JOURNAL OF ALGEBRA **202,** 690–703 (1998)
ARTICLE NO. JA977281

# Constructing Representations of Finite Groups and Applications to Finitely Presented Groups

W. Plesken*

*Lehrstuhl B für Mathematik. RWTH Aachen. Templergraben 64. D-52062.*



and

B. Souvignier†

*School of Mathematics and Statistics, University of Sydney, NSW 2006, Australia*

*Communicated by Gordon James*

Received June 17, 1997

## 1. INTRODUCTION

In this paper we attack the problem of proving a finitely presented group $G$ to be infinite by exploiting the representation theory of a finite factor group. It may be viewed as a continuation of [10, 15], where steps in the same direction have been taken. In [10], a cohomological criterion is used to decide whether an epimorphism onto a finite group can be lifted to an epimorphism onto an extension of a lattice by this finite group. In [15], modular representations are lifted to representations over a local ring and finally transformed into representations over a global field having an infinite image. In this paper we combine modular and global methods to decide whether an epimorphism of $G$ onto a finite group $H$ can be lifted to an epimorphism of $G$ onto an extension of some $\mathbb{Z}H$-lattice $L$ by $H$.

In Section 2 we compare $H^1(G, M)$ and $H^1(H, M)$ for $FH$-modules $M$ over prime fields $F$ to find $H$-modules in the kernel of an epimorphism $\varphi$ of $G$ onto $H$. Here $M$ is regarded as a $G$-module via $\varphi$. We demonstrate that the situation over finite fields imposes strong restrictions on the

*E-mail: plesken@willi.math.rwth-aachen.de.
† E-mail: bernd@maths.usyd.edu.au.



0021-8693/98 $25.00

situation over $\mathbb{Q}$ and derive a modular property of $\mathbb{Q}H$-modules that gives strong evidence for a $\mathbb{Q}H$-module to contain a lattice isomorphic to a $\mathbb{Z}H$-lattice in the kernel of $\varphi$.

In order to compute $H^1(G, M)$ one needs the action of $H$ on the module $M$ explicitly and therefore has to construct the corresponding representation. In [2] a formula is given to extend an absolutely irreducible monomial representation of a subgroup $S$ of a finite group $H$ to a representation of $H$ in case it exists. One of the drawbacks of the formula is that the field of definition gets rather big, because the monomial representation of $S$ often requires roots of unity which are unnecessary if the character is realized by a suitable equivalent representation. In Section 3 we exhibit a point of view which not only re-proves the Alperin–James formula in a more general context but allows us in principle to realize the representation over a minimal splitting field. Alternative methods to construct irreducible representations have been given in [12] and for the special case $H = L_2(p)$ in [3].

In Section 4 we investigate the case that the finitely presented group has an epimorphism onto $L_2(p)$ for some prime $p$. By a close analysis of the $p$-modular and the rational modules of $L_2(p)$ we can apply the results of Section 2 to arrive at a criterion which, given a finitely presented group $G$ and a prime $p$, extracts the characters of $\mathbb{Z}L_2(p)$-lattices $L$ such that $G$ is very likely to have an epimorphism onto an extension of $L$ by $L_2(p)$.

We conclude the paper with an application of our methods to the family of groups given by the presentation $\langle x, y, z | x^2, y^2, z^2, (xy)^2, (xz)^3, (yz)^7, (xyz)^n \rangle$ which is denoted by $G^{3,7,n}$ in [6]. In particular we prove:

THEOREM 1.1. *The group $G^{3,7,23}$ is infinite.*

This theorem is proved by showing that $K/K'$ has a $\mathbb{Z}H$-homomorphism to a lattice of dimension 276, where $K$ is the kernel of an epimorphism $G \twoheadrightarrow H \cong L_2(139)$.

We finally indicate that our method is often applicable and successful by giving tables for those groups $G^{3,7,n}$ where $n < 100$ is odd and $G^{3,7,n}$ has an epimorphism onto $L_2(p)$ for $p < 500$.

## 2. LIFTING HOMOMORPHISMS

DEFINITION 2.1. Let $G$ be a group, $H$ a finite group, and $\varphi\colon G \twoheadrightarrow H$ an epimorphism. A simple $FH$-module $M$ for some prime field $F$ is called *$\varphi$-extendable* if there is an exact sequence $0 \to M \to E \xrightarrow{\nu} H \to 1$ and a homomorphism $\psi\colon G \to E$ such that $\psi\nu = \varphi$ and $G\psi \ncong H$.

PROPOSITION 2.2. *Let $G$ be a group, $H$ a finite group, $\varphi: G \twoheadrightarrow H$ an epimorphism, and $M$ a simple $FH$-module $M$ for some prime field $F$. Let $K$ be the kernel of $\varphi$ and regard $M$ as an $FG$-module via $\varphi$.*

(i) *$M$ is $\varphi$-extendable if and only if* $\mathrm{Hom}_{FG}(K/K', M) \neq \{0\}$.

(ii) *If* $\dim_F H^1(G, M) > \dim_F H^1(H, M)$, *then $M$ is $\varphi$-extendable.*

(iii) *If* $H^2(H, M) = 0$, *then* $\dim_F H^1(G, M) > \dim_F H^1(H, M)$ *if and only if $M$ is $\varphi$-extendable.*

*Proof.* Part (i) is obvious.

Since $K$ acts trivially on $M$, the Lyndon–Hochschild–Serre spectral sequence yields the five-term exact sequence (cf. [17, Theorem 11.5])

$$0 \to H^1(H, M) \xrightarrow{\inf} H^1(G, M) \xrightarrow{\mathrm{res}} H^1(K, M) \to H^2(H, M).$$

This implies that $\dim_F H^1(K, M) \geq \dim_F H^1(G, M) - \dim_F H^1(H, M)$ and equality holds if $H^2(H, M) = 0$. But $H^1(K, M) \cong \mathrm{Hom}_{FG}(K/K', M)$, since $K$ acts trivially on $M$, hence (ii) and (iii) follow from (i). ∎

Consider the case $F = \mathbb{Q}$. Then clearly $H^i(H, M) = 0$ for $i \geq 1$, i.e., $MH$ is split. This is the case considered in [10]. The image of $G$ under $\psi$ is a split or non-split extension of a full $\mathbb{Z}H$-lattice $L$ in $M$ by $H$ and we conclude that $G$ is infinite. The cohomology group $H^1(G, M)$ can be computed from the presentation via derivations (in the same way as suggested in [19] for the computation of space groups), for instance using Fox derivatives (see [9, Chap. 4.2]). However, one requires the action of the generators of $H$ on $M$ explicitly. The construction of these representations will be discussed in Sections 3 and 4.

Next consider the case $F = \mathbb{F}_p$ for some prime $p$. In this case $\psi$ is necessarily an epimorphism. Usually there are other means to compute $H^i(H, M)$ in this situation, as is demonstrated for $H = L_2(p)$ in Section 4. The computation of $H^1(G, M)$ is done in the same way as for the rational number field; however, it is much easier in this case, as only linear algebra over a finite field is involved.

The rational case and the characteristic $p$ case are connected by the following trivial remark.

*Remark* 2.3. If the simple $\mathbb{Q}H$-module $M$ is $\varphi$-extendable, then for every prime $p$ there is some simple $\mathbb{F}_p H$-module which is also $\varphi$-extendable.

*Proof.* Let $L = K\psi$ be a full $\mathbb{Z}G$-lattice in $M$. Then any simple $\mathbb{F}_p H$-module in the head of $L/pL$ is $\varphi$-extendable. ∎

DEFINITION 2.4. Let $M$ be a simple $\mathbb{Q}H$-module with character $\chi$ and let $\chi = \sum_{i=1}^{s} \chi_i$ be its decomposition into absolutely irreducible characters. For a chosen prime $p$ denote by $\hat{\chi}_i$ the restriction of $\chi_i$ to the $p$-prime classes of $H$ and let $\hat{\chi}_i = \sum_j d_{ij} \beta_j$ be the decomposition into irreducible Brauer characters. The module $M$ is called a *$p$-candidate for $\varphi$* if for every $1 \le i \le s$ there exists an irreducible Brauer character $\beta_j$ such that

(i) $d_{ij} > 0$

(ii) $\beta_j$ occurs as a constituent of the Brauer character of a $\varphi$-extendable $\mathbb{F}_p H$-module.

COROLLARY 2.5. *A $\varphi$-extendable $\mathbb{Q}H$-module $M$ is a $p$-candidate for $\varphi$ for every prime $p$.*

The contraposition of Corollary 2.5 gives a strong criterion to rule out $\mathbb{Q}H$-modules to be $\varphi$-extendable. Although the converse of the corollary does certainly not hold in general, it is a good guideline to find promising candidates for $\varphi$-extendable modules. In fact, we have never encountered a $p$-candidate that is not $\varphi$-extendable (though such examples could certainly be constructed).

We therefore propose the following strategy:

- find an epimorphism $\varphi$ of $G$ onto a finite group $H$
- choose a (suitable) prime $p$
- find the $\varphi$-extendable simple $\mathbb{F}_p H$-modules
- determine the $p$-candidates for $\varphi$
- for each $p$-candidate $M$ for $\varphi$ construct the action of $H$ on $M$ and check whether $\dim_{\mathbb{Q}} H^1(G, M) > 0$.

## 3. CONSTRUCTION OF REPRESENTATIONS

In this section we describe a method to extend a representation in characteristic 0 from a subgroup $H$ to the full group $G$. The idea is to express the images of the elements in $G$ as linear combinations of the images of elements in $H$, if possible.

PROPOSITION 3.1. *Let $G$ be a finite group, $H$ a subgroup of $G$, $\chi$ a character of $G$, and $\Delta\colon H \to GL_n(K)$ a representation of $H$ with character $\chi_{|H}$, where $K$ is a field of characteristic 0. Assume that $(\chi, \chi)_G = (\chi_{|H}, \chi_{|H})_H$. Then the following holds*:

(i) *There exists a unique representation $\Gamma\colon G \to GL_n(L)$ with character $\chi$ such that $\Gamma_{|H} = \Delta$, where $L = K(\chi(g) | g \in G)$.*

(ii) *Let* $(b_1, \ldots, b_s)$ *be a basis of* $\Delta(KH)$ *and* $(b_1^*, \ldots, b_s^*)$ *the dual basis with respect to the trace bilinear form induced from* $K^{n\times n}$ *on* $\Delta(KH)$, *i.e.,* $Tr(b_i b_j^*) = \delta_{ij}$. *For* $g \in G$ *one has*

$$\Gamma(g) = \sum_{i=1}^{s} \chi(gb_i) b_i^*,$$

*where by slight abuse of notation the linear extension of* $\chi$ *to* $KG$ *is again denoted by* $\chi$.

*Proof.* Let $\overline{K}$ be the algebraic closure of $K$. Clearly $\Delta$ has some extension $\Gamma$ to $G$ over $\overline{K}$ with character $\chi$. For every $g \in G$ we have $\mathrm{Tr}(\Gamma(g)\Delta(h)) = \mathrm{Tr}(\Gamma(gh)) = \chi(gh)$ for all $h \in H$. But by the assumption on the norms of $\chi$ and $\chi_{|H}$ we have $\Gamma(\overline{K}G) = \overline{K} \otimes_K \Delta(KH)$. Hence, $\Gamma(g)$ has to be as given in part (ii) of the claim. Moreover, the formula for $\Gamma(g)$ shows that $\Gamma$ can be realized over $K(\chi(g) | g \in G)$. ∎

*Remark* 3.2. A slight generalization of the above may sometimes be useful. Let $\pi$ be a permutation of the elements of $\Delta(H)$ inducing a vector space automorphism on $\Delta(KH)$ also denoted by $\pi$ (for instance $x^\pi = x^{-1}$ for $x \in \Delta(H)$). Define a bilinear form $\Phi$ on $\Delta(KH)$ by $\Phi(X, Y) := \mathrm{Tr}(XY^\pi)$ for $X, Y \in \Delta(KH)$. Then in Proposition 3.1 the dual basis with respect to $\Phi$ can be considered, i.e., $\Phi(b_i, b_j^*) = \delta_{ij}$, since $\Phi$ is non-degenerate. This yields the following formula for $\Gamma(g)$:

$$\Gamma(g) = \sum_{i=1}^{s} \chi(gb_i^\pi) b_i^*.$$

The following example shows that Proposition 3.1 generalizes the main result in [2].

EXAMPLE 3.3. Let $G$ be a finite group and $H$ a subgroup of $G$. Let $\chi$ be an irreducible character of $G$ such that $\chi_{|H}$ is an irreducible monomial character of $H$, i.e., $\chi_{|H}$ is induced from a linear character $\vartheta$ of a subgroup $U$ of $H$. Let $\Delta$ be a representation of $H$ with character $\chi_{|H}$.

Define $e_{11} := \Delta(1/|U| \sum_{u \in U} \vartheta(u^{-1})u)$ to be the image in $\Delta(KH)$ of the central primitive idempotent corresponding to $\vartheta$. Let $h_1, \ldots, h_n$ be a transversal of $U$ in $H$.

Then $e_{ij} := \Delta(h_i e_{11} h_j^{-1})$, $1 \le i, j \le n$ form a basis of $\Delta(KH)$ and we have $e_{ij}^* = e_{ji}$. Proposition 3.1 now yields

$$\Gamma(g) = \sum_{i,j} \chi(ge_{ij}) e_{ji} = \sum_{i,j} 1/|U| \sum_{u \in U} \vartheta(u^{-1}) \chi(gu) e_{ji}$$

which is exactly the formula given in [2].

Note that this construction of $\Gamma$ requires the character values of $\vartheta$ as coefficients, which may lie in a much larger field than required to realize the character $\chi$. This can be avoided by choosing a suitable basis of $\Delta(K'H)$, where $K'$ is a subfield of $K$ over which $\chi_{|H}$ can be realized.

A different approach has recently been suggested in [12], where for irreducible $\chi$ and $\chi_{|H}$ the formula

$$\Gamma(g) = \frac{\chi(1)}{|H|} \sum_{h \in H} \chi(h^{-1}g)\Delta(h)$$

is proved, which allows us to construct $\Gamma$ over $K(\chi(g)|g \in G)$ as does Proposition 3.1.

The second example shows how the irreducible representations of degree $p-1$ of $L_2(p)$ can be constructed. An alternative construction for this situation is given in [3].

EXAMPLE 3.4. Let $\chi$ be an irreducible character of $L_2(p)$ with $\chi(1) = p-1$; then $\chi$ can be extended to an irreducible character of $PGL_2(p)$ which we again denote by $\chi$. The restriction of $\chi$ to the image $H$ of a Borel subgroup of $GL_2(p)$ is absolutely irreducible. Note that $H \cong C_p \rtimes C_{p-1}$ has a unique faithful irreducible character, hence any of the characters of degree $p-1$ must restrict to this character.

Now let $a$ be an element of order $p-1$ in $H$ and $b$ an element of order $p$. Then $A = \Delta(a)$ may be chosen as a permutation matrix and $B = \Delta(b)$ as the companion matrix of the $p$th cyclotomic polynomial. Moreover, the elements $A^iB^j$ with $0 \le i, j < p-1$ form a $\mathbb{Q}$-basis of $\Delta(\mathbb{Q}H)$. Define a bilinear form $\Phi$ on $\Delta(\mathbb{Q}H)$ by $\Phi(\Delta(h_1), \Delta(h_2)) := \mathrm{Tr}(\Delta(h_1)\Delta(h_2)^{-1})$ for $h_1, h_2 \in H$ as suggested in Remark 3.2. Evaluating this bilinear form on the basis yields

$$\Phi(A^iB^i, A^kB^l) = \mathrm{Tr}(A^iB^{j-l}A^{-k}) = \delta_{ik} * \big((-1) + \delta_{jl} * p\big)$$

since for $i \neq k$ the element $A^iB^{j-l}A^{-k}$ is non-trivial of order $\neq p$ and therefore has trace 0. Choosing the ordering of the basis such that $A^iB^j$ has position $(p-1)*i + j + 1$ in the basis, the Gram matrix for $\Phi$ is a block diagonal matrix with each block equal to $p * I_{p-1} - J_{p-1}$, where $I_{p-1}$ is the identity matrix of size $p-1$ and $J_{p-1}$ the matrix with all entries 1. The inverse of this matrix is $1/p * (I_{p-1} + J_{p-1})$. Since $\sum_{j=0}^{p-1} B^j = 0$ one has $\sum_{j=0}^{p-2} B^j = -B^{-1}$, hence the element of the dual basis corresponding to $A^iB^j$ is $1/p * A^i(B^j - B^{-1})$. To identify in which conjugacy class an arbitrary element $g$ of $PGL_2(p)$ lies it is enough to look at

the trace and determinant of a preimage of $g$ in $GL_2(p)$. The only classes which cannot be separated by the traces and determinants of their preimages are the class containing the identity and the class containing the elements of order $p$ which, however, are easy to distinguish.

## 4. MODULES OF $L_2(p)$

We first look at the simple modules of $L_2(p)$ in characteristic $p$. The simple $\mathbb{F}_p L_2(p)$-module $V_n$ of dimension $n$ can be obtained from the action of $SL_2(p)$ on the homogeneous polynomials of degree $n-1$ in two variables for odd $n \le p$. The cohomology groups $H^i(L_2(p), V_n)$ for $i = 1, 2$ can be read off the Brauer tree (see below) of $L_2(p)$ using dimension shifting. As an extension of [15, Lemma 3.4] we obtain:

LEMMA 4.1. *Let $H := L_2(p)$ with $p > 3$ prime and denote by $V_n$ the simple $\mathbb{F}_p H$-module of dimension $n$.*

$$\text{(i)} \quad \dim_{\mathbb{F}_p} H^1(H, V_n) = \begin{cases} 1 & \text{if } n = p-2 \\ 0 & \text{otherwise.} \end{cases}$$

$$\text{(ii)} \quad \dim_{\mathbb{F}_p} H^2(H, V_n) = \begin{cases} 1 & \text{if } n = 3 \\ 0 & \text{otherwise.} \end{cases}$$

We now turn to the situation in characteristic 0. The Frobenius characters of $L_2(p)$ are characterized by their degrees and values on fixed elements $x$ and $y$ of orders $(p-1)/2$ and $(p+1)/2$, respectively.

We first obtain characters of degree $p+1$ by inducing the linear characters of the Borel subgroup of $SL_2(p)$ having the center in their kernel. Let $\rho$ be a primitive $(p-1)$st root of unity. Then we obtain characters $\psi_i$ for $0 \le i \le (p-1)/2$ and $i$ even with $\psi_i(x) = 0$ and $\psi_i(y) = \rho^i + \rho^{-i}$.

We next define characters of degree $p-1$ belonging to the non-split torus in $SL_2(p)$. Let $\sigma$ be a primitive $(p+1)$st root of unity. Then we obtain characters $\theta_i$ for $1 \le i \le (p+1)/2$ and $i$ even with $\theta_i(x) = -(\sigma^i + \sigma^{-i})$ and $\theta_i(y) = 0$.

Now the absolutely irreducible characters of $L_2(p)$ are the following (cf. [18]): 1; $\pi := \psi_0 - 1$; $\theta_i$, $1 \le i \le (p-1)/2$, $i$ even; $\psi_i$, $1 \le i \le (p-3)/2$, $i$ even; a pair $\chi, \chi'$ of algebraic conjugate characters of degree $(p+\varepsilon)/2$, where $\varepsilon = \pm 1$ and $\varepsilon \equiv p \bmod 4$ such that $\chi + \chi' = \theta_{(p+1)/2}$ if $\varepsilon = -1$ and $\chi + \chi' = \psi_{(p-1)/2}$ if $\varepsilon = 1$.

PROPOSITION 4.2. *Let $H := L_2(p)$ for a prime $p > 3$. Let $M$ be a simple $\mathbb{Q}H$-module, $L$ a full $\mathbb{Z}H$-lattice in $M$, and $L_p := \mathbb{Z}_p \otimes L$ where $\mathbb{Z}_p$ denotes the ring of p-adic integers.*

(i) *The character of $H$ on $M$ is either of*:
$1, \pi, \theta_{(p+1)/2}$ *if* $p \equiv -1 \bmod 4$, $\psi_{(p-1)/2}$ *if* $p \equiv 1 \bmod 4$,
$\Theta_i := \sum_{(j, p+1)=i} \theta_j$, *where $i$ is an even divisor of $p+1$ and* $1 \le i \le (p-1)/2$,
$\Psi_i := \sum_{(j, p-1)=i} \psi_j$, *where $i$ is an even divisor of $p-1$ and* $1 \le i \le (p-3)/2$.

(ii) *$L_p$ is isomorphic to a direct sum of irreducible $\mathbb{Z}_p H$-lattices each of which is uniserial.*

(iii) *$L/pL$ is a direct sum of indecomposable $\mathbb{F}_p H$-modules, which are determined by the simple components of $L_p/\mathrm{rad}(L_p)$.*

*Proof.*

(i) This is clear, since the $\Theta_i$ and $\Psi_i$ are the sums over the Galois orbits of the $\theta_i$ and $\psi_i$, respectively.

(ii) The Schur indices of all characters are 1, hence every absolutely irreducible representation of $H$ can be realized over its character field.

For the characters of degree $p+1$ the character field is generated by $\rho + \rho^{-1}$ where $\rho$ is a root of unity of order dividing $p-1$. As $\mathbb{Q}_p$ contains these roots of unity it is a splitting field for the characters of degree $p+1$.

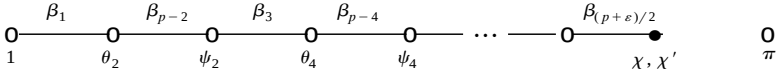
The character field for the characters of degree $p-1$ is generated by $\sigma + \sigma^{-1}$ where $\sigma$ is a root of unity of order dividing $p+1$. The unramified quadratic extension of $\mathbb{Q}_p$ contains the $(p+1)$st roots of unity and the Frobenius automorphism maps a $(p+1)$st root of unity to its inverse, hence $\mathbb{Q}_p$ is also a splitting field for the characters of degree $p-1$.

Finally, the splitting field for the characters of degree $(p \pm 1)/2$ is a ramified extension of degree 2 of $\mathbb{Q}_p$, hence the character $\chi + \chi'$ is irreducible over $\mathbb{Q}_p$. Over a splitting field, $M$ is a direct sum of absolutely irreducible modules of the same degree, hence the irreducible constituents have no common composition factors modulo $p$. It follows from [14, Theorem I.1] that $L$ is a direct sum.

Since the irreducible characters are of defect 1 (with the exception of $\pi$, which is of defect 0), [4, Theorem 11] implies that the irreducible $\mathbb{Z}_p H$-lattices are uniserial.

(iii) $L_p/\mathrm{rad}(L_p)$ is the direct sum of the simple modules in the head of the indecomposable modules in $L/pL$. ∎

We will now derive an explicit criterion, which, given an epimorphism $\varphi\colon G \twoheadrightarrow L_2(p)$ and the $\varphi$-extendable $\mathbb{F}_p L_2(p)$-modules, determines the simple $\mathbb{Q}L_2(p)$-modules which are $p$-candidates for $\varphi$ (Definition 2.4). The main ingredients are the above analysis of the rational $L_2(p)$-modules and the Brauer tree for $L_2(p)$ which looks as follows (cf. [1]; see [13, p. 22] for the identification of the Frobenius characters)




where $\varepsilon = \pm 1$ with $p \equiv \varepsilon \bmod 4$ and the exceptional vertex has multiplicity 2.

From the Brauer tree we see that the restriction of $\theta_i$ to the $p'$-classes decomposes as $\beta_{i-1} + \beta_{p-i}$ and that the restriction of $\psi_i$ decomposes as $\beta_{i+1} + \beta_{p-i}$. This leads to the following criterion for the simple $\mathbb{Q}L_2(p)$-modules to be $p$-candidates for $\varphi$.

COROLLARY 4.3. *The simple $\mathbb{Q}L_2(p)$-module with character $\chi$ is a $p$-candidate for $\varphi$ if and only if one of the following holds*:

(i) *$\chi$ is the trivial character and $V_1$ is $\varphi$-extendable*

(ii) *$\chi = \pi$ and $V_p$ is $\varphi$-extendable*

(iii) *$p \equiv -1 \bmod 4$, $\chi = \theta_{(p+1)/2}$, and $V_{(p-1)/2}$ is $\varphi$-extendable*

(iv) *$p \equiv 1 \bmod 4$, $\chi = \psi_{(p-1)/2}$, and $V_{(p+1)/2}$ is $\varphi$-extendable*

(v) *$\chi = \Theta_i$ and for every $j \le (p-1)/2$ with $(j, p-1) = i$ one of $V_{j-1}, V_{p-j}$ is $\varphi$-extendable*

(vi) *$\chi = \Psi_i$ and for every $j \le (p-3)/2$ with $(j, p-1) = i$ one of $V_{j+1}, V_{p-j}$ is $\varphi$-extendable*.

## 5. THE GROUPS $G^{3,7,n}$

In this section we apply the methods developed in the preceding sections to some groups of the family $G^{3,7,n}$ which is given by the presentation (cf. [6])

$$\left\langle x, y, z \mid x^2, y^2, z^2, (xy)^2, (xz)^3, (yz)^7, (xyz)^n \right\rangle.$$

We first deal with the case $n = 23$ in detail and prove Theorem 1.1.

Let $G := G^{3,7,23}$. By the methods described in [15] one easily checks that $G$ has an epimorphism onto $L_2(139)$ and that 139 is the only such prime. The epimorphism $\varphi$ can be given by

$$x \mapsto \pm\begin{pmatrix} 50 & 1 \\ 1 & 89 \end{pmatrix}, \qquad y \mapsto \pm\begin{pmatrix} 0 & 1 \\ 138 & 0 \end{pmatrix}, \qquad z \mapsto \pm\begin{pmatrix} 17 & 120 \\ 125 & 122 \end{pmatrix}.$$

Application of Proposition 2.2 and Lemma 4.1 to the simple $\mathbb{F}_{139}L_2(139)$-modules shows that the only $\varphi$-extendable modules are those of dimensions 41 and 125. It then follows from Corollary 4.3 that $\Theta_{14} = \theta_{14} + \theta_{42}$ is the only $p$-candidate for $\varphi$, hence no other $\mathbb{Q}L_2(139)$-module can be $\varphi$-extendable.

The representation of $L_2(139)$ on the module with character $\theta_{14}$ is constructed over $\mathbb{Q}(\zeta_{20} + \zeta_{20}^{-1})$ as described in Example 3.4. A good test for the assumption that this module is $\varphi$-extendable is to choose a prime $p$ not dividing the order of $L_2(139)$ such that the character $\theta_{14}$ can be realized over $\mathbb{F}_p$. Choosing $p = 41$ we find that the corresponding $\mathbb{F}_{41}$-module is in fact $\varphi$-extendable.

The next step is to set up the system of linear equations the solutions of which are the cocycles. Since the elements $y$ and $z$ generate a dihedral group of order 14 the cocycles may be chosen to be trivial on these two generators which gives a system of equations of size $138 \times 4 * 138$. Moreover, one easily computes from the character values that the fixed space of the group generated by the images of $y$ and $z$ has dimension 10, hence the space of coboundaries being trivial on $y$ and $z$ has dimension at most 10. The calculations over $\mathbb{F}_{41}$ prove that it has dimension exactly 10.

Unfortunately, there is no direct way of finding the dimension of the space of cocycles by going through a Gaussian elimination on the system of equations over the algebraic number field, since the size of the entries explodes already in the first few steps. We therefore replace $\zeta_{20} + \zeta_{20}^{-1}$ by its companion matrix, thus obtaining a rational system of equations of size $552 \times 2208$, which should have a space of solutions of dimension 44. Applying the modified LLL-algorithm (cf. [16]) to the lattice generated by the rows of this matrix we find that its rank is at most 508, hence by the modular computation over $\mathbb{F}_{41}$ it has exactly rank 508, which proves the existence of a non-trivial cocycle.

*Remark* 5.1. Although we are interested in $L_2(p)$-modules over $\mathbb{Q}$ it is convenient to work with representations over algebraic number fields. An obvious reason is that we try to keep the degrees of the representations as small as possible, but the crucial point is that we have to satisfy the assumptions of Proposition 3.1. Looking for instance at the characters $\Theta_i$ of $L_2(p)$, let $d$ be the degree of the character field of $\theta_i$ over $\mathbb{Q}$. As

described in Example 3.4 we regarded $\theta_i$ as a character of $PGL_2(p)$ and its restriction to the projective Borel subgroup $B$. Since all algebraic conjugates of $\theta_i$ restrict to the same (rational) character of $B$, we have $(\Theta_i,\Theta_i) = d$ and $(\Theta_{i|B}, \Theta_{i|B})_{|B} = d^2$. This shows that in this case we have to construct the representation with character $\theta_i$ over a field containing the character field.

In general, we obtain a rational module from a representation $\Delta$ of $H$ over an algebraic number field $F$ by replacing a generator of $F$ by its companion matrix in the entries of $\Delta$. If $\Delta$ is absolutely irreducible, the resulting $\mathbb{Q}H$-module is the $d$-fold direct sum of isomorphic simple $\mathbb{Q}H$-modules, where $d$ is the degree of $F$ over a minimal splitting field for $\Delta$. In particular, the $\mathbb{Q}H$-module is simple if and only if $F$ is a minimal splitting field.

One idea to simplify the problem of finding the dimension of the space of cocycles would be to perform a Galois descent before blowing up the system of equations to a rational matrix, since the constructed representation is written over an extension of degree 2 of its character field $\mathbb{Q}(\sqrt{5})$. It is not difficult to find a matrix $X$ such that for the Galois automorphism $\sigma$ of $\mathbb{Q}(\zeta_{20} + \zeta_{20}^{-1})$ fixing $\sqrt{5}$ one has $g^\sigma = XgX^{-1}$ for every $g$ in the representation of $L_2(139)$, since $X$ has to lie in the centralizer of the Borel subgroup in $L_2(139)$, which is isomorphic to $\mathbb{Q}(\sqrt{-139})$. However, for the Galois descent one has the additional condition $XX^\sigma = 1$, which is a relative norm equation. In this example the coefficients in this norm equation are of magnitude $10^7$, which makes it impossible to find a solution by the existing algorithmic methods.

The Galois descent can be performed in a different way once the cohomology computation has been completed. For this choose a non-trivial 1-cocycle $\delta$ from $G$ into the $\mathbb{Q}L_2(139)$-module $M$ with character $2\Theta_{14}$ and let $\psi$ be the homomorphism of $G$ into the extension of $M$ by $L_2(139)$ defined by $\delta$. Add relators $w_i$ to the given presentation of $G$ to obtain a presentation of $L_2(139)$. Now evaluating the relators $w_i$ on the images of the generators of $G$ under $\psi$ gives elements in $M$ which cannot all be zero. Each nonzero element obtained this way can be spun to a $\mathbb{Q}L_2(139)$-module with character $\Theta_{14}$. Viewing this module over its endomorphism field yields the desired Galois descent and gives a representation over the minimal splitting field.

We conclude this paper by illustrating that our method can also be successfully applied to other groups of the family $G^{3,7,n}$.

For $n = 2m$ the group $G^{3,7,2m}$ contains the group $(2, 3, 7; m)$ given by the presentation $\langle x, y | x^2, y^3, (xy)^7, [x, y]^m \rangle$ as a subgroup of index 2 (a quotient of the abstract triangle group $\Delta(2, 3, 7)$). These groups are well

understood and known to be finite for $m \leq 8$ and to be infinite for $m \geq 9$ (see [10, 11]). An interesting case is the group $(2, 3, 7; 84)$ which in [5] is proved to have the alternating and symmetric groups $A_n$ and $S_n$ as epimorphic images for all but finitely many values of $n$. It is not known whether $m = 84$ is the smallest value with this property.

The groups $G^{3,7,n}$ with odd $n$ are finite for $n \leq 17$. In [7] it is shown that $G^{3,7,27}$ is infinite and the same method (looking at the abelianization of subgroups of low index) proves infiniteness for the cases $n = 39, 49, 81, 91, 95$. It is stated in [8] that $G^{3,7,19}$ maps onto $J_1$ and $L_2(113)$ and that the group is likely to be infinite, but to the authors' knowledge this is still an open problem. Very little seems to be known about these groups for higher values of $n$.

Table I shows for $n$ odd and $19 \leq n < 100$ the primes $p$ such that $G^{3,7,n}$ has an epimorphism onto $L_2(p)$.

Table II gives for the pairs $(n, p)$ with $p < 500$ the $\varphi$-extendable $\mathbb{F}_p L_2(p)$-modules (denoted by their degrees) and the characters for $\varphi$-extendable $\mathbb{Q}L_2(p)$-modules. In all cases the $p$-candidates for $\varphi$ are in fact $\varphi$-extendable. The pairs $(n, p) = (19, 113)$, $(21, 43)$, $(39, 13)$, $(45, 29)$, $(57, 113)$, $(63, 43)$, $(65, 13)$, $(75, 29)$, $(91, 13)$, $(95, 113)$ are omitted, since no $\varphi$-extendable $\mathbb{F}_p L_2(p)$-module exists. Combining these results with the cases $n = 27, 39, 49, 81, 91, 95$ covered by the method of [7] we get the following:

COROLLARY 5.2. *The groups $G^{3,7,n}$ are infinite for* $n = 23, 27, 35, 39, 41, 45, 49, 53, 63, 69, 73, 77, 81, 91, 95$.

TABLE I

| $n$ | $p$ | $n$ | $p$ | $n$ | $p$ | $n$ | $p$ |
|---|---|---|---|---|---|---|---|
| 19 | 113 | | | | | | |
| 21 | 43 | 41 | 83 | 61 | 161407 | 81 | 5132161 |
| 23 | 139 | 43 | 8513 | 63 | 43, 127 | 83 | 1163, 564899 |
| 25 | 449 | 45 | 29, 181 | 65 | 13, 20411 | 85 | 2549, 75991 |
| 27 | — | 47 | 45121 | 67 | 10120753 | 87 | 1217, 189139 |
| 29 | 1217 | 49 | 97, 197 | 69 | 139, 126547 | 89 | 10501, 217517 |
| 31 | 743 | 51 | 29989 | 71 | 2639071 | 91 | 13, 181, 4733 |
| 33 | 727 | 53 | 211, 1483 | 73 | 293, 235789 | 93 | 743, 7253 |
| 35 | 71 | 55 | 216481 | 75 | 29, 449, 1499 | 95 | 113, 520981 |
| 37 | 1553 | 57 | 113, 7069 | 77 | 307, 461, 617 | 97 | 1163, 7732451 |
| 39 | 13, 701 | 59 | 797917 | 79 | 233968769 | 99 | 727, 2723687 |

TABLE II

| $n$ | $p$ | Brauer characters | Rational characters |
|---|---|---|---|
| 23 | 139 | 41, 125 | $\Theta_{14}$ |
| 25 | 449 | 41 | — |
| 35 | 71 | 41, 53, 65 | $\Theta_6, \Theta_{18}$ |
| 41 | 83 | 41, 53, 65, 69, 77 | $\theta_{42}, \Theta_6, \Theta_{14}$ |
| 45 | 181 | 41, 53, 65, 69, 77, 81, 83, 89, 125, 137, 149, 153, 161, 165, 167, 173, 177 | $\Theta_{14}, \Psi_4, \Psi_{20}$ |
| 49 | 97 | 41, 53, 65, 69, 77, 81, 83, 89, 93, 97 | $\pi, \Theta_{14}, \Psi_4, \Psi_8, \Psi_{16}, \Psi_{32}$ |
| 49 | 197 | 41, 53, 65, 69, 77, 81, 83, 89, 93–97, 125, 137, 149, 153, 161, 165, 167, 173, 177–181, 185, 189–193 | $\Theta_6, \Theta_{18}, \Theta_{66}, \Psi_4$ |
| 53 | 211 | 41, 53, 65, 69, 77, 81, 83, 89, 93–97, 101, 105, 125, 137, 149, 153, 161, 165, 167, 173, 177–181, 185, 189–197, 201–211 | $\pi, \theta_{106}, \Theta_2, \Psi_2, \Psi_{10}$ |
| 63 | 127 | 41, 53, 65, 69, 71, 77, 81, 83, 89, 93–101, 105–113, 117–125 | $\Theta_2, \Theta_{32}, \Psi_2, \Psi_{14}$ |
| 69 | 139 | 41, 125 | $\Theta_{14}$ |
| 73 | 293 | 41, 53, 65, 69, 77, 81, 83, 89, 93–97, 101, 105–113, 117–125, 129–145, 149, 153, 161, 165, 167, 173, 177–181, 185, 189–197, 201–209, 213–293 | $2\pi, \Theta_2, \Theta_6, 2\Theta_{14}, 3\Theta_{42}, 2\Theta_{98}, \Psi_2, 2\Psi_4$ |
| 75 | 449 | 41 | — |
| 77 | 307 | 41, 53, 65, 69, 77, 81, 83, 89, 93–97, 101, 105–113, 117–125, 129–153, 159, 161, 165, 167, 173, 177–181, 185, 189–197, 201–209, 213–307 | $2\pi, 2\theta_{154}, 2\Theta_2, \Theta_4, 3\Theta_{14}, 2\Theta_{22}, 2\Theta_{28}, \Theta_{44}, 2\Psi_2, \Psi_6, \Psi_{18}, 2\Psi_{34}, \Psi_{102}$ |
| 77 | 461 | 41, 53, 65, 69, 77, 81, 83, 89, 93–97, 101, 105–113, 117–125, 129–153, 161, 165, 167, 173, 177–181, 185, 189–197, 201–209, 213–461 | $4\pi, \psi_{230}, 2\Theta_2, 3\Theta_6, 3\Theta_{14}, 2\Theta_{22}, 4\Theta_{42}, 3\Theta_{66}, 4\Theta_{154}, 2\Psi_2, 3\Psi_4, 2\Psi_{10}, 3\Psi_{20}, 2\Psi_{46}, 3\Psi_{92}$ |
| 91 | 181 | 41, 53, 65, 69, 77, 81, 83, 89, 93–97, 101, 105–113, 117–125, 129–181 | $2\pi, 2\Theta_{14}, \Theta_{26}, 2\Psi_4, \Psi_{10}, \Psi_{12}, 2\Psi_{20}, \Psi_{30}, \Psi_{36}, \Psi_{60}$ |

## ACKNOWLEDGMENTS

We thank D. F. Holt for pointing out the infiniteness problem of $G^{3,7,23}$ to us and J. Cannon, M. Conder, G. Hiss, G. Nebe, R. M. Thomas, R. van der Waal, and the unknown referee for helpful references.

## REFERENCES

1. J. L. Alperin, ''Local Representation Theory,'' Cambridge Univ. Press, Cambridge, 1986.
2. J. L. Alperin and G. D. James, Bessel functions on finite groups, *J. Algebra* **171** (1995), 524–530.

3. S. Böge, Realisierung $(p-1)$-dimensionaler Darstellungen von $PSL(2, p)$, *Arch. Math.* **60** (1993), 121–127.
4. R. Brauer, Investigations on group characters, *Ann. of Math.* **42** (1941), 936–958.
5. M. Conder, A question by Graham Higman concerning quotients of the $(2, 3, 7)$ triangle group, *J. Algebra* **141** (1991), 275–286.
6. H. S. M. Coxeter, The abstract groups $G^{m,n,p}$, *Trans. Amer. Math. Soc.* **45** (1939), 73–150.
7. L. C. Grove and J. M. McShane, On Coxeter's groups $G^{p,q,r}$, *in* "Groups St. Andrews, 1989," (C. M. Campbell and E. F. Robertson, Eds.), Vol. 1, pp. 211–213, Cambridge Univ. Press, Cambridge, 1991.
8. G. Higman, Construction of simple groups from character tables, *in* "Finite Simple Groups," (M. P. Powell and G. Higman, Eds.), pp. 205–214, Academic Press, London, 1971.
9. D. F. Holt and W. Plesken, "Perfect Groups," Oxford Univ. Press, Oxford, 1989.
10. D. F. Holt and W. Plesken, A cohomological criterion for a finitely presented group to be infinite, *J. London Math. Soc.* (2) **45** (1992), 469–480.
11. J. Howie and R. M. Thomas, The groups $(2, 3, p; q)$; asphericity and a conjecture of Coxeter, *J. Algebra* **154** (1993), 289–309.
12. T. Minkwitz, Extensions of irreducible representations, *Appl. Algebra Engrg. Comm. Comput.* **7** (1996), 391–399.
13. G. Nebe and W. Plesken, Finite rational matrix groups, Mem. *Amer. Math. Soc.* **116,** No. 556 (1995).
14. W.Plesken, On reducible and decomposable representations of orders, *J. Reine Angew. Math.* **297** (1978), 188–210.
15. W. Plesken and B. Souvignier, Analyzing finitely presented groups by constructing representations, *J. Symbolic Comput.* **24**, Nos. 3–4 (1997), 335–350.
16. M. Pohst, A modification of the LLL-algorithm, *J. Symbolic Comput.* **4** (1987), 123–128.
17. J. J. Rotman, "An Introduction to Homological Algebra," Academic Press, New York, 1979.
18. I. Schur, Untersuchungen über die Darstellung der endlichen Gruppen durch gebrochene Substitutionen, *J. Reine Angew. Math.* **132** (1907), 85–137.
19. H. Zassenhaus, Über einen Algorithmus zur Bestimmung der Raumgruppen, *Comment. Math. Helv.* **21** (1948), 117–141.