# CLASSIFICATION OF DEMUSHKIN GROUPS

JOHN P. LABUTE

A pro-$p$-group $G$ is said to be a Demushkin group if

(1) $\dim_{\mathbf{F}_p} H^1(G, \mathbf{Z}/p\mathbf{Z}) < \infty$,

(2) $\dim_{\mathbf{F}_p} H^2(G, \mathbf{Z}/p\mathbf{Z}) = 1$,

(3) the cup product $H^1(G, \mathbf{Z}/p\mathbf{Z}) \times H^1(G, \mathbf{Z}/p\mathbf{Z}) \to H^2(G, \mathbf{Z}/p\mathbf{Z})$ is a non-degenerate bilinear form. Here $\mathbf{F}_p$ denotes the field with $p$ elements. If $G$ is a Demushkin group, then $G$ is a finitely generated topological group with $n(G) = \dim H^1(G, \mathbf{Z}/p\mathbf{Z})$ as the minimal number of topological generators; cf. §1.3. Condition (2) means that there is only one relation among a minimal system of generators for $G$; that is, $G$ is isomorphic to a quotient $F/(r)$, where $F$ is a free pro-$p$-group of rank $n = n(G)$ and $(r)$ is the closed normal subgroup of $F$ generated by an element $r \in F^p(F, F)$; cf. §1.4. (If $x, y$ are elements of a pro-$p$-group $H$, we let $(x, y)$ denote the commutator $x^{-1}y^{-1}xy$ and $(H, H)$ the closed subgroup generated by all commutators of $H$.) Hence *$G/(G, G)$ is isomorphic to $(\mathbf{Z}_p)^{n-1} \times (\mathbf{Z}_p/q\mathbf{Z}_p)$, where $q = q(G)$ is a uniquely determined power of $p$.* (By convention $p^\infty = 0$; $\mathbf{Z}_p$ denotes the ring of $p$-adic integers.)

If $q \neq 2$, Demushkin has shown **(1; 2)** that $n$ is even and that there exists a basis $x_1, \ldots, x_n$ of $F$ such that

$$r = x_1^q(x_1, x_2)(x_3, x_4) \ldots (x_{n-1}, x_n). \tag{1}$$

Moreover, for any relation $r$ of the form (1) with $n$ even and $q = p^g$, $g$ being an integer $\geqslant 1$ or $\infty$, the group $G = F/(r)$ is a Demushkin group with $n(G) = n$, $q(G) = q$.

To classify those Demushkin groups for which $q(G) = 2$, Serre **(8)** introduced a new invariant of a Demushkin group $G$ as follows: *There exists a unique continuous homomorphism $\chi$: $G \to \mathbf{U}_p$, the group of units of $\mathbf{Z}_p$, such that, if $I_j(\chi)$ denotes the G-module obtained by letting G act on $\mathbf{Z}/p^j\mathbf{Z}$ by means of $\chi$, the homomorphism $H^1(G, I_j(\chi)) \to H^1(G, I_1(\chi))$ is surjective for $j \geqslant 1$.* The invariant $\mathrm{Im}(\chi)$ makes the invariant $q(G)$ superfluous; in fact, $q = q(G)$ is the highest power of $p$ such that $\mathrm{Im}(\chi) \subset 1 + q\mathbf{Z}_p$; cf. §3. For a relation of the form (1) we have

$$\mathrm{Im}(\chi) = \mathbf{U}_p^{(g)} = 1 + p^g\mathbf{Z}_p \qquad \text{if } q = p^g \neq 2.$$

Received August 4, 1965. This paper is the author's doctoral dissertation submitted to Harvard University. The work was partially supported by N.S.F. Grant GP3512. The author wishes to express his thanks to Professors John Tate and Jean-Pierre Serre for their assistance and encouragement.

If $q(G) = 2$ and $n = n(G)$ is odd, Serre has shown **(8)** that there exists a basis $x_1, \ldots, x_n$ for $F$ such that

$$(2) \qquad r = x_1^2 x_2^{2^f}(x_2, x_3) \ldots (x_{n-1}, x_n)$$

where $f$ is an integer $\geqslant 2$ or $\infty$. Moreover, for any relation $r$ of the form (2) with $n$ odd and $f$ such an integer, the group $G = F/(r)$ is a Demushkin group with $n(G) = n$, $\mathrm{Im}(\chi) = \{\pm 1\} \times \mathbf{U}_2^{(f)}$.

In §3 of this paper we give proofs of the above results as well as a preliminary classification of those Demushkin groups with $q(G) = 2$, $n(G)$ even; cf. Theorem 3. The main section of this paper is §4, in which we prove the following theorem, thus completing the classification of Demushkin groups; cf. **(5)**.

THEOREM 1. *Let $r$ be an element of the free pro-$p$-group $F$ of rank $2N$, with $N \geqslant 1$, and let $G = F/(r)$. Suppose that $G$ is a Demushkin group with invariants $n(G) = 2N$, $q(G) = 2$ and $\mathrm{Im}(\chi) = A$. Then there exists a basis $x_1, \ldots x_n$ of $F$ such that*

$$(3) \qquad r = x_1^{2+2^f}(x_1, x_2)(x_3, x_4) \ldots (x_{2N-1}, x_{2N}) \qquad \text{if } (A:A^2) = 2,$$

*where $f$ is an integer $\geqslant 2$ or $\infty$, or*

$$(4) \qquad r = x_1^2(x_1, x_2)x_3^{2^f}(x_3, x_4) \ldots (x_{2N-1}, x_{2N}) \qquad \text{if } (A:A^2) = 4$$

*where $f$ is an integer $\geqslant 2$. Moreover, for any relation $r$ of the form* (3) (*of the form* (4)) *with $N$ an integer $\geqslant 1$ ($\geqslant 2$), and $f$ an integer $\geqslant 2$ or $\infty$, the group $G = F/(r)$ is a Demushkin group with invariants $n(G) = 2N$, $\mathrm{Im}(\chi) = \mathbf{U}_2^{[f]}$ ($\mathrm{Im}(\chi) = \{\pm 1\} \times \mathbf{U}_2^{(f)}$). Here $\mathbf{U}_2^{[f]}$ is the closed subgroup of $\mathbf{U}_2$ generated by $-1 + 2^f$.*

*Remarks.* (1) If the Demushkin group $G$ is infinite (or, equivalently, if $n(G) \neq 1$), Tate has shown that $G$ is of cohomological dimension two, and hence the character $\chi$ associated with $G$ is nothing but the character associated with the dualizing module of $G$; cf. **(8**, pp. 9–10**)**.

(2) For every pair $(n, A)$ where $n$ is an integer $\geqslant 1$ and $A$ is a closed subgroup of $\mathbf{U}_p^{(1)}$, there is a Demushkin group $G$ with invariants $n(G) = n$, $\mathrm{Im}(\chi) = A$, provided that either

(i) $n$ is even and $p^n > (A:A^p)$, or

(ii) $n$ is odd, $n \geqslant 3$, and $A = \{\pm 1\} \times \mathbf{U}_2^{(f)}$, with $f$ an integer $\geqslant 2$ or $\infty$, or

(iii) $n = 1$, $A = \{\pm 1\}$.

(3) The preceding results imply that two Demushkin groups with the same invariants $n$ and $\mathrm{Im}(\chi)$ are isomorphic; in fact they imply the following stronger theorem concerning relations:

THEOREM 2. *Let $r, r' \in F^p(F, F)$, where $F$ is a free pro-$p$-group, and let $G = F/(r)$, $G' = F/(r')$. Suppose that $G$, $G'$ are Demushkin groups with $\mathrm{Im}(\chi) = \mathrm{Im}(\chi')$. Then there exists an automorphism of $F$ which sends $r$ into $r'$.*

COROLLARY. *If* $(r) = (r')$ *and if the quotient* $F/(r)$ *is a Demushkin group, there is an automorphism of* $F$ *sending* $r$ *into* $r'$.

In §5 we shall use the above results to show that the Galois group of the maximal $p$-extension of a local field $K$ is completely determined by $[K:\mathbf{Q}_p]$ and the intersection $K'$ of the field of $p^N$th roots of unity ($N \to \infty$) with $K$.

On completion of this work I learned that Theorem 1 was also proved by S. Demushkin in his paper *Topological* 2-*groups with an even number of generators and one defining relation* (in Russian), Izvestia Akad. Nauk USSR, *29*, (1965), 3–10. However, Theorem 2 of that paper is incorrect, a counter-example being provided by the example at the end of §5 of our paper. The correct result is given by Theorem 9.

## §1. Preliminaries on profinite groups.

**1.1. Cohomology.** A topological group $G$ is called a *profinite* group if it is the projective limit of finite groups (each having the discrete topology). Such a group is compact and totally disconnected. Conversely, if $G$ is compact and totally disconnected, $G$ has a basis of neighbourhoods of the identity consisting of open normal subgroups $U$, and hence the canonical homomorphism

$$G \to \varprojlim G/U$$

is a bijection, which shows that $G$ is a profinite group.

Let $G$ be a profinite group and let $\mathscr{C}_G$ be a full subcategory of the category of topological $G$-modules $M$, where the abelian groups $M$ are either all discrete or all profinite. By definition the product $g\cdot m$, $g \in G$, $m \in M$, depends continuously on the pair $(g, m)$. An $n$-cochain of $G$ with values in $M$ is a continuous mapping $u$ of the $n$-fold product $G \times \ldots \times G$ into $M$. The coboundary $du$ of the cochain $u$ is defined by the usual formula:

$$du(g_1 \ldots, g_{n+1}) = g_1\cdot u(g_2, \ldots, g_{n+1}) + \sum_{j=1}^{j=n} (-1)^j u(g_1, \ldots, g_{j-1}\, g_{j+1}, \ldots, g_{n+1}) \\ + (-1)^{n+1} u(g_1, \ldots, g_n).$$

In this way we obtain a complex $C(G, M) = \{C^n(G, M)\}$ whose cohomology groups are denoted by $H^n(G, M)$. These groups coincide with the cohomology groups defined by Tate in case $M$ is discrete; cf. **(3)**. The group $H^0(G, M)$ may be identified with the set $M^G$ of elements of $M$ left invariant by $G$. A 1-cocycle $u$ is a continuous "crossed homomorphism" of $G$ into $M$, in other words, a continuous mapping satisfying the identity

$$u(gh) = u(g) + g\cdot u(h), \qquad g, h \in G.$$

It is a coboundary if there exists an element $m \in M$ such that $u(g) = g\cdot m - m$ for all $g \in G$.

Let $0 \to A \to B \to C \to 0$ be an exact sequence in $\mathscr{C}_G$. Then there exists a continuous section $C \to B$ and hence the sequence of complexes

$$0 \to C(G, A) \to C(G, B) \to C(G, C) \to 0$$

is exact. We thus obtain an exact sequence of cohomology groups

$$\ldots \to H^n(G, A) \to H^n(G, B) \to H^n(G, C) \to H^{n+1}(G, A) \to \ldots.$$

Let $F$ be a profinite group and let $R$ be a closed normal subgroup of $F$. Set $G = F/R$ and let the image of $x \in F$ in $G$ be denoted by $\bar{x}$. If $M \in \mathscr{C}_G$, the restriction and inflation homomorphisms

$$\mathrm{Res}: C^n(F, M) \to C^n(R, M), \qquad \mathrm{Inf}: C^n(G, M) \to C^n(F, M)$$

are defined as usual by the formulas

$$\mathrm{Res}\, u(r_1, \ldots, r_n) = u(r_1, \ldots, r_n), \qquad r_i \in R,$$
$$\mathrm{Inf}\, u(x_1, \ldots, x_n) = u(\bar{x}_1, \ldots, \bar{x}_n), \qquad x_i \in F.$$

We then obtain homomorphisms

$$\mathrm{Res}: H^n(F, M) \to H^n(R, M) \quad \text{and} \quad \mathrm{Inf}: H^n(G, M) \to H^n(F, M)$$

on cohomology.

$H^1(R, M)$ becomes an $F$-module if we define

$$(x \cdot u)(r) = xu(x^{-1}rx), \qquad x \in F, r \in R, u \in H^1(R, M).$$

If $F$ acts trivially on $M$, then $x \cdot u = u$ if and only if $u(x^{-1}rx) = u(r)$, that is, if and only if $u(r^{-1}x^{-1}rx) = 0$; hence $u \in H^1(R, M)^F$ if and only if $u$ is a continuous homomorphism of $R$ into $M$ which vanishes on $(F, R)$.

We now let $M \in \mathscr{C}_G$, with the action of $G$ on $M$ trivial, and establish the existence of an exact sequence

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

where tg is the so-called "transgression homomorphism" which we proceed to define below. Let $s: G \to F$ be a continuous section such that $s(1) = 1$ and let $\pi: F \to R$ be defined by $\pi(x) = xs(\bar{x})^{-1}$. Then if $x \in F$, $r \in R$, we have $\pi(r) = r$, $\pi(rx) = r\pi(x)$. Let $u \in H^1(R, M)^F$, $u_0 = u \circ \pi \in C^1(F, M)$, and $v_0 = du_0 \in C^2(F, M)$. If $r, t \in R$, $x, y \in F$, then

$$\begin{aligned} v_0(rx, ty) &= u_0(rx) + u_0(ty) - u_0(rxty) \\ &= u(r) + u_0(x) + u(t) + u_0(y) - u(r) - u_0(xty). \end{aligned}$$

But

$$\begin{aligned} u_0(xty) &= u(\pi(xty)) = u(xty\, s(\bar{x}\bar{y})^{-1}) \\ &= u(xtx^{-1}t^{-1}txy\, s(\bar{x}\bar{y})^{-1}) = u(t) + u_0(xy). \end{aligned}$$

Hence

$$v_0(rx, ty) = u_0(x) + u_0(y) - u_0(xy) = v_0(x, y),$$

which implies the existence of a unique 2-cocycle $v \in C^2(G, M)$ such that $v_0 = \mathrm{Inf}(v)$. We let $\mathrm{tg}(u)$ be the class of $v$ in $H^2(G, M)$. It is easy to show that $\mathrm{tg}(u)$ is independent of the choice of $s$.

The exactness of

$$0 \to H^1(G, M) \to H^1(F, M) \to H^1(R, M)^F$$

is clear, and

(i) $\mathrm{tg} \circ \mathrm{Res} = 0$: If $u = \mathrm{Res}(t)$ with $t \in H^1(F, M)$, then

$$\begin{aligned} v_0(x, y) = d(u \circ \pi)(x, y) &= u(xs(\bar{x})^{-1}) + u(ys(\bar{y})^{-1}) - u(xys(\bar{x}\bar{y})^{-1}) \\ &= -(u \circ s(\bar{x}) + u \circ s(\bar{y}) - u \circ s(\bar{x}\bar{y})). \end{aligned}$$

If $v_0 = \mathrm{Inf}(v)$, then

$$v(\bar{x}, \bar{y}) = v_0(x, y) = -d(u \circ s)(\bar{x}, \bar{y})$$

which implies that $\mathrm{tg}(u) = 0$.

(ii) $\mathrm{Ker}(\mathrm{tg}) \subset \mathrm{Im}(\mathrm{Res})$: Let $u \in H^1(R, M)^F$ with $\mathrm{tg}(u) = 0$. Then if $u_0 = u \circ \pi$, there is a 1-cochain $w \in C^1(G, M)$ such that if $v_0 = du_0$ and $v_0 = \mathrm{Inf}(v)$, then $v = dw$. If $w_0 = \mathrm{Inf}(w)$, then $v_0 = dw_0$, that is,

$$u_0(x) + u_0(y) - u_0(xy) = w_0(x) + w_0(y) - w_0(xy).$$

Hence if $t = u_0 - w_0$, then $t \in H^1(F, M)$ and

$$t(r) = u_0(r) - w_0(r) = u(r)$$

for all $r \in R$, that is, $u = \mathrm{Res}(t)$.

(iii) $\mathrm{Inf} \circ \mathrm{tg} = 0$: Immediate from the definition of tg.

(iv) $\mathrm{Ker}(\mathrm{Inf}) \subset \mathrm{Im}(\mathrm{tg})$: Let $a \in H^2(G, M)$ with $\mathrm{Inf}(a) = 0$. Let $v$ be a 2-cocycle representing $a$ such that $v(1, g) = v(g, 1) = 0$ for all $g \in G$. Then, if $v_0 = \mathrm{Inf}(v)$, we have

$$v_0(x, y) = u'(x) + u'(y) - u'(xy)$$

for some $u' \in C^1(F, M)$. If $u = \mathrm{Res}(u')$, then $u(rt) = u(r) + u(t)$ for all $r, t \in R$, and if $x \in F$, $r \in R$, we have

$$\begin{aligned} u(rxr^{-1}x^{-1}) &= u(r) + u(xr^{-1}x^{-1}) = u(r) + u(x) + u(r^{-1}x^{-1}) - v_0(x, r^{-1}x^{-1}) \\ &= u(r) + u(x) + u(r^{-1}) + u(x^{-1}) - v_0(r^{-1}, x^{-1}) - v_0(x, r^{-1}x^{-1}) \\ &= u(x) + u(x^{-1}) - v_0(x, x^{-1}) = u'(xx^{-1}) = u'(1) = 0. \end{aligned}$$

Hence $u \in H^1(R, M)^F$. If $u_0 = u \circ \pi$, then

$$\begin{aligned} (u' - u_0)(x) = u'(x) - u'(xs(\bar{x})^{-1}) &= u'(s(\bar{x})x^{-1}x) \\ &= u' \circ s(\bar{x}) = \mathrm{Inf}(u' \circ s)(x). \end{aligned}$$

Hence $du' - du_0 = \mathrm{Inf}(d(u' \circ s))$. But $du' = \mathrm{Inf}(v)$ and $du_0 = \mathrm{Inf}(v')$ where $v'$ is in the cohomology class of $\mathrm{tg}(u)$. Thus $v - v' = d(u' \circ s)$, which implies that $\mathrm{tg}(u) = a$.

This establishes the exactness of the sequence (A).

https://doi.org/10.4153/CJM-1967-007-8 Published online by Cambridge University Press

Let $M_1$, $M_2$, $M \in \mathscr{C}_G$ and suppose there exists a continuous bilinear mapping $M_1 \times M_2 \to M$ $((m_1, m_2) \mapsto m_1 \cdot m_2)$, such that $g(m_1 \cdot m_2) = (gm_1) \cdot (gm_2)$ for $g \in G$, $m_1, m_2 \in M$. We then define a cochain cup product

$$C^p(G, M_1) \times C^q(G, M_2) \to C^{p+q}(G, M)$$

by setting

$$u \cup v(g_1, \ldots, g_p, h_1, \ldots, h_q) = u(g_1, \ldots, g_p) \cdot g_1 g_2 \ldots g_p v(h_1, \ldots, h_q).$$

Using the easily derived formula $d(u \cup v) = du \cup v + (-1)^p u \cup dv$, we obtain a cup product on cohomology.

**1.2. Free pro-$p$-groups.** Let $p$ be a prime number. Then a profinite group $G$ is said to be a *pro-$p$-group* if $G$ is the projective limit of finite $p$-groups. Let $I$ be a finite set of cardinality $n$ and let $L(I)$ be the discrete free group with generators $x_1, \ldots, x_n \in I$. The *free pro-$p$-group* $F(I)$ *generated by* $x_1, \ldots, x_n$ is by definition the projective limit of the quotients of $L(I)$ which are finite $p$-groups. If $a_1, \ldots, a_n$ are arbitrary elements of a pro-$p$-group $G$, there exists a continuous homomorphism of $F(I)$ into $G$ sending $x_i$ into $a_i$. If $I = \{1, \ldots, n\}$, we write $F(n)$ in place of $F(I)$; the group $F(n)$ is the *free pro-$p$-group of rank $n$*.

**1.3. Interpretation of $H^1$: number of generators.** If $G$ is a pro-$p$-group, we let $H^i(G)$ denote the group $H^i(G, \mathbf{Z}/p\mathbf{Z})$ where the action of $G$ on $\mathbf{Z}/p\mathbf{Z}$ is trivial. $H^i(G)$ is then a vector space over $\mathbf{F}_p$. $H^1(G)$ is the set of all continuous homomorphisms of $G$ into the discrete group $\mathbf{Z}/p\mathbf{Z}$. Each such homomorphism vanishes on $G^* = G^p(G, G)$. Hence $H^1(G)$ may be identified with $H^1(G/G^*)$, which implies that the abelian groups $G/G^*$ and $H^1(G)$ are dual, the first group being compact and the second, discrete. It may be shown (**9**, ch. I, Prop. 25) that $g_1, \ldots, g_n$ generate $G$ topologically if and only if their images in $G/G^*$ generate this group. Hence, if $\dim H^1(G) = n < \infty$, $G$ is a finitely generated topological group with $n$ as the minimal number of generators.

**1.4. Interpretation of $H^2$: number of relations.** Let $R$ be a closed normal subgroup of a pro-$p$-group $F$. If $x \in F$ and $u \in H^1(R)$ then, as we have seen, $x \cdot u = u$ if and only if $u$ vanishes on $(R, F)$. Hence $H^1(R)^F$ may be identified with $H^1(R/R^p(R, F))$, which implies that the groups $R/R^p(R, F)$ and $H^1(R)^F$ are dual. If $r_1, \ldots, r_n \in R$, their conjugates generate a dense subgroup of $R$ if and only if the images of the $r_i$ in $R/R^p(R, F)$ generate this group (**9**, ch. I, Prop. 26). Hence $R = (r_1, \ldots, r_h)$ if $\dim H^1(R)^F = h$.

Suppose that $G$ is a pro-$p$-group with $n = n(G) < \infty$. Let $1 \to R \to F \to G \to 1$ be a presentation of $G$ with $F = F(n)$. Let $q = p^g$ $(g = 1, 2, \ldots, \infty)$ be such that $R \subset F^q(F, F)$ and let $k = \mathbf{Z}_p/q\mathbf{Z}_p$ where $k$ has the $p$-adic topology and the action of $G$ on $k$ is trivial. (Note that $R \subset F^p(F, F)$ as $H^1(G) \to H^1(F)$ is a bijection.) Then, since the homomorphism $H^1(G, k) \to H^1(F, k)$ is bijective, the exact sequence (A) shows that the transgression map is injective.

https://doi.org/10.4153/CJM-1967-007-8 Published online by Cambridge University Press

Now one may show that $H^2(F, k)$ classifies the group extensions of $F$ by $k$ in the category of pro-$p$-groups and, since $F$ is free, each such extension splits. Thus $H^2(F, k) = 0$, which shows that tg is surjective and hence bijective. In particular, if $k = \mathbf{Z}/p\mathbf{Z}$, the results of the preceding paragraph show that $R = (r_1, \ldots, r_h)$ if $\dim H^2(G) = h$.

**1.5. The algebra $\mathbf{Z}_p(G)$.** The completed algebra $\mathbf{Z}_p(G)$ of a pro-$p$-group $G$ is the projective limit of the group algebras of the finite quotients of $G$. $\mathbf{Z}_p(G)$ is then a compact totally disconnected ring and there is a canonical injection of $G$ into $\mathbf{Z}_p(G)$. If $G = \mathbf{Z}_p$, then $\mathbf{Z}_p(G)$ is isomorphic to the formal power series ring $\mathbf{Z}_p[[T]]$ (**9**, ch. I, Prop. 7). Moreover, the isomorphism can be so chosen as to map a given generator of $\mathbf{Z}_p$ onto $1 + T$. If $G, H$ are two pro-$p$-groups with $G$ finite, then $\mathbf{Z}_p(G \times H) = \mathbf{Z}_p(G) \otimes_{\mathbf{Z}_p} \mathbf{Z}_p(H)$. Finally, if $G$ is a pro-$p$-group and $E \in \mathscr{C}_G$ is compact, the continuous mapping $G \times E \to E$ extends to a continuous mapping $\mathbf{Z}_p(G) \times E \to E$, making $E$ into a $\mathbf{Z}_p(G)$-module. This follows from the fact that $E$ is the projective limit of finite $G$-modules.

**§2. A preliminary classification.** In the first part of this section we prove some general propositions on free pro-$p$-groups and cup products of 1-cocycles. We then apply these results to obtain a preliminary classification of Demushkin groups; cf. Theorem 3.

Let $F$ be the free pro-$p$-group of rank $n$ and let $q = p^g$, where $g$ is an integer $\geqslant 1$ or $\infty$. The descending $q$-central series of $F$ is the filtration $(F_i)$ defined inductively as follows:

$$F_1 = F, \qquad F_{i+1} = F_i^{\,q}(F_i, F).$$

The formulae $F_{i+1} \subset F_i$, $(F_i, F_j) \subset F_{i+j}$ imply that $\mathrm{gr}_i(F) = F_i/F_{i+1}$ is an abelian group (written additively), and that $\mathrm{gr}(F) = \sum \mathrm{gr}_i(F)$ is a Lie algebra over $\mathbf{Z}_p/q\mathbf{Z}_p$; cf. (**6**). The Lie bracket for homogenous elements of $\mathrm{gr}(F)$ is induced by the commutator, that is, if $\xi = \bar{x} \in \mathrm{gr}_i(F)$, and $\eta = \bar{y} \in \mathrm{gr}_j(F)$, then $[\xi, \eta]$ is the image of $(x, y) = x^{-1}y^{-1}xy$ in $\mathrm{gr}_{i+j}(F)$.

PROPOSITION 1. *If $x \in F_i$, $y \in F_j$, $a \in \mathbf{Z}_p$, then*

(1) $$(x, y)^a \equiv x^a y^a (y, x)^{\binom{a}{2}} \pmod{F_{i+j+1}},$$

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

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

*Proof.* The proposition is proved for positive integral $a$ by induction using the formulae

(i) $(uv, w) = (u, w)((u, w), v)(v, w)$,

(ii) $(u, vw) = (u, w)(u, v)((u, v), w)$.

The general result is obtained by passing to the limit.

https://doi.org/10.4153/CJM-1967-007-8 Published online by Cambridge University Press

Proposition 1 shows that the map $x \mapsto x^q$ of $F_i$ into $F_{i+1}$ induces a mapping $\pi_i$: $\mathrm{gr}_i(F) \to \mathrm{gr}_{i+1}(F)$. The family $(\pi_i)$ then induces a map $\pi_*$: $\mathrm{gr}(F) \to \mathrm{gr}(F)$. *Let $k = \mathbf{Z}_p/q\mathbf{Z}_p$ and let $\pi$ be an indeterminate over $k$ if $q \neq 0$ and the zero element of $k$ if $q = 0$. Then there exists a unique mapping*

$$\phi: k[\pi] \times \mathrm{gr}(F) \to \mathrm{gr}(F)$$

*which is k-linear in the first variable and such that $\phi(\pi^i, \xi) = \pi_*^i(\xi)$. If we let $\alpha\cdot\xi$ denote $\phi(\alpha, \xi)$, we have $\pi^i\cdot(\pi^j\cdot\xi) = \pi^{i+j}\cdot\xi$.* Proposition 1 now yields

PROPOSITION 2. *Let $\xi \in \mathrm{gr}_i(F)$, $\eta \in \mathrm{gr}_j(F)$. Then*

(1) $\pi\cdot(\xi + \eta) = \pi\cdot\xi + \pi\cdot\eta$ *if $i = j > 1$,*

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

(3) $\pi\cdot[\xi, \eta] = [\pi\cdot\xi, \eta] = [\xi, \pi\cdot\eta]$ *if $i \neq 1$ ($j \neq 1$),*

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

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

*Remarks.* Let $g$ be an integer $\geqslant 1$. If $q \neq 2^g$, then $\binom{q}{2} \equiv 0 \pmod q$ and $\mathrm{gr}(F)$ is a free Lie algebra over $k[\pi]$; cf. **(8)**. If $q = 2^g$, then $\binom{q}{2} \equiv 2^{g-1} \pmod q$ and $\mathrm{gr}(F)$ is not a Lie algebra over $k[\pi]$. In any case $\sum_{i>1} \mathrm{gr}_i(F)$ is a Lie algebra over $k[\pi]$.

Now let $r \in F^q(F, F)$ and let $\bar{r}$ be the image of $r$ in $\mathrm{gr}_2(F)$. Then

$$\bar{r} = \sum_{i=1}^{n} a_i\, \pi\cdot\xi_i + \sum_{i<j} a_{ij}[\xi_i, \xi_j]$$

where $\xi_1, \ldots, \xi_n$ is a basis of $\mathrm{gr}_1(F)$ and $a_i, a_{ij} \in k = \mathbf{Z}_p/q\mathbf{Z}_p$. *Identifying $H^1(F, k)$ with the dual of the k-module* $\mathrm{gr}_1(F)$, *we let $\chi_1, \ldots, \chi_n \in H^1(F, k)$ be the dual basis of $\xi_1, \ldots, \xi_n$. Let $R \subset F^q(F, F)$ be a closed normal subgroup of $F$ containing $r$ and let $G = F/R$.* We have seen (cf. §1.4) that in the above situation the transgression tg: $H^1(R, k)^F \to H^2(G, k)$ is bijective. *Hence we may define a k-linear homomorphism*

$$\bar{r}: H^2(G, k) \to k$$

*by setting $\bar{r}(a) = \mathrm{tg}^{-1}(a)(r^{-1})$ for any $a \in H^2(G, k)$.* If we identify $H^1(G, k)$ with $H^1(F, k)$, we have the following proposition.

PROPOSITION 3. *Let $\chi_i \cup \chi_j \in H^2(G, k)$ be the cup product of $\chi_i, \chi_j \in H^1(G, k)$ relative to the pairing $k \times k \to k$ defined by sending $(a, b)$ into $ab$. Then*

$$\bar{r}(\chi_i \cup \chi_j) = \begin{cases} a_{ij} & \text{if } i < j, \\ -a_{ji} & \text{if } i > j, \\ \binom{q}{2} a_i & \text{if } i = j. \end{cases}$$

*Proof.* Lift $\xi_1, \ldots, \xi_n$ to a basis $x_1, \ldots, x_n$ of $F$. The cohomology class $\chi_i \cup \chi_j$ can be represented by a 2-cocycle $c_0$ where $c_0(\sigma, \tau) = \chi_i(\sigma)\chi_j(\tau)$ for $\sigma, \tau \in G$. Let $c$ be the inflation of $c_0$ to $F$. Since $H^2(F, k) = 0$, there exists a cochain $u \in C^1(F, k)$ such that $b = du$ and, moreover, by subtracting from $u$ a suitable homomorphism, we can require that $u(x_h) = 0$ for $h = 1, \ldots, n$. Then

$$u(xy) = u(x) + u(y) - \chi_i(x)\chi_j(y), \qquad x, y \in F.$$

If $v$ is the restriction of $u$ to $R$, then $v = \mathrm{tg}^{-1}(\chi_i \cup \chi_j)$. Hence

$$\bar{r}(\chi_i \cup \chi_j) = v(r^{-1}) = -u(r).$$

Since $u(x^{-1}) + u(x) + \chi_i(x)\chi_j(x) = 0$ for $x \in F$, we have for $h < k$

$$\begin{aligned} u(x_h, x_k) &= u(x_h^{-1}) + u(x_k^{-1}x_h x_k) + \chi_i(x_h)\chi_j(x_h) \\ &= -\delta_{ih}\delta_{jh} + u(x_k^{-1}x_h x_k) + \delta_{ih}\delta_{jh} \\ &= u(x_k^{-1}) + u(x_h x_k) + \chi_i(x_k)\chi_j(x_h) + \chi_i(x_k)\chi_j(x_k) \\ &= -\delta_{ik}\delta_{jk} + u(x_h) + u(x_k) - \chi_i(x_h)\chi_j(x_k) + \delta_{ik}\delta_{jh} + \delta_{ik}\delta_{jk} \\ &= \delta_{ik}\delta_{jh} - \delta_{ih}\delta_{jk} = \begin{cases} -1 & \text{if } i = h, j = k, \\ 1 & \text{if } i = k, j = h, \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

If $i \neq j$, we have $u(x_h^{m+1}) = u(x_h^m)$ and $u(x_h^{-1}) = 0$ which implies that $u(x_h^m) = 0$ for any $m \in \mathbf{Z}$. If $i = j$, we have

$$u(x_h^{m+1}) = u(x_h^m) - \chi_i(x_h^m)\chi_i(x_h) = u(x_h^m) - m\delta_{ih},$$

which implies that

$$u(x_h^m) = -\binom{m}{2}\delta_{ih}$$

for $m = 1, 2, 3, \ldots$.

Noticing that $u$ restricted to $F_2$ is a homomorphism vanishing on $F_3$ we have

$$u(r) = \begin{cases} a_{ij} & \text{if } i < j, \\ -a_{ji} & \text{if } i > j, \\ \binom{q}{2}a_i & \text{if } i = j, \end{cases}$$

since

$$r \equiv \prod_{h=1}^{m} x_h^{qa_i} \prod_{h<k} (x_h, x_k)^{a_{hk}} \pmod{F_3}.$$

COROLLARY. *Suppose that $q \neq 0$ and let $s$ be any element of $F$ such that $r \equiv s^q$ (mod $(F, F)$). Then $s$ is uniquely determined modulo $(F, F)$ and*

$$\bar{r}(\chi \cup \chi) = \binom{q}{2}\chi(s) \qquad \textit{for any } \chi \in H^1(G, k).$$

https://doi.org/10.4153/CJM-1967-007-8 Published online by Cambridge University Press

*Proof.* The first statement follows from the fact that $F/(F, F)$ is a free $\mathbf{Z}_p$-module. As for the second, note that

$$s \equiv \prod_{i=1}^{n} x_i^{a_i} \pmod{(F, F)}.$$

Then by Proposition 3

$$\bar{r}(\chi_i \cup \chi_i) = \binom{q}{2} a_i = \binom{q}{2} \chi_i(s).$$

The corollary then follows by linearity.

*For the remainder of this section we suppose that* (i) $R = (r)$, (ii) $G = F/R$ *is a Demushkin group, and* (iii) $q = q(G)$. *Note that q is also the highest power of p such that* $r \in F^q(F, F)$. We now want to show that under these conditions the homomorphism $\bar{r}$: $H^2(G, k) \to k$ is bijective. For this it suffices to show that $M = R/R^q(R, F)$ is a free $k$-module of rank 1. But this follows from the fact that $N = R/(R, F)$ is a free $\mathbf{Z}_p$-module of rank 1 and that the image of $R^q(R, F)$ in $N$ is $qN$.

If we let $\chi \cup \chi'$ denote $\bar{r}(\chi \cup \chi')$, we obtain a $k$-bilinear form

$$H^1(G, k) \times H^1(G, k) \to k$$

which is non-degenerate since its reduction modulo $p$ is non-degenerate by definition of a Demushkin group. *If* $q \neq 0$, *we let* $\sigma$ *be the image in* $\mathrm{gr}_1(F)$ *of the element s described in the above corollary.* Then $\sigma$ may be completed to a basis of $\mathrm{gr}_1(F)$ and we have the following proposition.

PROPOSITION 4. (1) *If* $q = 0$, *then n is even and there exists a basis* $\chi_1, \ldots, \chi_n$ *of* $H^1(G, k)$ *such that*

$$\chi_1 \cup \chi_2 = \chi_3 \cup \chi_4 = \ldots = \chi_{n-1} \cup \chi_n = 1,$$

*and* $\chi_i \cup \chi_j = 0$ *for all other* $i < j$.

(2) *If* $q \neq 0$, *there exists a basis* $\chi_1, \ldots, \chi_n$ *of* $H^1(G, k)$ *such that* (a) $\chi_1(\sigma) = 1$, $\chi_i(\sigma) = 0$ *if* $i \neq 1$ *and* (b)

$$\chi_1 \cup \chi_2 = \chi_3 \cup \chi_4 = \ldots = \chi_{n-1} \cup \chi_n = 1$$

*with* $\chi_i \cup \chi_j = 0$ *for all other* $i < j$, *if n is even, or*

$$\chi_2 \cup \chi_3 = \chi_4 \cup \chi_5 = \ldots = \chi_{n-1} \cup \chi_n = 1$$

*with* $\chi_i \cup \chi_j = 0$ *for all other* $i < j$, *if n is odd. Moreover, n is even if* $q \neq 2$.

*Proof.* (1) This follows from the theory of non-degenerate alternate bilinear forms over a principal ideal domain.

(2) Case I: $q \neq 2$. The rank $n$ is even since the reduction of the cup product modulo $p$ is a non-degenerate alternate bilinear form over the field $\mathbf{F}_p$. Let $\chi_1, \ldots, \chi_n$ be any basis of $H^1(G, k)$ such that (a) holds. To find such a basis one only has to complete $\sigma$ to a basis of $\mathrm{gr}_1(F)$ and take the dual basis. Since

the cup product is non-degenerate, one of the elements $\chi_1 \cup \chi_i$ with $i > 1$ has to be a unit of $k$. After a permutation we may assume that $\chi_1 \cup \chi_2$ is a unit and multiplying $\chi_2$ by a unit we may even assume that $\chi_1 \cup \chi_2 = 1$. If $\chi_1 \cup \chi_i = a_i \neq 0$ for some $i > 2$, replace $\chi_i$ by $\chi_i - a_i \chi_2$. Since condition (a) is not altered by this substitution, we may assume that $\chi_1 \cup \chi_i = 0$ for $i > 2$. Now if $N$ is the subspace spanned by $\chi_3, \ldots, \chi_n$, our cup product restricted to $N \times N$ is non-degenerate and alternate. Hence we may choose $\chi_3, \ldots, \chi_n \in N$ such that (b) holds for $i, j > 2$. Condition (a) is still satisfied, $\chi_1 \cup \chi_2 = 1$, and $\chi_1 \cup \chi_i = 0$ for $i > 2$. If we replace $\chi_2$ by

$$\chi_2 + a_3 \chi_3 + \ldots + a_n \chi_n$$

with $a_{2i} = \chi_2 \cup \chi_{2i-1}$ and $a_{2i-1} = -\chi_2 \cup \chi_{2i}$, we have, in addition, $\chi_2 \cup \chi_i = 0$ for $i > 2$. Thus, the proof of Case I is complete.

Case II: $q = 2$. In virtue of the corollary to Proposition 3 it suffices to find a basis $\chi_i$ with $\chi_i \cup \chi_i = \delta_{1i}$ such that (b) holds. But this follows from a classical theorem on non-alternate, symmetric bilinear forms in characteristic 2; cf. (**4**, p. 170).

COROLLARY. *There exists a basis $x_1, \ldots, x_n$ for $F$ such that*

$$r \equiv \begin{cases} x_1^q (x_1, x_2)(x_3, x_4) \ldots (x_{n-1}, x_n) \pmod{F_3} & \text{if } n \text{ is even}, \\ x_1^q (x_2, x_3)(x_4, x_5) \ldots (x_{n-1}, x_n) \pmod{F_3} & \text{if } n \text{ is odd}. \end{cases}$$

*Proof.* Choose a basis $\chi_1, \ldots, \chi_n$ of $H^1(G, k)$ as in Proposition 4 and let $\xi_1, \ldots, \xi_n$ be the dual basis in $\mathrm{gr}_1(F)$. We obtain the required basis by lifting $\xi_1, \ldots, \xi_n$ to a basis $x_1, \ldots, x_n$ of $F$.

*For any basis $x = (x_i)$ of $F$ let*

$$r_0(x) = \begin{cases} x_1^q (x_1, x_2)(x_3, x_4) \ldots (x_{n-1}, x_n) & \text{if } n \text{ is even}, \\ x_1^q (x_2, x_3)(x_4, x_5) \ldots (x_{n-1}, x_n) & \text{if } n \text{ is odd}. \end{cases}$$

If $t_1, \ldots, t_n \in F_{j-1}$, with $j \geqslant 3$, and if $y_i = x_i t_i^{-1}$, then $y = (y_i)$ is a basis of $F$ and

$$r_0(x) = r_0(y) d_{j-1}(t_1, \ldots, t_n)$$

where $d_{j-1}(t_1, \ldots, t_n)$ is a uniquely determined element of $F_j$. A simple calculation using Proposition 1 shows that if $\tau_i$ is the image of $t_i$ in $\mathrm{gr}_{j-1}(F)$, then the image of $d_{j-1}(t_1, \ldots, t_n)$ in $\mathrm{gr}_j(F)$ is

$$\pi \cdot \tau_1 + \binom{q}{2} [\tau_1, \xi_1] + [\tau_1, \xi_2] + [\xi_1, \tau_2] + \ldots + [\tau_{n-1}, \xi_n] + [\xi_{n-1}, \tau_n]$$

if $n$ is even, and

$$\pi \cdot \tau_1 + [\tau_1, \xi_1] + [\tau_2, \xi_3] + [\xi_2, \tau_3] + \ldots + [\tau_{n-1}, \xi_n] + [\xi_{n-1}, \tau_n]$$

if $n$ is odd. Hence $d_{j-1}$ induces a $k$-linear homomorphism $\delta_{j-1}: \mathrm{gr}_{j-1}(F)^n \to \mathrm{gr}_j(F)$ for $j \geqslant 3$.

PROPOSITION 5. *Let $j \geqslant 3$. Then*

(1) $\mathrm{gr}_j(F) = \mathrm{Im}(\delta_{j-1})$ *if* $q \neq 2$.

(2) *The abelian group* $\mathrm{gr}_j(F)$ *is generated by* $\mathrm{Im}(\delta_{j-1})$ *and the elements* $\pi^{j-1}\cdot\xi_i$, *with* $i \neq 2$, *if* $q = 2$ *and* $n$ *is even.*

(3) *The abelian group* $\mathrm{gr}_j(F)$ *is generated by* $\mathrm{Im}(\delta_{j-1})$ *and the elements* $\pi^{j-1}\cdot\xi_i$, *with* $i \neq 1$, *if* $q = 2$ *and* $n$ *is odd.*

*Proof.* Let $H_j$ be defined as $\mathrm{Im}(\delta_{j-1})$ in Case 1, the group generated by $\mathrm{Im}(\delta_{j-1})$ and the elements $\pi^{j-1}\cdot\xi_i$ $(i \neq 2)$ in Case 2, and the group generated by $\mathrm{Im}(\delta_{j-1})$ and the elements $\pi^{j-1}\cdot\xi_i$ $(i \neq 1)$ in Case 3. Notice that in order to prove that $H_j = \mathrm{gr}_j(F)$, it suffices to show that $\pi\cdot\tau \in H_j$ for any $\tau \in \mathrm{gr}_{j-1}(F)$. Indeed, in any case $[\tau, \xi_i] \in \mathrm{Im}(\delta_{j-1})$ for $i \geqslant 3$ and $\pi\cdot\tau + [\tau, \xi_2]$, $[\tau, \xi_1] \in \mathrm{Im}(\delta_{j-1})$ if $n$ is even and $\pi\cdot\tau + [\tau, \xi_1]$, $[\tau, \xi_2] \in \mathrm{Im}(\delta_{j-1})$ if $n$ is odd. From this it follows that $\pi\cdot\tau$, $[\tau, \xi_i] \in H_j$ for all $\tau \in \mathrm{gr}_{j-1}(F)$ and $i \geqslant 1$. But the elements $\pi\cdot\tau$, $[\tau, \xi_i]$ with $\tau \in \mathrm{gr}_{j-1}(F)$ generate $\mathrm{gr}_j(F)$.

We now proceed by induction on $j$. Assume that we have shown that $H_j = \mathrm{gr}_j(F)$ for some $j \geqslant 3$. If $\tau \in \mathrm{gr}_j(F)$, then

$$\tau = \sum_{i=1}^{i=n} a_i\, \pi^{j-1}\cdot\xi_i + \delta_{j-1}(\tau_1, \ldots, \tau_n)$$

where $a_i \in k$, $\tau_1, \ldots, \tau_n \in \mathrm{gr}_{j-1}(F)$ and $a_2 = 0$ in Case 2, $a_1 = 0$ in Case 3, and all $a_i = 0$ in Case 1. But then

$$\pi\cdot\tau = \sum_{i=1}^{i=n} a_i\, \pi^{j}\cdot\xi_i + \delta_j(\pi\cdot\tau_1, \ldots, \pi\cdot\tau_m),$$

which implies that $\pi\cdot\tau \in H_{j+1}$ for any $\tau \in H_j$.

Thus we are reduced to proving the proposition for $j = 3$, that is, to proving that $\pi\cdot\tau \in H_3$ for any $\tau \in \mathrm{gr}_2(F)$. Moreover, it suffices to take $\tau$ of the form $\pi\cdot\xi_i$, $[\xi_i, \xi_j]$ since these elements generate $\mathrm{gr}_2(F)$.

Case 1. The ring $k$ is a local ring with maximal ideal $\mathfrak{M} = pk$. Hence by Nakayama's Lemma it suffices to prove that $\pi\mathrm{gr}_2(F) \subset H_3 + \mathfrak{M}\mathrm{gr}_3(F)$, since then we would have $\mathrm{gr}_3(F) = H_3 + \mathfrak{M}\mathrm{gr}_3(F)$. Set $M = \mathfrak{M}\mathrm{gr}_3(F)$. Then by Proposition 2 we have

$$\pi\cdot[\xi_i, \xi_j] = [\pi\cdot\xi_i, \xi_j] + m = [\xi_i, \pi\cdot\xi_j] + m',$$

where $m, m' \in M$. Therefore, since $[\tau, \xi_i] \in \mathrm{Im}(\delta_2)$ if $i \neq 2$, we have $\pi\cdot[\xi_i, \xi_j] \in H_3 + M$ for any $i$, $j$. Moreover, as $\pi\cdot\tau + [\tau, \xi_2] \in H_3$ for any $\tau \in \mathrm{gr}_2(F)$, we have $\pi^2\cdot\xi_i + [\pi\cdot\xi_i, \xi_2] \in H_3$ and, hence, $\pi^2\cdot\xi_i \in H_3 + M$ for any $i$.

Case 2. Since $\pi\cdot\tau + [\tau, \xi_2] \in H_3$ for any $\tau \in \mathrm{gr}_2(F)$, it follows that $\pi^2\cdot\xi_2$ and $[\pi\cdot\xi_i, \xi_2] \in H_3$. But

$$[\pi\cdot\xi_i, \xi_2] = \pi\cdot[\xi_i, \xi_2] + [[\xi_i, \xi_2], \xi_i];$$

hence $\pi \cdot [\xi_i, \xi_2] \in H_3$ as $[\tau, \xi_i] \in H_3$ for any $\tau \in \mathrm{gr}_2(F)$ if $i \neq 2$. For any $i, j$ we then have

$$[[\xi_i, \xi_j], \xi_2] = [[\xi_j, \xi_2], \xi_i] + [[\xi_2, \xi_i], \xi_j] \in H_3$$

and hence $\pi \cdot [\xi_i, \xi_j] \in H_3$.

Case 3. The proof of this case is the same as that of Case 2 except that here $\xi_1$ plays the role of $\xi_2$.

The object of this section is to prove the following theorem.

THEOREM 3. *Let $r \in F^p(F, F)$, where $F$ is a free pro-p-group of rank $n$. Suppose that $G = F/(r)$ is a Demushkin group with $q(G) = q$. Then,*

(1) *if $q \neq 2$, there exists a basis $x_1, \ldots, x_n$ of $F$ such that*

$$r = x_1^q(x_1, x_2)(x_3, x_4) \ldots (x_{n-1}, x_n);$$

(2) *if $q = 2$ and $n$ is odd, there exists a basis $x_1, \ldots, x_n$ of $F$ such that*

$$r = x_1^2 x_2^{2^f}(x_2, x_3)(x_4, x_5) \ldots (x_{n-1}, x_n)$$

*for some $f = 2, 3, \ldots, \infty$;*

(3) *if $q = 2$ and $n$ is even, there exists a basis $x_1, \ldots, x_n$ of $F$ such that*

$$r = x_1^{2+\alpha}(x_1, x_2)x_3^{2^f}(x_3, x_4)(x_5, x_6) \ldots (x_{n-1}, x_n)$$

*for some $f = 2, 3, \ldots, \infty$ and $\alpha \in 4Z_2$.*

*Proof.* We know that $r \equiv r_0(x) \pmod{F_3}$ for some basis $x = (x_1, \ldots, x_n)$ of $F$. We proceed by the method of successive approximation.

Suppose first that $q \neq 2$ and that we have found a basis $x = (x_1, \ldots, x_n)$ of $F$ such that $r \equiv r_0(x) \pmod{F_j}$ $(j \geqslant 3)$, that is, $r = r_0(x)e_j$ with $e_j \in F_j$. Then if $y_i = x_i t_i^{-1}$ with $t_i \in F_{j-1}$, we have $r = r_0(y)d_{j-1}(t_1, \ldots, t_n)e_j$. But in virtue of Proposition 5 we may choose the $t$'s so that

$$d_{j-1}(t_1, \ldots, t_n)e_j \equiv 0 \pmod{F_{j+1}}.$$

Hence $r \equiv r_0(y) \pmod{F_{j+1}}$. Iterate this process and pass to the limit. (This is possible since the successive corrections $t = (t_1, \ldots, t_n)$ converge to 1.) We thus obtain a basis $x = (x_1, \ldots, x_n)$ of $F$ such that $r = r_0(x)$.

Now assume that $q = 2$ and $n$ is even. Suppose that we have found a basis $x = (x_1, \ldots, x_n)$ of $F$ and 2-adic integers $\lambda_1, \ldots, \lambda_n$ divisible by 4 such that

$$r = x_1^{\lambda_1} r_0(x) x_3^{\lambda_3} \ldots x_n^{\lambda_n} e_j$$

for some $j \geqslant 3$ with $e_j \in F_j$. If we set $y_i = x_i t_i^{-1}$ with $t_i \in F_{j-1}$, then

$$r = y_1^{\lambda_1} r_0(y) y_3^{\lambda_3} \ldots y_n^{\lambda_n} d_{j-1}(t_1, \ldots, t_n)e'_j$$

with $e_j \equiv e'_j \pmod{F_{j+1}}$. By Proposition 5, there exist $t_1, \ldots, t_n$ in $F_{j-1}$ and integers $a_1, \ldots, a_n \in \{0, 1\}$ such that

$$d_{j-1}(t_1, \ldots, t_n)e'_j \equiv y_1^{a_1 2^{j-1}} \cdot y_3^{a_3 2^{j-1}} \ldots y_n^{a_n 2^{j-1}} \pmod{F_{j+1}}.$$

https://doi.org/10.4153/CJM-1967-007-8 Published online by Cambridge University Press

Hence

$$r = y_1^{\lambda_1 + a_1 2^{j-1}} r_0(y) y_3^{\lambda_3 + a_3 2^{j-1}} \ldots y_n^{\lambda_n + a_n 2^{j-1}} e_{j+1}$$

with $e_{j+1} \in F_{j+1}$. Iterating this process and passing to the limit we find a basis $x_1, \ldots, x_n$ of $F$ and 2-adic integers $\alpha_1, \ldots, \alpha_n$ divisible by 4 such that

$$r = x_1^{\alpha_1} r_0(x) x_3^{\alpha_3} \ldots x_n^{\alpha_n}.$$

Now, using Proposition 3, we see that the relation

$$r' = (x_3, x_4) \ldots (x_{n-1}, x_n) x_3^{\alpha_3} \ldots x_n^{\alpha_n}$$

is a Demushkin relation in the variables $x_3, \ldots, x_n$. Its $q$-invariant is $2^f$ for some $f \geqslant 2$. Hence by Theorem 3, Case 1, we can choose the variables $x_3, \ldots, x_n$ so that

$$r' = x_3^{2^f}(x_3, x_4) \ldots (x_{n-1}, x_n).$$

Since $r = x_1^{2+\alpha_1}(x_1, x_2) r'$, our proof is complete.

Since the case $q = 2$, $n$ odd is entirely analogous to the case $q = 2$, $n$ even, we shall not discuss it here. For more details cf. (**8**, pp. 7–8).

**§3. The invariant** $\operatorname{Im}(\chi)$. In this section we discuss the invariant $\operatorname{Im}(\chi)$ which was mentioned in the Introduction. We shall see that the existence and uniqueness of $\chi$ follow easily from Theorem 3 and at the same time we shall give a procedure for computing it.

Let $G$ be a pro-$p$-group, $\mathbf{U}_p$ the group of $p$-adic units with the $p$-adic topology, and $\chi$ a continuous homomorphism of $G$ into $\mathbf{U}_p$. If we define $\sigma \cdot x = \chi(\sigma)x$ for all $\sigma \in G$, $x \in \mathbf{Z}_p$, then $\mathbf{Z}_p$, with the $p$-adic topology, becomes a topological $G$-module which we denote by $I = I(\chi)$. We then have the following proposition:

PROPOSITION 6. *If* $\dim H^1(G) < \infty$, *the following are equivalent:*

(1) *For all* $i \geqslant 1$ *the canonical homomorphism* $H^1(G, I/p^i I) \to H^1(G, I/pI)$ *is surjective.*

(2) *For all* $i \geqslant 1$ *we may arbitrarily prescribe the values of crossed homomorphisms of* $G$ *into* $I/p^i I$ *on a minimal system of generators of* $G$.

(3) *We may arbitrarily prescribe the values of crossed homomorphisms of* $G$ *into* $I$ *on a minimal system of generators of* $G$.

*Proof.* (3) follows from (2) by passing to the limit, and (1) immediately follows from (3). To prove that (1) implies (2) we proceed by induction on $i$, using the exact sequence

$$0 \to I/p^{i-1}I \xrightarrow{\lambda} I/p^i I \to I/pI \to 0$$

where $\lambda$ is induced by multiplication by $p$. The statement (2) is true if $i = 1$ since $\operatorname{Im}(\chi) \subset 1 + p\mathbf{Z}_p$ implies that $G$ acts trivially on $I/pI = \mathbf{Z}/p\mathbf{Z}$. Now

https://doi.org/10.4153/CJM-1967-007-8 Published online by Cambridge University Press

let $g_1, \ldots, g_n$ be a minimal system of topological generators of $G$ and let $a_1, \ldots, a_n \in I/p^iI$ with $i > 1$. Using (1) we can find a crossed homomorphism $D_1$ of $G$ into $I/p^iI$ such that $b_i = D_i(g_i) - a_i \in \operatorname{Im}(\lambda)$. By the inductive hypothesis there exists a crossed homomorphism $D_2$ of $G$ into $I/p^{i-1}I$ such that $D_2(g_i) = \lambda^{-1}(b_i)$. Then $D = D_1 - \lambda \circ D_2$ is a crossed homomorphism of $G$ into $I/p^iI$ such that $Dg_i = a_i$.

COROLLARY. *If $G$ is a free pro-$p$-group, the statements* (1), (2), (3) *are true.*

*Proof.* In virtue of the Proposition it suffices to prove (1). But this follows from the fact that $H^2(G, I/p^iI) = 0$ for $i \geqslant 1$.

THEOREM 4. *Suppose that the pro-$p$-group $G$ is a Demushkin group. Then there exists a unique continuous homomorphism $\chi: G \to \mathbf{U}_p$ such that $I(\chi)$ has the equivalent properties* (1), (2), (3) *of Proposition* 6.

*Proof.* If $\dim H^1(G) = n$, we know that $G$ is isomorphic to a quotient of the free pro-$p$-group $F = F(n)$ by a closed normal subgroup $R = (r)$. Moreover, in each of the cases (1) $q \neq 2$, (2) $q = 2$, $n$ odd, (3) $q = 2$, $n$ even, there is a basis $x_1, \ldots, x_n$ of $F$ such that $r$ has the form described in Theorem 3.

In each of these cases we define a continuous homomorphism $\chi: F \to \mathbf{U}_p$ by setting

(1) $\chi(x_2) = (1 - q)^{-1}, \quad \chi(x_i) = 1 \quad$ if $i \neq 2$,

(2) $\chi(x_1) = -1, \quad \chi(x_3) = (1 - 2^f)^{-1}, \quad \chi(x_i) = 1 \quad$ if $i \neq 1, 3$,

(3) $\chi(x_2) = -(1 + \alpha)^{-1}, \quad \chi(x_4) = (1 - 2^f)^{-1}, \quad \chi(x_i) = 1 \quad$ if $i \neq 2, 4$.

In each case $\chi(r) = 0$ so that $\chi$ induces a continuous homomorphism $\chi: G \to \mathbf{U}_p$. Now let $D$ be any crossed homomorphism of $F$ into $I(\chi)$. Then, using the formula

$$D(x, y) = x^{-1}y^{-1}(Dx - yDx + xDy - Dy),$$

we find

(1) $Dr = (q + \chi(x_2)^{-1} - 1)Dx_1 = 0$,

(2) $Dr = (1 + \chi(x_1))Dx_1 + (2^f + \chi(x_3)^{-1} - 1)Dx_2 = 0$,

(3) $Dr = (2 + \alpha + \chi(x_2)^{-1} - 1)Dx_1 + (2^f + \chi(x_4)^{-1} - 1)Dx_3 = 0$.

It follows that $D$ induces a derivation of $G$ into $I(\chi)$. Since $F$ has property (3) of Proposition 6, it follows that $G$ does. Hence the existence of $\chi$ is established.

To prove the uniqueness of $\chi$ let us show that our definition was forced. Let $D_i$ be the derivation of $F$ into $I(\chi)$ such that $D_i(r) = 0$ and $D_i(x_j) = \delta_{ij}$. Then

$$\begin{aligned}
(1) \qquad D_2(r) &= \chi(x_1)^{q-1}\chi(x_2)(\chi(x_1) - 1) && \Rightarrow \chi(x_1) = 1,\\
D_1(r) &= q + \chi(x_2) - 1 && \Rightarrow \chi(x_2) = (1 - q)^{-1},\\
D_{2i}(r) &= \chi(x_{2i})^{-1}(1 - \chi(x_{2i-1})), \quad i \neq 1 && \Rightarrow \chi(x_{2i-1}) = 1,\\
D_{2i-1}(r) &= \chi(x_{2i-1})^{-1}(\chi(x_{2i})^{-1} - 1), \quad i \neq 1 && \Rightarrow \chi(x_{2i}) = 1.
\end{aligned}$$

(2) $$\begin{aligned} D_1(r) &= 1 + \chi(x_1) && \Rightarrow \chi(x_1) = -1, \\ D_i(r) &= -D_i(x_2^{2^f}(x_2, x_3) \ldots (x_{n-1}, x_n)), && \\ & && i \neq 1 \Rightarrow \chi(x_2) = 1, \\ & && \chi(x_3) = (1 - 2^f)^{-1}, \\ & && \chi(x_i) = 1 \text{ for } i > 3. \end{aligned}$$

(3) $$\begin{aligned} D_2(r) &= \chi(x_1)^{1+\alpha}\chi(x_2)^{-1}(\chi(x_1) - 1) && \Rightarrow \chi(x_1) = 1, \\ D_4(r) &= \chi(x_3)^{2^f-1}\chi(x_4)^{-1}(\chi(x_3) - 1) && \Rightarrow \chi(x_3) = 1, \\ D_1(r) &= 2 + \alpha + \chi(x_2)^{-1} - 1 && \Rightarrow \chi(x_2) = -(1+\alpha)^{-1}, \\ D_3(r) &= 2^f + \chi(x_4) - 1 && \Rightarrow \chi(x_4) = (1 - 2^f)^{-1}, \\ D_i(r) &= D_i((x_5, x_6) \ldots (x_{n-1}, x_n)), \quad i > 4 && \Rightarrow \chi(x_i) = 1. \end{aligned}$$

COROLLARY. (i) $\mathrm{Im}(\chi)$ *is an invariant of* $G$.

(ii) $q = q(G)$ *is the highest power of* $p$ *such that* $\mathrm{Im}(\chi) \subset 1 + q\mathbf{Z}_p$.

(iii) *In Theorem* 3 *we have*

$$\mathrm{Im}(\chi) = \begin{cases} 1 + q\mathbf{Z}_p & \text{in Case 1,} \\ \{\pm 1\} \times \mathbf{U}_2^{(f)} & \text{in Case 2,} \\ \{\pm 1\} \times \mathbf{U}_2^{(f)} & \text{in Case 3 if } v_2(\alpha) \geqslant f, \\ \mathbf{U}_2^{[f']} & \text{in Case 3 if } f' = v_2(\alpha) < f. \end{cases}$$

*Remarks*. The mapping log: $\mathbf{U}_p^{(f)} \rightarrow p^f\mathbf{Z}_p$ defined by

$$\log(1 + x) = x - x^2/2 + x^3/3 - \ldots$$

is a continuous homomorphism of $\mathbf{U}_p^{(f)}$ into $p^f\mathbf{Z}_p$. It is an isomorphism if $p \neq 2$ or if $p = 2$ and $f \geqslant 2$. Hence, if $p \neq 2$, the only closed subgroups of $\mathbf{U}_p^{(1)}$ are the groups $\mathbf{U}_p^{(f)}$ with $f \geqslant 1$. In the case $p = 2$, however,

$$\mathbf{U}_p^{(1)} = \{\pm 1\} \times \mathbf{U}_2^{(2)}.$$

It is then easy to check that the closed subgroups of $\mathbf{U}_2^{(1)}$ are either of the form $\mathbf{U}_2^{(f)}$ with $f \geqslant 2$ or of the form $\{\pm 1\} \times \mathbf{U}_2^{(f)}$ with $f \geqslant 2$ or of the form $\mathbf{U}_2^{[f]}$ with $2 \leqslant f < \infty$. Note that $\mathbf{U}_2^{[f]}$ is isomorphic to $\mathbf{Z}_2$ if $2 \leqslant f < \infty$.

**§4. The case $q = 2$, $n$ even.** Let $F$ be a free pro-2-group of even rank $n$ and let $r \in F^2(F, F) = F_2$ be a Demushkin relation with $q$-invariant equal to 2. Let $\chi = \chi_r$ be the associated character.

DEFINITION. *Let* $X = \ker(\chi)$, $E = X/(X, X)$, $\Gamma = F/X$, $\Lambda = \mathbf{Z}_2(\Gamma)$; cf. §1.5. *We make* $E$ *into a topological* $\Gamma$*-module in the following way. If* $\xi = \bar{x} \in E$ *and* $\alpha = \bar{y} \in \Gamma$, *then* $\alpha \cdot \xi$ *is the image of* $y^{-1}xy$ *in* $E$. *Since* $E$ *is profinite, we may consider* $E$ *as a* $\Lambda$*-module;* cf. §1.5.

Now by the Corollary to Theorem 4 we have $\Gamma \cong \mathbf{Z}/2\mathbf{Z}$, $\mathbf{Z}_2$, or $(\mathbf{Z}/2\mathbf{Z}) \times \mathbf{Z}_2$. If $\Gamma \cong \mathbf{Z}/2\mathbf{Z}$, then by Theorem 3 and the Corollary to Theorem 4 there is a basis $x_1, \ldots, x_n$ for $F$ such that

$$r = x_1^2(x_1, x_2) \ldots (x_{n-1}, x_n).$$

https://doi.org/10.4153/CJM-1967-007-8 Published online by Cambridge University Press

If $\Gamma \cong \mathbf{Z}_2$, then $\mathbf{Z}_2(\Gamma) \cong \mathbf{Z}_2[[T]]$ with a generator of $\Gamma$ corresponding to $1 + T$; cf. §1.5. If $\Gamma \cong (\mathbf{Z}/2\mathbf{Z}) \times \mathbf{Z}_2$, then $\mathbf{Z}_2(\Gamma) \cong \mathbf{Z}_2[S] \otimes_{\mathbf{Z}_2} \mathbf{Z}_2[[T]]$ where $S$ corresponds to the generator of $\mathbf{Z}/2\mathbf{Z}$.

*Note.* In this section, $(F_i)$ is the descending 2-central series of $F$; cf. §2.

**4.1.** $\mathrm{Im}(\chi) \cong \mathbf{Z}_2$. In this case $\mathrm{Im}(\chi) = \mathbf{U}_2^{[f]}$ with $f \neq \infty$. Then by Theorem 3 and the Corollary to Theorem 4 there exists a basis $w_1, \ldots, w_n$ of $F$ such that

$$r = w_1^{2+\alpha}(w_1, w_2)w_3^{2^g}(w_3, w_4)(w_5, w_6) \ldots (w_{n-1}, w_n)$$

where $\alpha$ is a 2-adic integer with $f = v_2(\alpha) \geqslant 2$ and $2^g$ is an integer with $g > v_2(\alpha)$. (If $n = 2$, then by the above we mean $r = w_1^{2+\alpha}(w_1, w_2)$ where $\alpha$ is a 2-adic integer with $f = v_2(\alpha) \geqslant 2$. By this convention we include the case $n = 2$ in what follows.)

In the proof of Theorem 4 we showed that

$$\chi(w_2) = -(1 + \alpha)^{-1}, \qquad \chi(w_4) = (1 - 2^g)^{-1}, \qquad \chi(w_i) = 1 \text{ otherwise.}$$

Let $a$ be the (unique) 2-adic unit such that $(1 + 2^f)^a = 1 + \alpha$, and $b$ the (unique) 2-adic integer such that $(1 + \alpha)^b = 1 - 2^g$. Note that $b$ is divisible by 2. Now set

$$y_2 = w_2^{a^{-1}}, \qquad y_4 = w_4 w_2^{-b}, \qquad y_i = w_i \text{ otherwise.}$$

Then $y_1, \ldots, y_n$ is a basis of $F$ and

$$\chi(y_1) = 1, \qquad \chi(y_2) = -(1 + 2^f)^{-1}, \qquad \chi(y_i) = 1 \text{ for } i > 2$$

with

$$r = y_1^{2+\alpha}(y_1, y_2^a)y_3^{2^g}(y_3, y_4 y_2^{ab})(y_5, y_6) \ldots (y_{n-1}, y_n).$$

If $\gamma$ is the image of $y_2$ in $\Gamma$, then $\gamma$ is a topological generator of $\Gamma$. Hence there exists an isomorphism of $\mathbf{Z}_2(\Gamma)$ onto $\mathbf{Z}_2[[T]]$ sending $\gamma$ into $1 + T$. If we let $\bar{r}$ and $\bar{y}_i$ be the image of $r$ and $y_i$ respectively in $E$, then

$$\bar{r} = (1 + \alpha + (1 + T)^a)\bar{y}_1 + (2^g + (1 + T)^{ab} - 1)\bar{y}_3.$$

LEMMA *If $\psi(T) \in \mathbf{Z}_2[[T]]$, $c \in 2\mathbf{Z}_2$, then $T - c$ divides $\psi(T)$ in $\mathbf{Z}_2[[T]]$ if and only if $\psi(c) = 0$.*

*Proof.* We may assume that $c \neq 0$. If $\psi(T) = (T - c)\phi(T)$ with $\phi(T) \in \mathbf{Z}_2[[T]]$, then $\psi(c) = (c - c)\phi(c) = 0$, the substitution being possible since all series involved are convergent. Conversely, if

$$\psi(c) = b_0 + b_1 c + b_2 c^2 + \ldots + b_j c^j + \ldots = 0$$

and

$$c_j = -(b_0 + b_1 c + \ldots + b_j c^j)/c^{j+1},$$

then $c_j \in \mathbf{Z}_2$ for $j \geqslant 0$. If we set

$$\phi(T) = c_0 + c_1 T + c_2 T^2 + \ldots + c_j T^j + \ldots,$$

then $\phi(T) \in \mathbf{Z}_2[[T]]$ and $\psi(T) = (T - c)\phi(T)$.

If we set

$$\psi_1(T) = 1 + \alpha + (1 + T)^a \quad \text{and} \quad \psi_2(T) = 2^g - 1 + (1 + T)^{ab},$$

then

$$\psi_1(-2 - 2^f) = 1 + \alpha + (-1 - 2^f)^a = 1 + \alpha - (1 + 2^f)^a = 0$$

and

$$\psi_2(-2 - 2^f) = 2^g - 1 + (-2 - 2^f)^{ab} = 2^g - 1 + (-(1 + \alpha))^b = 2^g - 1 + (1 + \alpha)^b = 0.$$

Hence by the lemma there are power series $\phi_1(T)$, $\phi_2(T)$ in $\mathbf{Z}_2[[T]]$ such that

$$\psi_i(T) = (2 + 2^f + T)\phi_i(T) \qquad \text{for } i = 1, 2.$$

Then

$$\bar{r} = (2 + 2^f + T)(\phi_1(T)\bar{y}_1 + \phi_2(T)\bar{y}_3).$$

Let $z_1$ be an element of $X$ whose image in $E = X/(X, X)$ is

$$\phi_1(T)\bar{y}_1 + \phi_2(T)\bar{y}_3$$

and let $z_i = y_i$ for $i \neq 1$. Then, since $\phi_1(0)$ is a unit and $\phi_2(0) \in 2\mathbf{Z}_2$, we have $z_i \equiv y_i \pmod{F_2 \cap X}$ and

$$\bar{r} = (2 + 2^f + T)\bar{z}_1.$$

Hence $z_1, \ldots, z_n$ is a basis of $F$ with $\chi(y_i) = \chi(z_i)$, and

$$r = z_1^{2+2^f}(z_1, z_2)(z_3, z_4) \ldots (z_{n-1}, z_n)e$$

with $e \in (X, X)$. If we set $y_i = t_i z_i$ ($t_i \in F_2$) in the expression for $r$ in terms of the basis $(y_i)$ and make use of Proposition 1, we also see that $e \in F_3$.

THEOREM 5. *Let $r$ be a Demushkin relation in the free pro-2-group $F$ of even rank $n$. Let $\chi$ be the character associated with the Demushkin group $G = F/(r)$, and suppose that* $\mathrm{Im}(\chi) = \mathbf{U}_2^{[f]}$ *with $f \neq \infty$. Then there exists a basis $x_1, \ldots, x_n$ of $F$ such that*

$$r = x_1^{2+2^f}(x_1, x_2)(x_3, x_4) \ldots (x_{n-1}, x_n).$$

*Proof.* For any basis $x = (x_i)$ of $F$ let

$$r_0(x) = x_1^{2+2^f}(x_1, x_2)(x_3, x_4) \ldots (x_{n-1}, x_n).$$

The above results show that there exists a basis of $F$ such that $r = r_0(x)e_3$ with $e_3 \in (X, X) \cap F_3$. Fix this basis and let $\xi_i$ be the image of $x_i$ in $\mathrm{gr}_1(F)$. We shall show that it is possible to correct $x$ successively by factors $t$ in $X$ so that the desired result is obtained by passing to the limit.

Let $\mathrm{gr}(X)$ be the Lie algebra associated with the filtration $(X_i)$ of $X$ where $X_i = X \cap F_i$. Then the inclusion $X \subset F$ defines an injection of the Lie algebra $\mathrm{gr}(X)$ into the Lie algebra $\mathrm{gr}(F)$, and we use this homomorphism to identify $\mathrm{gr}(X)$ with its image in $\mathrm{gr}(F)$. Now let $y = (y_i)$ be a basis of $F$ with

$y_i \equiv x_i \pmod{X_2}$ and let $t = (t_1, \ldots, t_n)$ be a family of elements in $X_{j-1}$ for some $j \geqslant 3$. If $z_i = y_i t_i^{-1}$, then $z = (z_i)$ is a basis of $F$ and

$$r_0(y) = r_0(z) d_{j-1}(t)$$

where $d_{j-1}(t)$ is a uniquely defined element of $X_j$. Noting that the image of $y_i$ in $\mathrm{gr}_1(F)$ is $\xi_i$, the image of $d_{j-1}(t)$ in $\mathrm{gr}_j(X)$ is

$$\pi \cdot \tau_1 + [\tau_1, \xi_1] + [\tau_1, \xi_2] + [\xi_1, \tau_2] + \ldots + [\tau_{n-1}, \xi_n] + [\xi_{n-1}, \tau_n]$$

where $\tau_i$ is the image of $t_i$ in $\mathrm{gr}_{j-1}(X)$. Hence $d_{j-1}$ induces a linear map

$$\delta_{j-1}\colon \mathrm{gr}_{j-1}(X)^n \to \mathrm{gr}_j(X).$$

LEMMA 1. *$\mathrm{gr}(X)$ is an ideal of $\mathrm{gr}(F)$ and for $i \geqslant 1$ the abelian group $\mathrm{gr}_i(F)$ is generated by $\mathrm{gr}_i(X)$ and $\pi^{i-1} \cdot \xi_2$. Moreover, $\pi^{i-1} \cdot \xi_2 \notin \mathrm{gr}_i(X)$.*

*Proof.* We have an exact sequence

$$0 \to X \to F \xrightarrow{\phi} 2Z_2 \to 0$$

where $\phi$ is the continuous homomorphism defined by

$$\phi(x_2) = 2, \qquad \phi(x_i) = 0 \quad \text{for } i \neq 2.$$

The groups $\phi(F_i) = 2^i \mathbf{Z}_2$ give a filtration of $2\mathbf{Z}_2$ whose associated Lie algebra may be identified with the abelian Lie algebra $\pi \mathbf{F}_2[\pi]$, with the graduation defined by the fact that $\pi^i$ is of degree $i$. ($\pi^i$ is the image of $2^i$ in $2^i\mathbf{Z}_2/2^{i+1}\mathbf{Z}_2$.) The above exact sequence induces an exact sequence of graded Lie algebras cf. (**6**, p. 112, Theorem 2.4),

$$0 \longrightarrow \mathrm{gr}(X) \longrightarrow \mathrm{gr}(F) \xrightarrow{\phi_*} \pi \mathbf{F}_2[\pi] \longrightarrow 0$$

with $\phi_*(\pi^{i-1} \cdot \xi_2) = \pi^i$. But this implies our lemma.

LEMMA 2. *For $i \geqslant 3$, the abelian group $\mathrm{gr}_i(X)$ is generated by elements of the form $\pi \cdot \tau$, $[\tau, \xi_j]$ with $\tau \in \mathrm{gr}_{i-1}(X)$.*

*Proof.* Let $\mathfrak{A}_i$ be the subgroup of $\mathrm{gr}_i(X)$ generated by the elements $\pi \cdot \tau$, $[\tau, \xi_j]$ with $\tau \in \mathrm{gr}_{i-1}(X)$ and let $\xi \in \mathrm{gr}_i(X)$. Then

$$\xi = \pi \cdot \tau_0 + \sum_{j=1}^{m} [\tau_j, \xi_j]$$

where $\tau_j \in \mathrm{gr}_{i-1}(F)$. But by Lemma 1,

$$\tau_j = a_j \pi^{i-2} \cdot \xi_2 + h_j \qquad \text{with} \quad a_j \in \mathbf{F}_2, \quad h_j \in \mathrm{gr}_{i-1}(X).$$

Now if $j \neq 0$, we have

$$\begin{aligned}
[\tau, \xi_j] &= a_j \pi^{i-3} \cdot [\pi \cdot \xi_2, \xi_j] + [h_j, \xi_j] \\
&= a_j \pi^{i-2} \cdot [\xi_2, \xi_j] + a_j \pi^{i-3} \cdot [[\xi_2, \xi_j], \xi_2] + [h_j, \xi_j] \\
&= \pi \cdot (a_j \pi^{i-3} \cdot [\xi_2, \xi_j]) + [a_j \pi^{i-3} \cdot [\xi_2, \xi_j], \xi_2] + [h_j, \xi_j] \in \mathfrak{A}_i
\end{aligned}$$

https://doi.org/10.4153/CJM-1967-007-8 Published online by Cambridge University Press

since $a_j \pi^{i-3} \cdot [\xi_2, \xi_j] \in \mathrm{gr}_{i-1}(X)$. In particular, this implies that $\pi \cdot \tau_0 \in \mathrm{gr}_i(X)$. But $\pi \cdot \tau_0 = a_0 \pi^{i-1} \cdot \xi_2 + \pi \cdot h_0$ implies that $a_0 = 0$. Hence $\pi \cdot \tau_0 \in \mathfrak{A}_i$, which means that $\xi \in \mathfrak{A}_i$. Consequently, $\mathfrak{A}_i = \mathrm{gr}_i(X)$.

LEMMA 3. *If $i \geqslant 3$, the abelian group $\mathrm{gr}_i(X)$ is generated by $\mathrm{Im}(\delta_{i-1})$ and the elements $\pi^{i-1} \cdot \xi_j$ with $j \neq 2$.*

*Proof.* Let $\mathfrak{H}_i$ be the group generated by $\mathrm{Im}(\delta_{i-1})$ and $\pi^{i-1} \cdot \xi_j$ with $j \neq 2$. $\mathrm{Im}(\delta_{i-1})$ is generated by elements of the form

$$\pi \cdot \tau + [\tau, \xi_2], \quad [\tau, \xi_j] \qquad (j \neq 2), \qquad \text{with} \quad \tau \in \mathrm{gr}_{i-1}(X).$$

To prove that $\mathfrak{H}_i = \mathrm{gr}_i(X)$, it suffices to show that $\pi \cdot \tau \in \mathfrak{H}_i$ for any $\tau \in \mathrm{gr}_{i-1}(X)$ by virtue of Lemma 2. Using induction it suffices, therefore, to show that (a) $\pi \mathfrak{H}_{i-1} \subset \mathfrak{H}_i$ for $i \geqslant 4$ and (b) $\pi \mathrm{gr}_2(X) \subset \mathfrak{H}_3$. Now (a) follows because $\delta_i \pi = \pi \delta_{i-1}$ for $i \geqslant 3$. We have only to show (b).

By Lemma 1 the group $\mathrm{gr}_2(X)$ is generated by the elements $\pi \cdot \xi_j$ $(j \neq 2)$, $[\xi_j, \xi_k]$ $(j < k)$. To prove that $\pi \cdot \tau \in \mathfrak{H}_3$ for any $\tau \in \mathrm{gr}_2(X)$, it suffices to show that $\pi^2 \cdot \xi_j$ $(j \neq 2)$, $\pi \cdot [\xi_j, \xi_k]$ $(j < k)$ are in $\mathfrak{H}_3$. But the elements $\pi^2 \cdot \xi_j$ $(j \neq 2)$ are in $\mathfrak{H}_3$ by definition. If $j, k \neq 2$, then $[[\xi_j, \xi_k], \xi_2] \in \mathfrak{H}_3$ by virtue of Jacobi's identity. Hence $\pi \cdot [\xi_j, \xi_k] \in \mathfrak{H}_3$ if $j, k \neq 2$. But

$$[\pi \cdot \xi_j, \xi_2] = \pi \cdot [\xi_j, \xi_2] + [[\xi_j, \xi_2], \xi_j]$$

and $[\pi \cdot \xi_j, \xi_2], [[\xi_j, \xi_2], \xi_j] \in \mathfrak{H}_3$ imply that $\pi \cdot [\xi_j, \xi_2] \in \mathfrak{H}_3$. Hence (b) is proved and the proof of the lemma is complete.

LEMMA 4. *Let $I = I(\chi)$ be the $F$-module defined in §3 and let $D$ be a crossed homomorphism of $F$ into $2I$. Then, if we identify $\sum_{i \geqslant 1} 2^i I / 2^{i+1} I$ with $\pi \mathbf{F}_2[\pi]$ as in the proof of Lemma 1, we have*

(1) *$D$ induces a linear map $\Delta: \mathrm{gr}(F) \to \pi \mathbf{F}_2[\pi]$,*

(2) $\Delta \circ \delta_i = 0$,

(3) *if $D_i$ is the crossed homomorphism with $D_i(x_j) = 2\delta_{ij}$ and $\Delta_i$ is the corresponding linear map, then*

$$\Delta_i(\pi^{j-1} \xi_k) = \pi^j \delta_{ik} \qquad \textit{if } k \neq 2,$$

(4) $\mathrm{Im}(\delta_{i-1}) = \bigcap_\Delta (\ker(\Delta) \cap \mathrm{gr}_i(X)) \qquad$ *for $i \geqslant 3$.*

*Proof.* (1) We first prove $D(F_i) \subset 2^i I$. By hypothesis $D(F_1) \subset 2I$. If $D(F_i) \subset 2^i I$ and $x \in F_i$, then

$$Dx^2 = Dx + xDx = (1 + \chi(x))Dx \subset 2^{i+1} I$$

since $\chi(x)$ is a unit. Also

$$D(x, y) = x^{-1} y^{-1}((1 - \chi(y))Dx + (\chi(x) - 1)Dy \in 2^{i+1} I$$

for any $y \in F$. Since the elements $x^2$, $(x, y)$ with $x \in F_i$, $y \in F$ generate $F_{i+1}$, we have $D(F_{i+1}) \subset 2^{i+1} I$.

https://doi.org/10.4153/CJM-1967-007-8 Published online by Cambridge University Press

Now let $x \in F_i$, $y \in F_{i+1}$. Then $Dxy - Dx = xDy \in 2^{i+1}I$. Hence $D$ induces a map $\Delta$: $\mathrm{gr}_i(F) \to 2^iI/2^{i+1}I$. Moreover, if $x, y \in F_i$, then

$$Dxy = Dx + xDy = Dx + (1 + 2u)Dy \qquad \text{with } u \in \mathbf{Z}_2,$$

which implies that $Dxy - Dx - Dy \in 2^{i+1}I$. Hence $\Delta$ is linear.

(2) If $t_1, \ldots, t_n \in X_{i-1}$, then

$$\begin{aligned} &D(t_1^{2+2^f}(t_1, x_1)(t_1, x_2)(x_1, t_2) \ldots (t_{n-1}, x_n)(x_{n-1}, t_n)) \\ &\quad = (2 + 2^f)Dt_1 + D(t_1, x_2) = (2 + 2^f)Dt_1 + (\chi(x_2)^{-1} - 1)Dt_1 \\ &\quad = (2 + 2^f - 1 - 2^f - 1)Dt_1 = 0. \end{aligned}$$

(3) $D_i(x_k^{2^{j-1}}) = 2^{j-1}D_i(x_k) = 2^j\delta_{ik}$ if $k \neq 2$.

(4) Follows from Lemma 3 and (1)–(3) of this lemma.

We are now in a position to complete the proof of Theorem 5. Suppose that $r = r_0(y)e_j$, where

(i) $y_1, \ldots, y_n$ is a basis of $F$ with $y_i \equiv x_i \pmod{X_2}$;

(ii) $e_j \in X_j$ with $j \geqslant 3$ and $De_j = 0$ for any crossed homomorphism $D$ of $F$ into $I$.

(If $j = 3$, choose $y_i = x_i$. Then (ii) is satisfied since $D(X, X) = 0$.) If $z_i = y_i t_i^{-1}$ with $t_i \in X_{j-1}$, then working modulo $(X, X) \cap F_{j+1}$ we obtain $r = r_0(z)e_1 e_j$ with

$$e_1 = t_1^{2+2^f}(t_1, z_1)(t_1, z_2)(z_1, t_2) \ldots (t_{n-1}, z_n)(z_{n-1}, t_n) \in X_j.$$

Hence $r \equiv r_0(z)e_{j+1}$ with $e_{j+1} = e_1 e_j e'_1$, where $e'_1 \in (X, X) \cap F_{j+1}$. Now if $D$ is a crossed homomorphism of $F$ into $I$ we have

$$De_{j+1} = De_1 + De_j + De'_1.$$

But $De_j = 0$ by (ii), $De'_1 = 0$ since $D$ vanishes on $(X, X)$, and $De_1 = 0$ as in the proof of Lemma 4, 2. If $\epsilon_j$ and $\epsilon_{j+1}$ are the images of $e_j$ and $e_{j+1}$ respectively in $\mathrm{gr}_j(F)$, we have

$$\epsilon_{j+1} = \epsilon_j + \delta_{j-1}(\tau_1, \ldots, \tau_n)$$

where $\tau_i$ is the image of $t_i$ in $\mathrm{gr}_{j-1}(X)$. By virtue of Lemma 3 we can choose the $t_i$ so that

$$\epsilon_j = \sum_{i\neq 2} a_i \pi^{j-1}\xi_i + \delta_j(\tau_1, \ldots, \tau_n).$$

But if $i \neq 2$,

$$0 = \Delta_i(\epsilon_j) = a_i \pi^j,$$

which implies that $a_i = 0$. Hence $\epsilon_{j+1} = 0$. This means that we have found a basis $z_1, \ldots, z_n$ of $F$ with $r = r_0(z)e_{j+1}$, where (i) and (ii) are satisfied with $y_i$ and $j$ replaced by $z_i$ and $j + 1$ respectively. Iterating this process and passing to the limit we obtain the desired result.

**4.2.** $\mathrm{Im}(\chi) \cong (\mathbf{Z}/2\mathbf{Z}) \times \mathbf{Z}_2$. In this section

$$\mathrm{Im}(\chi) = \{\pm 1\} \times \mathbf{U}_2^{(f)} \qquad \text{with } f \geqslant 2, f \neq \infty.$$

Then by Theorem 3 and the Corollary to Theorem 4, we have $n \geqslant 4$ and there exists a basis $w_1, \ldots, w_n$ for $F$ such that

$$r = w_1^{2+\alpha}(w_1, w_2)w_3^{2^f}(w_3, w_4) \ldots (w_{n-1}, w_n)$$

where $\alpha \in 4\mathbf{Z}_2$ and $f \leqslant v_2(\alpha)$. We want to find a basis such that $r$ has the above form with $\alpha$ replaced by 0. Hence we may assume that $\alpha \neq 0$. We also lose no generality if we assume that $n = 4$.

The proof of Theorem 4 implies that

$$\chi(w_1) = 1, \quad \chi(w_2) = -(1+\alpha)^{-1}, \quad \chi(w_3) = 1, \quad \chi(w_4) = (1-2^f)^{-1}.$$

Let $b$ be the unique 2-adic integer such that $(1-2^f)^b = 1 + \alpha$ and let

$$y_2 = w_2 w_4^{-b}, \qquad y_i = w_i \quad \text{for } i \neq 2.$$

Then $y_1, \ldots, y_4$ is a basis of $F$, and
$\chi(y_1) = 1, \quad \chi(y_2) = -1, \quad \chi(y_3) = 1, \quad \chi(y_4) = (1-2^f)^{-1},$

$$r = y_1^{2+\alpha}(y_1, y_2)(y_1, y_4^b)y_3^{2^f}(y_3, y_4)((y_1, y_4^b), y_2)e_0$$

with $e_0 \in (X, X)$. Let $H$ and $K$ be the subgroups of $\Gamma$ generated by $S = \bar{y}_2$ and $\gamma = \bar{y}_4$ respectively. Then $\Gamma = H \times K$ with $H \cong \mathbf{Z}/2\mathbf{Z}$, $K \cong \mathbf{Z}_2$ and there is an isomorphism of $\mathbf{Z}_2(\Gamma)$ onto $\mathbf{Z}_2[S] \otimes_{\mathbf{Z}_2} \mathbf{Z}_2[[T]]$ sending $S$ into $S$ and $\gamma$ into $1 + T$. Thus, if $\bar{r}$ is the image of $r$ in $E$, we have

$$\begin{aligned}\bar{r} &= (2 + \alpha + S - 1 + (1+T)^b - 1 + (S-1)((1+T)^b - 1))\bar{y}_1 \\ &\qquad\qquad + (2^f + T)\bar{y}_3 \\ &= (1 + \alpha + S(1+T)^b)\bar{y}_1 + (2^f + T)\bar{y}_3.\end{aligned}$$

LEMMA. *There exists* $\phi(S, T) \in \mathbf{Z}_2[S] \otimes_{\mathbf{Z}_2} \mathbf{Z}_2[[T]]$ *such that*

$$(1 + \alpha + S(1+T)^b)(1+\alpha)^{-1} + (2^f + T)\phi(S, T) = 1 + \mathrm{S}.$$

*Proof.* Let

$$\theta(S, T) = (1 + \alpha + S(1+T)^b)(1+\alpha)^{-1} - S - 1.$$

Then

$$\theta(S, T) = S((1+T)^b(1+\alpha)^{-1} - 1) = S\theta(T).$$

Now

$$\theta(-2^f) = (1-2^f)^b(1+\alpha)^{-1} - 1 = (1+\alpha)(1+\alpha)^{-1} - 1 = 0.$$

Hence there exists $\phi(T) \in \mathbf{Z}_2[[T]]$ such that $\theta(T) = (2^f + T)\phi(T)$. Then $\phi(S, T) = S\phi(T)$ is the required element.

Now let $z_1, z_2$ be elements of $X$ such that their images in $E$ are respectively $(1+\alpha)\bar{y}_1$, $\bar{y}_3 - (1+\alpha)\phi(S, T)\bar{y}_1$. Then $\bar{y}_1 = (1+\alpha)^{-1}\bar{z}_1$, $\bar{y}_3 = \phi(S, T)\bar{z}_1 + \bar{z}_3$ and

$$\begin{aligned}\bar{r} &= ((1 + \alpha + S(1+T)^b)(1+\alpha)^{-1} + (2^f + T)\phi(S, T))\bar{z}_1 + (2^f + T)\bar{z}_3 \\ &= (1 + S)\bar{z}_1 + (2^f + T)\bar{z}_3.\end{aligned}$$

Hence, if we set $z_2 = y_2$, $z_4 = y_4$, then $z_1, \ldots, z_4$ is a basis of $F$,

$$\chi(z_1) = 1, \quad \chi(z_2) = -1, \quad \chi(z_3) = 1, \quad \chi(z_4) = (1 - 2^f)^{-1},$$

and

$$r = z_1^2(z_1, z_2)z_3^{2^f}(z_3, z_4)e_1$$

with $e_1 \in (X, X)$.

Now $e_1 = (z_1, z_3)^a e'_1$ where $a \in \mathbf{Z}_2$ and $e'_1 \in (X, X) \cap F_3$. Set

$$x_1 = z_i \text{ if } i \neq 2 \quad \text{and } x_2 = z_2 z_3^{-a}.$$

Then $x_1, \ldots, x_4$ is a basis of $F$, $\chi(x_i) = \chi(z_i)$, and

$$r = x_1^2(x_1, x_2)x_3^{2^f}(x_3, x_4)(x_1, x_3)^{2a}e''_1$$

with $e''_1 \in (X, X) \cap F_3$.

THEOREM 6. *Let $r$ be a Demushkin relation in the free pro-2-group $F$ of even rank $n$. Let $\chi$ be the character associated with the Demushkin group $G = F/(r)$ and suppose that* $\mathrm{Im}(\chi) = \{\pm 1\} \times \mathbf{U}_2^{(f)}$ *with* $2 \leqslant f < \infty$. *Then there exists a basis $x_1, \ldots, x_n$ of $F$ such that*

$$r = x_1^2(x_1. x_2)x_3^{2^f}(x_3, x_4)(x_5, x_6) \ldots (x_{n-1}, x_n).$$

*Proof.* By an earlier remark it suffices to prove the theorem in the case $n = 4$. For any basis $x = (x_i)$ of $F$, set

$$r_0(x) = x_1^2(x_1, x_2)x_3^{2^f}(x_3, x_4).$$

The above results show that there exists a basis $x = (x_i)$ of $F$ such that

$$\chi(x_1) = 1, \quad \chi(x_2) = -1, \quad \chi(x_3) = (1 - 2^f)^{-1}, \quad \chi(x_4) = 1,$$

and

$$r = r_0(x)e_3$$

where $e_3 \in (X, X) \cap F_3$. We fix this basis and let $\xi_i$ be the image of $x_i$ in $\mathrm{gr}_i(F)$. Then, as in the proof of Theorem 5, we define the Lie algebra $\mathrm{gr}(X)$ and the linear map $\delta_{j-1}\colon \mathrm{gr}_{j-1}(X)^4 \to \mathrm{gr}_j(X)$. Recall that

$$\delta_{j-1}(\tau_1, \ldots, \tau_4) = \pi \cdot \tau_1 + [\tau_1, \xi_1] + [\tau_1, \xi_2] + [\xi_1, \tau_2] + \ldots$$

for $\tau_1, \ldots, \tau_4 \in \mathrm{gr}_{j-1}(X)$.

LEMMA 1. *For $i \geqslant 2$ the abelian group $\mathrm{gr}_i(F)$ is generated by $\mathrm{gr}_i(X)$ and $\pi^{i-1}\cdot\xi_4$. Moreover, $\pi^{i-1}\cdot\xi_4 \notin \mathrm{gr}_i(X)$.*

*Proof.* We have an exact sequence

$$0 \to X \to F \xrightarrow{\phi} (\mathbf{Z}/2\mathbf{Z}) \times (2\mathbf{Z}_2) \to 0$$

where $\phi(x_4) = 2 \in 2\mathbf{Z}_2$, $\phi(x_2) = 1 \in \mathbf{Z}/2\mathbf{Z}$, $\phi(x_1) = \phi(x_3) = 0$. Then $\phi(F_i) = \{0\} \times 2^i\mathbf{Z}_2$ for $i \geqslant 2$ and $\mathfrak{A}_i = \phi(F_i)/\phi(F_{i+1}) \cong 2^i\mathbf{Z}_2/2^{i+1}\mathbf{Z}_2$. If $\mathfrak{A}$

is the abelian Lie algebra $\sum \mathfrak{A}_i$, we have the exact sequence of graded Lie algebras

$$0 \longrightarrow \mathrm{gr}(X) \longrightarrow \mathrm{gr}(F) \xrightarrow{\phi_*} \mathfrak{A} \longrightarrow 0$$

with $\phi_*(\pi^{i-1}\cdot\xi_4) \neq 0$.

LEMMA 2. *For $i \geqslant 3$ the abelian group $\mathrm{gr}_i(X)$ is generated by elements of the form $\pi\cdot\tau$, $[\tau, \xi_j]$ with $\tau \in \mathrm{gr}_{i-1}(X)$.*

*Proof.* Follows from Lemma 1 as in §4.1.

LEMMA 3. *If $i \geqslant 3$ the abelian group $\mathrm{gr}_i(X)$ is generated by $\mathrm{Im}(\delta_{i-1})$ and the elements $\pi^{i-2}\cdot[\xi_2, \xi_4]$, $\pi^{i-1}\cdot\xi_1$, $\pi^{i-1}\cdot\xi_3$.*

*Proof.* As in the proof of the corresponding Lemma 3 in §4.1, it suffices to prove that $\pi\mathrm{gr}_2(X) \subset \mathfrak{H}_3$ where $\mathfrak{H}_3$ is the group generated by $\mathrm{Im}(\delta_{i-1})$ and the elements $\pi^{i-2}\cdot[\xi_2, \xi_4]$, $\pi^{i-1}\cdot\xi_1$, and $\pi^{i-1}\cdot\xi_3$. By Lemma 3, group $\mathrm{gr}_2(X)$ is generated by $\pi\cdot\xi_j$ $(j \neq 4)$ and $[\xi_j, \xi_k]$ $(j > k)$. Now $\pi^2\cdot\xi_1, \pi^2\cdot\xi_3 \in \mathfrak{H}_3$ by definition and

$$\pi^2\cdot\xi_2 + [\pi\cdot\xi_2, \xi_2] = \pi^2\cdot\xi_2 \in \mathrm{Im}(\delta_2).$$

If $j, k \neq 2$, then $[[\xi_j, \xi_k], \xi_2] \in \mathrm{Im}(\delta_2)$ by virtue of Jacobi's identity. Hence $\pi\cdot[\xi_j, \xi_k] \in \mathfrak{H}_3$ if $j, k \neq 2$. If $j \neq 4$, then $\pi^2\cdot\xi_j + [\pi\cdot\xi_j, \xi_2] \in \mathrm{Im}(\delta_2)$ which implies that $[\pi\cdot\xi_j, \xi_2] \in \mathfrak{H}_3$. Now

$$[\pi\cdot\xi_j, \xi_2] = \pi\cdot[\xi_j, \xi_2] + [[\xi_j, \xi_2], \xi_j];$$

hence $[\pi\cdot\xi_j, \xi_2] \in \mathfrak{H}_3$ if $j \neq 4$. But $\pi\cdot[\xi_4, \xi_2] \in \mathfrak{H}_3$ by definition. Hence $\pi\cdot\tau \in \mathfrak{H}_3$ for any $\tau \in \mathrm{gr}_2(X)$ and the proof of the lemma is complete.

LEMMA 4. *Same as Lemma 4 of §4.1 except that (3) is to be replaced by*

(3) *Let $D_i$ be the crossed homomorphism of $F$ into $I$ such that $D_i(x_j) = 2\delta_{ij}$. Then if $\Delta_i$ is the corresponding linear map of $\mathrm{gr}(F)$ into $\pi\mathbf{F}_2[\pi]$, we have*

$$\Delta_i(\pi^{j-1}\cdot\xi_k) = \pi^j\,\delta_{ik} \quad \textit{if} \quad k \neq 2,4 \quad \textit{and} \quad \Delta_4(\pi^{j-2}\cdot[\xi_2, \xi_4]) = \pi^j.$$

*Proof.* It suffices to prove (2) and (3).

(2) If $t_1, \ldots, t_4 \in X_{i-1}$, then

$$\begin{aligned} &D(t_i^2(t_1, x_1)(x_1, t_2)(t_1, x_2)t_3^{2^f}(t_3, x_4)(x_3, t_4)) \\ &\quad = 2Dt_1 + (\chi(x_2) - 1)Dt_1 + 2^f Dt_3 + (\chi(x_4)^{-1} - 1)Dt_3 \\ &\quad = (2 - 2)Dt_1 + (2^f + 1 - 2^f - 1)Dt_3 = 0. \end{aligned}$$

(3) $D_i(x_k^{2^{j-1}}) = 2^{j-1}D_i(x_k) = 2^j\delta_{ik}$ if $k \neq 2, 4$ and

$$D_2(x_2, x_4)^{2^{j-2}} = 2^{j-2}D_2(x_2, x_4) = -2^{j-2}(1 - 2^f)(\chi(x_2) - 1)D_4 x_4 = 2^j(1 - 2^f).$$

We can now complete the proof of Theorem 6. Suppose that $r = r_0(y)e_j$ where

(i) $y_1, \ldots, y_4$ is a basis of $F$ with $y_i \equiv x_i \pmod{X_2}$;

(ii) $e_j \in X_j$ $(j \geqslant 3)$ and $De_j = 0$ for any crossed homomorphism of $F$ into $I$.

Note that (i) and (ii) are satisfied for $j = 3$ if we choose $y_i = x_i$.

https://doi.org/10.4153/CJM-1967-007-8 Published online by Cambridge University Press

If $z_i = y_i t_i^{-1}$ with $t_i \in X_{j-1}$, then $r = r_0(z)e_{j+1}$, where $e_{j+1} = e_1 e_j e'_1$ with $e'_1 \in (X, X) \cap F_{j+1}$ and

$$e_1 = t_1^2(t_1, z_1)(t_1, z_2)(z_1, t_2)t_3^{2^f}(t_3, z_4)(z_3, t_4) \in X_j.$$

If $D$ is a derivation of $F$ into $I$, then

$$De_{j+1} = De_1 + De_j + De'_1 = 0.$$

If $\epsilon_j$ and $\epsilon_{j+1}$ are the images of $e_j$ and $e_{j+1}$ respectively in $\mathrm{gr}_j(X)$, then

$$\epsilon_{j+1} = \epsilon_j + \delta_j(\tau_1, \ldots, \tau_n)$$

where $\tau_i$ is the image of $t_i$ in $\mathrm{gr}_{j-1}(X)$. By Lemma 3, we may choose $t_1, \ldots, t_4$ so that

$$\epsilon_j = a\pi^{j-2}\cdot[\xi_2, \xi_4] + a_1\pi^{j-1}\cdot\xi_1 + a_3\pi^{j-1}\cdot\xi_3 + \delta_{j-1}(\tau_1, \ldots, \tau_n).$$

But $0 = \Delta_4(\epsilon_j) = a\pi^j$ implies that $a = 0$, and $0 = \Delta_i(a_i\pi^{j-1}\cdot\xi_i) = a_i\pi^{j-1}$ for $i = 1, 3$ implies that $a_1 = a_3 = 0$. Hence $\epsilon_{j+1} = 0$. This means that we have found a basis $z_1, \ldots, z_4$ for $F$ with $r = r_0(z)e_{j+1}$ where (i) and (ii) are satisfied with $y_i$ and $j$ replaced by $z_i$ and $j + 1$ respectively. Iterating this process and passing to the limit, we obtain the desired result.

Theorem 1 now follows immediately from Theorems 3–6.

**§5. Applications: The group of the maximal $p$-extension of a local field.** Let $\mathbf{Q}_p$ be the field of $p$-adic rationals and let $K$ be a finite extension of $\mathbf{Q}_p$ of degree $d$. Let $K(p)$ be the largest Galois extension of $K$ whose Galois group $G$ is a pro-$p$-group. The field $K(p)$ is called the maximal $p$-extension of $K$. In this section we shall determine the structure of $G$.

If $K$ does not contain a primitive $p$th root of unity, Shafarevich **(10)** has shown that $G$ is a free pro-$p$-group of rank $d + 1$. Suppose then that $K$ contains a primitive $p$th root of unity. Following Serre **(8)** we shall show that $G$ is a Demushkin group. By local class field theory $G/(G, G)$ is isomorphic to the $p$-completion of $K^*$, that is, to the product $(\mathbf{Z}/q\mathbf{Z}) \times \mathbf{Z}_p^{d+1}$ where $q$ is a finite power of $p$. The integer $q$ is the highest power of $p$ such that $K$ contains a primitive $q$th root of unity. Hence $H^1(G) \cong (\mathbf{Z}/p\mathbf{Z})^{d+2}$, which implies that $n(G) = d + 2$. Choosing a primitive $p$th root of unity we may identify $\mathbf{Z}/p\mathbf{Z}$ with the group of $p$th roots of unity in $K$. We then have the exact sequence

$$0 \to \mathbf{Z}/p\mathbf{Z} \to K(p)^* \xrightarrow{p} K(p)^* \to 0.$$

Taking cohomology, we obtain the exact sequences

(1) $$K^* \xrightarrow{p} K^* \to H^1(G) \to 0,$$

(2) $$0 \to H^2(G) \to H^2(G, K(p)^*) \xrightarrow{p} H^2(G, K(p)^*).$$

By local class field theory we have

$$H^2(G, K(p)^*) = \mathbf{Q}_p/\mathbf{Z}_p.$$

Hence by (2),

$$H^2(G) = \mathbf{Z}/p\mathbf{Z}.$$

On the other hand, using the sequence (1) we see that $H^1(G)$ may be identified with $K^*/K^{*p}$. With the above identifications Serre has shown **(7**, ch. XIV**)** that the cup product

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

corresponds to the Hilbert symbol $(a, b)$. It is well known that this symbol is non-degenerate. Hence $G$ is a Demushkin group with invariants $n(G) = d + 2$, $q(G) = q$. Using Theorem 3, we obtain the following theorem due to Demushkin **(1; 2)**.

THEOREM 7. *If $q \neq 2$, the group $G$ can be defined by $d + 2$ generators $x_1, \ldots, x_{d+2}$ with the single relation*

$$x_1^q(x_1, x_2)(x_3, x_4)\ldots(x_{d+1}, x_{d+2}) = 1.$$

In order to determine $G$ in the case $q = 2$, we must determine the invariant $\operatorname{Im}(\chi)$ where $\chi\colon G \to \mathbf{U}_p$ is the character defined in §3. Let

$$\mathbf{Q}_p(\zeta_{p^\infty}) = \bigcup_{N=1}^{\infty} \mathbf{Q}_p(\zeta_{p^N})$$

be the field of $p^N$th $(N \to \infty)$ roots of unity. The Galois group of $\mathbf{Q}_p(\zeta_{p^\infty})/\mathbf{Q}_p$ is canonically isomorphic to $\mathbf{U}_p$ under the map $a \mapsto \sigma_a$, where $\sigma_a(\zeta) = \zeta^a$ for all roots of unity $\zeta$. Since $\mathbf{Q}_p(\zeta_{p^\infty}) \subset K(p)$, we obtain a continuous homomorphism $\chi'\colon G \to \mathbf{U}_p$ where $\operatorname{Im}(\chi')$ is the Galois group of $\mathbf{Q}_p(\zeta_{p^\infty})/K'$, with $K' = K \cap \mathbf{Q}_p(\zeta_{p^\infty})$. Using the exact sequence

$$0 \longrightarrow \mu_{p^n} \longrightarrow K(p)^* \xrightarrow{p^n} K(p)^* \longrightarrow 0$$

and choosing the primitive $p^n$th root of unity $\zeta_{p^n}$ properly for $n \geqslant 1$ (that is, so that $\zeta_{p^{n+1}}{}^p = \zeta_{p^n}$ for $n \geqslant 1$), we obtain a commutative diagram

$$\begin{array}{ccccc} K^*/K^{*p^n} & \to & H^1(G, \mu_{p^n}) & \to & H^1(G, I/p^nI) \\ \downarrow & & \downarrow & & \downarrow \\ K^*/K^{*p} & \to & H^1(G, \mu_p) & \to & H^1(G, I/pI) \end{array}$$

for $n \geqslant 1$, where $I = I(\chi')$ is the profinite $G$-module defined in §3. Since the horizontal arrows are all isomorphisms and $K^*/K^{*p^n} \to K^*/K^{*p}$ is surjective, we see that $H^1(G, I/p^nI) \to H^1(G, I/pI)$ is surjective for $n \geqslant 1$. Hence, by Theorem 4, $\chi = \chi'$.

If $q = 2$ and $d$ is odd, then $K' = K$ and hence $\operatorname{Im}(\chi) = \mathbf{U}_2^{(1)} = \{\pm 1\} \times \mathbf{U}_2^{(2)}$. Using Theorem 3 and the Corollary to Theorem 4, we obtain the following theorem due to Serre **(8)**.

THEOREM 8. *If $q = 2$ and $d$ is odd, then the group $G$ can be defined by $d + 2$ generators $x_1, \ldots, x_{d+2}$ with the single relation*

$$x_1^2 x_2^4 (x_2, x_3)(x_4, x_5) \ldots (x_{d+1}, x_{d+2}) = 1.$$

As for the case $q = 2$, $d$ even, we have by Theorem 1:

THEOREM 9. *If $q = 2$ and $d$ is even, then the group $G$ can be defined by $d + 2$ generators $x_1, \ldots, x_{d+2}$ with the single relation*

$$x_1^{2+2^f}(x_1, x_2)(x_3, x_4) \ldots (x_{d+1}, x_{d+2}) = 1 \qquad \textit{if } \mathrm{Im}(\chi) = \mathbf{U}_2^{[f]}, f \geqslant 2,$$

*or*

$$x_1^2(x_1, x_2)x_3^{2^f}(x_3, x_4) \ldots (x_{d+1}, x_{d+2}) = 1 \qquad \textit{if } \mathrm{Im}(\chi) = \{\pm 1\} \times \mathbf{U}_2^{(f)}, f \geqslant 2.$$

*Example.* If $A$ is a closed subgroup of $\mathbf{U}_2$ of finite index, let $K \subset \mathbf{Q}_2(\zeta_{2^\infty})$ be the fixed field of $A$. Then $K$ is a local field with $d = (\mathbf{U}_2:A)$. Since $\mathbf{Q}_2$ contains a primitive square root of unity, the group $G$ is a Demushkin group with $\mathrm{Im}(\chi) = A$. In particular, if $A = \mathbf{U}_2^{[2]}$, then $(\mathbf{U}_2:A) = 2$ and $K = \mathbf{Q}_2(\sqrt{-2})$. Hence $G$ can be generated by four elements $x, y, z, w$ with the single relation

$$x^6(x, y)(z, w) = 1.$$

## REFERENCES


**1.** S. Demushkin, *On the maximal p-extension of a local field* (Russian), Izv. Akad. Nauk, USSR. Math. Ser., *25* (1961), 329–346.

**2.** ——— *On 2-extensions of a local field* (Russian), Sibirsk. Mat. Z., *4* (1963), 951–955.

**3.** A. Douady, *Cohomologie des groupes totalement discontinus*, Séminaire Bourbaki, Vol. 12 (1959/60). no. 189.

**4.** N. Jacobson, *Lectures in abstract algebra*, Vol. II (New York, 1953).

**5.** J. Labute, *Classification des groupes de Demushkin*, C. R. Acad. Sci. Paris, *260* (1965), 1043–1046.

**6.** M. Lazard, *Sur les groupes nilpotents et les anneaux de Lie*, Ann. Ec. Norm. Sup., *71* (1954), 101–190.

**7.** J. P. Serre, *Corps locaux* (Paris, 1962).

**8.** ——— *Structure de certains pro-p-groupes*, Séminaire Bourbaki (1962/63), no. 252.

**9.** ——— *Cohomologie Galoisienne* (Berlin, 1964).

**10.** I. Shafarevich, *On p-extensions* (Russian), Mat. Sb., *20* (1947), 351–363 (Amer. Math. Soc. Trans., Ser. 2, *4* (1956), 59–72).


*Harvard University*

https://doi.org/10.4153/CJM-1967-007-8 Published online by Cambridge University Press