ON THE EMBEDDING OF CENTRAL EXTENSIONS INTO WREATH PRODUCTS

ANDREI V. ZAVARNITSINE

ABSTRACT. We find a necessary condition for the embedding of a central extension of a group $G$ with elementary abelian kernel into the wreath product that corresponds to a permutation action of $G$. The proof uses purely group-theoretic methods.

KEYWORDS: permutation module, central extension, wreath product.

MSC2010: 20D99

The finite group $G = \text{PSL}_2(q)$, $q$ odd, acts naturally by permutations on the projective line of order $q + 1$. In [5], we studied the embedding of $\text{SL}_2(q)$ into the wreath product of $\mathbb{Z}/2\mathbb{Z}$ and $G$ that corresponds to this permutation action. This problem was generalized in [6] to arbitrary groups $\text{PSL}_n(q)$ and their central extensions with kernel of prime order. In this paper, we obtain a further generalisation of these results.

Let $G$ be a finite group, $\Omega$ a finite set, and let $\rho : G \to \text{Sym}(\Omega)$ be a permutation representation. For $\omega \in \Omega$ we denote by $\text{St}(\omega)$ the stabilizer of $\omega$ in $G$.

For a commutative unital ring $A$ of prime characteristic $p$, consider the (right) $AG$-module $V$ corresponding to $\rho$ with basis (identified with) $\Omega$ and its submodule $0 \to I \to 'V$ generated by $\omega_0 = \sum_{\omega \in \Omega} \omega$. Clearly, there is an $AG$-module isomorphism $\alpha : A \to I$ defined by $\alpha : 1 \mapsto \omega_0$. Let $G \rtimes 'V$ denote the natural semidirect product.

Assume that we also have a central extension

$$1 \to A \to H \xrightarrow{\pi} G \to 1,$$

i.e. one with $\text{Im} \, \iota \leq \text{Z}(H)$, where we identify $A$ with its additive group $A^+$. A subgroup $S \leq G$ is liftable to $H$ if the full preimage $S\pi^{-1}$ splits over $\text{Im} \, \iota$. We say that $H$ is a subextension of $G \rtimes 'V$ with respect to the embedding (1), if there is an embedding $\beta : H \to G \rtimes 'V$ such that the following diagram commutes

$$
\begin{array}{ccccccc}
1 & \rightarrow & A & \xrightarrow{\iota} & H & \xrightarrow{\pi} & G & \rightarrow & 1 \\
\downarrow & & \downarrow & & \downarrow & & \| & & \\
1 & \rightarrow & V & \rightarrow & G \rtimes 'V & \rightarrow & G & \rightarrow & 1,
\end{array}
$$

where we identify $I = \text{Im} \, \alpha$ with its image in $V$ under (1).

The main result to be proved in Section 4 is the following necessary condition.

**Theorem 1.** In the above notation, if a central extension $H$ is a subextension of $G \rtimes 'V$ with respect to the embedding (1) then $\text{St}(\omega)$ is liftable to $H$ for every $\omega \in \Omega$.

The proof generalises some ideas presented in [5] [6]. In particular, we also prove an auxiliary result about presentations of $p$-groups.
Let $F = F\langle X \rangle$ be a free group with basis $X$. Every $w \in F$ can be written in the form
\[ w = x_{i_1}^{e_1} \ldots x_{i_t}^{e_t}, \]
where $x_i \in X$ and $\varepsilon = \pm 1$. For $x \in X$, we define
\[ \mu_x(w) = \sum_{x_i = x} \varepsilon_i. \]

The following fact is proven in Section 3.

**Proposition 2.** Every finite $p$-group $P$ has a finite presentation $\langle X \mid R \rangle$ such that $\mu_x(r) \equiv 0 \pmod{p}$ for all $x \in X$ and $r \in R$.

1. Fox derivatives

Let $X = \{x_1, \ldots, x_n\}$ and let $F = F\langle X \rangle$ be a free group with basis $X$. Recall that the (right) Fox derivative $\partial / \partial x_i : F \to \mathbb{Z}F$ is the map satisfying $\partial x_j / \partial x_i = \delta_{ij}$, $1 \leq j \leq n$ and
\[ \partial(\mu v) / \partial x_i = \partial u / \partial x_i v + \partial v / \partial x_i \]
for all $u, v \in F$ and $1 \leq i \leq n$. Let $w = w(x_1, \ldots, x_n) \in F$ and write
\[ w = x_{i_1}^{e_1} \ldots x_{i_t}^{e_t}, \]
where $x_{ik} \in X$ and $\varepsilon_k = \pm 1$ for all $k$. It can be shown [2, Proposition 2.73] that
\[ \frac{\partial w}{\partial x_i} = \sum_{\{k \mid i_k = i\}} \varepsilon_k f_k, \]
where
\[ f_k = \begin{cases} x_{i_{k+1}}^{e_{k+1}} x_{i_j}^{e_j} & \varepsilon_k = 1, \\ x_{i_{k+1}}^{e_{k+1}} x_{i_j}^{e_j} & \varepsilon_k = -1. \end{cases} \quad (4) \]

Let $G$ be a group and $V$ a $G$-module. Fixing a homomorphism $F \to G \times V$ we write the image of each $x_i$ as $g_i v_i$ for suitable $g_i \in G$, $v_i \in V$. Then using the additive notation in $V$ we can write
\[ w(g_1 v_1, \ldots, g_n v_n) = w(g_1, \ldots, g_n)(v_1 \frac{\partial w}{\partial y_1} + \ldots + v_n \frac{\partial w}{\partial y_n}), \quad (5) \]
where $\partial / \partial g_i$ is the short-hand notation for the composition of $\partial / \partial x_i$ and the homomorphism $\mathbb{Z}F \to \mathbb{Z}G$ which extends the map $x_i \mapsto g_i, i = 1, \ldots, n$. For details, see [3, §1.9].

2. Presentations of group extensions

Let
\[ 1 \to N \to G \to Q \to 1 \]
be a short exact sequence of groups. Suppose that $N$ has presentation $\langle Y \mid S \rangle$ and $Q$ has presentation $\langle X \mid R \rangle$. Using this information it is possible to describe a presentation of $G$. Let $Y$ be the image of $Y$ under $\iota : \overline{Y} \mapsto y$ and let
\[ S = \{ s \mid s \in \overline{S} \}, \]
where $s$ is the word in $Y$ obtained from $\overline{s}$ by replacing each $\overline{y}$ with $y$. Choose $X \subseteq G$ so that $x \pi = \overline{x} \in \overline{X}$ for all $x \in X$. For every $\overline{r} \in \overline{R}$, let $r$ be the word in $X$.
obtained from \( \tau \) by replacing each \( \tau \) with \( x \). Clearly, \( r \) as an element of \( G \) lies in \( \text{Ker} \pi = \text{Im} \iota \) and so is a word, say \( w_{r} \), in \( Y \). Define
\[
R = \{ r w_{r}^{-1} \mid r \in \overline{R} \}.
\]
Also, since \( \text{Im} \iota \trianglelefteq G \), the element \( x^{-1}y x \) lies in \( \text{Im} \iota \) for all \( y \in Y, x \in X \) and so is a word, say \( w_{xy} \), in \( Y \). We set
\[
T = \{ x^{-1}y x w_{xy}^{-1} \mid x \in \overline{X}, y \in \overline{Y} \}.
\]

**Proposition 3.** [3 Proposition 10.2.1], [2 Proposition 2.55] In the above notation,
\[
\langle X \cup Y \mid R \cup S \cup T \rangle
\]
is a presentation of \( G \).

3. **Proof of Proposition 2**

Recall that \( \Omega_{1}(P) \) denotes the subgroup of a \( p \)-group \( P \) generated by all elements of order \( p \).

**Proof.** We use induction on \(|P|\). If \(|P| = 1\), the claim holds. Assume \(|P| > 1\) and let \( N = \Omega_{1}(\text{Z}(P)) \). Note that \( N \) is a nontrivial elementary abelian \( p \)-group and
\[
1 \rightarrow N \rightarrow P \rightarrow Q \rightarrow 1
\]
is a central extension. By induction, \( Q \) has a finite presentation \( \langle \overline{X} \mid \overline{R} \rangle \) that satisfies the required property. Clearly, \( N \) also has a presentation \( \langle \overline{Y} \mid \overline{S} \rangle \), where \( \overline{Y} \) is finite and
\[
\overline{S} = \{ y^{p}, [y_{1}, y_{2}] \mid y, y_{1}, y_{2} \in \overline{Y} \},
\]
which has the required property. Note that we may take any basis of \( N \) as \( \overline{Y} \). We define the sets of generators \( X \) and \( Y \) and relators \( R, S, \) and \( T \) as before Proposition 3 where \( G = P \). Since the relators in \( S \) are rewritten from those of \( \overline{S} \), they have the required property, i.e., the exponent sum for each generator in each relator is a multiple of \( p \). Also, since \( \text{Im} \iota \) is central in \( P \), we have \( w_{xy} = y \) for all \( x \in X, y \in Y \), and so \( T \) consists of commutators which have the required property.

We now consider the relators \( rw_{r}^{-1} \) in \( R \). Some of them will be eliminated, while in others we will replace the subwords \( w_{r} \) with ones satisfying the required property. Indeed, we can choose a maximal linearly independent subset of
\[
W = \{ w_{r} \mid r \in R \} \subseteq \text{Im} \iota
\]
and complete it to a basis of \( \text{Im} \iota \). As we have mentioned, without loss of generality we may assume that this basis coincides with \( Y \). All generators \( y = w_{r} \in W \cap Y \) may be eliminated, because we have a relation \( w_{r} = r \) and \( r \) does not involve any \( y \in Y \). The remaining words \( w_{r} \in W \setminus Y \) are linear combinations of such generators, hence after the elimination they will become words in \( R \) which satisfy the needed property by induction. The words in \( S \cup T \) are commutators and powers \( y^{p} \), hence will retain the needed property, too. The resulting presentation of \( P \) clearly has the required property. \( \square \)
4. Proof of main theorem

The following result will be used.

**Proposition 4** (Gaschütz’ Theorem [11, (10.4)]). Let \( p \) be a prime, \( V \) a normal abelian \( p \)-subgroup of a finite group \( G \), and \( P \in \text{Syl}_p(G) \). Then \( G \) splits over \( V \) if and only if \( P \) splits over \( V \).

We are now ready to prove Theorem 1.

**Proof.** We denote \( \omega_0 = \sum_{\omega \in \Omega} \omega \). Assume to the contrary that there is \( \omega \in \Omega \) such that \( S = \text{St}(\omega) \) is not liftable to \( H \). Let \( P = \text{Syl}_p(S) \). Since \( A \) is an abelian \( p \)-group, Proposition 4 implies that \( P \) is not liftable to \( H \). Let \( \langle X \mid R \rangle \) be a finite presentation for \( P \) with the property that \( \mu_x(r) \equiv 0 \pmod{p} \) for every \( x \in X \), \( r \in R \). Such a presentation exists by Proposition 2.

Let \( F = F(X) \) be the free group with basis \( X = \{x_1, \ldots, x_n\} \). For every \( x \in X \), we denote \( \bar{x} = x\gamma \in P \), where \( \gamma : F \rightarrow P \) is the presentation homomorphism, and choose \( \bar{x} \in H \) so that
\[
\bar{x} \pi = x. \tag{7}
\]

There exists a relator \( r = r(x_1, \ldots x_n) \in R \) such that \( \bar{x} = r(\bar{x}_1, \ldots, \bar{x}_n) \neq 1 \) in \( H \).

Indeed, otherwise the subgroup
\[
\bar{T} = \langle \bar{x} \mid x \in X \rangle \leq H
\]
would satisfy the same relations as \( P \) and so the map \( [x \mapsto \bar{x}], x \in X \), would give rise to a homomorphism \( \sigma : P \rightarrow \bar{T} \) with the property \( \sigma \pi = \text{id}_P \). But this means that \( \bar{T} \) would be a splitting of the full preimage \( P \pi^{-1} \) contrary to the assumption.

Since
\[
\bar{x} \pi = x,
\]
we see that \( \bar{x} = a\bar{t} \) for a nonzero \( a \in A \). By assumption, \( H \) is a subextension of \( G \times V \) with respect to \([1]\). Hence \( \bar{x} \beta = a\omega_0 \), where the embedding \( \beta \) is as in \([4]\).

Also, we can write \( \bar{x}_i = g_i v_i, i = 1, \ldots, n \), for suitable \( g_i \in G \), \( v_i \in V \). Observe that \( g_i = x_i \) due to \([7]\) and the commutativity of diagram \([3]\). Let \( r = x_{i_1}^{\varepsilon_1} \cdots x_{i_l}^{\varepsilon_l} \) with \( k = 1, \ldots, l \). Define a homomorphism \( F \rightarrow G \times V \) by extending the map \( x_i \mapsto x_i v_i, i = 1, \ldots, n \). Using \([5]\) and \([8]\), we have
\[
\epsilon \omega_0 = \bar{x} \pi = r(\bar{x}_1 \beta, \ldots, \bar{x}_n \beta) = r(\bar{x}_1 v_1, \ldots, \bar{x}_n v_n) = r(\bar{x}_1, \ldots, \bar{x}_n)
\]
\[
\times (v_1 \frac{\partial r}{\partial \bar{x}_1} + \cdots + v_n \frac{\partial r}{\partial \bar{x}_n} - v_1 \sum_{\{k \mid \epsilon_k = 1\}} \varepsilon_k f_k \gamma + \cdots + v_n \sum_{\{k \mid \epsilon_k = n\}} \varepsilon_k f_k \gamma), \tag{9}
\]
where \( f_k \in F \) is given by \([4]\) and \( f_k \gamma \in P \). We can decompose
\[
V = A\omega \oplus V_0,
\]
where \( V_0 \) the \( A \)-linear span of \( \Omega \setminus \omega \), and write \( v_i = a_i \omega + w_i, i = 1, \ldots, n \), for suitable \( a_i \in A \) and \( w_i \in V_0 \). Since \( f_k \gamma \in S \) stabilizes \( \omega \), it also stabilizes \( V_0 \).

Therefore, the right-hand side of \([9]\) can be rewritten as
\[
a_1 \left( \sum_{\{k \mid \epsilon_k = 1\}} \varepsilon_k \right) \omega + w_1' + \cdots + a_n \left( \sum_{\{k \mid \epsilon_k = n\}} \varepsilon_k \right) \omega + w_n', \tag{10}
\]
where $w'_i = \sum_k \varepsilon_k w_{i, f_k}$ lies in $V_0$ for each $i$. Observe that
\[ \sum_{\{k \mid i_k = i\}} \varepsilon_k = \mu_{x_i}(r) \equiv 0 \pmod{p} \]
for every $i$ by assumption. Since $A$ has characteristic $p$, (10) equals $\sum_i w'_i = w'$, an element of $V_0$. We now compare the coefficients of $\omega$ for $w'$ and $a\omega_0$. Since $V$ is free as an $A$-module, these coefficients must coincide. However, the former is 0 and the latter is $a \neq 0$, a contradiction. \[\Box\]

References

[1] M. Aschbacher, Finite group theory. 2nd ed., Cambridge Studies in Advanced Mathematics, vol. 10, Cambridge University Press, Cambridge, 2000.

[2] D. F. Holt, B. Eick, and E. A. O’Brien, Handbook of computational group theory, Discrete Mathematics and its Applications, Chapman & Hall/CRC Press, Boca Raton, FL, 2005.

[3] D. L. Johnson, Presentations of groups. 2nd ed., London Math. Soc. Student Texts, vol. 15, Camb. Univ. Press, Cambridge, 1997.

[4] Yu. V. Kuzmin, Homological group theory, Advanced Studies in Mathematics and Mechanics, vol. 1, Factorial Press, Moscow, 2006.

[5] A.V. Zavarnitsine, Subextensions for a permutation $\text{PSL}_2(q)$-module, Sib. Elect. Math. Reports 10 (2013), 551–557.

[6] ____, Embedding central extensions of simple linear groups into wreath products, Sib. Elect. Math. Reports 13 (2016), 361–365.

Andrei V. Zavarnitsine, Sobolev Institute of Mathematics, 4, Koptyug av., 630090, Novosibirsk, Russia, 
E-mail address: zav@math.nsc.ru