In this paper we consider pro-$p$ Poincaré groups of dimension 2, also called “Demuškin groups”. These groups are defined as follows: a pro-$p$-group $G$ is called a Demuškin group if its cohomology has the following properties:

\[
\dim_{\mathbb{F}_p} H^1(G, \mathbb{Z}/p\mathbb{Z}) < \infty, \\
\dim_{\mathbb{F}_p} H^2(G, \mathbb{Z}/p\mathbb{Z}) = 1, \text{ and the cup-product} \\
H^1(G, \mathbb{Z}/p\mathbb{Z}) \times H^1(G, \mathbb{Z}/p\mathbb{Z}) \xrightarrow{\cup} H^2(G, \mathbb{Z}/p\mathbb{Z}) \text{ is non-degenerate.}
\]

In the following we exclude the exceptional case that $G \cong \mathbb{Z}/2\mathbb{Z}$. 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 as Galois groups of the maximal $p$-extension of $p$-adic number fields (if these fields contain the group of $p$-th roots of unity) and 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 $\Delta$ 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 $\overline{G(k|\mathbb{Q}_p)} \cong \mathbb{Z}/(p-1)\mathbb{Z}$ acts on the Demuškin group $D = G(k(p)|k)$, where $k(p)$ is the maximal $p$-extension of $k$. Of particular interest is the case where $\Delta$ is generated by an involution, e.g. $\overline{G(k|\mathbb{Q}_p(\zeta_p + \zeta_p^{-1}))} \cong \mathbb{Z}/2\mathbb{Z}$ acts on $D$; see [8] where Demuškin groups with involution were considered.

In the following, we are mainly interested in free pro-$p$-quotients of a Demuškin group $G$ which are invariant under a given action of $\Delta$ on $G$. We show the existence of $\Delta$-invariant free quotients $F$ of $G$ such that $F^{ab}$ has a prescribed action of $\Delta$. 
If $p$ is odd and $\Delta \cong \mathbb{Z}/2\mathbb{Z}$ acts on a $p$-Demushkin group $G$ of rank $n + 2$, then there exists a $\Delta$-invariant free quotient $F$ of $G$ such that $\text{rank}_{\mathbb{Z}/p}(F^+) = 1$ and $\text{rank}_{\mathbb{Z}/p}(F^-) = n/2$. This situation occurs for number fields 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 $G(k|k^+)$ acts on the Galois group $G(k_{sp}(p)|k)$ of the maximal $p$-extension $k_{sp}(p)$ of $k$ which is unramified outside $p$. Let $k_p$ be the completion of $k$ with respect to the unique prime $p$ of $k$ above $p$ and let $k_p(p)$ its maximal $p$-extension. Then we have a surjection

$$G(k_p(p)|k_p) \twoheadrightarrow G(k_{sp}(p)|k)$$

of the Demushkin group $G(k_p(p)|k_p)$ of rank $p + 1$ onto the free pro-$p$-group $G(k_{sp}(p)|k)$ of rank $(p + 1)/2$ and

$$\text{rank}_{\mathbb{Z}/p}(G(k_{sp}(p)|k)^+) = 1, \quad \text{rank}_{\mathbb{Z}/p}(G(k_{sp}(p)|k)^-) = (p - 1)/2.$$

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

1 Operators

Let $p$ be a prime number and let

$$1 \to G \overset{s}{\to} \mathcal{G} \to \Delta \to 1,$$

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

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

**Proposition 1.1** With the notation and assumptions as above there is a canonical isomorphism

$$G_\Delta \overset{\sim}{\longrightarrow} \mathcal{G}(p).$$

Furthermore, if $H^2(G, \mathbb{Z}/p\mathbb{Z})^\Delta = 0$, then $G_\Delta$ is a free pro-$p$-group.
Proof: Consider the exact commutative diagram

\[
\begin{array}{ccccccc}
1 & N \cap G & N & \Delta & 1 \\
1 & G & \mathcal{G} & \Delta & 1
\end{array}
\]

\[
\tilde{G} \quad \mathcal{G}(p),
\]

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 \(\Delta\) acts on \(N \cap G\) via \(s\), we obtain an induced action on \(\tilde{G}\). This action is trivial because

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

and so we get a surjection

\[
\varphi : \Delta \rightarrow \tilde{G}.
\]

Consider the exact commutative diagram

\[
\begin{array}{ccccccc}
0 & H^1(\tilde{G}) & H^1(\Delta) & H^1(\ker \varphi)^{\Delta} & H^2(\tilde{G}) & H^2(\Delta) \\
& \text{res} & \text{res} & \text{res} & \text{res} & \text{res}
\end{array}
\]

\[
\begin{array}{cccc}
H^1(\mathcal{G}(p)) & \text{inf}_1 & H^1(\mathcal{G}) & H^2(\mathcal{G}(p)) & \text{inf}_2 & H^2(\mathcal{G})
\end{array}
\]

where \(H^i(-) = H^i(-, \mathbb{Z}/p\mathbb{Z})\), and the bijectivity of \(\text{inf}_1\) and the injectivity of \(\text{inf}_2\) follows from \(\text{Hom}(N, \mathbb{Z}/p\mathbb{Z}) = 0\). We see that \(H^1(\ker \varphi)^{\Delta} = 0\), and so \(\ker \varphi = 1\), i.e. \(\Delta \cong \tilde{G} \cong \tilde{G}(\Delta)\).

Furthermore, it follows that

\[
H^2(\Delta) \xrightarrow{\text{inf}} H^2(\Delta)
\]

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

In the following lemma let \(G\) be a finitely generated pro-\(p\)-\(\Delta\) operator group, i.e. there is a homomorphism of profinite groups \(\Delta \rightarrow \text{Aut}(G)\), cf. [4] 5.1. Let

\[
1 \rightarrow R \rightarrow F \rightarrow G \rightarrow 1
\]

be a minimal presentation of the group \(G\) by a free pro-\(p\)-group \(F\) of rank \(\dim_{\mathbb{F}_p} H^1(G, \mathbb{Z}/p\mathbb{Z})\) and a normal subgroup \(R\).
Lemma 1.2 With the notation as above there exists a continuous action of $\Delta$ on $F$ extending the action on $G$, i.e. the surjection $F \rightarrow G$ is $\Delta$-invariant.

Proof: We may assume that the action of $\Delta$ on $G$ is faithful, i.e. $\Delta$ injects into $\text{Aut}(G)$. Let $\sigma \in \Delta$. Since $F$ is free, there exists a homomorphism $\tilde{\sigma} : F \rightarrow F$ such that the diagram

\[
\begin{array}{ccc}
F & \xrightarrow{\tilde{\sigma}} & F \\
\downarrow & & \downarrow \\
G & \xrightarrow{\sigma} & G
\end{array}
\]

commutes. The map $\tilde{\sigma}$ is necessarily an automorphism of $F$ since it induces a bijection on $F/F^2 \cong G/G^2$.

Let $\hat{\Delta}$ be the subgroup of $\text{Aut}(F)$ generated by all lifting $\tilde{\sigma}$ of the elements $\sigma \in \Delta$. Recall that the kernels of the homomorphisms $\text{Aut}(G) \rightarrow \text{Aut}(G/G^2)$ and $\text{Aut}(F) \rightarrow \text{Aut}(F/F^2)$ are pro-$p$-groups, cf. [4] 5.5, and that $\Delta$ has an order prime to $p$. Therefore, we can consider $\Delta$ as a subgroup of $\text{Aut}(G/G^2) \cong \text{Aut}(F/F^2)$, and there exists a subgroup $\Delta'$ of $\hat{\Delta}$ such the diagram

\[
\begin{array}{ccc}
\Delta' & \subseteq & \hat{\Delta} \\
& & \text{Aut}(F)
\end{array}
\]

\[
\begin{array}{ccc}
\Delta & \subseteq & \text{Aut}(F/F^2)
\end{array}
\]

commutes. Since every lifting $\tilde{\sigma}$ respects $R$, the same is true for the elements of $\Delta'$, i.e. $\Delta'$ consists of liftings of elements of $\Delta$. This proves the lemma. \(\Box\)

Now we assume that

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

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

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

is exact.

The dualizing module $I$ of $G$ is defined as

$$I = \lim_{\longrightarrow} \lim_{m \rightarrow U} H^2(U, \mathbb{Z}/p^m \mathbb{Z})^*,$$

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

4
Let 
\[ \chi : G \longrightarrow \text{Aut}(I) \cong \mathbb{Z}_p^\times \]
be the character given by the action of \( G \) on \( I \). We denote the canonical quotient \( G/\ker(\chi) \) by \( \Gamma \), i.e.
\[ \chi_0 : \Gamma \longrightarrow \text{Aut}(I). \]
In the following we assume that
\[ G \text{ acts non-trivially on } I \]
(thus \( \Gamma \cong \mathbb{Z}_p \)), and we define the (finite) invariant \( q \) of \( G \) by
\[ q = \#(I^G). \]
Then we have a \( \Delta \)-invariant isomorphism
\[ H^2(G, \mathbb{Z}/q\mathbb{Z}) \cong \text{Hom}(I^G, \mathbb{Z}/q\mathbb{Z}) \quad (\cong \mathbb{Z}/q\mathbb{Z} \text{ as an abelian group}) \]
and a \( \Delta \)-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 \( 0 \rightarrow \mathbb{Z}/q\mathbb{Z} \xrightarrow{q} \mathbb{Z}/q^2\mathbb{Z} \rightarrow \mathbb{Z}/q\mathbb{Z} \rightarrow 0 \), 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 \( \Delta \)-invariant.

For a pro-\( p \)-group \( P \) 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 \( G \) and \( F \) respectively.

**Proposition 1.3** With the notation as above let \( q > 2 \) and \( m \geq 2 \). Assume that there exists a surjection
\[ \varphi_{m+1} : \mathcal{G} \longrightarrow \mathcal{F}/F^{m+1}. \]
Then there exists a surjection
\[ \varphi : \mathcal{G} \longrightarrow \mathcal{F} \]
inducing the surjection \( \varphi_m : \mathcal{G} \xrightarrow{\varphi_{m+1}} \mathcal{F}/F^{m+1} \text{ can } \mathcal{F}/F^m. \]
**Proof:** Assume that we have already found a surjection
\[ \varphi_{i+1} : G / F^{i+1} \]
for \( i \geq m \) which induces \( \varphi_m \), and let \( \varphi_i : G \rightarrow F / F^{i+1} \) con. \( F / F^i \).

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
\[ w^q[w, \bar{\gamma}] \mod F^{i+2}, \quad [w, \bar{x}_k] \mod F^{i+2}, \quad k \geq 0, \quad w \in F^i, \]
where \( \bar{\gamma}, \bar{x}_k \in F \) are lifts of \( \varphi_2(\gamma), \varphi_2(x_k) \in F / F^2 \).

This shown in [3] prop. 5(i) (observe, that we have a surjecti on \( G / G^{i+1} \rightarrow F / F^{i+1} \), 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

\[
\begin{array}{ccccccccc}
G & \xrightarrow{\varphi_i} & 1 & F^i / F^{i+2} & \longrightarrow & F / F^{i+2} & \longrightarrow & F / F^i & 1.
\end{array}
\]

Since \( i \geq m \geq 2 \), the group \( F^i / F^{i+2} \) is abelian,
\[ [F^i, F^i] \subseteq F^{2i} \subseteq F^{i+2}, \]
and we consider \( F^i / F^{i+2} \) as a \( G \)-module via \( \varphi_i \). Since the dualizing module \( I \) of \( G \) is isomorphic to \( \mathbb{Q}_p / \mathbb{Z}_p \) as an abelian group, 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 \( \Delta \)-invariant exact sequence
\[
0 \longrightarrow \text{Hom}_G(F^i / F^{i+2}, I) \longrightarrow \text{Hom}_G(F^i / F^{i+1}, I) \longrightarrow \text{Hom}_G(F^{i+1} / F^{i+2}, I).
\]
Let \( f \in \text{Hom}_G(F^i / F^{i+2}, I). \) Then
\[
\begin{align*}
 f([w, \bar{x}_k] \mod F^{i+2}) &= f(w \mod F^{i+2})x_k^{-1} = 0 \quad \text{for } k \geq 0, \\
 f(w^q[w, \bar{\gamma}] \mod F^{i+2}) &= f(w \mod F^{i+2})q + f(w \mod F^{i+2})\gamma^{-1} \\
 &= f(w \mod F^{i+2})(q - q) = 0.
\end{align*}
\]
Using the claim, we see that \( f \) vanishes on \( F^{i+1} / F^{i+2} \), and so
\[ \text{Hom}_G(F^i / F^{i+1}, I) \xrightarrow{\sim} \text{Hom}_G(F^i / F^{i+2}, I). \]
By duality, cf. [5] (3.7.6), (3.7.1), (3.4.6), we get
\[ H^2(G, F^i / F^{i+2}) \xrightarrow{\sim} H^2(G, F^i / F^{i+1}), \]
6
and so
\[ H^2(G, F^{i}/F^{i+2}) \xrightarrow{\Delta} H^2(G, F^{i}/F^{i+1}), \]
Since the order of \( \Delta \) is prime to \( p \), we obtain the isomorphism
\[ H^2(G, F^{i}/F^{i+2}) \xrightarrow{\sim} H^2(G, F^{i}/F^{i+1}). \]

Now we prove that the embedding problem \( \ast \) is solvable. For this we have
\[ [\beta_i] \in H^2(F/F^i, F^i/F^{i+2}) \]
is mapped to zero under the inflation map \( \inf = \varphi_i^* \),
\[ H^2(F/F^i, F^i/F^{i+2}) \xrightarrow{\inf} H^2(G, F^{i}/F^{i+2}), \]
where \( \beta_i \) is the 2-cocycle corresponding to the group extension in \( \ast \), see [5] (9.4.2). From the commutative exact diagram
\[ \begin{array}{cccccc}
1 & F^i/F^{i+2} & F/F^{i+2} & F/F^i & 1 & \beta_i \\
& can & & can & & \\
1 & F^i/F^{i+1} & F/F^{i+1} & F/F^i & 1 & \alpha_i
\end{array} \]
we get a commutative diagram
\[ H^2(F/F^i, F^i/F^{i+1}) \xrightarrow{\varphi_i^*} H^2(G, F^{i}/F^{i+1}) \]
\[ \xrightarrow{can_*} H^2(F/F^i, F^i/F^{i+2}) \]
\[ \xrightarrow{\varphi_i^*} H^2(G, F^{i}/F^{i+2}). \]
Since there exists the solution \( \varphi_{i+1} \) for the embedding problem \( \alpha_{i} \), 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
\[ \varphi_{i+2} : G \rightarrow F/F^{i+2} \]
of the embedding problem corresponding to \( \beta_i \). This homomorphism is necessarily surjective and induces \( \varphi_m \), because \( \varphi_i \) has these properties, cf. [5] (3.9.2).

Using a compactness argument, we get in the limit a surjection \( \varphi : G \rightarrow F \)
inducing \( \varphi_m \). This finishes the proof of the proposition. \( \square \)
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 1.4** 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 $G_\Delta$ 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 $G_\Delta$ 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 $\text{Aut}(I) \cong \mathbb{Z}_p^\times$ is abelian, the surjection $G \twoheadrightarrow \Gamma$ factors through $G_{\Delta}$. With the notation of the proof of proposition 1.1, 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] chap.II, §7, ex.3. Using the Hochschild-Serre spectral sequence and the fact that $\text{Hom}(N, \mathbb{Z}/p\mathbb{Z}) = 0$, we see that $\inf_2$ is an isomorphism, and so

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

(i) By proposition 1.1, $G_{\Delta}$ 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 $\Delta$-invariant, it follows 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 $G_{\Delta}$ is a $p$-Demuškin group. Finally, since $G_{\Delta}$ 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 $G_{\Delta}$. \(\blacksquare\)
2 Free Quotients

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 2.1** 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,

$$\text{rank } F \leq \frac{n}{2} + 1.$$

**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

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

$$H^1(F, \mathbb{Z}/q\mathbb{Z}) \times H^1(F, \mathbb{Z}/q\mathbb{Z}) \xrightarrow{\inf} H^2(F, \mathbb{Z}/q\mathbb{Z}) = 0$$

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 $\dim_{\mathbb{F}_p} H^1(F, \mathbb{Z}/p\mathbb{Z}) = \text{rank}_{\mathbb{Z}/q\mathbb{Z}} H^1(F, \mathbb{Z}/q\mathbb{Z}) \leq n/2 + 1$. From the commutative diagram

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

$$H^1(F, \mathbb{Z}/q\mathbb{Z}) \xrightarrow{B} H^2(F, \mathbb{Z}/q\mathbb{Z}) = 0$$

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

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

$$\chi_0 : \Gamma \rightarrow \text{Aut}(I).$$

**Lemma 2.2** 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

\[
\begin{array}{ccc}
H^1(G, qI) \times H^1(G, \mathbb{Z}/q\mathbb{Z}) & \cup & H^2(G, qI) \\
\delta & & \ \ \ \ B \\
H^0(G, qI) \times H^2(G, \mathbb{Z}/q\mathbb{Z}) & \cup & H^2(G, \mathbb{Z}/q\mathbb{Z})
\end{array}
\]

which is induced by the exact sequences

\[
0 \rightarrow \mathbb{Z}/q\mathbb{Z} \xrightarrow{q} \mathbb{Z}/q^2\mathbb{Z} \rightarrow \mathbb{Z}/q\mathbb{Z} \rightarrow 0 \quad \text{and} \quad 0 \rightarrow qI \xrightarrow{q^2} q^2I \rightarrow qI \rightarrow 0.
\]

Let \(\zeta_{q^2}\) be a generator of \(q^2I\), and so \(\zeta_q = (\zeta_{q^2})^q\) is a generator of \(qI\). By definition of the homomorphism \(\delta\), i.e.

\[
\delta : H^0(G, qI) \rightarrow H^1(G, qI), \quad (\zeta_q)^i \mapsto \left\{ G \rightarrow qI, \ g \mapsto ((\zeta_{q^2})^i)g^{-1} \right\},
\]

we see that the image of \(\delta\) is \(H^1(\Gamma, qI)\). Since the pairings above are non-degenerated, it follows that \(H^1(\Gamma, \mathbb{Z}/q\mathbb{Z}) = H^1(\Gamma, qI)\) is orthogonal to \(\ker B\), and since \(\text{rank}_{\mathbb{Z}/q\mathbb{Z}}(\ker B)^\perp = 1\), we prove the lemma. \(\square\)

**Proposition 2.3** 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

\[
\begin{array}{ccc}
G & \twoheadrightarrow & F \\
& & \downarrow \\
& & \Gamma
\end{array}
\]

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 \((G')^{ab}\) is the image of \(G'\) in \(F\) under the projection \(G \twoheadrightarrow F\) and \(\Gamma'\) is the image of \(G'\) under the projection \(G \twoheadrightarrow \Gamma\). Let \(q' = \#(\Gamma') = \#(I\Gamma')\). 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 2.1. From lemma 2.2 we know that \(H^1(I\Gamma', \mathbb{Z}/q'\mathbb{Z})\) is orthogonal to \(\ker B'\), and so also to \(H^1(F', \mathbb{Z}/q'\mathbb{Z})\). Thus \(H^1(F', \mathbb{Z}/q'\mathbb{Z}) \oplus H^1(I\Gamma', \mathbb{Z}/q'\mathbb{Z})\) 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. \(\square\)

For the existence of free quotients of Demuškin groups we have the following
Theorem 2.4 Let $G$ be a $p$-Demushkin group of rank $n + 2$ with finite invariant $q > 2$ and let $\Delta$ 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 $\Delta$-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 $\Delta$-invariant surjection $F \twoheadrightarrow G$ onto a free quotient $\tilde{F}$ of $G$ such that $H^1(\tilde{F}, \mathbb{Z}/q\mathbb{Z}) = V$.

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 1.2, we extend the action of $\Delta$ to $F_{n+2}$. Let $\gamma, x_0, \ldots, x_n$ be a basis of $F_{n+2}$ such that

(i) each element of the basis of $F_{n+2}$ generates a $\Delta$-invariant subgroup isomorphic to $\mathbb{Z}/p\mathbb{Z}$ on which $\Delta$ 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

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

where $f \in (F_{n+2})^3$,
(iii) $V^* = \text{Hom}(V, \mathbb{Z}/q\mathbb{Z})$ has a basis \{ $v_i \mod (F_{n+2})^2, 1 \leq i \leq r = \text{rank}_{\mathbb{Z}/q\mathbb{Z}} V$ \} such that

\[ \{v_1, \ldots, v_r\} \quad \text{is a subset of} \quad \{\gamma, x_1, \ldots, x_n\} \]

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

Such a basis exists: by [1] prop.(2.3), we find a basis of $F_{n+2}$ with the property (i) (since $\Delta$ is abelian of exponent $p - 1$, the $\mathbb{Z}/q\mathbb{Z}[\Delta]$-module $F_{n+2}/(F_{n+2})^2$ decomposes into a sum of $\mathbb{Z}/q\mathbb{Z} \otimes_{\mathbb{Z}/p\mathbb{Z}} \Delta$-modules which are free $\mathbb{Z}/q\mathbb{Z}$-modules of rank equal to 1). The $\Delta$-invariance of the cup-product and the Bockstein homomorphism implies that we find a basis satisfying (i) and (ii), cf. [8] lemma 3 in the case where $\Delta \cong \mathbb{Z}/2\mathbb{Z}$. Using the assumptions on $V$, we can also satisfy (iii).

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

\[ \{\gamma, x_k, 0 \leq k \leq n\} \setminus \{v_1, \ldots, v_r\}, \]

11
then $F := F_{n+2}/N$ is a free pro-$p$-group of rank $r$, $N$ is $\Delta$-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 $\Delta$-invariant surjection

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

factors through a $\Delta$-invariant surjection

$$G \twoheadrightarrow F/F^3.$$ 

Applying proposition 1.3, we get a $\Delta$-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 $F/F^2 \cong V^*$, and so $H^1(F, \mathbb{Z}/q\mathbb{Z}) = V$. This finishes the proof of the theorem. \qed

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

**Corollary 2.5** Let $p$ be an odd prime number and let $G$ be a $p$-Demuškin group of rank $n + 2$, $n \geq 0$, with finite invariant $q$. Let $\Delta \cong \mathbb{Z}/2\mathbb{Z}$ acting on $G$ such that $H^2(G, \mathbb{Z}/q\mathbb{Z}) = H^2(G, \mathbb{Z}/q\mathbb{Z})^\perp$. Let

$$u^+, u^- \geq 0 \text{ be integers such that } u^+ + u^- = n/2.$$  

Then there exists a $\Delta$-invariant surjection

$$\varphi: G \twoheadrightarrow F$$

such that

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

**Proof:** Since $H^2(G, \mathbb{Z}/q\mathbb{Z}) = H^2(G, \mathbb{Z}/q\mathbb{Z})^\perp$, 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 $H^1(G, \mathbb{Z}/q\mathbb{Z})^+$ of rank $1 + u^+$ containing $H^1(\Gamma, \mathbb{Z}/q\mathbb{Z})$, and $V^-$ is a free $\mathbb{Z}/q\mathbb{Z}$-submodule of $\ker B^-$ of rank $u^-$ being orthogonal to $V^+$, i.e. $V$ is maximal totally isotropic and contained in $\ker B$. 

12
It is easy to see that $V^-$ exists (see also the remark below): by lemma 2.2 $H^1(\Gamma, \mathbb{Z}/q\mathbb{Z}) \subseteq (\ker B^-)^\perp$, and since

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

there exists a free submodule of $\ker B^-$ of rank $u^-$ which is orthogonal to $V^+$. Now theorem 2.4 gives us a free $\Delta$-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 $F^\text{ab}$ is free $\mathbb{Z}_p$-module, we obtain assertion (ii). \qed

**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 $\Delta$. Let $\gamma, x_0, \ldots, x_n$ be a basis of $F_{n+2}$ such that $R$ is generated by the element

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

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

$$\gamma^\sigma = \gamma \cdot a, \quad x_i^\sigma = x_i \cdot a_i \quad \text{for } i = 2, 4, \ldots, n,$$

$$x_0^\sigma = x_0^{-1} \cdot b, \quad x_i^\sigma = x_i^{-1} \cdot b_i \quad \text{for } i = 1, 3, 5, \ldots, n - 1,$$

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

$$\gamma' := \gamma \cdot a^1, \quad x_i' := x_i \cdot a_i^1 \quad \text{for } i = 2, 4, \ldots, n,$$

$$x_0' := b^{-1} \cdot x_0, \quad x_i' := b_i^{-1} \cdot x_i \quad \text{for } i = 1, 3, 5, \ldots, n - 1,$$

then

$$(\gamma')^\sigma = \gamma', \quad (x_i')^\sigma = x_i' \quad \text{for } i \geq 2 \text{ even},$$

$$(x_0')^\sigma = (x_0')^{-1}, \quad (x_i')^\sigma = (x_i')^{-1} \quad \text{for } i \geq 1 \text{ odd},$$

and

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

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

$$V^* := \mathbb{Z}/q\mathbb{Z} \cdot \bar{\gamma} \bigoplus_{i=1,3,\ldots,u} \mathbb{Z}/q\mathbb{Z} \cdot \bar{x}_{i+1} \bigoplus_{i=u+3,\ldots,n} \mathbb{Z}/q\mathbb{Z} \cdot \bar{x}_{i-1}$$

$$\cong (\mathbb{Z}/q\mathbb{Z}[\Delta]^+)^{u^+ + 1} \oplus (\mathbb{Z}/q\mathbb{Z}[\Delta]^-)^{u^-}$$
gives an example for a submodule with the properties (i)-(iii) in the proof of corollary 2.5. The free quotient of \( G \) is obtained in the following way: if
\[
N' = (x'_0, x'_1, x'_3, \ldots, x'_u, x'_{u+3}, \ldots, x'_n) \subseteq F_{n+2},
\]
\[\text{times}\]
\[
\text{times}
\]
then \( F = F_{n+2}/N' \) is a free pro-\( p \)-group of rank \( n/2 + 1 \), \( N' \) is \( \Delta \)-invariant, \( R \subseteq N(F_{n+2})^3 \) and \( V^* = F/F^2 \). Using proposition 1.3 we get the desired quotient of \( G \).

With the notation and assumptions of corollary 2.5, we make for a \( \Delta \)-invariant free quotient \( F \) of \( G \) of rank \( n/2 + 1 \) the following

**Definition 2.6** We call the tuple \((u^+, u^-)\) the **signature** of \( F \), if
\[
F/F^2 \cong (\mathbb{Z}/q\mathbb{Z}[\Delta]^+)u^+ + 1 \oplus (\mathbb{Z}/q\mathbb{Z}[\Delta])^{-}u^-.
\]

It is easy to see that 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 2.7** Let \( p \) be an odd prime number and let \( \Delta \) be of order 2. Let \( G \) be a \( p \)-Demuškin group of rank \( n + 2 \) with finite invariant \( q \) on which \( \Delta \) acts such that \( H^2(G, \mathbb{Z}/p\mathbb{Z})^\Delta = 0 \). Let \( F \) be a free \( \Delta \)-invariant quotient of \( G \) of rank \( n/2 + 1 \), i.e. the canonical surjection
\[
G \rightarrow F
\]
is \( \Delta \)-invariant. If the induced action of \( \Delta \) on \( F/F^2 \) is trivial, i.e. \( F \) has signature \((n/2, 0)\), then \( F \) is equal to the maximal quotient \( G_\Delta \) of \( G \) with trivial \( \Delta \)-action. In particular, a free quotient of \( G \) with the properties above is unique.

**Proof:** As in the remark after the proof of corollary 2.5, we find generators of \( F \) on which \( \Delta \) acts trivially, and so \( F \) has a trivial \( \Delta \)-action. Thus we have a surjection
\[
\varphi : G_\Delta \rightarrow F.
\]
Since \( G_\Delta \) is free of rank \( n/2 + 1 = \dim_{\mathbb{Z}} H^1(F, \mathbb{Z}/p\mathbb{Z}) \) by proposition 1.4(i), it follows that \( \varphi \) is an isomorphism. Thus \( F \) is the maximal quotient of \( G \) with trivial \( \Delta \)-action. \( \square \)
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 1999

[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. 4e série **22** (1989) 555-567

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

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