Canad. Math. Bull. Vol. **32** (2), 1989

$\mathbf{Z}_p$-TOWERS IN DEMUŠKIN GROUPS

BY

LLOYD D. SIMONS

ABSTRACT. In this note, we develop the notion of a $\mathbf{Z}_p$-tower in a Demuškin group, and apply the results of Koch and Wingberg on the uniqueness of so-called Demuškin formations to give a classification of such towers in the case $p \neq 2$.

1. **Introduction.** We first recall some well-known facts about Demuškin groups. For proofs, see Labute [6] or Serre [7], [8]. Let p be a prime, and let X be a Demuškin p-group. That is, X is a profinite p-group satisfying the axioms:

(i) $\dim_{\mathbf{F}_p} H^1(X, \mathbf{Z}/p\mathbf{Z}) = n < \infty$;

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

(iii) the cup-product $H^1(X, \mathbf{Z}/p\mathbf{Z}) \times H^1(X, \mathbf{Z}/p\mathbf{Z}) \longrightarrow H^2(X, \mathbf{Z}/p\mathbf{Z})$ is a nondegenerate bilinear form.

With the exception of the trivial case $p = 2$, $n = 1$, these axioms suffice to show that the p-cohomological dimension of $X(cd_p(X))$ is 2, and one can associate to X its "dualizing module":

$$I_X = \varinjlim_{U} \varinjlim_{s} H^2(U, \mathbf{Z}/p^s\mathbf{Z})^*,$$

where the $*$ denotes the Pontrjagin dual, and where the direct limit is taken over all open subgroups $U \leqq X$ and over integers $s \geqq 1$. It is well known ([7], I–52) that as an abelian group $I_X \cong Q_p/\mathbf{Z}_p$, and to X can be associated the character $\chi : X \longrightarrow \mathbf{Z}_p^\times$ giving the natural action of X on $I_X : g \cdot \zeta = \chi(g)\zeta$ for all $\zeta \in I_X$ and $g \in X$. The invariant χ together with the rank n completely determine the isomorphism class of X; in particular, the torsion invariant $q = p^s$ of X (i.e., the order of $X^{\text{ab}}_{\text{tor}}$) is the cardinality of I_X^X, the X-fixed points of I_X.

By a $\mathbf{Z}_p$-tower in the Demuškin group X we shall mean a continuous epimorphism $\phi : X \longrightarrow \mathbf{Z}_p$; if the torsion invariant of X is q, then $X^{\text{ab}} \cong \mathbf{Z}_p^{n-1} \oplus \mathbf{Z}/q\mathbf{Z}$, so that a good many such towers exist. We will call two such towers ϕ_1 and ϕ_2 equivalent if there is an automorphism π of X so that $\phi_1 = \phi_2 \circ \pi$. The object of this note is to classify $\mathbf{Z}_p$-towers in a given Demuškin group X up to equivalence.

2. **The Main Theorem.** Let ϕ be a $\mathbf{Z}_p$-tower in the Demuškin group X, and define the m^{th} level subgroup of the tower to be $X_m = \phi^{-1}(p^m\mathbf{Z}_p)$. This gives a

Received by the editors December 16, 1987.

AMS Subject Classification (1980): 11S25, 12G05

chain of normal subgroups $X = X_0 \supset X_1 \supset \ldots$ with $X/X_m = G_m \cong \mathbf{Z}/p^m\mathbf{Z}$ and $\cap X_m = V = \ker \phi$.

We will assume from now on that the strict p-cohomological dimension of X ($\mathrm{scd}_p X$) is two. In this case, the image of the invariant χ is infinite ([7], I–52) and possesses a unique quotient isomorphic to $\mathbf{Z}_p$. Explicitly, if $q \neq 2$ is the torsion invariant of X, then im $\chi = 1 +_q \mathbf{Z}_p \cong \mathbf{Z}_p$. If $q = 2$ and im $\chi = \{\pm 1\} \times \{1 + 2^s\mathbf{Z}_2\}$ with $s \geqq 2$, then projection onto the second factor will work. The remaining case has im $\chi = \langle -1 + 2^s \rangle \cong \mathbf{Z}_p$. In each case, we get (by choice of a topological generator) a $\mathbf{Z}_p$-tower ϕ_X, which we call a basic tower.

LEMMA 1. *Let $U \leqq X$ be open. The $U^{\mathrm{ab}}_{\mathrm{tor}} \cong I^U_X$.*

PROOF. The exact sequence $0 \longrightarrow \mathbf{Z}/p^t\mathbf{Z} \longrightarrow Q_p/\mathbf{Z}_p \xrightarrow{p^t} Q_p/\mathbf{Z}_p \longrightarrow 0$ gives the long exact sequence

$$0 \longrightarrow H^1(U, \mathbf{Z}/p^t\mathbf{Z}) \longrightarrow H^1(U, Q_p/\mathbf{Z}_p) \xrightarrow{p^t} H^1(U, Q_p/\mathbf{Z}_p) \longrightarrow H^2(U, \mathbf{Z}/p^t\mathbf{Z}),$$

where the last map is surjective since $\mathrm{scd}_p U = 2$. Dualizing gives the exact sequence

$$0 \longrightarrow H^2(U, \mathbf{Z}/p^t\mathbf{Z})^* \longrightarrow U^{\mathrm{ab}} \xrightarrow{p^t} U^{\mathrm{ab}}.$$

Thus for t large enough, $U^{\mathrm{ab}}_{\mathrm{tor}} \cong H^2(U, \mathbf{Z}/p^t\mathbf{Z})^*$, and this latter group is easily seen to inject into I^U_X. Let V be the maximal subgroup of X which fixes I^U_X — since $H^2(V, \mathbf{Z}/p^t\mathbf{Z})^* \longrightarrow H^2(U, \mathbf{Z}/p^t\mathbf{Z})^*$ is injective, $V^{\mathrm{ab}} \longrightarrow U^{\mathrm{ab}}$ is injective, and it suffices to prove the lemma for V. Let the generator ζ of I^V_X come from $H^2(W, \mathbf{Z}/p^t\mathbf{Z})^*$ for some open normal subgroup W of X, so that $\zeta \in (W^{\mathrm{ab}}_{\mathrm{tor}})^V$. By propositions 10 and 11 of [3], the transfer map Ver : $V^{\mathrm{ab}} \longrightarrow (W^{\mathrm{ab}})^V$ is an isomorphism, so that $\zeta \in V^{\mathrm{ab}}$ already. □

COROLLARY. *The level subgroups of the tower ϕ_X are characteristic subgroups of X.*

PROOF. Let $\zeta \in I_X$, and $W = C_X(\zeta)$ be the centralizer of ζ in X. If $I^W_X = \langle \zeta' \rangle$, and if $W' = C_X(\zeta')$, then $W = W'$, so we may assume that $\zeta = \zeta'$. We claim that W is a characteristic subgroup of X: by Lemma 1, $W^{\mathrm{ab}}_{\mathrm{tor}} \cong I^W_X$. If $\alpha \in \mathrm{Aut}(X)$ and $W' = \alpha(W)$, then W'^{ab} and W^{ab} have isomorphic torsion subgroups, so that $I^W_X = I^{W'}_X$. By the maximality of W, it follows that $W = W'$. The intersection of these characteristic subgroups $C_X(\zeta)$ is the characteristic subgroup $V = \ker \chi$.

If im $\chi \cong \mathbf{Z}_p$, we are done. If im $\chi = \{\pm 1\} \times \{1 + 2^s\mathbf{Z}_2\}$, then $V_0 = \chi^{-1}(\pm 1)$ (which is the kernal of ϕ_X) is characteristic in X — this follows because V_0/V is the torsion subgroup of X/V. □

REMARK. The level subgroups of the tower ϕ_X can be 'constructed' without explicitly referring to the dualizing module as follows (see the author's thesis [9], §3.3, for details): let q be the torsion invariant of X, and let B be the Bockstein operator, defined to be the connecting homomorphism $H^1(X, \mathbf{Z}/q\mathbf{Z}) \longrightarrow H^2(X, \mathbf{Z}/q\mathbf{Z})$ in the long exact sequence coming from the exact sequence $0 \longrightarrow \mathbf{Z}/q\mathbf{Z} \longrightarrow \mathbf{Z}/q^2\mathbf{Z} \longrightarrow \mathbf{Z}/q\mathbf{Z} \longrightarrow 0$. One checks that

$$\ker B = \{\psi \in H^1(x, \mathbf{Z}/q\mathbf{Z}) | \psi(x) = 0 \text{ for all } \bar{x} \in X^{\mathrm{ab}}_{\mathrm{tor}}\}.$$

Thus $\ker B$ has co-dimension 1 in $H^1(X, \mathbf{Z}/q\mathbf{Z})$, and $(\ker B)^{\perp}$ (the orthogonal complement with respect to the form given by the cup-product) is free of rank one over $\mathbf{Z}/q\mathbf{Z}$, generated by some homomorphism θ. One can show that $Y = \ker\theta$ is the (unique) subgroup of X of index q having maximal torsion invariant. If the image of the invariant χ is cyclic, then $\ker\theta$ is the $\log_p q$'th level subgroup in the tower ϕ_X. If $\mathrm{im}(\chi) \cong \mathbf{Z}_2 \oplus \mathbf{Z}/2\mathbf{Z}$, let $q' \neq 2$ be the torsion invariant of Y and use the above procedure to find $\theta' \in H^1(Y, \mathbf{Z}/q\mathbf{Z})$ whose kernal is the $\log_2 q$'th level subgroup of Y. Then θ' comes via restriction from $H^1(X, \mathbf{Z}/q\mathbf{Z})$, and its kernel (as a homomorphism on X) is the $\log_2 q$'th level subgroup of the tower ϕ_X.

Let ϕ be a $\mathbf{Z}_p$-tower in the Demuškin group X which is not a basic tower, and let $V = \ker\phi$. Then,

$$I_X^V \cong \mathbf{Z}/p^s\mathbf{Z}$$

for some positive integer s, and we will call p^s the torsion invariant of the tower ϕ. Identifying X/V with $\mathbf{Z}_p$ (via ϕ) defines a character

$$\alpha : \mathbf{Z}_p \longrightarrow (\mathbf{Z}/p^s\mathbf{Z})^{\times}$$

giving the action of X/V on I_X^V. Explicitly, if $\gamma \in \mathbf{Z}_p$ and $\phi(X) = \gamma$, one has $\alpha(\gamma) \equiv \chi(x) (\mathrm{mod}\ p^s)$. Our main result is the following theorem.

THEOREM 1. *Let X be a Demuškin group with rank $n+2$ such that* $\mathrm{scd}_p X = 2$, *and let ϕ and ψ be two $\mathbf{Z}_p$-towers in X having the same tower-invariants $p^s \neq 2$ and α. Then there is an automorphism β of X such that $\phi \circ \beta = \psi$.*

3. **Proof of the Theorem.** The proof of the theorem consists in showing that the pairs (X, ϕ) and (X, ψ) are "Demuškin formations over $\mathbf{Z}_p$" (described below; the idea is due to Koch [5]), and invoking the uniqueness theorem of Koch/Wingberg (Proposition 1 below) to determine the existence of the automorphism β.

Let $\mathcal{G}'$ be the profinite group generated by elements σ and τ, subject to the single relation:

$$\sigma\tau\sigma^{-1} = \tau^{p^f},$$

and let $\mathcal{G}$ be any p-closed quotient thereof (i.e., any quotient whose order is divisible by p^{∞}). Let $n, s \geqq 1$ be integers, and let $\alpha : \mathcal{G} \longrightarrow (\mathbf{Z}/p^s\mathbf{Z})^{\times}$ be a given homomorphism. A Demuškin formation (X, ϕ) over $\mathcal{G}$ with invariants n, s, and α is a surjective homomorphism $\phi : X \longrightarrow \mathcal{G}$ of topological groups, with a pro-p kernel V, satisfying axioms (1), (2), and (3) below. For any $\mathcal{H} \lhd \mathcal{G}, \mathcal{H} \subset \ker(\alpha), G = \mathcal{G}/\mathcal{H}$, and $X_{\mathcal{H}} = \phi^{-1}(\mathcal{H})$, we have:

https://doi.org/10.4153/CMB-1989-032-9 Published online by Cambridge University Press

(1) the maximal pro-p quotient $\tilde{X}_{\mathcal{H}}$ of $X_{\mathcal{H}}$ is a Demuškin group of rank $n|G|+2$, having torsion invariant p^s;

(2) the symplectic space $H^1(\mathcal{H}, \mathbf{Z}/p\mathbf{Z})^{\perp}/H^1(\mathcal{H}, \mathbf{Z}/p\mathbf{Z})$ is a free $\mathbf{F}_p[G]$-module of rank n, and the bilinear form (induced on this space by the cup-product) is hyperbolic: there exists a decomposition of this space into two totally isotropic submodules;

(3) G acts on $H^2(X_{\mathcal{H}}, \mathbf{Z}/p^s\mathbf{Z})^*$ by means of character α.

In our situation, X is a Demuškin group, $\mathcal{G} = \mathbf{Z}_p$, and p^s and α are defined for the $\mathbf{Z}_p$-tower ϕ as in §2 above. The subgroups $\mathcal{H}$ are of the form $p^m\mathbf{Z}_p$, and we continue to write X_m in place of $X_{\mathcal{H}}$.

The rank statement of axiom (1) is well-known, following from a computation of Euler-Poincaré characteristics (see Serre, [8]; the paper [2] of Dummit and Labute is also of interest). The rest of axiom (1) and axiom (3) follow from the definition of α. To show the second axiom holds, we need a few lemmas.

Let $\phi_m \in H^1(X_m, \mathbf{Z}/p\mathbf{Z})$ be defined by

$$\phi_m(x) = \frac{1}{p^m}\mathrm{Res}_{X_m}\phi(x) \pmod p.$$

LEMMA 2. *ϕ_m is fixed under the action of $G = X/X_m$.*

PROOF. If $\phi(y) = 1$, then $\{1, y, \ldots, y^{p^m-1}\}$ is a complete set of coset representatives of X_m in X. Letting σ denote the coset yX_m, we have for any $x \in X_m$,

$$\begin{aligned}\phi_m^{\sigma}(x) = \phi_m(y^{-1}xy) &= \frac{1}{p^m}\phi(y^{-1}xy) \pmod p \\ &= \frac{1}{p^m}\phi(x) \pmod p \\ &= \phi_m(x).\end{aligned}$$ □

Let W be a profinite group, and let U be an open normal subgroup with quotient group H. Then for A a W-module, the composition

$$\mathrm{Res} \circ \mathrm{Cor} : H^i(U, A) \longrightarrow H^i(W, A) \longrightarrow H^i(U, A)$$

is the map on cohomology coming from the maps

$$M_W^U(A) \xrightarrow{\pi} A \xrightarrow{\iota} M_W^U(A).$$

Here $M_W^U(A)$ is the induced module, $\pi(f) = \Sigma g f(g^{-1})$ (where the sum runs over a set of representatives of U in W), and $\iota(a)(x) = x.a$ (see e.g., Serre [7], I–13). A direct computation shows that for $i = 0$ this composition is just the group-ring trace operator Tr_H, and by dimension-shifting we find that this is also the case for general i.

LEMMA 3. *For $m \geqq 1$, the image of ϕ_m under* $\mathrm{Cor} : H^1(X_m, \mathbf{Z}/p\mathbf{Z}) \longrightarrow H^1(X, \mathbf{Z}/p\mathbf{Z})$ *is ϕ_0.*

PROOF. Since $\mathrm{Res} \circ \mathrm{Cor}(\phi_m) = \mathrm{Tr}_G.\phi_m = |G|\phi_m = 0$, $\mathrm{Cor}(\phi_m) \in \ker(\mathrm{Res})$. On the other hand, $\ker(\mathrm{Res}) = \langle \phi_0 \rangle$, so that $\mathrm{Cor}(\phi_m) = a\phi_0$ for some a (mod p) satisfying

$$a = \mathrm{Cor}(\phi_m)(y) = \phi_m(\mathrm{Ver}\ _{X \to X_m}(y)) = \phi_m\left(\prod_{i=0}^{p^m-1} \widetilde{yy_i}^{-1} yy^i\right) = \phi_m(y^{p^m}) = 1,$$

where Ver is the group-theoretic transfer map, and $\tilde{z}$ is that element of the set $\{1, y, \ldots, y^{p^m-1}\}$ representing the coset zX_m. □

The nondegeneracy of the cup-product allows us to choose $\eta \in H^1(X, \mathbf{Z}/p\mathbf{Z})$ so that $\eta \cup \phi_0 = 1$; let $V_0 = \langle \eta, \phi_0 \rangle^{\perp}$ be the orthogonal complement of the space generated by η and ϕ_0 — the restriction of the cup-product to V_0 is a nondegenerate form. It should be remarked here that if $p = 2$ and the rank of the Demuškin group X is odd, then the torsion invariant of every $\mathbf{Z}_2$-tower is 2; this case is excluded from Theorem 1. In particular, the possibility that $\eta \in \langle \phi_0 \rangle$ does not arise for us.

Since Cor is an isomorphism of $H^2(X_m, \mathbf{Z}/p\mathbf{Z})$ with $H^2(X, \mathbf{Z}/p\mathbf{Z})$, we have

$$\mathrm{Res}(\eta) \cup \phi_m = \eta \cup \mathrm{Cor}(\phi_m) = \eta \cup \phi_0 = 1,$$

from which it follows that $\mathrm{Res}(\eta)$ and ϕ_m generate a G-stable subspace of $H^1(X_m, \mathbf{Z}/p\mathbf{Z})$ on which the cup product is nondegenerate. Let V_m denote the orthogonal complement of this space — V_m is a G-stable vector space of dimension $n|G| = np^m$ on which the cup-product restricts to a nondegenerate, G-invariant bilinear form.

LEMMA 4. *Let X be a Demuškin group with $scd_pX = 2$, and let $\omega \in H^1(X, \mathbf{Z}/p\mathbf{Z})$. If $Y = \ker(\omega)$, then one as an exact sequence*

$$H^1(Y, \mathbf{Z}/p\mathbf{Z}) \xrightarrow{\mathrm{Cor}} H^1(X, \mathbf{Z}/p\mathbf{Z}) \xrightarrow{\cdot\cup\omega} H^2(X, \mathbf{Z}/p\mathbf{Z}) \longrightarrow 0.$$

PROOF. We first mention that $\langle \omega \rangle$ is the kernel of $\mathrm{Res} : H^1(X, \mathbf{Z}/p\mathbf{Z}) \longrightarrow H^1(Y, \mathbf{Z}/p\mathbf{Z})$. The equality $\mathrm{Cor}(f \cup \mathrm{Res}(g)) = \mathrm{Cor}(f) \cup g$ gives the commutative diagram,

$$\begin{array}{ccccc}
H^1(X, \mathbf{Z}/p\mathbf{Z}) & \times & H^1(X, \mathbf{Z}/p\mathbf{Z}) & \xrightarrow{\cdot\cup\cdot} & H^2(X, \mathbf{Z}/p\mathbf{Z}) \\
\mathrm{Res}\downarrow & & \uparrow\mathrm{Cor}_1 & & \uparrow\mathrm{Cor}_2 \\
H^1(Y, \mathbf{Z}/p\mathbf{Z}) & \times & H^1(Y, \mathbf{Z}/p\mathbf{Z}) & \xrightarrow{\cdot\cup\cdot} & H^2(Y, \mathbf{Z}/p\mathbf{Z})
\end{array}$$

where Cor_2 is an isomorphism. Let $W = im(\mathrm{Cor}_1)$; given any $\theta_1 \in W, \theta_1 \notin \langle \omega \rangle$, there is a $\theta_2 \in H^1(Y, \mathbf{Z}/p\mathbf{Z})$ so that

$$1 = \mathrm{Res}(\theta_1) \cup \theta_2 = \theta_1 \cup \mathrm{Cor}_1(\theta_2).$$

Hence either the radical of W is $\langle \omega \rangle$, or the restriction of the cup-product to W is nondegenerate. In the former case, let $\psi \in H^1(X, \mathbf{Z}/p\mathbf{Z})$ such that $\psi \cup \omega = 1$ and let

W' be the space generated by W and ψ. Then the cup-product is nondegenerate on W'; if $\gamma \in W'^{\perp}$ is non-zero, then there is a $\gamma' \in H^1(Y, \mathbf{Z}/p\mathbf{Z})$ so that $\gamma \cup \mathrm{Cor}_1(\gamma') = \mathrm{Res}(\gamma) \cup \gamma' = 1$, a contradiction. It follows that W is of codimension 1 in $H^1(X, \mathbf{Z}/p\mathbf{Z})$ and clearly contained in $\ker(\mathrm{Cor}_1)$, so in fact $W = \ker(\mathrm{Cor}_1)$.

If the restriction of the cup-product to W is nondegenerate, then $\omega \in W^{\perp}$, and reasoning similar to the above shows that ω and W generate all of $H^1(X, \mathbf{Z}/p\mathbf{Z})$. In particular, W is again of codimension 1, and must be all of $\ker(\cdot \cup \omega)$. □

LEMMA 5. *Cor* : $V_m \longrightarrow V_0$ *is surjective.*

PROOF. If $W \leqq Y \leqq Z$ are pro-p groups, then $\mathrm{Cor} : H^q(W, \mathbf{Z}/p\mathbf{Z}) \longrightarrow H^q(Z, \mathbf{Z}/p\mathbf{Z})$ "factors through" $H^q(Y, \mathbf{Z}/p\mathbf{Z})$ — this follows easily from an explicit calculation on cochains. Thus it suffices to show that $\mathrm{Cor} : V_m \longrightarrow V_{m-1}$ is surjective. Given $\theta \in V_{m-1}$, lemma 4 allows us to find a $\theta' \in H^1(X_m, \mathbf{Z}/p\mathbf{Z})$ such that $\mathrm{Cor}(\theta') = \theta$, and we may write $\theta' = a\phi_m + b\eta + c\gamma$ with $\gamma \in V_m$, and $a, b, c \in \mathbf{Z}/p\mathbf{Z}$ (here we abuse notation by writing η in place of $\mathrm{Res}(\eta)$). We find that $a = 0$ by examining $\eta \cup \theta'$, and since $\mathrm{Cor}(\theta') = \mathrm{Cor}(\theta' - b\eta)$ it follows that $\mathrm{Cor}(c\gamma) = \theta$, whence $\mathrm{Cor}(V_m) = V_{m-1}$. □

Let σ be a generator of the group G. The group ring $\mathbf{F}_p[G]$ is a local ring with principal maximal ideal generated by $\pi = \sigma - 1$, and the group ring trace Tr_G is just π^{q-1}, where $q = p^m$ is the order of σ. It is well known that every indecomposable left $\mathbf{F}_p[G]$-module is isomorphic to a power of the maximal ideal; from this it follows that if M is a finitely generated $\mathbf{F}_p[G]$-module, and if r is the rank of a maximal free summand of M, then the $\mathbf{F}_p$-rank of $\mathrm{Tr}_G M = r$.

Let M be an $\mathbf{F}_p[G]$-module with a G-invariant bilinear form Φ. The G-invariance of Φ is equivalent to the property that for any $\gamma \in \mathbf{F}_p[G]$ and $\theta, \theta' \in M, \Phi(\lambda\theta, \theta') = \Phi(\theta, \lambda^*\theta')$, where $(\Sigma a_g g)^* = \Sigma a_g g^{-1}$ is the natural involution on the group ring $\mathbf{F}_p[G]$. We say that the form Φ satisfies the "trace condition" if for any $\theta \in M, \Phi(\theta, \theta) = \Phi(\theta, \mathrm{Tr}_G\theta)$.

LEMMA 6. *Let M be a free $\mathbf{F}_p[G]$-module of even rank n, with $\Phi(\cdot, \cdot)$ a nondegenerate, G-invariant, alternating bilinear form on M which satisfies the trace condition. Then M possesses a hyperbolic decomposition into two totally isotropic submodules.*

PROOF. Let θ be an $\mathbf{F}_p[G]$-generator of M, and find a $\theta' \in M$ so that $\Phi(\theta', \mathrm{Tr}_G\theta) \neq 0$. It follows easily that θ and θ' generate a free rank two $\mathbf{F}_p[G]$-submodule of M on which the restriction of Φ is nondegenerate, and any such subspace has a hyperbolic decomposition (see [9], propositions 1.1 and 1.2 ($p \neq 2$) and proposition 1.3 ($p = 2$) for the details). Applying this procedure to the orthogonal complement of this rank two space in M and proceeding inductively completes the lemma. □

LEMMA 7. *The space V_m is a free $\mathbf{F}_p[G]$-module of rank n, and as a symplectic space possesses a hyperbolic decomposition.*

PROOF. The composition $\mathrm{Res} \circ \mathrm{Cor} : V_m \longrightarrow V_0 \longrightarrow V_m$ is the trace operator Tr_G, and the $\mathbf{F}_p$-rank of the image of this map is the rank of a maximal free $\mathbf{F}_p[G]$-summand of V_m. Since Cor is surjective and Res is injective, this rank is n. It now follows by computing $\mathbf{F}_p$-ranks that in fact V_m is free as an $\mathbf{F}_p[G]$-module. The restriction of the cup-product to V_m is a nondegenerate, antisymmetric G-invariant bilinear form Φ.

If $p \neq 2$, the cup-product is automatically alternating. If $p = 2$, then in our situation the torsion invariant 2^s of the tower is not 2; the cup-product on $H^1(X_m, \mathbf{Z}/2^s\mathbf{Z})$ thus gives a nondegenerate form into $H^2(X_m, \mathbf{Z}/2^s\mathbf{Z}) \cong \mathbf{Z}/2^s\mathbf{Z}$ such that for any $\theta \in H^1(X_m, \mathbf{Z}/2^s\mathbf{Z})$, $2\theta \cup \theta = 0$. The maps induced on cohomology from the surjections $\mathbf{Z}/2^s\mathbf{Z} \longrightarrow \mathbf{Z}/2\mathbf{Z}$ give the commutative diagram (see [4], Satz 3.26),

$$\begin{array}{ccccc} H^1(X_m, \mathbf{Z}/2^s\mathbf{Z}) & \times & H^1(X_m, \mathbf{Z}/2^s\mathbf{Z}) & \longrightarrow & H^2(X_m, \mathbf{Z}/2^s\mathbf{Z}) \\ \downarrow & & \downarrow & & \downarrow \\ H^1(X_m, \mathbf{Z}/2\mathbf{Z}) & \times & H^1(X_m, \mathbf{Z}/2\mathbf{Z}) & \longrightarrow & H^2(X_m, \mathbf{Z}/2\mathbf{Z}) \end{array}$$

the vertical maps being essentially reduction (mod 2). It follows that the cup product on V_m is alternating in this case also. Note that the restriction of the cup product to V_0 is also alternating: if the torsion invariant of X is greater than 2, this follows from the above discussion. If the torsion invariant of X is 2, then it can be shown that ϕ_0 represents the homomorphism $\theta \longmapsto \theta \cup \theta$ on $H^1(X, \mathbf{Z}/2\mathbf{Z})$ — hence $\theta \cup \theta = \theta \cup \phi_0 = 0$ on $V_0 \subset \langle \phi_0 \rangle^\perp$.

Finally, the trace condition is satisfied on V_m: given $\theta \in V_m$, we have $\Phi(\theta, \theta) = 0$. On the other hand,

$$\Phi(\theta, \mathrm{Tr}_G\theta) = \Phi(\theta, \mathrm{Res} \circ \mathrm{Cor}(\theta)) = \Phi'(\mathrm{Cor}(\theta), \mathrm{Cor}(\theta)) = 0,$$

where $\Phi'(\cdot, \cdot)$ is the restriction of the cup-product to V_0. We may thus apply lemma 6. □

With $\mathcal{H} = p^m\mathbf{Z}_p$ and $X_m = \phi^{-1}(\mathcal{H})$, we have a natural projection $X_m \longrightarrow \mathcal{H}$; on cohomology this induces the inflation map inf : $H^1(\mathcal{H}, \mathbf{Z}/p\mathbf{Z}) \longrightarrow H^1(X_m, \mathbf{Z}/p\mathbf{Z})$, which is injective with image generated by ϕ_m. It follows that

$$V_m \cong \frac{H^1(\mathcal{H}, \mathbf{Z}/p\mathbf{Z})^\perp}{H^1(\mathcal{H}, \mathbf{Z}/p\mathbf{Z})},$$

and the requirements of axiom (2) of Demuškin formation over $\mathbf{Z}_p$.

The proof of Theorem 1 is now a consequence of the following uniqueness theorem for Demuškin formations:

Proposition 1. *Let (X, ϕ) and (X, ψ) be two Demuškin formations over $\mathcal{G}$ with the same invariants $n, p^s \neq 2$, and α. Then there exists an automorphism β of X such that $\phi \circ \beta = \psi$.*

Proof. This uniqueness theorem was first stated by Koch for $p \neq 2$ (§3 of [5]), and proved in detail by Wingberg ([10], Satz 1). The case $p = 2$ and $p^s \neq 2$ was proved by Diekert (§2 of [1]).

References

1. V. Diekert, *Uber die Absolute Galoisgruppe dyadischer Zahlköper*, Journal für die reine und angewandte Mathematik **350** (1984).

2. D. Dummit, J. P. Labute, *On a new characterization of Demuškin groups*, Inv. Math. **73** (1983).

3. K. Haberland, *Galois cohomology of algebraic number fields*, VEB Deutcher Verlag der Wissenschaften (1978).

4. H. Koch, *Galoissche Theorie der p-Erweiterungen*, Springer-Verlag (1970).

5. ———, *The Galois group of a p-closed extension of a local number field*, Soviet Math. Dokl. **19** (1978).

6. J. P. Labute, *Classification of Demuškin groups*, Canad. J. of Math. **19** (1967).

7. J. P. Serre, *Cohomologie galoisienne*, Lecture Notes in Mathematics **7** (1963).

8. ———, *Structure de certains pro-p groupes*, Seminaire Bourbaki **252** (1962).

9. L. Simons, *The structure of the Hilbert symbol for unramified extensions of a 2-adic number field*, Ph.D. Thesis, McGill University (1986).

10. K. Wingberg, *Der Eindeutigkeitssatz für Demuškinformationen*, Inv. Math. **70** (1982).

University of Vermont
Burlington, Vermont

Current address:
St. Michael's College
Winooski, Vermont.