Free quotients of Demuškin groups with operators

by Kay Wingberg at Heidelberg

This paper concerns the problem of the existence of Galois extensions of a local number field k whose Galois groups are free pro-p groups.

If k is a $\mathfrak{p}$-adic field, then the Galois group $G(k(p)|k)$ of the maximal p-extension of k is a free pro-p group if k does not contain the group of p-th roots of unity, and otherwise $G(k(p)|k)$ is a Demuškin group, i.e. a pro-p Poincaré group of dimension 2. These groups are defined as follows: a pro-p group G is called a Demuškin group if its cohomology has the following properties:

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

$$\dim_{\mathbb{F}_p} H^2(G, \mathbb{Z}/p\mathbb{Z}) = 1, \quad \text{and the cup-product}$$

$$H^1(G, \mathbb{Z}/p\mathbb{Z}) \times H^1(G, \mathbb{Z}/p\mathbb{Z}) \xrightarrow{\cup} H^2(G, \mathbb{Z}/p\mathbb{Z}) \quad \text{is non-degenerate.}$$

In the following we exclude the exceptional case that $G \cong \mathbb{Z}/2\mathbb{Z}$. Then the dualizing module I of G is isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p$ as an abelian group and we have a canonical action of G on I.

Demuškin groups occur not only as Galois groups of the maximal p-extension of $\mathfrak{p}$-adic number fields (if these fields contain the group of p-th roots of unity) but also as the p-completion of the fundamental group of a compact oriented Riemann surface. In the first case the action of G on I is non-trivial whereas in the second case G acts trivially on I. We will only consider Demuškin groups acting non-trivially on its dualizing module and we are interested in free pro-p quotients of these groups. Possible ranks of such free quotients were first calculated in [7], [6] and [2].

In many cases of interest a finite group Δ of order prime to p acts on a Demuškin group. As an example consider the local field $k = \mathbb{Q}_p(\zeta_p)$, where p is an odd prime number. Then $G(k|\mathbb{Q}_p) \cong \mathbb{Z}/(p-1)\mathbb{Z}$ acts on the Demuškin group $G(k(p)|k)$. Of particular interest is the case where Δ is generated by an involution, e.g. $G(k|\mathbb{Q}_p(\zeta_p+\zeta_p^{-1}))\cong\mathbb{Z}/2\mathbb{Z}$ acts on $G(k(p)|k)$; see [8] where Demuškin groups with involution were considered.

In this paper we are interested in free pro-p quotients F of a Demuškin group G which are invariant under a given action of Δ on G and where the maximal abelian factor group $F^{ab}=F/[F,F]$ of F has a prescribed action of Δ.

In particular, we will show the following: if p is odd and $\Delta\cong\mathbb{Z}/2\mathbb{Z}$ acts on a p-Demuškin group G of rank $n+2$, then there exists a Δ-invariant free quotient F of G such that $\mathrm{rank}_{\mathbb{Z}_p}(F^{ab})^+=1$ and $\mathrm{rank}_{\mathbb{Z}_p}(F^{ab})^-=n/2$ (here the $(\pm)$-eigenspaces of a $\mathbb{Z}_p[\Delta]$-module M are denoted by $M^{\pm}$). This situation occurs as the following example shows: Let p be an odd regular prime number and consider the CM-field $k=\mathbb{Q}(\zeta_p)$ with maximal totally real subfield $k^+=\mathbb{Q}(\zeta_p+\zeta_p^{-1})$. Then the Galois group $G(k|k^+)\cong\mathbb{Z}/2\mathbb{Z}$ acts on the Galois group $G(k_{S_p}|k)$ of the maximal p-extension k_{S_p} of k which is unramified outside p. Let $k_{\mathfrak{p}}$ be the completion of k with respect to the unique prime $\mathfrak{p}$ of k above p and let $k_{\mathfrak{p}}(p)$ its maximal p-extension. Since we assume that k has no unramified p-extension, we have a surjection

$$G(k_{\mathfrak{p}}(p)|k_{\mathfrak{p}})\twoheadrightarrow G(k_{S_p}|k)$$

of the Demuškin group $G(k_{\mathfrak{p}}(p)|k_{\mathfrak{p}})$ of rank $p+1$ onto the free pro-p group $G(k_{S_p}|k)$ of rank $(p+1)/2$ (see [5] X.6 example 2) and

$$\mathrm{rank}_{\mathbb{Z}_p}(G(k_{S_p}|k)^{ab})^+=1,\quad \mathrm{rank}_{\mathbb{Z}_p}(G(k_{S_p}|k)^{ab})^-=(p-1)/2\,,$$

since $(G(k_{S_p}|k)^{ab})^+\cong G((k^+)_{S_p}|k^+)^{ab}\cong\mathbb{Z}_p$.

It would be of interest under which conditions there exist large free quotients of $G(k_{S_p}(p)|k)$ for an arbitrary CM-field k. If we assume that no prime $\mathfrak{p}$ above p splits in the extension $k|k^+$, such a quotient should be defined by free quotients of the local groups $G(k_{\mathfrak{p}}(p)|k_{\mathfrak{p}})$, $\mathfrak{p}|p$, with an acting of $G(k_{\mathfrak{p}}|k_p^+)\cong G(k|k^+)$ as above.

1 Pro-p Operator Groups

Let p be a prime number. For a pro-p group G we denote its Frattini subgroup by $G^*=G^p[G,G]$ and its descending p-central series by

$$G^{(1)}=G\qquad\text{and}\qquad G^{(i+1)}=(G^{(i)})^p[G^{(i)},G],\quad i\geq 1.$$

For the cohomology groups of G with coeffients in $\mathbb{Z}/p\mathbb{Z}$ we often set $H^i(G)=H^i(G,\mathbb{Z}/p\mathbb{Z})$. If A is an abelian group, then $A^\vee$ denotes its Pontryagin dual.

Let

$$1\longrightarrow H\longrightarrow\mathcal{H}\longrightarrow\Delta\longrightarrow 1$$

be an exact sequence of profinite groups where H is a pro-p group and the (supernatural) order of $\varDelta$ is prime to p. Let G be a pro-p-$\mathcal{H}$ operator group (see [5] IV.3 ex.3).

Proposition 1.1 *With the notation as above the following is true:*

(i) *Let $A \subseteq G/G^*$ be a $\mathbb{F}_p[\![\mathcal{H}]\!]$-submodule which is free as a $\mathbb{F}_p[\![H]\!]$-module. Then there exists a pro-p-$\mathcal{H}$ operator subgroup U of G such that the canonical map*

$$U/U^* \longrightarrow G/G^*$$

is injective with image equal to A.

(ii) *Let $B \subseteq G^{ab}$ be a $\mathbb{Z}_p[\![\mathcal{H}]\!]$-submodule which is free as a $\mathbb{Z}_p[\![H]\!]$-module. Then there exists a pro-p-$\mathcal{H}$ operator subgroup V of G such that the canonical map*

$$V^{ab} \longrightarrow G^{ab}$$

is injective with image equal to B.

If $\mathcal{H} = \varDelta$ is finite of order prime to p and G is a finitely generated pro-p group with an action by $\varDelta$, then case (i) is a result of N. Boston, see [1], prop. (2.3).

Proof: We only prove case (i), since the proof of case (ii) is completely analogously. Let

$$\mathcal{U} = \{U \subseteq G \,|\, U \text{ is an } \mathcal{H}\text{-invariant subgroup, } UG^*/G^* = A\}.$$

Then $\mathcal{U}$ is not empty since the full pre-image of A under the canonical $\mathcal{H}$-invariant map $G \twoheadrightarrow G/G^*$ is an element of $\mathcal{U}$. Furthermore, if $\{U_\lambda,\, \lambda \in I\}$ is a totally ordered subset of $\mathcal{U}$, then $V = \bigcap U_\lambda$ is an $\mathcal{H}$-invariant subgroup of G and

$$VG^*/G^* = \varprojlim U_\lambda G^*/G^* = A,$$

and so $V \in \mathcal{U}$. By Zorn's lemma there exists a minimal element $U_0 \in \mathcal{U}$. The $\mathcal{H}$-invariant map

$$U_0/U_0^* \twoheadrightarrow U_0G^*/G^* = A$$

has an $\mathcal{H}$-invariant splitting s. Indeed, by assumption, A is projective as a $\mathbb{F}_p[\![H]\!]$-module, and so A is a projective $\mathbb{F}_p[\![\mathcal{H}]\!]$-module, see [5] V.2 ex. 7). Let W be the full pre-image of $s(A) \subseteq U_0/U_0^*$ under the canonical map $U_0 \twoheadrightarrow U_0/U_0^*$. Then W is $\mathcal{H}$-invariant, $W/U_0^* = s(A)$ and we have the commutative diagram

$$\begin{array}{ccccccc}
U_0^* & \hookrightarrow & U_0 & \twoheadrightarrow & U_0/U_0^* & \twoheadrightarrow & U_0G^*/G^* = A \subseteq G/G^* \\
\| & & \uparrow & & \uparrow & \nearrow_{\sim} & \\
U_0^* & \hookrightarrow & W & \twoheadrightarrow & W/U_0^* & &
\end{array}$$

Since $WG^*/G^* = A$, it follows that $W \in \mathcal{U}$, and so $W = U_0$ because of the minimality of U_0. We obtain that $U_0/U_0^* = W/U_0^* \xrightarrow{\sim} U_0G^*/G^* = A$ which finishes the proof of the proposition. □

If k is a field and Δ a finite group of order prime to the characteristic of k, then by Maschke's theorem the category of $k[\Delta]$-modules is semi-simple. If Δ is abelian und k is splitting field for Δ, then every simple $k[\Delta]$-module has k-dimension equal to 1; one has a decomposition into eigenspaces

$$M = \prod_{\chi \in \Delta^\vee} M^\chi ,$$

where $M^\chi = \{x \in M \mid x^\sigma = x^{\chi(\sigma)} \text{ for all } \sigma \in \Delta\}$ is the isotypic component of a $k[\Delta]$-module M with respect to the character χ of Δ

Corollary 1.2 *Let p be an odd prime number and let Δ be a finite abelian group of exponent $p-1$ with character group $\Delta^\vee$. Let G be a pro-p-Δ operator group and let*

$$G/G^* = \prod_{\chi \in \Delta^\vee} (G/G^*)^\chi,$$

be the decomposition of G/G^* in χ-eigenspaces. Then there exist subsets M_χ of G such that

(i) $\bigcup_{\chi \in \Delta^\vee} M_\chi$ *is a minimal set of generators of G,*

(ii) $\overline{M}_\chi = \{x \bmod G^* \mid x \in M_\chi\}$ *is a basis of $(G/G^*)^\chi$ for all $\chi \in \Delta^\vee$,*

(iii) $x^\sigma = x^{\chi(\sigma)}$ *for $x \in M_\chi$ and $\sigma \in \Delta$.*

Proof: This follows directly from proposition (1.1)(i) with $H = 1$ and A a 1-dimensional subspace of an eigenspace $(G/G^*)^\chi$. □

Let Δ be a finite group of order prime to p and G a pro-p-Δ operator group which is finitely generated as a pro-p group. Let

$$1 \longrightarrow R \longrightarrow E \xrightarrow{\varphi} G \longrightarrow 1$$

be an exact sequence of pro-p groups such that the surjection φ induces an isomorphism $E/E^* \xrightarrow{\sim} G/G^*$. A lemma, which we will need later, is the following.

Lemma 1.3 *With the notation and assumptions as above there exists a continuous action of $\varDelta$ on E extending the action on G, i.e. the surjection $E \twoheadrightarrow G$ is $\varDelta$-invariant and R is a $\varDelta$-operator group.*

Proof: We consider the natural homomorphism

$$\mathrm{Aut}_R(E) \longrightarrow \mathrm{Aut}(G)$$

where $\mathrm{Aut}_R(E) \subseteq \mathrm{Aut}(E)$ denotes the group of automorphisms θ of E such that $\theta(R) \subseteq R$. Recall that the kernel of the homomorphism $\mathrm{Aut}(G) \to \mathrm{Aut}(G/G^*)$ is a pro-p group, cf. [4] 5.5. Therefore the commutative diagram

$$\begin{array}{ccc} & & \varDelta \\ & & \downarrow \\ \mathrm{Aut}_R(E) & \longrightarrow & \mathrm{Aut}(G) \\ \downarrow & & \downarrow \\ \mathrm{Aut}(E/E^*) & \xrightarrow{\sim} & \mathrm{Aut}(G/G^*) \end{array}$$

shows that the image of the prime-to-p group $\varDelta$ in $\mathrm{Aut}(G)$ is contained in the image of $\mathrm{Aut}_R(E) \to \mathrm{Aut}(G)$. Since the kernel of $\mathrm{Aut}(E) \twoheadrightarrow \mathrm{Aut}(E/E^*)$ is a pro-p group, and $\mathrm{Aut}(E/E^*) \xrightarrow{\sim} \mathrm{Aut}(G/G^*)$ is an isomorphism, it follows that the kernel of $\mathrm{Aut}_R(E) \to \mathrm{Aut}(G)$ is a pro-p group. Using again that $\varDelta$ is a prime-to-p group, we get a commutative diagram

$$\begin{array}{ccc} & \swarrow\!\cdot\!\cdot\!\cdot & \varDelta \\ & & \downarrow \\ \mathrm{Aut}_R(E) & \longrightarrow & \mathrm{Aut}(G). \end{array}$$

This proves the lemma. $\square$

Let p be a prime number and let

$$1 \longrightarrow G \longrightarrow \mathcal{G} \underset{\curvearrowleft s}{\longrightarrow} \varDelta \longrightarrow 1\,,$$

be a split exact sequence of profinite groups where G is a pro-p group and $\varDelta$ is a finite group of order prime to p. Thus $\mathcal{G}$ is the semi-direct product of $\varDelta$ by G and G is a pro-p-$\varDelta$ operator group where the action of $\varDelta$ on G is defined via the splitting s. Conversely, given a pro-p-$\varDelta$ operator group G, we get a semi-direct product $\mathcal{G} = G \rtimes \varDelta$ where the action of $\varDelta$ on G is the given one.

Let $\mathcal{G}(p)$ be the maximal pro-p quotient of $\mathcal{G}$ and let $G_\varDelta$ be the maximal quotient of G with trivial $\varDelta$-action. Observe that $G_\varDelta$ is well-defined.

Proposition 1.4 *With the notation and assumptions as above there is a canonical isomorphism*

$$G_\Delta \xrightarrow{\sim} \mathcal{G}(p)\,.$$

Furthermore, if Δ_0 is a subgroup of Δ such that $H^2(G,\mathbb{Z}/p\mathbb{Z})^{\Delta_0}=0$, then G_{Δ_0} is a free pro-p group.

Proof: Consider the exact commutative diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & N\cap G & \longrightarrow & N & \underset{\xleftarrow{\;s\;}}{\longrightarrow} & \Delta & \longrightarrow & 1\\
 & & \downarrow & & \downarrow & & \| & & \\
1 & \longrightarrow & G & \longrightarrow & \mathcal{G} & \underset{\xleftarrow{\;s\;}}{\longrightarrow} & \Delta & \longrightarrow & 1\\
 & & \downarrow & & \downarrow & & & & \\
 & & \tilde{G} & \xrightarrow{\sim} & \mathcal{G}(p)\,, & & & &
\end{array}$$

where N is the kernel of the canonical surjection $\mathcal{G}\twoheadrightarrow\mathcal{G}(p)$ and $\tilde{G}$ denotes the quotient $G/N\cap G$. Since Δ acts on $N\cap G$ via s, we obtain an induced action on $\tilde{G}$. This action is trivial because

$$g^{s(\sigma)-1}=[s(\sigma),g]\in N\cap G \qquad \text{for } g\in G \text{ and } \sigma\in\Delta\,,$$

and so we get a surjection

$$\varphi: G_\Delta \twoheadrightarrow \tilde{G}\,.$$

Consider the exact commutative diagram

$$\begin{array}{ccccccccc}
0 \longrightarrow & H^1(\tilde{G}) & \longrightarrow & H^1(G_\Delta) & \longrightarrow & H^1(\ker\varphi)^{G_\Delta} & \longrightarrow & H^2(\tilde{G}) & \longrightarrow & H^2(G_\Delta)\\
 & \uparrow & & \sim\downarrow inf & & & & \uparrow & & \downarrow inf\\
 & res\ \sim & & H^1(G)^\Delta & & & & res\ \sim & & H^2(G)^\Delta\\
 & & & \sim\uparrow res & & & & & & \sim\uparrow res\\
 & H^1(\mathcal{G}(p)) & \xrightarrow[\sim]{inf_1} & H^1(\mathcal{G}) & & & & H^2(\mathcal{G}(p)) & \xhookrightarrow{inf_2} & H^2(\mathcal{G})\,,
\end{array}$$

where the map inf_1 is bijective and inf_2 is injective because $\mathrm{Hom}(N,\mathbb{Z}/p\mathbb{Z})=0$. Therefore $H^1(\ker\varphi)^{G_\Delta}=0$, and so by the Frattini argument, see [5] (1.7.4), $\ker\varphi=1$, i.e. $G_\Delta\cong\tilde{G}\cong\mathcal{G}(p)$. Furthermore, it follows that

$$H^2(G_\Delta)\xrightarrow{inf}H^2(G)^\Delta$$

is injective. Therefore, if $H^2(G)^\Delta=0$, then $H^2(G_\Delta)=0$, and so G_Δ is a free pro-p group.

For a subgroup Δ_0 of Δ let $\mathcal{G}_0$ be the semi-direct product $G\rtimes\Delta_0$. Replacing in the proof above Δ by Δ_0 and $\mathcal{G}$ by $\mathcal{G}_0$, we obtain the assertion for every subgroup. □

2 Demuškin Groups with Operators

In this section we assume that

Δ is a finite group of order prime to p and
G is a p-Demuškin group of rank $n+2, n \geq 0$, with dualizing module I and an action by Δ.

Let $\mathcal{G}$ be the semi-direct product of Δ by G, i.e. the sequence

$$1 \longrightarrow G \longrightarrow \mathcal{G} \longrightarrow \Delta \longrightarrow 1$$

is split-exact.

The dualizing module I of G is defined as

$$I = \varinjlim_{m} \varinjlim_{U} H^2(U, \mathbb{Z}/p^m\mathbb{Z})^{\vee},$$

where the second limit is taken over the maps $cor^{\vee}$, the dual to the corestriction, and U runs through the open normal subgroups of G; the first limit is taken with respect to the multiplication by p.

Let

$$\chi : G \longrightarrow \mathrm{Aut}(I) \cong \mathbb{Z}_p^{\times}$$

be the character given by the action of G on I. We denote the canonical quotient $G/\ker(\chi)$ by Γ, i.e.

$$\chi_0 : \Gamma \hookrightarrow \mathrm{Aut}(I)\,.$$

In the following we assume that

$$G \quad \text{acts non-trivially on} \quad I$$

(thus $\Gamma \cong \mathbb{Z}_p$), and we define the (finite) invariant q of G by

$$q = \#(I^G).$$

Then we have a Δ-invariant isomorphism

$$H^2(G, \mathbb{Z}/q\mathbb{Z}) \cong \mathrm{Hom}(I^G, \mathbb{Z}/q\mathbb{Z}) \quad (\cong \mathbb{Z}/q\mathbb{Z} \text{ as an abelian group})$$

and a Δ-invariant non-degenerate pairing

$$H^1(G, \mathbb{Z}/q\mathbb{Z}) \times H^1(G, \mathbb{Z}/q\mathbb{Z}) \xrightarrow{\cup} H^2(G, \mathbb{Z}/q\mathbb{Z})\,.$$

From the exact sequence $0 \to \mathbb{Z}/q\mathbb{Z} \xrightarrow{q} \mathbb{Z}/q^2\mathbb{Z} \to \mathbb{Z}/q\mathbb{Z} \to 0$, we get the Bockstein homomorphism

$$B : H^1(G, \mathbb{Z}/q\mathbb{Z}) \longrightarrow H^2(G, \mathbb{Z}/q\mathbb{Z})$$

which is surjective and Δ-invariant.

Let P be a pro-p group. In this section we denote by P^i, $i \geq 1$, the descending q-central series, i.e.

$$P^1 = P \quad \text{and} \quad P^{i+1} = (P^i)^q[P^i, P] \quad \text{for } i \geq 1\,.$$

Let

$$1 \longrightarrow F \longrightarrow \mathcal{F} \longrightarrow \Delta \longrightarrow 1$$

be an exact sequence of profinite groups where F is a finitely generated pro-p group. Obviously, G^i and F^i are normal open subgroups of $\mathcal{G}$ and $\mathcal{F}$ respectively.

Proposition 2.1 *With the notation as above let $q > 2$ and $m \geq 2$. Assume that there exists a surjection*

$$\varphi_{m+1} : \mathcal{G} \twoheadrightarrow \mathcal{F}/F^{m+1}\,.$$

Then there exists a surjection

$$\varphi : \mathcal{G} \twoheadrightarrow \mathcal{F}$$

inducing the surjection $\quad \varphi_m : \mathcal{G} \xrightarrow{\varphi_{m+1}} \mathcal{F}/F^{m+1} \xrightarrow{can} \mathcal{F}/F^m\,.$

Proof: Assume that we have already found a surjection

$$\varphi_{i+1} : \mathcal{G} \twoheadrightarrow \mathcal{F}/F^{i+1}$$

for $i \geq m$ which induces φ_m, and let $\quad \varphi_i : \mathcal{G} \xrightarrow{\varphi_{i+1}} \mathcal{F}/F^{i+1} \xrightarrow{can} \mathcal{F}/F^i\,.$

Let $\gamma, x_0, \ldots, x_n$ be a minimal system of generators of G such that $x_k \in \ker(\chi)$ for $k \geq 0$ and $\chi(\gamma) = 1 - q$.

Claim: The group F^{i+1}/F^{i+2} is generated by elements of the form

$$w^q[w, \bar{\gamma}] \bmod F^{i+2}\,, \quad [w, \bar{x}_k] \bmod F^{i+2},\ k \geq 0, \quad w \in F^i\,,$$

where $\bar{\gamma}, \bar{x}_k \in F$ are lifts of the images of γ, x_k in F/F^2 under the surjection $G \twoheadrightarrow F/F^2$.

This shown in [3] prop. 5(i) (observe, that we have a surjection $G/G^{i+1} \twoheadrightarrow F/F^{i+1}$, and so the group F/F^{i+1} is generated by the elements $\bar{\gamma}, \bar{x}_k \mod F^{i+1}$).

Consider the diagram with exact line

(∗)
$$\begin{array}{ccccccccc} & & & & & & \mathcal{G} & & \\ & & & & & & \downarrow \varphi_i & & \\ 1 & \longrightarrow & F^i/F^{i+2} & \longrightarrow & \mathcal{F}/F^{i+2} & \longrightarrow & \mathcal{F}/F^i & \longrightarrow & 1 \,. \end{array}$$

Since $i \geq m \geq 2$, we have

$$[F^i, F^i] \subseteq F^{2i} \subseteq F^{i+2}\,,$$

and so the group F^i/F^{i+2} is abelian; we consider F^i/F^{i+2} as a $\mathcal{G}$-module via φ_i. The canonical exact sequence

$$0 \longrightarrow F^{i+1}/F^{i+2} \longrightarrow F^i/F^{i+2} \longrightarrow F^i/F^{i+1} \longrightarrow 0$$

induces a $\varDelta$-invariant exact sequence

$$0 \longrightarrow \mathrm{Hom}_G(F^i/F^{i+1}, I) \longrightarrow \mathrm{Hom}_G(F^i/F^{i+2}, I) \longrightarrow \mathrm{Hom}_G(F^{i+1}/F^{i+2}, I)\,.$$

Let $f \in \mathrm{Hom}_G(F^i/F^{i+2}, I)$. Then

$$\begin{array}{rcl} f([w, \bar{x}_k] \mod F^{i+2}) & = & f(w \mod F^{i+2})^{x_k - 1} = 0 \quad \text{for } k \geq 0, \\ f(w^q[w, \bar{\gamma}] \mod F^{i+2}) & = & f(w \mod F^{i+2})q + f(w \mod F^{i+2})^{\gamma - 1} \\ & = & f(w \mod F^{i+2})(q - q) = 0\,. \end{array}$$

Using the claim, we see that f vanishes on F^{i+1}/F^{i+2}, and so

$$\mathrm{Hom}_G(F^i/F^{i+1}, I) \xrightarrow{\sim} \mathrm{Hom}_G(F^i/F^{i+2}, I)\,.$$

By duality, cf. [5] (3.7.6), (3.7.1), (3.4.6), we get

$$H^2(G, F^i/F^{i+2}) \xrightarrow{\sim} H^2(G, F^i/F^{i+1})\,,$$

and so

$$H^2(G, F^i/F^{i+2})^{\varDelta} \xrightarrow{\sim} H^2(G, F^i/F^{i+1})^{\varDelta}\,.$$

Since the order of $\varDelta$ is prime to p, the Hochschild-Serre spectral sequence

$$H^i(\varDelta, H^j(G, -)) \Rightarrow H^{i+j}(\mathcal{G}, -)$$

degenerates, i.e. $H^j(G, -)^{\varDelta} \cong H^j(\mathcal{G}, -)$. Therefore we obtain the isomorphism

$$H^2(\mathcal{G}, F^i/F^{i+2}) \xrightarrow{\sim} H^2(\mathcal{G}, F^i/F^{i+1})\,.$$

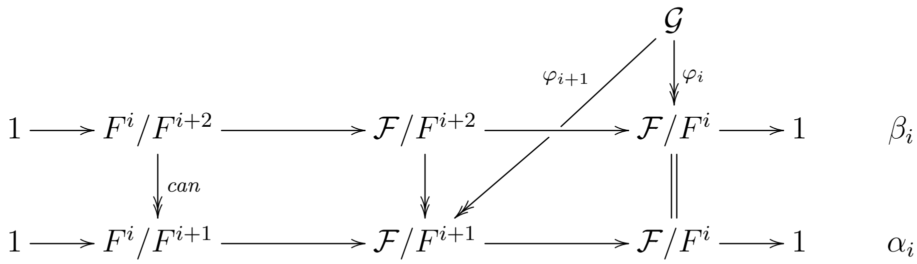
Now we prove that the embedding problem (∗) is solvable. For this we have to show that the 2-class

$$[\beta_i] \in H^2(\mathcal{F}/F^i, F^i/F^{i+2})$$

is mapped to zero under the inflation map $\mathit{inf} = \varphi_i^*$,

$$H^2(\mathcal{F}/F^i, F^i/F^{i+2}) \xrightarrow{\mathit{inf}} H^2(\mathcal{G}, F^i/F^{i+2}),$$

where β_i is the 2-cocycle corresponding to the group extension in $(*)$, see [5] (9.4.2). From the commutative exact diagram



we get a commutative diagram

$$\begin{array}{ccc} H^2(\mathcal{F}/F^i, F^i/F^{i+2}) & \xrightarrow{\varphi_i^*} & H^2(\mathcal{G}, F^i/F^{i+2}) \\ {\scriptstyle can_*}\downarrow & & {\scriptstyle can_*}\downarrow\wr \\ H^2(\mathcal{F}/F^i, F^i/F^{i+1}) & \xrightarrow{\varphi_i^*} & H^2(\mathcal{G}, F^i/F^{i+1}) \end{array}.$$

Since there exists the solution φ_{i+1} for the embedding problem α_i, we have $\varphi_i^*([\alpha_i]) = 0$, and so

$$can_* \circ \varphi_i^*([\beta_i]) = \varphi_i^* \circ can_*([\beta_i]) = \varphi_i^*([\alpha_i]) = 0.$$

From the injectivity of the map can_* on the right-hand side of the diagram above it follows that $\varphi_i^*([\beta_i]) = 0$, and so there exists a solution

$$\varphi_{i+2} : \mathcal{G} \longrightarrow \mathcal{F}/F^{i+2}$$

of the embedding problem corresponding to β_i. This homomorphism is necessarily surjective and induces φ_m, because φ_i has these properties, cf. [5] (3.9.1).

Using a compactness argument, we get in the limit a surjection $\varphi : \mathcal{G} \twoheadrightarrow \mathcal{F}$ inducing φ_m. This finishes the proof of the proposition. □

In the following let p be an odd prime number and let $\Delta = \langle\sigma\rangle \cong \mathbb{Z}/2\mathbb{Z}$ be cyclic of order 2. We denote, as usual, the $(\pm)$-eigenspaces of a $\mathbb{Z}_p[\Delta]$-module M by $M^\pm$.

Proposition 2.2 *Let p be an odd prime number and let G be a p-Demuškin group of rank $n+2$, $n \geq 0$, with dualizing module I and invariant $q = \#(I^G) < \infty$. Assume that $\Delta \cong \mathbb{Z}/2\mathbb{Z}$ acts on G. Then the following holds:*

(i) *If $H^2(G, \mathbb{Z}/p\mathbb{Z}) = H^2(G, \mathbb{Z}/p\mathbb{Z})^-$, then G_Δ is a free pro-p group of rank $n/2+1$.*

(ii) *If $H^2(G, \mathbb{Z}/p\mathbb{Z}) = H^2(G, \mathbb{Z}/p\mathbb{Z})^+$, then G_Δ is a p-Demuškin group of rank $m+2$, $0 \leq m \leq n$, with invariant q and dualizing module I.*

Proof: We start with the following remark. Since $\mathrm{Aut}(I) \cong \mathbb{Z}_p^\times$ is abelian, the surjection $G \twoheadrightarrow \Gamma$ factors through G_Δ. With the notation of the proof of proposition (1.4), it follows that $N \cap G$ has infinite index in G and therefore $cd_p(N) = cd_p(N \cap G) \leq 1$, cf. [5] III.7 ex.3. Using the Hochschild-Serre spectral sequence and the fact that $\mathrm{Hom}(N, \mathbb{Z}/p\mathbb{Z}) = 0$, we see that inf_2 is an isomorphism, and so the commutative diagram in the proof of (1.4) shows the surjectivity of the map $H^2(G_\Delta) \hookrightarrow H^2(G)^\Delta$, hence

$$H^2(G_\Delta) \cong H^2(G)^\Delta.$$

(i) By proposition (1.4) and $H^2(G_\Delta) = 0$, G_Δ is a free pro-p group. Since the non-degenerate pairing

$$H^1(G) \times H^1(G) \xrightarrow{\cup} H^2(G) \cong \mathbb{Z}/p\mathbb{Z}$$

is Δ-invariant, it follows from $H^2(G) = H^2(G)^-$ that

$$\dim_{\mathbb{F}_p} H^1(G)^\pm = n/2+1\,.$$

Therefore

$$\dim_{\mathbb{F}_p} H^1(G_\Delta) = \dim_{\mathbb{F}_p} H^1(G)^\Delta = n/2+1\,.$$

(ii) If $H^2(G) = H^2(G)^+$, then $H^2(G_\Delta) \cong H^2(G)$, and we obtain a non-degenerate pairing

$$H^1(G_\Delta) \times H^1(G_\Delta) \xrightarrow{\cup} H^2(G_\Delta) \cong \mathbb{Z}/p\mathbb{Z}$$

showing that G_Δ is a p-Demuškin group. Finally, since G_Δ is non-trivial and its rank has to be even, it follows that $\dim_{\mathbb{F}_p} H^1(G_\Delta) \geq 2$, and since $\ker(G \twoheadrightarrow G_\Delta)$ acts trivially on I, we have $\#(I^{G_\Delta}) = \#(I^G) = q$ and I is also the dualizing module of G_Δ. □

3 Free Quotients of Demuškin Groups

As before, let G be a p-Demuškin group of rank $n+2$ with dualizing module I and assume that $2 < q < \infty$. We are interested in quotients of G which are free pro-p groups. First we calculate the possible ranks of such quotients.

Proposition 3.1 *Let G be a Demuškin group of rank $n+2$ with finite invariant $q > 2$ and let F be a free quotient of G. Then*

(i) *$H^1(F, \mathbb{Z}/q\mathbb{Z})$ lies in the kernel of the Bockstein homomorphism and*

(ii) *$H^1(F, \mathbb{Z}/q\mathbb{Z})$ is a totally isotropic free $\mathbb{Z}/q\mathbb{Z}$-submodule of $H^1(G, \mathbb{Z}/q\mathbb{Z})$ with respect to the pairing given by the cup-product.*

In particular,

$$\operatorname{rank} F \le \frac{n}{2} + 1\,.$$

Proof: Since F is free, $H^1(F, \mathbb{Z}/q\mathbb{Z})$ is a free $\mathbb{Z}/q\mathbb{Z}$-module. The commutative diagram

$$\begin{array}{ccc} H^1(G,\mathbb{Z}/q\mathbb{Z})\times H^1(G,\mathbb{Z}/q\mathbb{Z}) & \xrightarrow{\ \cup\ } & H^2(G,\mathbb{Z}/q\mathbb{Z}) \\ {\scriptstyle (inf\,,inf\,)}\big\uparrow & & \big\uparrow{\scriptstyle inf} \\ H^1(F,\mathbb{Z}/q\mathbb{Z})\times H^1(F,\mathbb{Z}/q\mathbb{Z}) & \xrightarrow{\ \cup\ } & H^2(F,\mathbb{Z}/q\mathbb{Z}) = 0 \end{array}$$

shows that $H^1(F, \mathbb{Z}/q\mathbb{Z})$ is a totally isotropic $\mathbb{Z}/q\mathbb{Z}$-submodule of $H^1(G, \mathbb{Z}/q\mathbb{Z})$, and so $\dim_{\mathbb{F}_p} H^1(F, \mathbb{Z}/p\mathbb{Z}) = \operatorname{rank}_{\mathbb{Z}/q\mathbb{Z}} H^1(F, \mathbb{Z}/q\mathbb{Z}) \le n/2 + 1$. From the commutative diagram

$$\begin{array}{ccc} H^1(G,\mathbb{Z}/q\mathbb{Z}) & \xrightarrow{\ B\ } & H^2(G,\mathbb{Z}/q\mathbb{Z}) \\ {\scriptstyle inf}\big\uparrow & & \big\uparrow{\scriptstyle inf} \\ H^1(F,\mathbb{Z}/q\mathbb{Z}) & \xrightarrow{\ B\ } & H^2(F,\mathbb{Z}/q\mathbb{Z}) = 0 \end{array}$$

follows that $H^1(F, \mathbb{Z}/q\mathbb{Z}) \subseteq \ker(B)$. □

Recall that Γ is the canonical quotient $G/\ker(\chi)$ of G, where $\chi : G \longrightarrow \operatorname{Aut}(I)$ is the character given by the action of G on I, i.e. $\Gamma \hookrightarrow \operatorname{Aut}(I)$.

Lemma 3.2 *The submodules $H^1(\Gamma, \mathbb{Z}/q\mathbb{Z})$ and $\ker B$ of $H^1(G, \mathbb{Z}/q\mathbb{Z})$ are orthogonal to each other, more precisely*

$$H^1(\Gamma, \mathbb{Z}/q\mathbb{Z}) = (\ker B)^{\perp}\,.$$

Proof: Consider the commutative diagram of non-degenerate pairings

$$\begin{array}{ccccccc} H^1(G,{}_qI) & \times & H^1(G,\mathbb{Z}/q\mathbb{Z}) & \xrightarrow{\cup} & H^2(G,{}_qI) & \xrightarrow{\sim} & \mathbb{Z}/q\mathbb{Z} \\ \delta\big\uparrow & & \big\downarrow B & & \big\| & & \\ H^0(G,{}_qI) & \times & H^2(G,\mathbb{Z}/q\mathbb{Z}) & \xrightarrow{\cup} & H^2(G,{}_qI) & \xrightarrow{\sim} & \mathbb{Z}/q\mathbb{Z} \end{array}$$

which is induced by the exact sequences

$$0 \longrightarrow \mathbb{Z}/q\mathbb{Z} \xrightarrow{q} \mathbb{Z}/q^2\mathbb{Z} \longrightarrow \mathbb{Z}/q\mathbb{Z} \longrightarrow 0 \quad \text{and} \quad 0 \longrightarrow {}_qI \longrightarrow {}_{q^2}I \xrightarrow{q} {}_qI \longrightarrow 0\,.$$

The image of $H^0(G,{}_qI) = H^0(\Gamma,{}_qI)$ under δ is contained in $H^1(\Gamma,{}_qI)$, and from $({}_{q^2}I)^\Gamma = {}_qI$ it follows that $\operatorname{im}\delta = H^1(\Gamma,{}_qI)$. Since the pairings above are non-degenerated, $H^1(\Gamma,\mathbb{Z}/q\mathbb{Z}) = H^1(\Gamma,{}_qI)$ is orthogonal to $\ker B$. Since $\operatorname{rank}_{\mathbb{Z}/q\mathbb{Z}}\ker B = \operatorname{rank}_{\mathbb{Z}/q\mathbb{Z}} H^1(G,Z/q\mathbb{Z}) - 1$, and so $\operatorname{rank}_{\mathbb{Z}/q\mathbb{Z}}(\ker B)^\perp = 1$, we prove the lemma. □

Proposition 3.3 *Let G be a p-Demuškin group of rank $n+2$ with finite invariant $q > 2$ and let F be a free factor of G of rank $n/2+1$. Then the canonical surjection $G \twoheadrightarrow \Gamma$ factors through F, i.e. there is a commutative diagram*

$$\begin{array}{ccc} G & \twoheadrightarrow & \Gamma \\ & \searrow \quad \nearrow & \\ & F & \end{array}.$$

Proof: Suppose the contrary. Then there exists an open subgroup G' of G which has a surjection

$$(G')^{ab} \twoheadrightarrow (F')^{ab} \times \Gamma'\,,$$

where F' is the image of G' in F under the projection $G \twoheadrightarrow F$ and Γ' is the image of G' under the projection $G \twoheadrightarrow \Gamma$. Let $q' = \#(I^{G'}) = \#(I^{\Gamma'})$ and let

$$B' : H^1(G', Z/q'\mathbb{Z}) \longrightarrow H^2(G', Z/q'\mathbb{Z})$$

be the corresponding Bockstein map. Since F' is free, it follows that $H^1(F',\mathbb{Z}/q'\mathbb{Z})$ is a totally isotropic submodule of $H^1(G',\mathbb{Z}/q'\mathbb{Z})$ and contained in $\ker B'$ by proposition (3.1). From lemma (3.2) we know that $H^1(\Gamma',\mathbb{Z}/q'\mathbb{Z})$ is orthogonal to $\ker B'$, and so also to $H^1(F',\mathbb{Z}/q'\mathbb{Z})$. Thus $H^1(F',\mathbb{Z}/q'\mathbb{Z}) \oplus H^1(\Gamma',\mathbb{Z}/q'\mathbb{Z})$ is totally isotropic. But $H^1(F',\mathbb{Z}/q'\mathbb{Z})$ is a maximal totally isotropic $\mathbb{Z}/q'\mathbb{Z}$-submodule of $H^1(G',\mathbb{Z}/q'\mathbb{Z})$ of rank $d \cdot n/2 + 1$, where $d = (G : G')$. This contradiction proves the proposition. □

For the existence of free quotients of Demuškin groups we have the following

Theorem 3.4 *Let G be a p-Demuškin group of rank $n+2$ with finite invariant $q > 2$ and let Δ be a finite abelian group of exponent $p-1$ acting on G. Let V be a $\mathbb{Z}/q\mathbb{Z}$-submodule of $H^1(G, \mathbb{Z}/q\mathbb{Z})$ such that*

(i) *V is $\mathbb{Z}/q\mathbb{Z}$-free and Δ-invariant,*
(ii) *V is totally isotropic with respect to the pairing given by the cup-product,*
(iii) *V lies in the kernel of the Bockstein map $B : H^1(G, \mathbb{Z}/q\mathbb{Z}) \to H^2(G, \mathbb{Z}/q\mathbb{Z})$.*

Then there exists a Δ-invariant surjection

$$G \twoheadrightarrow F$$

onto a free quotient F of G such that $H^1(F, \mathbb{Z}/q\mathbb{Z}) = V$.

Proof: Let

$$1 \longrightarrow R \longrightarrow F_{n+2} \longrightarrow G \longrightarrow 1$$

be a minimal presentation of G, where F_{n+2} is a free pro-p group of rank $n+2$. Using lemma (1.3), we extend the action of Δ to F_{n+2}. Let $\gamma, x_0, \dots, x_n$ be a basis of F_{n+2} such that

(i) each element of the basis of F_{n+2} generates a Δ-invariant subgroup isomorphic to $\mathbb{Z}_p$ on which Δ acts by some character $\psi : \Delta \to \mu_{p-1}$,

(ii) R, as a normal subgroup of F_{n+2}, is generated by the element

$$w = (x_0)^q [x_0, \gamma][x_1, x_2][x_3, x_4] \cdot \dots \cdot [x_{n-1}, x_n] \cdot f, \quad \text{where } f \in (F_{n+2})^3,$$

(iii) $V^\vee = \mathrm{Hom}(V, \mathbb{Z}/q\mathbb{Z})$ has a basis $\{v_i \mod (F_{n+2})^2, 1 \le i \le r = \mathrm{rank}_{\mathbb{Z}/q\mathbb{Z}} V\}$ such that

$$\{v_1, \dots, v_r\} \quad \text{is a subset of} \quad \{\gamma, x_1, \dots, x_n\}$$

and, if $v_i = x_{j(i)}$, then $x_{j(i)+1} \notin \{v_1, \dots, v_r\}$ or $x_{j(i)-1} \notin \{v_1, \dots, v_r\}$ according to whether $j(i)$ is odd or even.

Such a basis exists: by corollary (1.2), we find a basis of F_{n+2} with the property (i). Let $\psi_0 : \Delta \longrightarrow \mu_{p-1}$ be the character such that $H^2(G, \mathbb{Z}/q\mathbb{Z}) = H^2(G, \mathbb{Z}/q\mathbb{Z})^{\psi_0}$. The Δ-invariance of the cup-product gives us the perfect pairing

$$H^1(G, \mathbb{Z}/q\mathbb{Z})^{\psi} \times H^1(G, \mathbb{Z}/q\mathbb{Z})^{\psi^{-1}\psi_0} \xrightarrow{\cup} H^2(G, \mathbb{Z}/q\mathbb{Z})$$

for every character $\psi \in \Delta^\vee$ and the Bockstein homomorphism restricts to a surjection

$$H^1(G, \mathbb{Z}/q\mathbb{Z})^{\psi_0} \twoheadrightarrow H^2(G, \mathbb{Z}/q\mathbb{Z}).$$

Applying the usual procedure in order to get a basis with property (ii), see [5] (3.9.16), on the eigenspaces $H^1(G,\mathbb{Z}/q\mathbb{Z})^{\psi}$, $\psi \in \Delta^{\vee}$, we find a basis satisfying (i) and (ii). Using the assumptions on V, we can also satisfy (iii).

Let N be the normal subgroup of F_{n+2} generated by the set

$$\{\gamma, x_k,\, 0 \le k \le n\} \smallsetminus \{v_1, \ldots, v_r\},$$

then $F := F_{n+2}/N$ is a free pro-p group of rank r, N is Δ-invariant and we have

$$R \subseteq N(F_{n+2})^3$$

by the properties (ii) and (iii) of the basis $\gamma, x_0, \ldots, x_n$. Thus the Δ-invariant surjection

$$F_{n+2} \twoheadrightarrow F/F^3 = F_{n+2}/N(F_{n+2})^3$$

factors through a Δ-invariant surjection $G \twoheadrightarrow F/F^3$. Applying proposition (2.1), we get a Δ-invariant surjection from G onto a free pro-p group F which induces a surjection $G \twoheadrightarrow F/F^2 \cong F_{n+2}/N(F_{n+2})^2$.

By construction, we have $F/F^2 \cong V^{\vee}$, and so $H^1(F,\mathbb{Z}/q\mathbb{Z}) = V$. This finishes the proof of the theorem. □

Now we consider free quotients of a Demuškin group G which are invariant under a given Δ-action of G, where Δ is a group of order 2.

Corollary 3.5 *Let p be an odd prime number and let G be a p-Demuškin group of rank $n+2$, $n \ge 0$, with finite invariant q. Let $\Delta \cong \mathbb{Z}/2\mathbb{Z}$ acting on G such that $H^2(G,\mathbb{Z}/q\mathbb{Z}) = H^2(G,\mathbb{Z}/q\mathbb{Z})^-$. Let*

$$u^+,\, u^- \ge 0 \quad \textit{be integers such that} \quad u^+ + u^- = n/2\,.$$

Then there exists a Δ-invariant surjection

$$\varphi : G \twoheadrightarrow F$$

such that

(i) *F is a free pro-p group of rank $n/2+1$,*
(ii) $\mathrm{rank}_{\mathbb{Z}_p}(F^{ab})^+ = u^+ + 1$ *and* $\mathrm{rank}_{\mathbb{Z}_p}(F^{ab})^- = u^-$.

Proof: Since $H^2(G,\mathbb{Z}/q\mathbb{Z}) = H^2(G,\mathbb{Z}/q\mathbb{Z})^-$, the submodules $H^1(G,\mathbb{Z}/q\mathbb{Z})^{\pm}$ are maximal totally isotropic with respect to the cup-product pairing, and so

$$\mathrm{rank}_{\mathbb{Z}/q\mathbb{Z}} H^1(G,\mathbb{Z}/q\mathbb{Z})^{\pm} = n/2+1.$$

Let

$$V = V^+ \oplus V^-,$$

where V^+ is a free $\mathbb{Z}/q\mathbb{Z}$-submodule of $H^1(G, \mathbb{Z}/q\mathbb{Z})^+ \subseteq \ker B$ of rank $1 + u^+$ containing $H^1(\Gamma, \mathbb{Z}/q\mathbb{Z})$, and V^- is defined as follows. By lemma (3.2)

$$H^1(\Gamma, \mathbb{Z}/q\mathbb{Z}) \subseteq (\ker B^-)^\perp,$$

and since

$$\mathrm{rank}_{\mathbb{Z}/q\mathbb{Z}} H^1(G, \mathbb{Z}/q\mathbb{Z})^+ - \mathrm{rank}_{\mathbb{Z}/q\mathbb{Z}} V^+ = n/2 + 1 - (1 + u^+) = u^- ,$$

there exists a free $\mathbb{Z}/q\mathbb{Z}$-submodule V^- of $(\ker B)^-$ of rank u^- which is orthogonal to V^+. It follows that V is maximal totally isotropic and contained in $\ker B$.

By theorem (3.4), we obtain a free Δ-invariant quotient F of G of rank $n/2+1$ such that

$$H^1(F, \mathbb{Z}/q\mathbb{Z}) = V \cong (\mathbb{Z}/q\mathbb{Z}[\Delta]^+)^{u^+ + 1} \oplus (\mathbb{Z}/q\mathbb{Z}[\Delta]^-)^{u^-}.$$

Since F^{ab} is a free $\mathbb{Z}_p$-module, we obtain assertion (ii). □

Remark: Explicitly, we get a submodule V with the properties as above in the following way: let

$$1 \longrightarrow R \longrightarrow F_{n+2} \longrightarrow G \longrightarrow 1$$

be a minimal presentation of G, where F_{n+2} is a free pro-p group of rank $n+2$ with the extended action of Δ. Let $\gamma, x_0, \ldots, x_n$ be a basis of F_{n+2} such that R is generated by the element

$$w = (x_0)^q [x_0, \gamma][x_1, x_2][x_3, x_4] \cdot \cdots \cdot [x_{n-1}, x_n] \cdot f ,$$

$f \in (F_{n+2})^3$, and

$$\begin{aligned} \gamma^\sigma &= \gamma \cdot a , & x_i^\sigma &= x_i \cdot a_i & &\text{for } i = 2, 4, \ldots, n , \\ x_0^\sigma &= x_0^{-1} \cdot b, & x_i^\sigma &= x_i^{-1} \cdot b_i & &\text{for } i = 1, 3, 5, \ldots, n-1 . \end{aligned}$$

with a, b, a_i, $b_i \in (F_{n+2})^2$. Such a basis exists by the Δ-invariance of the cup-product and the Bockstein homomorphism, cf. [8] lemma 3. If we put

$$\begin{aligned} \gamma' &:= \gamma \cdot a^{\frac{1}{2}} , & x_i' &:= x_i \cdot a_i^{\frac{1}{2}} & &\text{for } i = 2, 4, \ldots, n , \\ x_0' &:= b^{-\frac{1}{2}} \cdot x_0 , & x_i' &:= b_i^{-\frac{1}{2}} \cdot x_i & &\text{for } i = 1, 3, 5, \ldots, n-1 , \end{aligned}$$

then

$$\begin{aligned} (\gamma')^\sigma &= \gamma' , & (x_i')^\sigma &= x_i' & &\text{for } i \geq 2 \text{ even}, \\ (x_0')^\sigma &= (x_0')^{-1}, & (x_i')^\sigma &= (x_i')^{-1} & &\text{for } i \geq 1 \text{ odd}, \end{aligned}$$

and

$$w = (x_0')^q[x_0', \gamma'][x_1', x_2'][x_3', x_4'] \cdot \dots \cdot [x_{n-1}', x_n'] \cdot f'$$

where $f' \in (F_{n+2})^3$. Let $u = 2u^+ - 1$. If we denote $x \bmod F^2$ by $\bar{x}$, then the dual of

$$\begin{aligned} V^\vee &:= \mathbb{Z}/q\mathbb{Z} \cdot \bar{\gamma} \oplus \bigoplus_{i=1,3,\dots,u} \mathbb{Z}/q\mathbb{Z} \cdot \bar{x}_{i+1} \oplus \bigoplus_{i=u+3,\dots,n} \mathbb{Z}/q\mathbb{Z} \cdot \bar{x}_{i-1} \\ &\cong (\mathbb{Z}/q\mathbb{Z}[\Delta]^+)^{u^++1} \oplus (\mathbb{Z}/q\mathbb{Z}[\Delta]^-)^{u^-} \end{aligned}$$

gives an example for a submodule with the properties (i)-(iii) in the proof of corollary (3.5). The free quotient of G is obtained in the following way: if

$$N = (x_0', \underbrace{x_1', x_3', \dots, x_u'}_{u^+\text{-times}}, \underbrace{x_{u+3}', \dots, x_n'}_{u^-\text{-times}}) \trianglelefteq F_{n+2}\,,$$

then $F = F_{n+2}/N$ is a free pro-p group of rank $n/2 + 1$, N is Δ-invariant, $R \subseteq N(F_{n+2})^3$ and $V^\vee = F/F^2$. Using proposition (2.1) we get the desired quotient of G.

With the notation and assumptions of corollary (3.5), we make for a Δ-invariant free quotient F of G of rank $n/2 + 1$ the following

Definition 3.6 *We call the tuple (u^+, u^-) the* **signature** *of F, if*

$$F/F^2 \cong (\mathbb{Z}/q\mathbb{Z}[\Delta]^+)^{u^++1} \oplus (\mathbb{Z}/q\mathbb{Z}[\Delta]^-)^{u^-}\,.$$

One can show that in general the signature of a maximal free quotient F of G does not determine F. But if the signature is equal to $(n/2, 0)$, then we have the following proposition.

Proposition 3.7 *Let p be an odd prime number and let Δ be of order 2. Let G be a p-Demuškin group of rank $n + 2$ with finite invariant q on which Δ acts such that $H^2(G, \mathbb{Z}/p\mathbb{Z})^\Delta = 0$. Let F be a free Δ-invariant quotient of G of rank $n/2 + 1$, i.e. the canonical surjection*

$$G \twoheadrightarrow F$$

is Δ-invariant. If the induced action of Δ on F/F^2 is trivial, i.e. F has signature $(n/2, 0)$, then F is equal to the maximal quotient G_Δ of G with trivial Δ-action. In particular, a free quotient of G with the properties above is unique.

Proof: As in the remark after the proof of corollary (3.5), we find generators of F on which Δ acts trivially, and so F has a trivial Δ-action. Thus we have a surjection $\varphi : G_\Delta \twoheadrightarrow F$. Since G_Δ is free of rank $n/2+1 = \dim_{\mathbb{F}_p} H^1(F, \mathbb{Z}/p\mathbb{Z})$ by proposition (2.2)(i), it follows that φ is an isomorphism. Thus F is the maximal quotient of G with trivial Δ-action. □

References

[1] Boston, N. *Explicit deformation of Galois representations.* Invent. Math. **103** (1991), 181-196.

[2] Jannsen, U., Wingberg, K. *Einbettungsprobleme und Galoisstruktur lokaler Körper.* J. reine u. angew. Math. **319** (1980) 196-212

[3] Labute, J.,P. *Classification of Demuškin groups.* Can. J. Math. **19** (1967) 106-132.

[4] Lubotzky, A. *Combinatorial group theory for pro-p-groups.* J. of Pure and Appl. Algebra **25** (1982) 311-325.

[5] Neukirch, J., Schmidt, A., Wingberg, K. *Cohomology of Number Fields.* Springer 2000

[6] Nguyen-Quand-Do, T. *Sur la structure galoisienne des corps locaux et la théorie d'Iwasawa.* Compos. Math. **46** (1982) 85-119.

[7] Sonn, J. *Epimorphisms of Demushkin Groups.* Israel J. Math. **17** (1974) 176-190.

[8] Wingberg, K. *On Demuškin groups with involution.* Ann. Sci. Éc. Norm. Sup. 4^e série **22** (1989) 555-567.

Mathematisches Institut
der Universität Heidelberg
Im Neuenheimer Feld 288
69120 Heidelberg
Germany

e-mail: wingberg@mathi.uni-heidelberg.de