EPIMORPHISMS OF DEMUSHKIN GROUPS

BY

JACK SONN

ABSTRACT

A necessary condition that a continuous epimorphism from a Demushkin group G onto a finite p-group H can be factored epimorphically through a free pro p-group S is given, which is sufficient when H is abelian of exponent $p^m \neq 2$, m depending on G, $1 \leqq m \leqq \infty$. In particular a free pro p-factor group S of G can have rank at most one half rank G. Application is made to embedding problems over local p-adic fields.

An *embedding problem* is shown in Fig. 1 where G is a profinite group [7, Sect. 1], E and H are finite groups, and f and g are epimorphisms, f continuous. From here on, we assume that all homomorphisms are continuous. A (proper) solution is given by an epimorphism $h: G \to E$ which makes the resulting diagram commute.

The embedding problem is of particular interest when G is the Galois group of the algebraic closure of a field k, and H is the Galois group of a finite extension K/k. In this paper, we let k be a local p-adic field, that is a finite extension of the p-adic rational numbers $\mathbb{Q}_p$, p a rational prime. We also assume that E and H are p groups. In this case, it is clear that we may take G to be the Galois group of the maximal p-extension k^* of k, which is a pro p-group [7, Sect. 1]. The following proposition is due to Shafarevitch [10]. For a proof see [10] or [4].

PROPOSITION 1. *An embedding problem* (*Fig.* 1) *in which G is a free pro p-group* [7, Sect. 1] *of rank $n > 0$ has a solution if and only if rank $E \leqq n$.*

If k is a local p-adic field not containing the pth roots of unity, then $G(k^*/k)$ is a free pro p-group of rank $[k:\mathbb{Q}_p] + 1$ (see [10], [5]). In this case, Proposition 1 gives the complete picture. From now on we assume k contains the pth roots

Received January 19, 1973 and in revised form June 21, 1973

$$\begin{tikzcd} & G \arrow[d, "f"] \\ E \arrow[r, "g"'] & H \end{tikzcd}$$

Fig. 1

of unity. In this case $G = G(k^*/k)$ is not free, but its structure is well known (see [2], [8], [6]). In particular, G can be shown to have the following properties [6, Sect. 5]: set $H^i(G)$ equal to the ith cohomology group of G over $\mathbb{Z}/p\mathbb{Z}$ with trivial action. Then

(i) $\dim H^1(G) < \infty$ (in fact $= [k:\mathbb{Q}_p] + 2$),

(ii) $\dim H^2(G) = 1$,

(iii) the cup product $H^1(G) \times H^1(G) \to H^2(G) \cong \mathbb{Z}/p\mathbb{Z}$ is non degenerate. A pro p-group G satisfying (i), (ii), and (iii) is called a *Demushkin group*. Thus $G(k^*/k)$ is a Demushkin group when k contains the pth roots of unity. Condition (i) states that G is finitely generated of rank $n = \operatorname{rank} H^1(G)$; (ii) states that the minimal number of defining relations of G is 1 [7, Sect. 1], that is, G is a one-relator pro p-group of rank n. Thus there is a continuous epimorphism $e: F \to G$, F a free pro p-group of rank n, such that ker (e) is the closed normal subgroup of F generated by an element $r \in F^p[F,F]$, the closed subgroup of F generated by pth powers and commutators. The complete classification of Demushkin groups is summarized in Proposition 2. (See [6, Th. 1, 3].)

PROPOSITION 2. *Let G be a Demushkin group, F, r as above, and let q be the largest power of p such that $r \in F^q[F,F]$ $(p^\infty = 0)$.*

(i) *If $q \neq 2$, there exists a basis $x_1, \cdots, x_n$ of F such that*

$$r = x_1^q[x_1,x_2][x_3,x_4]\cdots[x_{n-1},x_n]$$

and n is necessarily even.

(ii) *If $q = 2$ and n is odd, then there is a basis $x_1, \cdots, x_n$ of F such that*

$$r = x_1^2 x_2^{2^f}[x_2,x_3][x_4,x_5]\cdots[x_{n-1},x_n].$$

(iii) *If $q = 2$ and n is even, then there is a basis $x_1, \cdots, x_n$ of F such that*

$$r = x_1^{2+2^f}[x_1,x_2][x_3,x_4]\cdots[x_{n-1},x_n] \text{ or } r = x_1^2[x_1,x_2]x_3^{2^f}[x_3,x_4]\cdots[x_{n-1},x_n]$$

where f is an integer $\geqq 2$, depending only on G.

Let G be a Demushkin group in Fig. 1. Suppose that S is a free pro p-group and that f can be factored *epimorphically* through S, that is, there exist epimorphisms

$f_1 : G \to S$, $f_2 : S \to H$ such that $f = f_2 f_1$. It then follows from Proposition 1 that if rank $E \leqq$ rank S, then there exists an epimorphism $f_3 : S \to E$ such that $gf_3 = f_2$, whence $h = f_3 f_1$ is a solution to Fig. 1. It therefore makes sense to ask when can f be factored epimorphically through a free pro p-group S.

We will see that a necessary condition for a free pro p-group S to be a homomorphic image of G is that rank $S \leqq \frac{1}{2}n$. Moreover, a glance at the relators r in Proposition 2 shows that this condition is also sufficient.

The main purpose of this paper is to give, in the case $q \neq 2$, a necessary condition for an epimorphic factorization of f through S, which is also sufficient if H is abelian of exponent q. We will also obtain some information about epimorphisms of G onto free pro p-groups S.

1. Symplectic modules over $\mathbb{Z}_p / q\, \mathbb{Z}_p$

Let $\mathbb{Z}_p$ denote the ring of p-adic integers, B the ring $\mathbb{Z}_p / q\, \mathbb{Z}_p$, where $q = 0$ or $q = p^m \neq 2$, p a rational prime. Let M be a finitely generated free B module equipped with a pairing

$$M \times M \to B$$
$$(a, b) \mapsto ab$$

which is bilinear, skew symmetric ($ab = -ba$ for all $a, b \in M$), and non singular, (that is, the determinant of the pairing relative to a basis of M is a unit of B). Note that if $q \neq 2^m$, $aa = 0$ for all $a \in M$, and if $q = 2^m > 2$, then aa is a multiple of 2. A submodule N of M is called *isotropic* if $ab = 0$ for all $a, b \in N$, *pure* if $ra \in N$, $r \in B$, $a \in M$ implies $ra = rb$ for some $b \in N$. Note that N is pure if and only if rank $N = \dim\, (N + pM)/pM$, where rank denotes the minimal number of generators. (To see this, apply the basis theorem for finitely generated $\mathbb{Z}_p$ modules to the pair M, N considered as $\mathbb{Z}_p$ modules.) A *symplectic* basis of M is a B basis $a_1, b_1, \cdots, a_t, b_t$ of M such that $a_i b_j = 1$ if $i = j$, 0 if $i \neq j$, $a_i a_j = b_i b_j = 0$ for $i \leqq i < j \leqq t$.

Proposition 3. *Let N be a pure isotropic submodule of M, and suppose* rank $(N) = s$. *Then there exists a symplectic basis $a_1, b_1, \cdots, a_t, b_t$ $(s \leqq t)$ of M over B such that $a_1, \cdots a_s$ is a basis of N. Moreover, one of the basis elements $a_i \in N$ $(1 \leqq i \leqq s)$ can be prescribed.*

Proof. Let $a_1, \cdots, a_s$ be a basis of N. Let $\bar{M} = M/pM$, $\bar{B} = B/pB \cong \mathbb{Z}/p\mathbb{Z}$. The given pairing induces a pairing

$$\bar{M} \times \bar{M} \to \bar{B}$$
$$(\bar{a}, \bar{b}) \mapsto \bar{a}\,\bar{b} = \overline{ab}$$

where $a \mapsto \bar{a} = a + pB$ is the canonical homomorphism $B \to \bar{B}$. This pairing is bilinear, alternating ($\bar{a}\bar{a} = 0$ for all $\bar{a} \in \bar{M}$) since $q \neq 2$, and non singular. Since $\bar{B}$ is a field, $\bar{M}$ is simply an ordinary non degenerate, symplectic space, and the image $\bar{N}$ of N in $\bar{M}$ is an s dimensional isotropic subspace of $\bar{M}$ with basis $\bar{a}_1, \cdots \bar{a}_s$ over $\bar{B}$, since N is pure. By a known theorem on symplectic spaces [1, p. 20] $\bar{a}_1, \cdots, \bar{a}_s$ can be extended to a symplectic basis

$$\bar{a}_1, \bar{b}_1, \cdots \bar{a}_s, \bar{b}_s$$

of a non degenerate subspace $\bar{M}_1$ of $\bar{M}$. If $\bar{M} \neq \bar{M}_1$, then $\bar{M}$ has an orthogonal decomposition $\bar{M} = \bar{M}_1 \perp \bar{M}_1^{\perp}$, so there is a symplectic basis $\bar{a}_{s+1}, \bar{b}_{s+1}, \cdots, \bar{a}_t, \bar{b}_t$ of the non singular subspace $\bar{M}_1^{\perp}$. Then $\bar{a}_1, \bar{b}_1, \cdots, \bar{a}_t, \bar{b}_t$ is a symplectic basis of $\bar{M}$. It follows that $a_1, b_1, \cdots, a_t, b_t$ is a basis of M over B (also for $q = 0$!) such that

$$
\begin{aligned}
a_i b_i &\equiv 1 \pmod{p} \quad i = 1, \cdots, t \\
a_i b_j &\equiv 0 \pmod{p} \quad \text{for } i \neq j \\
a_i a_j \equiv b_i b_j &\equiv 0 \pmod{p} \quad \text{for } i < j.
\end{aligned}
\tag{1}
$$

Multiply b_1 by a unit of B if necessary so that $a_1 b_1 = 1$. We already know that $a_i a_j = 0$ for $1 \leqq i, j \leqq s$. If $a_1 a_i = \alpha \neq 0$ for some $i > s$, $\alpha \in pB$, replacing a_i by $a_i - \alpha b_1$ gives $a_1 a_i = 0$. The congruences (1) are unaffected by this substitution. Similarly, replacing b_i ($i > 1$) by a suitable $b_i - \beta b_1$ ($\beta \in pB$) gives $a_1 b_i = 0$ for $i > 1$. Again (1) is unaffected. Similarly, if $b_1 a_j = \gamma \neq 0$ for $j > 1$, replace a_j by $a_j + \gamma a_1$ to obtain $b_1 a_j = 0$. Note that if $j \leqq s$, $a_j + \gamma a_1 \in N$ and is congruent to a_j mod pM. (1) and $a_1 a_j = 0$ are unaffected. Finally, if $b_1 b_j = \delta \neq 0$ for $j > 1$, replace b_j by $b_j + \delta a_1$ to obtain $b_1 b_j = 0$. Again (1) and $a_1 b_j = 0$ are unaffected. Setting $P = Ba_1 + Bb_1$, the submodule

$$P^{\perp} = \{x \in M \mid xy = 0 \text{ for all } y \in P\}$$

has trivial intersection with P and contains $a_2, b_2, \cdots, a_t, b_t$, so that $P^{\perp} = Ba_2 + Bb_2 + \cdots + Ba_t + Bb_t$. We may now proceed inductively to arrive at the desired basis, noting that each change either leaves $\{a_1, \cdots, a_s\}$ alone or replaces it with another basis of N, and a_1 is not changed at all. Q.E.D.

COROLLARY 4. *Let N be as in Proposition 2, and assume q odd. If $a \in M$ and $N + Ba$ is isotropic, then there is a pure isotropic submodule $N' \supseteq N + Ba$.*

PROOF. By Proposition 2, there is a symplectic basis $a_1, b_1, \cdots a_t, b_t$ of M such that $a_1, \cdots, a_s$, $s \leqq t$, is a basis of N. Clearly $N^\perp = \{x \in M \mid xN = 0\}$ has basis $a_1, \cdots, a_s, a_{s+1}, b_{s+1}, \cdots a_t, b_t$, and $a \in N^\perp$. We may assume $a \notin N$. Write

$$a = \sum_{i=1}^{t} \alpha_i a_i + \sum_{j=s+1}^{t} \beta_j b_j, \quad \alpha_i, \beta_j \in B.$$

Set $p^l = \gcd\{\alpha_{s+1}, \cdots, \alpha_t, \beta_{s+1}, \cdots, \beta_t\}$, and write $a = \sum_{i=1}^{s} \alpha_i a_i + p^l a'$. Clearly Ba' is pure $(a' \notin pM)$, and $Ba' \cap N = 0$, so that $N' = Ba' \oplus N$ is pure. It is also isotropic since $a' \in N^\perp$, and if q is odd, the pairing is alternate, hence $a'a' = 0$.

REMARK. The only place we used q odd was to assert $a'a' = 0$.

DEFINITION. Given submodules A, A' of M, set $AA' = \{aa' \mid a \in A, a' \in A'\}$. AA' is closed under multiplication by elements of B. But it is easy to see that every such subset of B is closed under subtraction. Hence AA' is an ideal of B. Let A be a submodule of M, and let $\Gamma(A)$ be the family of all pure submodules of M containing A.

Set

$$I(A) = \bigcap \{CC \mid C \in \Gamma(A)\}.$$

Clearly $I(A)$ is an ideal of B.

LEMMA 5. *$I(A) = CC$ for some $C \in \Gamma(A)$. In particular, $I(A) = 0$ if and only if A is contained in a pure isotropic submodule of M.*

PROOF. If $q \neq 0$ the assertion is obvious, since there are only finitely many ideals in B. If $q = 0$, M is torsion free, and by the basis theorem for finitely generated $\mathbb{Z}_p$ modules, there is a unique pure submodule C of M such that $C \supseteq A$, rank C = rank A, namely the submodule C such that C/A is the torsion submodule of M/A. Clearly $I(A) = CC$.

2. Demushkin groups

Let G be a Demushkin group of rank n, F a free pro p-group of rank n, $G \cong F/R$, R the closed normal subgroup generated by an element $r \in F^p[F,F]$, and q, as before, is the largest power of p such that $r \in F^q[F,F]$. We define the q central series F_n by setting $F_0 = F$, $F_n = F_{n-1}^q[F_{n-1}, F]$ for $n > 0$. Let $B = \mathbb{Z}_p / q\, \mathbb{Z}_q$ be considered as a G module with trivial action, and let $H^i(G, B)$ denote the ith cohomology group. Set $M = H^1(G, B)$, a free B module.

We need the following additional facts from [6, Sect. 1,2]. The cup product

$$H^1(G,B) \times H^1(G,B) \to H^2(G,B) \cong B$$

is a skew symmetric, non singular, bilinear form. The transgression map

$$tg: H^1(R,B)^F \to H^2(G,B)$$

is an isomorphism, and $H^1(R,B)^F$ can be identified with $\mathrm{Hom}(R/[R,F],B)$. We may therefore define a B linear homomorphism

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

by

$$\bar{r}(a) = (tg^{-1}a)(r^{-1}).$$

$\bar{r}$ is an isomorphism, and we therefore write $\chi \cup \chi'$ to mean $\bar{r}(\chi \cup \chi')$ from now on, $\chi, \chi' \in M$. Suppose $q \neq 0$. Let s be an element of F such that $s^q \equiv r$ (mod $[F,F]$). Since $F/[F,F]$ is free abelian pro p, s is uniquely determined mod $[F,F]$. Let $e: F \to G$ be a fixed epimorphism with kernel R, and set $\sigma = e(s)$.

Now since the cup product $M \times M \to B$ is bilinear and non singular, it induces a canonical isomorphism $M \to G/G_1$ ($G_1 = G^q[G,G]$) as follows. Let $\chi \in M$. Then the mapping

$$\chi^*: \eta \mapsto \eta \cup \chi$$

belongs to $\mathrm{Hom}_B(M,B)$. Since $M = H^1(G,B)$ is canonically isomorphic to $\mathrm{Hom}_B(G,B)$, $\mathrm{Hom}_B(M,B)$ is the second dual of G/G_1, hence canonically isomorphic to G/G_1. Therefore χ is mapped canonically onto the element $\bar{\tau} \in G/G_1$ corresponding to χ^*, namely that element $\bar{\tau}$ of G/G_1 such that $\eta \cup \chi = \eta(\bar{\tau})$ for every $\eta \in M$. (Note $H^1(G,B) \cong H^1(G/G_1,B)$ canonically.) Under this correspondence, we set χ_σ equal to that element of M which corresponds to $\bar{\sigma}$, where $\bar{\sigma}$ is the image of σ in G/G_1. Thus for all $\eta \in M$, $\eta(\sigma) = \eta \cup \chi_\sigma$.

Lemma 6. (*Demushkin.*) *Let $\chi_1, \cdots, \chi_n$ be a basis of M such that $\chi_{2i-1} \cup \chi_{2i} = 1$ for $1 \leqq i \leqq \frac{1}{2}n$, and $\chi_i \cup \chi_j = 0$ for $i < j$ otherwise. If $q \neq 0$, suppose also that $\chi_2 = \chi_\sigma$. Let $\sigma_1, \cdots, \sigma_n$ be a basis of G dual to $\chi_1, \cdots, \chi_n$, that is, $\chi_i(\sigma_j) = \delta_{ij}$, $1 \leqq i, j \leqq n$, and let $x_1 \cdots, x_n$ be a basis of F such that $e(x_i) = \sigma_i$, $1 \leqq i \leqq n$.*

Then $r \equiv x_1^q [x_1, x_2] \cdots [x_{n-1}, x_n]$ (mod F_2).

Proof. We base the proof on [6]. We may write

$$r \equiv \prod_{i=1}^{n} x_i^{qa_i} \prod_{i<j} [x_i, x_j]^{a_{ij}} \,(\mathrm{mod}\, F_2),\ a_i, a_{ij} \in B.$$

To see this, first observe that r has a unique expression $\prod_{i=1}^{n} x_i^{qa_i}(\mathrm{mod}\,[F,F])$, $a_i \in \mathbb{Z}_p$, since $r \in F_1 = F^q[F,F]$. Hence $r = \prod_{i=1}^{n} x_i^{qa_i} \cdot c$, $c \in [F,F]$. By well-known commutator identities [3, p. 150] (which are valid also for topological groups), the set $\{[x_i,x_j] : 1 \leqq i < j \leqq n\}$ forms a basis of the free $\mathbb{Z}_p$ module $[F,F]/[[F,F],F]$. Hence

$$r \equiv \prod_{i=1}^{n} x_i^{qa} \prod_{i<j} [x_i,x_j]^{a_{ij}} \ (\mathrm{mod}\,[[F,F],F]); \ a_i, a_{ij} \in \mathbb{Z}_p.$$

Since $[[F,F],F] \subseteq F_2$, reducing the last expression mod F_2 yields the same expression with the a_i and a_{ij} reduced mod q.

By [6, Prop. 3], we have

$$a_{ij} = \chi_i \cup \chi_j \text{ for } i<j.$$

Therefore

$$r \equiv \prod_{i=1}^{n} x_i^{qa_i} [x_1,x_2]\,[x_3,x_4] \cdots [x_{n-1},x_n] \ (\mathrm{mod}\, F_2). \tag{2}$$

If $q = 0$ we are finished. We now assume $q \neq 0$. It suffices to show that

$$r \equiv x_1^q \ (\mathrm{mod}\, F_2[F,F] = F^{q^2}[F,F]),$$

since (2) becomes $r \equiv \prod_{i=1}^{n} x_i^{qa_i}(\mathrm{mod}\ F_2[F,F])$.

If we can show that $s \equiv x_1 \ (\mathrm{mod}\ F_1)$, then

$$x_1 s^{-1} \in F_1,\ (x_1 s^{-1})^q \in F_1^q \subseteq F_1^q[F,F],$$

hence

$$(x_1 s^{-1})^q \equiv x_1^q s^{-q} \equiv 1 \ (\mathrm{mod}\, F_1^q[F,F]),$$

and

$$x_1^q \equiv s^q \equiv r \ (\mathrm{mod}\ F_1^q[F,F]),$$

as desired.

Now $s \equiv x_1 \ (\mathrm{mod}\, F_1)$ if and only if $\sigma \equiv \sigma_1 \ (\mathrm{mod}\, G_1)$, since $e(s) = \sigma$, $e(x_1) = \sigma_1$. Further, $\sigma \equiv \sigma_1 \ (\mathrm{mod}\ G_1)$ if and only if $\eta(\sigma) = \eta(\sigma_1)$ for all $\eta \in M$. By definition of χ_σ, we have $\eta(\sigma) = \eta \cup \chi_\sigma$ for every $\eta \in M$. For $\eta = \chi_i$, we have

$$\chi_i(\sigma) = \chi_i \cup \chi_\sigma = \delta_{1i} = \chi_i(\sigma_1),\ i = 1,\cdots,n \ \text{ since } \chi_\sigma = \chi_2.$$

Therefore $\eta(\sigma) = \eta(\sigma_1)$ for every $\eta \in M$. Q.E.D.

Now let $f: G \to H$ be an epimorphism, H a finite p group. f induces a monomorphism

$$f^*: H^1(H,B) \to H^1(G,B).$$

Set A = image $(f^*) + B\chi_\sigma$ if $q \neq 0$, A = image (j^*) if $q = 0$. A is a submodule of M, and the invariant $I(A)$ is defined (see Section 1).

Theorem 7. *Let $q \neq 2$. A necessary condition that f admit an epimorphic factorization*

$$G \xrightarrow[f_1]{} S \xrightarrow[f_2]{} H \tag{4}$$

*through a free pro p-*group *S is that rank $H \leqq \frac{1}{2}n$ and $I(A) = 0$. If H is abelian of exponent q, then the condition $I(A) = 0$ is also sufficient.*

Proof. First assume that f admits an epimorphic factorization (4). We have a commutative diagram shown in Fig. 2 where f_1^*, f_1^{**} are induced by f_1 and $\cup$ denotes the cup product. $H^2(S,B) = 0$ since S is free, hence the submodule image(f_1^*) of $H^1(G,B) = M$ is isotropic. Furthermore, N = image (f_1^*) is pure in M. This follows from the commutative diagram shown in Fig. 3, from the injectivity of the horizontal arrows, and from the surjectivity of the vertical arrows (using the criterion preceding Proposition 3). Since N is isotropic, we apply Proposition 3 and obtain rank $H \leqq$ rank $N \leqq \frac{1}{2}n$, since M is non singular. This argument shows that *if a free pro p-group S is a homomorphic image of G, then rank $S \leqq \frac{1}{2}n$.* (This holds even for $q = 2$.) If $q = 0$, then $I(A) = 0$. We now assume $q \neq 0$.

$$\begin{tikzcd}
H^1(S,B) \times H^1(S,B) \arrow[r, "\cup"] \arrow[d, "f_1^* \times f_1^*"] & H^2(S,B) = 0 \arrow[d, "f_1^{**}"] \\
H^1(G,B) \times H^1(G,B) \arrow[r, "\cup"] & H^2(G,B)
\end{tikzcd}$$

Fig. 2

Let σ be the same as before, so that $\sigma^q \equiv 1 \pmod{[G,G]}$. Then since $S/[S,S]$

$$\begin{tikzcd}
H^1(S,B) \arrow[r, "f_1^*"] \arrow[d] & H^1(G,B) = M \arrow[d] \\
H^1(S,\mathbf{Z}_p/p\mathbf{Z}_p) \arrow[r] & H^1(G,\mathbf{Z}_p/p\mathbf{Z}_p) \cong M/pM
\end{tikzcd}$$

Fig. 3

is torsion free, $f_1(\sigma) \equiv 1 \pmod{[S,S]}$, so that if $\eta \in H^1(S,B)$ and $\chi = f_1^*(\eta)$, then $\chi(\sigma) = 0$. Since $\chi(\sigma) = \chi \cup \chi_\sigma$ for every $\chi \in M$, it follows that $\chi \cup \chi_\sigma = 0$ for every $\chi \in N$, whence $N + B\chi_\sigma$ is isotropic. If q is odd, then by Corollary 4, it is contained in a pure isotropic submodule N' of M. If $q = 2^m$, $m \geqq 2$, it is necessary to verify this separately. We may assume $\chi_\sigma \notin N$. By Proposition 3, there is a basis $\chi_1,\cdots,\chi_n$ of M such that $\chi_{2i-1} \cup \chi_{2i} = 1$ for $1 \leqq i \leqq \frac{1}{2}n$, $\chi_i \cup \chi_j = 0$ for $i < j$ otherwise, and $\chi_2, \chi_4 \cdots, \chi_{2s}$, $s \leqq \frac{1}{2}n$, is a basis of N. Then as in the proof of Corollary 4,

$$N^\perp = \sum_{i=1}^{s} B\chi_{2i} + \sum_{i=2s+1}^{n} B\chi_i.$$

Since $\chi_\sigma \in N^\perp$, $\chi_\sigma = \chi_0 + \eta$, $\chi_0 \in N$, $0 \neq \eta = \sum_{i=2s+1}^{n} b_i\chi_i$, $b_i \in B$.

Write

$$\eta = b\eta',\ b = 2^l = \gcd\{b_{2s+1},\cdots b_n\},$$

so that $\eta' \in N^\perp$ and $N' = N + B\eta'$ is pure. To show that N' is isotropic it suffices to show $\eta' \cup \eta' = 0$. By the corollary to [6, Prop. 3],

$$\chi \cup \chi = \binom{q}{2}\chi(\sigma)$$

for every $\chi \in M$. In particular $\chi_\sigma \cup \chi_\sigma = \binom{q}{2}\chi_\sigma(\sigma)$. On the other hand, $\chi \cup \chi_\sigma = \chi(\sigma)$ for every $\chi \in M$, so setting $\chi = \chi_\sigma$, $\chi_\sigma \cup \chi_\sigma = \chi_\sigma(\sigma)$. Hence $(\binom{q}{2} - 1)\chi_\sigma(\sigma) = 0$, whence $\chi_\sigma(\sigma) = 0$. Let $\chi_1',\cdots,\chi_n'$ be a basis of M such that $\chi_i'(\sigma) = \delta_{i1}$. (Such a basis exists since we extend σ to a basis of G and take the dual basis.) Then

$$\sigma^\perp = \{\chi \in M \mid \chi(\sigma) = 0\} = B\chi_2' + \cdots + B\chi_n'.$$

We know that $N \subseteq \sigma^\perp$ and $\chi_\sigma \in \sigma^\perp$. It follows that $\eta = b\eta' = \chi_\sigma - \chi_0 \in \sigma^\perp$ whence the coefficient c_1 of χ_1' in the expression $\eta' = \sum_{i=1}^{n} c_i\chi_i'$ satisfies $bc_1 = 0$ since

$$b\eta'(\sigma) = bc_1 = 0.$$

Since $b \neq 0$, $c_1 \in 2B$. But then

$$\eta' \cup \eta' = \sum_{i=1}^{n} c_i^2(\chi_i' \cup \chi_i') = \sum_{i=1}^{n} c_i^2 \binom{q}{2} \chi_i'(\sigma) = c_1^2\binom{q}{2} = 0.$$

(The first equality holds since $c_ic_j\chi_i' \cup \chi_j' + c_jc_i\chi_j' \cup \chi_i' = 0$.) Thus $N + B\chi_\sigma$ is contained in a pure isotropic submodule N' of M.

Now $f_2\colon S \to H$ induces a monomorphism $f_2^*\colon H^1(H,B) \to H^1(S,B)$ and

$$\begin{aligned} A &= \text{image}\, f^* + B\chi_\sigma \\ &= \text{image}\, f_1^* f_2^* + B\chi_\sigma \\ &\subseteq N + B\chi_\sigma \\ &\subseteq N'. \end{aligned}$$

Hence $I(A) = 0$. (Note that this part of the theorem is valid for H a pro p-group.)

Conversely, suppose $I(A) = 0$. Then by Lemma 5, A is contained in a pure isotropic submodule N' of M. By Proposition 3, there is a basis $\chi_1 \cdots, \chi_n$ of M such that $\chi_{2i-1} \cup \chi_{2i} = 1$ for $1 \leqq i \leqq \frac{1}{2}n$, $\chi_i \cup \chi_j = 0$ for $i < j$ otherwise, χ_2, $\chi_4, \cdots \chi_{2s}$ is a basis of N', $s \leqq \frac{1}{2}n$ and $\chi_2 = \chi_\sigma$ if $q \neq 0$. By virtue of Burnside's basis theorem, let $\sigma_1, \cdots \sigma_n$ be a basis of G dual to $\chi_1 \cdots, \chi_n$, $x_1, \cdots x_n$ a basis of F such that $e(x_i) = \sigma_i$ for $1 \leqq i \leqq n$ as above. Then by Lemma 6,

$$r \equiv x_1^q [x_1, x_2] \cdots [x_{n-1}, x_n] \pmod{F_2}.$$

We now proceed exactly as in proof [6, Th. 3]: suppose

$$r \equiv x_1^q \ [x_1, x_2] \cdots [x_{n-1}, x_n] \ (\text{mod}\, F_j) \ j \geqq 2.$$

By [6, Prop. 5], there exist $t_1, \cdots, t_n \in F_{j-1}$ such that

$$r \equiv y_1^q [y_1, y_2] \cdots [y_{n-1}, y_n] \pmod{F_{j+1}}$$

where

$$y_i = x_i t_i^{-1}, 1 \leqq i \leqq n.$$

Passing to the limit, we obtain a new basis of F, which we also denote by $x_1, \cdots, x_n$, such that

(i) $r = x_1^q [x_1, x_2] \cdots [x_{n-1}, x_n]$,

(ii) the new $\sigma_i = e(x_i)$ are still dual to $\chi_1, \cdots \chi_n$. (At each step, $y_i \equiv x_i$ (mod F_1).)

We now produce the factorization of f. Let $y_1, \cdots, y_{\frac{1}{2}n}$ be a basis of S and define $f_1'\colon F \to S$ by

$$f_1'(x_{2i-1}) = 1, \ f_1'(x_{2i}) = y_i, \ 1 \leqq i \leqq \tfrac{1}{2}n.$$

Then $f_1'(r) = 1$, and f_1' induces an epimorphism $f_1\colon G \to S$ satisfying $f_1' = f_1 e$.

Define $f_2\colon S \to H$ by

$$f_2(y_i) = f(\sigma_{2i}), \qquad 1 \leqq i \leqq \tfrac{1}{2}n.$$

Now for

$$1 \leqq i \leqq \tfrac{1}{2}n, f_2f_1(\sigma_{2i}) = f_2f_1e(x_2) = f_2f_1'(x_{2i}) = f_2(y_i) = f(\sigma_{2i}),$$

and

$$f_2j_1(\sigma_{2i-1}) = f_2f_1'(x_{2i-1}) = f_2(1) = 1.$$

It follows that $f = f_2f_1$ if and only if $f(\sigma_{2i-1}) = 1$ for $1 \leqq i \leqq \frac{1}{2}n$. If H is abelian of exponent q, then an element $\tau \in H$ is equal to 1 if $\chi'(\tau) = 0$ for all $\chi' \in \mathrm{Hom}\ _B(H,B)$. For $\tau = f(\sigma_{2i-1})$, this condition amounts to

$$f^*H^1(H,B) \subseteq \Sigma \{B\chi_j \mid j \neq 2i - 1\}$$

since

$$\chi' f(\sigma') = f^*(\chi')(\sigma') \text{ for } \sigma' \in G.$$

If we now let $i = 1, \cdots, \frac{1}{2}n$, then $f = f_2f_1$ if and only if

$$f^*H^1(H,B) \subseteq \Sigma\{B\chi_{2i} \mid 1 \leqq i \leqq \tfrac{1}{2}n\}.$$

But this is true since

$$f^*H^1(H,B) = \text{image} f^* \subseteq A \subseteq N' \subseteq \Sigma\{B\chi_{2i} \mid 1 \leqq i \leqq \tfrac{1}{2}n\}, \qquad \text{Q.E.D.}$$

REMARK. If G is the Galois group of the maximal p-extension k^* of a local p-adic field k containing the pth roots of unity, and K is the fixed field of $\ker(f)$, then $I(A)$ is an arithmetic invariant of K. Namely, if K is abelian of exponent q (if not, replace K/k by the maximal abelian subextension K'/k of exponent q) then by Kummer theory, $K = k(D^{1/q})$, where D is a subgroup of $k^\times$ (multiplicative group of k) containing $k^{\times q}$ and $D^{1/q}$ is the set of all qth roots of elements of D. Note that q is the highest power of p such that k contains the qth roots of unity [6, Sect. 5]. We may as well replace D by $D/k^{\times q}$and write $D \subseteq J = k/k^{\times q}$. Each $a \in J$ determines a character

$$\chi_a \colon G \to W = q\text{th roots of unity},$$

as follows. Set

$$\chi_a(\sigma) = \sigma(a^{1/q})/a^{1/q} \in W.$$

If we fix an isomorphism between W and the additive group $B = \mathbb{Z}_p/q\mathbb{Z}_p$, then $a \leftrightarrow \chi_a$ is an isomorphism between J and $M = H^1(G,B)$. Furthermore, if $H = G(K/k)$ and $f: G \to H$ is the restriction map, then $H^1(H,B) \cong D$ and $f^*: H^1(H\ B) \to H^1(G,B)$ corresponds to the inclusion $D \to J$. Still further, the cup product $M \times M \to B$ corresponds to the qth power norm residue symbol

$J \times J \to W$ [9, Chap. XIV]. Now since σ generates the torsion part of $G/[G,G]$, σ corresponds to some generator ζ of $W \subseteq k$ under the reciprocity isomorphism. Finally, χ_σ is identified with χ_ζ relative to a suitable identification between W and B. To see this, we assume an arbitrary identification between W and B and show that $B\chi_\sigma = B\chi_\zeta$. Let $\chi_1, \cdots, \chi_n$ be the basis of M of Lemma 6, and let $a_1, \cdots, a_n \in k^*$ such that $\chi_i = \chi_{a_i}$, $1 \leqq i \leqq n$. Since $\chi_2 = \chi_\sigma$, by assumption, and χ_ζ has order q, it suffices to show that $\chi_\zeta \cup \chi_i = 0$ for $2 \leqq i \leqq n$, since then $\chi_\zeta^\perp = \chi_2^\perp = \chi_\sigma^\perp$ so that $B\chi_\sigma = B\chi_\zeta$. Now $\chi_\zeta \cup \chi_i = 0 \Leftrightarrow \zeta$ is a norm from $k(a_i^{1/q}) \Leftrightarrow \zeta$ is in the kernel of the reciprocity map of the extension $k(a_i^{1/q}) \Leftrightarrow \sigma$ acts trivially on $k(a_i^{1/q})$. (The reciprocity map commutes with the restriction $K \to k(a_i^{1/q})) \Leftrightarrow \chi_i(\sigma) = 0 \Leftrightarrow 2 \leqq i \leqq n$ since $\sigma \equiv \sigma_1$ (mod $[G,G]$.)

Thus A = image $f^* + B\chi_\sigma$ corresponds to the subgroup DW of $J = k^*/k^{*q}$, and the condition $I(A) = 0$ means that DW is contained in a pure isotropic submodule of J (with respect to the qth power norm residue symbol).

We conclude with a remark on epimorphisms of G onto a free pro p-group S of rank $\leqq \frac{1}{2}n$. As we noted in the proof of Theorem 7, the existence of such an epimorphism implies rank $S \leqq \frac{1}{2}n$. If we denote G/G_2, S/S_2 by $G^{(2)}$, $S^{(2)}$ respectively, an epimorphism $h\colon G \to S$ induces an epimorphism $h'\colon G^{(2)} \to S^{(2)}$, since $h(G_2) = S_2$. If rank $S = \frac{1}{2}n$, and if $\sigma_1, \cdots \sigma_n$ is a basis of $G^{(2)}$ satisfying $\sigma_1^q[\sigma_1\ \sigma_2] \cdots [\sigma_{n-1}, \sigma_n] = 1$, and $y_1\ \cdots, y_{\frac{1}{2}n}$ is a basis of $S^{(2)}$, then any mapping which sends σ_{2i-1} into S_1/S_2, σ_{2i} onto y_i, for $1 \leqq i \leqq \frac{1}{2}n$, defines an epimorphism of $G^{(2)}$ onto $S^{(2)}$, since the left side of the relation on $\sigma_1, \cdots, \sigma_n$ collapses to 1 under the mapping.

THEOREM 8. *Let S be a free pro p-group, $g\colon G^{(2)} \to S^{(2)}$ an epimorphism. Then rank $S \leqq \frac{1}{2}n$. If rank $S = \frac{1}{2}n$, then there exists a basis $\sigma_1, \cdots, \sigma_n$ of $G^{(2)}$ satisfying $\sigma_1^q[\sigma_1, \sigma_2] \cdots [\sigma_{n-1}, \sigma_n] = 1$ and a basis $y_1, \cdots, y_{\frac{1}{2}n}$ of $S^{(2)}$ such that $g(\sigma_{2i-1}) \in S_1/S_2$ and $g(\sigma_{2i}) = y_i$, for $1 \leqq i \leqq \frac{1}{2}n$.*

PROOF. Consider the diagram shown in Fig. 4 in which the vertical arrows are canonical and $e^{(2)}$ is induced by e. The map from F onto $S^{(2)}$ defined by the

$$\begin{tikzcd}
F \arrow[r, "e"] \arrow[d] \arrow[rr, dashed, bend left, "h"] & G \arrow[d] & S \arrow[d] \\
F^{(2)} \arrow[r, "e^{(2)}"] & G^{(2)} \arrow[r, "g"] & S^{(2)}
\end{tikzcd}$$

Fig. 4

diagram can be factored epimorphically through S; because a set of free generators of F map onto a set of generators of $S^{(2)}$. Using the Burnside basis theorem, it is easy to check that the preimages of these generators in S generate S, hence we can use them as images of the generators of F in defining the desired epimorphism $h\colon F \to S$. By commutativity of the diagram, $h(RF_2) \subseteq S_2$.

Consider next the commutative diagram shown in Fig. 5 in which all the tg are isomorphisms (by Hochschild-Serre; for example the first tg is part of the Hochschild-Serre exact sequence

$$H^1(S^{(2)},B) \to H^1(S,B) \to H^1(S_2,B)^S \xrightarrow{tg} H^2(S^{(2)},B) \to H^2(S,B) = 0,$$

in which the first arrow is an isomorphism, and the second and last are zero). h^* is induced by h and is well defined since $h[RF_2,F] \subseteq [S_2,S]$.

$$\begin{tikzcd}
H^1(S_2,B)^S \arrow[r, "h^*"] \arrow[d, "tg"] & H^1(RF_2,B)^F \arrow[r] \arrow[d, "tg"] & H^1(R,B)^F \arrow[d, "tg"] \\
H^2(S^{(2)}B) \arrow[r, "g^{**}"] & H^2(G^{(2)},B) \arrow[r] & H^2(G,B)
\end{tikzcd}$$

Fig. 5

Now to cup products. Consider the commutative diagram shown in Fig. 6 where $\bar{r}(a) = tg^{-1}(a)\,(r^{-1})$ for $a \in H^2(G,B)$, and similarly for the first two rows.

$$\begin{tikzcd}
H^1(S^{(2)},B) \times H^1(S^{(2)},B) \arrow[r, "\cup"] \arrow[d, "g^* \times g^*"] & H^2(S^{(2)},B) \arrow[r, "\overline{h(r)}"] \arrow[d, "g^{**}"] & B \arrow[d, "id"] \\
H^1(G^{(2)},B) \times H^1(G^{(2)},B) \arrow[r, "\cup"] \arrow[d] & H^2(G^{(2)},B) \arrow[r, "\bar{r}"] \arrow[d] & B \arrow[d, "id"] \\
H^1(G,B) \times H^1(G,B) \arrow[r, "\cup"] & H^2(G,B) \arrow[r, "\bar{r}"] & B
\end{tikzcd}$$

Fig. 6

Since $h(r) \in S_2$, $\overline{h(r)} = 0$. We may now extract the following information: the image of N of $H^1(S^{(2)},B)$ in $M = H^1(G,B)$ is an isotropic submodule of M; it is also pure, as in the proof of Theorem 7. Since N has rank $\frac{1}{2}n$ (Proposition 3)

$$N^{\perp} = \{\chi \in M \mid \chi \cup \eta = 0 \text{ for all } \eta \in N\} = N,$$

where $\chi \cup \eta$ again denotes the image $\bar{r}(\chi \cup \eta)$ of $\chi \cup \eta$ in B.

Now if $q \neq 0$, let σ, χ_σ be defined as above. Exactly as in the proof of Theorem 7, we have

$$\chi(\sigma) = \chi \cup \chi_\sigma = 0 \text{ for } \chi \in N, \chi_\sigma \in N^{\perp} = N.$$

By Proposition 2, there is a basis $\chi_1, \cdots, \chi_n$ of M such that $\chi_{2i-1} \cup \chi_{2i} = 1$ for $1 \leqq i \leqq \frac{1}{2}n$, $\chi_i \cup \chi_j = 0$ for $i < j$ otherwise, $\chi_2 = \chi_\sigma$ if $q \neq 0$, and $\chi_2, \chi_4, \cdots, \chi_n$ is a basis of N. Choose a basis $\sigma_1, \cdots, \sigma_n$ of $G^{(2)}$ dual to $\chi_1, \cdots, \chi_n$. By Lemma 6, $\sigma_1^q[\sigma_1, \sigma_2] \cdots [\sigma_{n-1}, \sigma_n] = 1$. Set $y_i = g(\sigma_{2i})$, $1 \leqq i \leqq \frac{1}{2}n$, and let $\eta_1, \cdots, \eta_{\frac{1}{2}n}$ be the basis of $H^1(S^{(2)}, B)$ dual to $y_1, \cdots, y_{\frac{1}{2}n}$. Then $g^*(\eta_i)(\sigma_j) = \eta_i g(\sigma_j) = \delta_{j,2i}$ for $1 \leqq j \leqq n$, $1 \leqq i \leqq \frac{1}{2}n$, hence $g^*(\eta_i) = \chi_{2i}$, $1 \leqq i \leqq \frac{1}{2}n$. $y \in S^{(2)}$ belongs to S_1/S_2 if and only if $\eta(y) = 0$ for every $\eta \in H^1(S^{(2)}, B)$. (It is clear that $\eta(S_1/S_2) = 0$ for every η, and given $y \in S^{(2)}$, y has a unique expression $\prod_{i=1}^{\frac{1}{2}n} y_i^{a_i} - z$, $z \in S_1/S_2$, $a_i \in B$, hence if $y \notin S_1/S_2$, some $a_i \neq 0$, so $\eta_i(y) = a_i \neq 0$.) It follows that $g(\sigma_{2i-1}) \in S_1/S_2$ for $1 \leqq i \leqq \frac{1}{2}n$; since $\eta_j g(\sigma_{2i-1}) = (g^*\eta_j)(\sigma_{2i-1}) = \chi_{2j}(\sigma_{2i-1}) = 0$ for $1 \leqq i, j \leqq \frac{1}{2}n$. Q.E.D.

REMARK. If rank $S < \frac{1}{2}n$, the situation is a bit more complicated. It can be verified that if rank $S = s < \frac{1}{2}n$, then a necessary and sufficient condition that there is a basis $\sigma_1, \cdots, \sigma_n$ of $G^{(2)}$ satisfying $\sigma_1^q[\sigma_1, \sigma_2] \cdots [\sigma_{n-1}, \sigma_n] = 1$ and a basis $y_1, \cdots, y_s$ of $S^{(2)}$ such that

$$g(\sigma_{2i-1}) \in S_1/S_2 \text{ for } 1 \leqq i \leqq \tfrac{1}{2}n,\ g(\sigma_{2i}) = y_i \text{ for } 1 \leqq i \leqq s,$$

and

$$g(\sigma_{2i}) \in S_1/S_2 \text{ for } s + 1 \leqq i \leqq \tfrac{1}{2}n,$$

is that

$$g^*H^1(S^{(2)}, B) \cap B\chi_\sigma$$

is either 0 or all of $B\chi_\sigma$.

REFERENCES

1. E. Artin, *Geometric Algebra*, Interscience, New York, 1957.

2. S. Demushkin, *The group of the maximal p-extension of a local field*, Izv. Akad. Nauk SSSR, Ser. Mat. **25** (1961), 329–346.

3. M. Hall, *The Theory of Groups*. Macmillan, New York, 1951.

4. K. Hoechsmann, *Zum Einbettungsproblem*, J. Reine Angew. Math. **229** (1968), 81–106.

5. K. Hoechsmann, *l*-extensions, *Algebraic Number Theory*, Thompson, Washington, D.C. 1967, pp. 297–304.

6. J. Labute, *Classification of Demushkin groups*, Canad. J. Math. **19** (1967), 106–132.

7. J. P. Serre, *Cohomologie Galoisienne*, Springer-Verlag, Berlin, 1965.

8. J. P. Serre, *Structure de certaines pro-p-groupes*, Sem. Bourbaki (1963) Exp. 252.

9. J. P. Serre, *Corps Locaux*, Hermann, Paris, 1962.

10. I. R. Shafarevitch, *On p-extensions*, Amer. Math. Soc. Transl. (2) **4** (1956), 59–72.

ISRAEL INSTITUTE OF TECHNOLOGY
HAIFA, ISRAEL