EMBEDDING CENTRAL EXTENSIONS OF SIMPLE LINEAR GROUPS INTO WREATH PRODUCTS

ANDREI V. ZAVARNITSINE

Abstract. We find a criterion for the embedding of a nonsplit central extension of $\text{PSL}_n(q)$ with kernel of prime order into the permutation wreath product that corresponds to the action on the projective space.

Keywords: finite simple groups, permutation module, central cover, group cohomology.

1. Introduction

A group $B$ included in a short exact sequence of groups

$$1 \to A \xrightarrow{\iota} B \xrightarrow{\pi} C \to 1$$

is called an extension of $A$ by $C$ and denoted by $A.C$ in general, or by $A \rtimes C$ if it is split. The extension $B$ is central if $\iota(A) \subseteq Z(B)$.

We write $\mathbb{Z}_n$ for a cyclic group of order $n$ and $(m,n)$ for $\gcd(m,n)$.

This note concerns the following problem:

Problem 1. Let $G = \text{PSL}_n(q)$, where $q$ is a prime power, and let $r$ be a prime divisor of $(n,q-1)$. Does the permutation wreath product $\mathbb{Z}_r \wr \rho G$ contain a subgroup isomorphic to the nonsplit central extension $\mathbb{Z}_r.G$, where $\rho$ is the natural permutation representation of $G$ on the points of the projective space $\mathbb{P}^{n-1}(q)$?

We remark that the nonsplit extension $\mathbb{Z}_r.G$ mentioned in Problem 1 is unique up to isomorphism and is a quotient of $\text{SL}_n(q)$. This problem is a generalization of the one raised in [1, p. 67], where the case $n = r$ is considered. The case $n = 2$ was...
studied in [2], where it was shown that the embedding holds if and only if $q \equiv -1 \mod 4$. We generalize this result by proving the following

**Theorem 1.** In the notation of Problem 1, the nonsplit central extension $\mathbb{Z}_r.G$ is embedded into $\mathbb{Z}_r \wr \rho G$ if and only if $r$ does not divide $(q - 1)/(n, q - 1)$.

The main method that we use is based on some cohomological considerations and is similar to that of [2].

2. Preliminaries

Let $G$ be a group and let $L, M$ be right $G$-modules. Suppose

\[ 0 \to L \to M \to 1 \]

and

\[ 1 \to M \to E \xrightarrow{\pi} G \to 1 \]

are exact sequences of modules and groups, where the conjugation action of $E$ on $M$ agrees with the $G$-module structure, i.e. $m^e = m \cdot \pi(e)$ for all $m \in M$ and $e \in E$, and we identify $M$ with its image in $E$. A subgroup $S \triangleleft E$ such that

\[ S \cap M = L, \quad SM = E, \]

where we also identify $L$ with its image in $M$, which is itself an extension of $L$ by $G$, will be called a subextension of $E$ that corresponds to the embedding (1).

It is known [3] that the equivalence classes of extensions of $L$ by $G$ are in a one-to-one correspondence with (thus are defined by) the elements of the second cohomology group $H^2(G, L)$. Furthermore, the sequence (1) gives rise to a homomorphism

\[ H^2(G, L) \xrightarrow{\phi} H^2(G, M). \]

**Lemma 2.** [2, Lemma 2] Let $L, M$ be $G$-modules and $E$ an extension as specified above. Let $\bar{\gamma} \in H^2(G, M)$ be the element that defines $E$. Then the set of elements of $H^2(G, L)$ that define the subextensions $S$ of $E$ corresponding to the embedding (1) coincides with $\varphi^{-1}(\bar{\gamma})$, where $\varphi$ is the induced homomorphism (3). In particular, $E$ has such a subextension $S$ if and only if $\bar{\gamma} \in \text{Im} \varphi$.

We now present a slight generalization of the argument in [2, Section 7].

Denote by $\mathbb{F}_q$ a finite field of order $q$. The order of a group element $g$ will be denoted by $|g|$.

Let $G$ be a finite group, $X$ a set, and let $\rho$ be a permutation representation of $G$ on $X$. For a prime $p$, we consider the permutation $\mathbb{F}_p G$-module $V$ that corresponds to $\rho$ with basis (identified with) $X$ and its trivial submodule $I$ spanned by $\sum_{x \in X} x$. Clearly, the wreath product $\mathbb{Z}_p \wr G$ is the natural split extension $V \times G$.

**Lemma 3.** In the above notation, if a central extension $S = \mathbb{Z}_p.G$ is a subextension of $V \times G$ that corresponds to the embedding of $\mathbb{F}_p G$-modules $I \to V$ then $S$ has no element $s$ that satisfies the following three conditions

(i) $|s| = p^2$,
(ii) $|g| = p$, where $g \in G$ is the image of $s$ under the natural epimorphism $S \to G$,
(iii) $\rho(g)$ has a fixed point on $X$. 

Proof. Assume to the contrary that $s$ is such an element. Denote $t = \sum_{x \in X} x \in I$. Since $S = IG$, we have $s^p = ct$ for a nonzero $c \in \mathbb{F}_p$, and since $S$ is a subextension of $V \rtimes G$ with respect to $I \to V$, there exists $v \in V$ such that $s = gv$. Therefore, we have $ct = s^p = (gv)^p = vh$, where
\[ h = 1 + g + \ldots + g^{p-1}. \]
Let $x \in X$ be a fixed point of $\rho(g)$. We can write $v = a_x x + w$, for some $a_x \in \mathbb{F}_p$, where $w = \sum_{y \in X \setminus \{x\}} a_y y$. Clearly, $wh$ is a linear combination of elements of $X \setminus \{x\}$, and
\[ (a_x x)h = a_x (x + \ldots + x) = a_x px = 0. \]
Hence, the coefficient of $x$ in $ct = vh$ is zero, which contradicts $c \neq 0$. \hfill \Box

3. A permutation module for $\text{PSL}_n(q)$

We henceforth denote $G = \text{PSL}_n(q)$ and fix a prime divisor $r$ of $(n, q - 1)$. The natural permutation action $\rho$ of $G$ on the points of the projective space $\mathcal{P} = \mathbb{F}_q^{n-1}(q)$ gives rise to a permutation $\mathbb{F}_q G$-module $V$. As every permutation module, $V$ has a trivial submodule $I$ spanned by $\sum_{x \in \mathcal{P}} x$, and the augmentation submodule $V_0$ that consists of the elements $\sum_{x \in \mathcal{P}} a_x x$ with $\sum a_x = 0$. Since $\dim V = 1 + q + \ldots + q^{n-1} \equiv 0 \pmod{r}$, we have $I \subseteq V_0$, and the quotient $U = V_0/I$ is known [4] to be absolutely irreducible whenever $n \geq 3$. It was noticed by various authors [5, 6] that $U$ is one of the few known examples of modules with 2-dimensional 1-cohomology, namely we have:

Lemma 4. In the above notation, $H^1(G, U) \cong \mathbb{Z}_r^2$, whenever $n \geq 3$.

We will also require the 1-cohomology of $V$.

Lemma 5. Let $V$ be the above-defined permutation module. Then we have
\[ H^1(G, V) \cong \begin{cases} \mathbb{Z}_r, & r \text{ divides } (q - 1)/(n, q - 1), \\ 0, & \text{otherwise}. \end{cases} \]

Proof. We will assume that $n \geq 3$, as the claim holds for $n = 2$ by [2, Lemma 12]. Since the action of $G$ on $\mathcal{P}$ is transitive, we have $V \cong T^G$, where $T$ is the principal $\mathbb{F}_q H$-module for a point stabilizer $H$. By Shapiro’s lemma [7, §6.3], we have $H^1(G, V) \cong H^1(H, T) \cong \text{Hom}(H/H', T)$. The structure of $H$ is known [8, Section 2] and has the shape $\text{ASL}_{n-1}(q) \rtimes \mathbb{Z}_{(q-1)/(n, q-1)}$. Since $n \geq 3$ and $(n, q - 1) > 1$, the group $\text{ASL}_{n-1}(q)$ is perfect and so $H/H' \cong \mathbb{Z}_{(q-1)/(n, q-1)}$. As $T$ is cyclic of order $r$, the claim follows. \hfill \Box

4. Proof

We can now prove Theorem 1. Due to [2], we may assume that $n \geq 3$. We denote by $S$ the nonsplit central extension $\mathbb{Z}_r G$. Since $G$ is simple, the only possibility for $S$ to be a subgroup of the extension $V \rtimes G$ is if $S$ is its subextension, and since $I$ is the unique trivial submodule of $V$, this subextension must be with respect to the embedding $I \to V$. Being split, the extension $V \rtimes G$ is defined by the zero element of $H^2(G, V)$. Hence, Lemma 2 implies that all subextensions of $V \rtimes G$ with respect to $I \to V$ are defined by the elements of $\text{Ker} \varphi$, where $\varphi$ is the induced homomorphism
\[ H^2(G, I) \to H^2(G, V). \]
The short exact sequence of modules
\[ 0 \to I \to V \to V^0 \to 0, \]
where \( V^0 \cong V/I \), gives rise to the long exact sequence
\[ H^1(G, I) \to H^1(G, V) \cong H^1(G, V^0) \xrightarrow{\delta} H^2(G, I) \xrightarrow{\phi} H^2(G, V), \]
which implies that \( \text{Ker} \phi = \text{Im} \delta \). Observe that \( H^1(G, I) \cong \text{Hom}(G/G', I) = 0 \), since \( G \) is simple. Therefore, the map \( \alpha \) in (5) is an embedding, and \( \text{Ker} \phi \cong H^1(G, V^0)/H^1(G, V) \).

The structure of \( V \), see [4, Lemma 2], allows us to include \( V^0 \) in the nonsplit short exact sequence
\[ 0 \to U \to V^0 \to I \to 0, \]
which gives rise to the exact sequence
\[ H^0(G, V^0) \to H^0(G, I) \to H^1(G, U) \to H^1(G, V^0) \to H^1(G, I). \]
Now, \( H^0(G, V^0) = 0 \), since \( V^0 \) has no trivial submodules, and \( H^1(G, I) = 0 \) as above. Therefore, \( H^1(G, V^0) \cong H^1(G, U)/H^0(G, I) \). Since \( H^0(G, I) \cong \mathbb{Z}_r \), Lemma 4 implies \( H^1(G, V^0) \cong \mathbb{Z}_r \), and so \( \text{Ker} \varphi \) is 0 or \( \mathbb{Z}_r \) according as \( r \) divides \( q - 1 \) or otherwise, by Lemma 5. It follows that the nonzero element of \( H^3(G, I) \) that defines the nonsplit extension \( S \) lies in \( \text{Ker} \varphi \) if and only if \( r \) does not divide \( q - 1 \). By Lemma 2, this completes the proof of the theorem. \( \square \)

**Remark.** In the case when \( r \) divides \( (q - 1)/(n, q - 1) \), we can also prove the nonembedding of \( S \) into \( V \times G \) in a different way. Suppose this is the case. Then \( \mathbb{F}_q \) has an element \( a \) of multiplicative order \( r(n, q - 1) \). Let \( s \) be the image in \( S \) of \( \text{diag}(a, a, \ldots, a, a^{1-n}) \) under the epimorphism \( \text{SL}_n(q) \to S \). We have \( |s| = r^2 \) and \( |g| = r \), where \( g \) is the image of \( s \) under the epimorphism \( S \to G \). Observe that \( \rho(g) \) has a fixed point on \( \mathcal{P} \), because every diagonal element of \( \text{SL}_n(q) \) fixes a point on \( \mathcal{P} \), e.g. the projective image of the basis vector \((1, 0, \ldots, 0)\). Therefore, \( S \) cannot be a subextension of \( V \times G \) by Lemma 3.

**References**

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