let \(\gamma_m = \bar{z}_m \circ \gamma\), where \(\bar{z}_m\) is the canonical homomorphism of \(\mathbb{Z}_p / p^n \mathbb{Z}_p\). Then \(G\) has the property \(P_n\) with respect to \(\gamma_m\), and \(J / p^n J = J(\gamma_m)\) where \(J = J(\gamma)\). If \(a^{(m)}_i = \bar{z}_m(a_i)\), then by what we have shown above, there exists a continuous crossed homomorphism \(D^{(m)}\) of \(G\) into \(J / p^n J\) such that \(D^{(m)}(g_i) = a^{(m)}_i\). Passing to the limit, we obtain the required crossed homomorphism \(D\).

Proposition 13. — Let \(G\) be a Demuškin group of rank \(\aleph_0\) with \(s(G) = p^r\), and let \(\gamma : G \rightarrow (\mathbb{Z}_p / p^n \mathbb{Z}_p)^*\) be the character associated to the dualizing module of \(G\). Then \(G\) has the property \(P_c\) with respect to \(\gamma\).

Proof. — If \(J = J(\gamma)\), then \(I = \text{Hom}(J, Q_p / \mathbb{Z}_p)\) is the dualizing module of \(G\). It follows that \(H^1(G, J / p^n J)\) 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

\[
0 \rightarrow H^1(G, J / p^{n-1} J) \xrightarrow{\gamma} H^2(G, J / p^n J) \rightarrow H^2(G, J / p J) \rightarrow 0
\]

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

\[\text{Ker}(\gamma) = \text{Coker}(H^1(G, J / p^n J) \rightarrow H^1(G, J / p J))\]

which proves the proposition.

5.2. Proof of Theorem 4. — Let \(F\) be a free pro-\(p\)-group of rank \(\aleph_0\), with basis \((x_i)_{i \in \mathbb{N}}\), and let \(r\) be a relation satisfying the hypotheses of the theorem. The fact that \(G = F / (r)\) is a Demuškin 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 \(\gamma\), where \(\gamma\) is the character associated to the dualizing module of \(G\). We do this for a relation of the form (i), the same method applying, with obvious modifications, to relations of the form (2), \ldots, (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

\[
(16) \quad g_i (g_i, g_{i+1}) \prod_{i \geq 2} g_i^{it-1} (g_{2i-1}, g_{2i}) = 1,
\]

where \( q = p^r, s = p^e, e, f \in \mathbb{N} \). Suppose that \( G \) has the property \( P_u \) with respect to some homomorphism \( \theta \). Then, by Proposition 12, there exists a continuous crossed homomorphism \( \delta_i \) of \( G \) into \( J(\theta) \) such that \( \delta_i (g_i) = \delta_i \). Applying \( \delta_i \) to both sides of \( (16) \), we obtain

\[
0 (g_i) \theta (g_i) = 0 (g_i) \theta (g_i) \theta (g_i) = 0 (g_i) = 0,
\]

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

\[
\theta (g_i) = (1 - q)^{-1}.
\]

Similarly, \( \theta (g_i) = (1 - q)^{-1} \) for \( i \geq 2 \). But, since \( \theta \) 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 \( P_u \) with respect to \( \chi \). It also follows that \( G \) has the property \( Q_e \), and that

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

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

\[
\theta_0 (x_i) = (1 - q)^{-1}, \quad \theta_0 (x_i) = 1 \quad \text{otherwise}.
\]

Then \( \theta_0 (r) = 1 \), and \( \theta_0 \) induces a homomorphism \( \theta \) of \( G \) into \( (\mathbb{Z}/p^n \mathbb{Z})^* \). 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 \( \theta \). 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 \( K, \Gamma, G \) be as in the statement of the theorem. Let \( (U_i) \in \mathbb{N} \) be a decreasing sequence of open subgroups of \( \Gamma \) containing \( G \) such that \( \bigcap U_i = G \). 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 $\psi_i$ is surjective and that the subgroups $H_i = \text{Ker}(\psi_i)$ 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 $\zeta_p$, let $K' = K(\zeta_p)$, and let $\Gamma'$ be the Galois group of $\overline{K}/K'$. Then $G$ is a Sylow $p$-subgroup of $\Gamma'$ 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 Demuskin group of rank $[K_i : \mathbb{Q}_p] + 2$, and its dualizing module is $\psi_{p,x} (\text{cf. [12], p. II-30})$. Since $H^1(G)$ is the union of the $H^1(G_i)$, it follows that $G$ is of rank $\mathfrak{s}_0$.

By Theorem 1, we see that $G$ is either a Demuskin 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 Demuskin group. To show that $\psi_{p,x}$ is the dualizing module, it suffices to show that the canonical homomorphism

$$\varphi : H^1(G, \psi_{p,x}) \to H^1(G, \psi_p) = H^1(G)$$

is surjective for $n \geq 1$ (cf. § 5.1). But since $\psi_{p,x}$ is the dualizing module of $G$, we have a commutative diagram

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

in which $\varphi_i$ is surjective for $n \geq 1$. Passing to the limit, we obtain the surjectivity of $\varphi$.

To prove the assertion concerning $t(G)$, it suffices to consider the case $q(G) = 2$, for otherwise $l(G) = 1$ and $[K(\zeta_p) : \mathbb{Q}_p]$ 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 $\dim(V_i) = [K_i : \mathbb{Q}_p] + 2$ and $[K_i : K]$ is odd, we have

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

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 $l(G) = 1$ or $-1$ since $s(G) = 0$. Hence, since $V$ is the union of the $V_i$, it follows from the definition of $l(G)$ together with the proof of Proposition 11 and its Corollary that

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

for $i$ sufficiently large.

Q. E. D.
BIBLIOGRAPHY.


(Manuscrit reçu le 13 juin 1966.)

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