Journal of Algebra 322 (2009) 94–107

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Compression of finite group actions and covariant dimension, II ☆

Hanspeter Kraft [a,*], Roland Lötscher [a], Gerald W. Schwarz [b]

[a] *Mathematisches Institut der Universität Basel, Rheinsprung 21, CH-4051 Basel, Switzerland*
[b] *Department of Mathematics, Brandeis University, PO Box 549110, Waltham, MA 02454-9110, USA*

ARTICLE INFO

Article history:
Received 13 July 2008
Available online 31 March 2009
Communicated by Peter Littelmann

Keywords:
Essential dimension
Covariant dimension
Finite group actions
Faithful groups
Multihomogeneous covariants

ABSTRACT

Let G be a finite group and $\varphi : V \to W$ an equivariant polynomial map between finite dimensional G-modules. We say that φ is faithful if G acts faithfully on $\varphi(V)$. The covariant dimension of G is the minimum of the dimension of $\overline{\varphi(V)}$ taken over all faithful φ. In [Hanspeter Kraft, Gerald W. Schwarz, Compression of finite group actions and covariant dimension, J. Algebra 313 (1) (2007) 268–291] we investigated covariant dimension and were able to determine it in many cases. Our techniques largely depended upon finding homogeneous faithful covariants. After publication of the paper, the junior author of this article pointed out several gaps in our proofs. Fortunately, this inspired us to find better techniques, involving multihomogeneous covariants, which have enabled us to extend and complete the results, simplify the proofs and fill the gaps of our previous work.

☆ The first two authors are partially supported by the Swiss National Science Foundation (Schweizerischer Nationalfonds), and the third author by NSA Grant H98230-06-1-0023.

* Corresponding author.
E-mail addresses: hanspeter.kraft@unibas.ch (H. Kraft), roland.loetscher@unibas.ch (R. Lötscher), schwarz@brandeis.edu (G.W. Schwarz).

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2009.01.039

1. Introduction

For simplicity we take our ground field to be the field $\mathbb{C}$ of complex numbers. Much work has been done in the context of more general fields (see, for example, [Flo08,JLY02,Led07,KM08]). In [Löt08] our results are extended to this context. (See the remarks at the end of this section.)

Let G be a finite group. All G-modules that we consider will be finite dimensional. A *covariant* of G is an equivariant morphism (= polynomial map) $\varphi : V \to W$ where V and W are G-modules. The *dimension* of φ is defined to be the dimension of the image of φ:

$$\dim \varphi := \dim \overline{\varphi(V)}.$$

The covariant φ is *faithful* if the group G acts faithfully on the image $\varphi(V)$. Equivalently, there is a point $w \in \varphi(V)$ with trivial isotropy group G_w. The *covariant dimension* $\operatorname{covdim} G$ of G is defined to be the minimum of $\dim \varphi$ where $\varphi : V \to W$ runs over all faithful covariants of G. If $\dim \varphi = \operatorname{covdim} G$ we say that φ is a *minimal covariant*. In [KS07, Proposition 2.1] we show that there is a minimal covariant $\varphi : V \to W$ if V and W are faithful. In particular, if V is a faithful G-module, then there is a minimal faithful covariant $\varphi : V \to V$.

Suppose that $\varphi : V \to W$ is a *rational map* which is G-equivariant. We call φ a *rational covariant*. Then one can define the notion of φ being faithful and the dimension of φ as in the case of ordinary covariants. The *essential dimension* $\operatorname{edim} G$ of G is the minimum dimension of all its faithful rational covariants. It is easy to see that

$$\operatorname{edim} G \leqslant \operatorname{covdim} G \leqslant \operatorname{edim} G + 1$$

(see [Rei04] or the proof of Theorem 2.6 below).

Our results in [KS07] were largely based upon finding homogeneous minimal covariants. Unfortunately, this is not always possible [KS07, Remark 4.1]. In this paper, however, we are able to show that there are always *multihomogeneous* minimal covariants. This allows us to improve upon the results of [KS07]. In particular, we are able to obtain the exact relation between covariant and essential dimension (Theorem 3.1):

$$\operatorname{covdim} G = \begin{cases} \operatorname{edim} G + 1 & \text{if the center of } G \text{ is trivial,} \\ \operatorname{edim} G & \text{otherwise.} \end{cases}$$

In certain cases we are able to describe the image of a covariant (Proposition 4.1) and deduce that for a *faithful* group G (i.e., G admits an irreducible faithful module) we have $\operatorname{covdim}(G \times \mathbb{Z}/p\mathbb{Z}) = \operatorname{covdim} G + 1$ if and only if the prime p divides the order $|Z(G)|$ of the center of G. This completes the analysis of [KS07, §5–6]. In the process we repair the proofs of Corollaries 6.1 and 6.2 of [KS07]. They are supposed to be corollaries of Proposition 6.1, but the hypotheses of the proposition are not fulfilled. In Section 5 we give some examples of covariant dimensions of groups, in part generalizing [KS07, Proposition 6.2]. In Sections 6 and 7 we repair two proofs, one concerning a characterization of faithful groups and their subgroups, and one about the classification of non-faithful groups of covariant dimension 2. In Section 8 we list some minor errata from [KS07].

In the case of a general field k, our considerations must be limited to groups admitting a completely reducible faithful k-representation. We also need k to contain a primitive root of unity of order equal to the exponent of $Z(G)$ for every group G appearing in our arguments. In [Löt08] this last restriction can sometimes be avoided. If k is finite, some arguments do not go through since there may exist no k-rational points with trivial stabilizer in the image of a faithful covariant.

2. Multihomogeneous covariants

Let $V = \bigoplus_{i=1}^{n} V_i$ and $W = \bigoplus_{j=1}^{m} W_j$ be direct sums of vector spaces and let $\varphi = (\varphi_1, \ldots, \varphi_m): V \to W$ be a morphism where none of the φ_j are zero. We say that φ is *multihomogeneous of degree* $A = (\alpha_{ji}) \in M_{m\times n}(\mathbb{Z})$ if, for an indeterminate s, we have

$$\varphi_j(v_1, \ldots, sv_i, \ldots, v_n) = s^{\alpha_{ji}} \varphi_j(v_1, \ldots, v_n) \quad \text{for all } j = 1, \ldots, m, \; i = 1, \ldots, n.$$

Whenever we consider the degree matrix A of some φ, we are always tacitly assuming that $\varphi_j \neq 0$ for all j.

We now give a way to pass from a general φ to the multihomogeneous case. For indeterminates $s_1, \ldots, s_n$, we have $\varphi_j(s_1 v_1, \ldots, s_n v_n) = \sum_\alpha \varphi_j^{(\alpha)} s^\alpha$ for each j, where $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ and $s^\alpha = s_1^{\alpha_1} \cdots s_n^{\alpha_n}$. If $\beta \in \mathbb{R}^n$, let $\alpha \cdot \beta$ denote the usual inner product. Now suppose for illustration that $m = 1$ and $\dim W_1 = \dim V_i = 1$, $i = 1, \ldots, n$. Then $\varphi = \varphi_1$ is just a polynomial in n variables. If the entries of β are linearly independent over $\mathbb{Q}$, then we can assign to any polynomial φ its initial term (corresponding to the monomial $\varphi^{(\alpha)}$ with the highest value of $\alpha \cdot \beta$.) In the yoga of Gröbner basis theory [CLO07,Stu96] we are assigning to each φ its initial term with respect to the weighted monomial ordering given by β. This initial term is well-defined for any φ. In our situation, we only need the initial terms to be well-defined for a finite collection of polynomials and we can choose $\beta \in \mathbb{N}^n$.

Returning to the general case, let $\beta \in \mathbb{N}^n$ and set $h_j = \max\{\alpha \cdot \beta \mid \varphi_j^{(\alpha)} \neq 0\}$, $j = 1, \ldots, m$. For $r \in \mathbb{N}$ set $\varphi_j^{(r)} = \sum_{\alpha\cdot\beta=r} \varphi_j^{(\alpha)}$. Now we fix a β such that, for each $r \in \mathbb{N}$ and each j, $\{\alpha \mid \alpha \cdot \beta = r$ and $\varphi_j^{(\alpha)} \neq 0\}$ has cardinality at most 1. Thus $\varphi_j^{(r)}$ is zero or consists of one non-zero term $\varphi_j^{(\alpha)}$. Moreover, $\varphi_j^{(h_j)} \neq 0$ for all j and $\varphi_{\max} := (\varphi_1^{(h_1)}, \ldots, \varphi_m^{(h_m)})$ is multihomogeneous. Note that the h_j and so $\varphi_{\max}$ depend upon our choice of β.

Remarks 2.1.

(1) If the V_i and W_j are G-modules and φ is equivariant, so are all the $\varphi_j^{(\alpha)}$ and $\varphi_{\max}$. Note that no entry in $\varphi_{\max}$ is zero since the same is true of φ.
(2) If $\varphi: V \to W$ is multihomogeneous of degree $A = (\alpha_{ji})$ and $\psi: W \to U = \bigoplus_{k=1}^{\ell} U_\ell$ is multihomogeneous of degree $B = (\beta_{kj})$ and all components of $\psi \circ \varphi$ are non-zero, then the composition $\psi \circ \varphi: V \to U$ is multihomogeneous of degree BA.

Concerning $\varphi_{\max}$ there is the following main result.

Lemma 2.2. *Let $\varphi: V \to W$ be a morphism where no φ_j is zero. Then* $\dim \varphi_{\max} \leqslant \dim \varphi$.

Proof. Let β and $h_1, \ldots, h_m$ be as above. We have an action λ of $\mathbb{C}^*$ on W where $\lambda(t)(w) = (t^{h_1} w_1, \ldots, t^{h_m} w_m)$ for $w \in W$ and $t \in \mathbb{C}^*$. We also have an action μ of $\mathbb{C}^*$ on V by $\mu(t)(v_1, \ldots, v_n) = (t^{\beta_1} v_1, \ldots, t^{\beta_n} v_n)$ where $t \in \mathbb{C}^*$ and $v \in V$. Let ${}^t\varphi(v)$ denote $\lambda(t)(\varphi(\mu(t^{-1})(v)))$ for $t \in \mathbb{C}^*$ and $v \in V$. Then ${}^t\varphi(v) = \varphi_{\max}(v) + t\psi(t, v)$ for some morphism $\psi: \mathbb{C} \times V \to W$. Consider the morphism

$$\Phi: \mathbb{C} \times V \to \mathbb{C} \times W, \qquad (t, v) \mapsto \bigl(t, {}^t\varphi(v)\bigr)$$

where ${}^0\varphi := \varphi_{\max}$. Let Y denote $\operatorname{Im} \Phi$. Let $p: \bar{Y} \to \mathbb{C}$ be the morphism induced by the projection $\mathbb{C} \times W \to \mathbb{C}$ where $\bar{Y}$ denotes the closure of Y. Clearly, we have $Y \cap (\{t\} \times W) = \{t\} \times \operatorname{Im} {}^t\varphi$ for $t \in \mathbb{C}$. Then

$$\bar{Y} \cap \bigl(\mathbb{C}^* \times W\bigr) = \bigcup_{t \neq 0} \{t\} \times \lambda(t) X$$

where $X := \overline{\operatorname{Im}\varphi}$, because the right-hand side is closed in $\mathbb{C}^* \times W$. As a consequence, we get

$$\bar{Y} = \overline{\Phi\big(\mathbb{C}^* \times W\big)},$$

hence $p^{-1}(t) = \{t\} \times \overline{\operatorname{Im}{}^t\varphi}$ for $t \neq 0$ and $p^{-1}(0) \supset \{0\} \times \overline{\operatorname{Im}\varphi_{\max}}$. Since $\bar{Y}$ is irreducible, it follows that $\dim\varphi_{\max} \leqslant \dim\varphi$. □

Corollary 2.3. *Let $p : \bar{Y} \to \mathbb{C}$ be as in the proof above. If $\dim\varphi = \dim\varphi_{\max}$ and $\operatorname{Im}\varphi$ is $\mathbb{C}^*$-stable, then $p^{-1}(0)$ is $\mathbb{C}^*$-stable.*

Proof. The hypotheses imply that $\{0\} \times \overline{\operatorname{Im}\varphi_{\max}}$ is an irreducible component of $p^{-1}(0)$. Since $\operatorname{Im}\varphi$ is $\mathbb{C}^*$-stable, then so is $\operatorname{Im}{}^t\varphi$ for all $t \neq 0$ which implies that $\bar{Y}$ is stable under the $\mathbb{C}^*$-action $\lambda \cdot (t, w) := (t, \lambda w)$ on $\mathbb{C} \times W$. It follows that $p^{-1}(0)$ is $\mathbb{C}^*$-stable. □

Theorem 2.4. *Let G be a finite group and let $V = \bigoplus_{i=1}^n V_i$ and $W = \bigoplus_{j=1}^m W_j$ be faithful G-modules where the V_i and W_j are irreducible submodules. Then there is a minimal multihomogeneous covariant $\varphi : V \to W$ all of whose components are non-zero.*

Proof. Let $\varphi : V \to W$ be a minimal covariant. We can always arrange that for given $v \in V$ and $w \in W$, both with trivial stabilizer in G, we have $\varphi(v) = w$. (See [KS07, Proposition 2.1]. This is also proved in [Pop94, Theorem 7.1.12], cf. [BR97, Lemma 3.2a]). Thus we can assume that all components of φ are non-zero. Then $\varphi_{\max} : V \to W$ is a multihomogeneous covariant, $\dim\varphi_{\max} \leqslant \dim\varphi$ and $\varphi_{\max}$ is faithful since all its components are non-zero [KS07, Lemma 4.1]. □

Corollary 2.5. *Let V_i be a faithful irreducible module of the group G_i, $i = 1, \dots, n$. Then $V = \bigoplus_{i=1}^n V_i$ is a faithful G-module where $G := G_1 \times \cdots \times G_n$, and there is a minimal multihomogeneous covariant $\varphi : V \to V$.*

We want to prove similar results for a *rational* covariant $\psi : V \to W$. It is obvious how to extend the definitions of *minimal* and *multihomogeneous of degree A* to rational covariants where in this case the matrix A might contain negative entries.

Theorem 2.6. *Let G be a finite group and let $V = \bigoplus_{i=1}^n V_i$ and $W = \bigoplus_{j=1}^m W_j$ be faithful G-modules where the V_i and W_j are irreducible submodules. Then there is a minimal rational multihomogeneous covariant $\psi : V \to W$ all of whose components are non-zero and which is of the form $\psi = h^{-1}\varphi$ where h is a multihomogeneous invariant and $\varphi : V \to W$ a multihomogeneous minimal regular covariant.*

Proof. Let $\psi : V \to W$ be a minimal rational covariant. We can assume that all components of ψ are non-zero. There is a non-zero invariant $f \in \mathcal{O}(V)^G$ such that $f\psi$ is regular. Define the regular covariant

$$\varphi := (f\psi, f) : V \to W \oplus \mathbb{C}, \qquad v \mapsto \big(f\psi(v), f(v)\big)$$

which is faithful since ψ is. Moreover, either $\dim\varphi = \dim\psi$ or $\dim\varphi = \dim\psi + 1$, where the second case takes place if and only if $\overline{\varphi(V)}$ is stable under scalar multiplication with $\mathbb{C}^*$. This follows from the fact that the composition of rational maps $V \to W \oplus \mathbb{C} \to \mathbb{P}(W \oplus \mathbb{C}) \to W$ is ψ.

As above we obtain a multihomogeneous covariant $\varphi_{\max} : V \to W \oplus \mathbb{C}$ which has the form $\varphi_{\max} = (\varphi_1, \dots, \varphi_m, h)$. Now define the multihomogeneous rational covariant

$$\psi_{\max} := \left(\frac{\varphi_1}{h}, \dots, \frac{\varphi_m}{h}\right) : V \to W$$

which is again faithful. Moreover, $\dim\psi_{\max} \leqslant \dim\varphi_{\max} \leqslant \dim\varphi$. So if $\dim\varphi = \dim\psi$ then $\psi_{\max}$ is a minimal multihomogeneous rational covariant and we are done.

Now assume that $\dim\varphi = \dim\psi + 1$ so that $\overline{\varphi(V)}$ is $\mathbb{C}^*$-stable. If φ is not minimal then there is a minimal multihomogeneous regular covariant $\tilde{\varphi}$ of dimension $\leqslant \dim\psi$ and we are again done. Therefore we can assume that φ is minimal, hence $\dim\varphi_{\max} = \dim\varphi$. Since $\overline{{}^t\varphi(V)}$ is $\mathbb{C}^*$-stable for all $t \neq 0$ it follows from Corollary 2.3 that $\overline{\varphi_{\max}(V)}$ is $\mathbb{C}^*$-stable, too, and so

$$\dim\psi_{\max} \leqslant \dim\varphi_{\max} - 1 = \dim\varphi - 1 = \dim\psi.$$

Hence, $\psi_{\max}$ is a minimal multihomogeneous rational covariant. □

3. Covariant dimension and essential dimension

In this section we extend [KS07, Corollary 4.2] to arbitrary groups and give the exact relation between covariant and essential dimension of finite groups.

Theorem 3.1. *Let G be a non-trivial finite group. Then* $\operatorname{covdim} G = \operatorname{edim} G$ *if and only if G has a non-trivial center.*

The proof is given in Corollary 3.5 and Proposition 3.6 below. We need some preparation. In this section we have faithful G-modules $V = \bigoplus_{i=1}^n V_i$ and $W = \bigoplus_{j=1}^m W_j$ where the V_i and W_j are irreducible submodules. We have a natural action of the tori $\mathbb{C}^{*n}$ on V and $\mathbb{C}^{*m}$ on W. These actions are free on the open sets $V' := \{v = (v_1, \ldots, v_n) \mid v_i \neq 0 \text{ for all } i\} \subset V$ and $W' \subset W$ defined similarly. If $\varphi : V \to W$ is multihomogeneous of degree $A = (\alpha_{ji})$ then φ is equivariant with respect to the homomorphism

$$T(A) : \mathbb{C}^{*n} \to \mathbb{C}^{*m}, \qquad s = (s_1, \ldots, s_n) \mapsto \left(s^{\alpha_1}, s^{\alpha_2}, \ldots, s^{\alpha_m}\right)$$

where $\alpha_j := (\alpha_{j1}, \alpha_{j2}, \ldots, \alpha_{jn})$ and $s^{\alpha_j} = s_1^{\alpha_{j1}} s_2^{\alpha_{j2}} \cdots s_n^{\alpha_{jn}}$, as before. This implies that the (closure of the) image of φ is stable under the subtorus $\operatorname{Im} T(A) \subset \mathbb{C}^{*m}$. The actions of G and $\mathbb{C}^{*n}$ commute and since each V_i is irreducible, considered as subgroups of $\mathrm{GL}(V)$, we have $\mathbb{C}^{*n} \cap G = Z(G)$.

Remark 3.2. Let $\varphi : V \to W$ be a multihomogeneous covariant of degree A. If $\mu \in A\mathbb{Q}^n \cap \mathbb{Z}^m$, then $\varphi(V) \subset W$ is stable under the $\mathbb{C}^*$-action $\rho(t)(w_1, \ldots, w_m) := (t^{\mu_1} w_1, \ldots, t^{\mu_m} w_m)$. It follows that for any invariant $f \in \mathcal{O}(V)^G$ the morphism

$$\tilde{\varphi} : v = (v_1, \ldots, v_n) \mapsto \left(f(v)^{\mu_1}\varphi_1(v), \ldots, f(v)^{\mu_m}\varphi_m(v)\right) \tag{1}$$

is a rational covariant with $\tilde{\varphi}(V) \subset \varphi(V)$, hence $\dim\tilde{\varphi} \leqslant \dim\varphi$. Moreover, if φ is faithful and f multihomogeneous, then $\tilde{\varphi}$ is faithful and multihomogeneous of degree $\tilde{A} := \mu \deg f + A$, i.e., $\tilde{\alpha}_{ji} = \mu_j \deg_{V_i} f + \alpha_{ji}$. Clearly $\tilde{\phi}$ is regular if $\mu \in \mathbb{N}^m$.

This has the following application which will be used later in the proof of Corollary 4.4: *Let p be a prime which does not divide the order of the center of a non-trivial group G. Then there is a minimal multihomogeneous covariant $\varphi : V \to V$ of degree $A \not\equiv 0 \bmod p$.* (Start with a minimal multihomogeneous covariant $\varphi : V \to V$ of degree A and assume that $A \equiv 0 \bmod p$. Since A is non-zero and has only non-negative entries we can choose a $\mu \in A\mathbb{Q}^n \cap \mathbb{N}^n$ such that $\mu_{j_0} \not\equiv 0 \bmod p$ for at least one j_0. Moreover, there is a multihomogeneous invariant f of total degree $\not\equiv 0 \bmod p$ (see [KS07, Lemma 4.3]). But then $\mu \deg f \not\equiv 0 \bmod p$, and so the covariant $\tilde{\varphi}$ given in (1) is minimal and has degree $\mu \deg f + A \not\equiv 0 \bmod p$.)

For the next results we need some preparation. Let $\varphi : V \to W$ be a multihomogeneous faithful covariant of degree $A = (\alpha_{ji})$ where all components φ_j are non-zero. Define $W' := \{(w_1, \ldots, w_m) \in W \mid w_i \neq 0 \text{ for all } i\} = \prod_{j=1}^m (W_j \setminus \{0\})$. The group $\mathbb{C}^{*m}$ acts freely on W' and $W' \to \prod_{j=1}^m \mathbb{P}(W_j)$ is the geometric quotient. Let $X := \overline{\varphi(V)}$ and $\mathbb{P}(X) \subset \prod_{j=1}^m \mathbb{P}(W_j)$ the image of X, and set $X' := X \cap W'$.

Finally, denote by $S \subset \mathbb{C}^{*m}$ the image of the homomorphism $T(A): \mathbb{C}^{*n} \to \mathbb{C}^{*m}$. Then we have the following.

Lemma 3.3.

(1) $\dim \mathbb{P}(X) \leqslant \dim X - \dim S \leqslant \dim X - \operatorname{rank} Z(G)$.
(2) *The kernel of the action of G on $\mathbb{P}(X)$ is equal to $Z(G)$.*

Proof. We may regard G as a subgroup of $\prod_{i=1}^m \mathrm{GL}(V_i)$ and of $\prod_{j=1}^m \mathrm{GL}(W_j)$, and so $Z(G) = G \cap \mathbb{C}^{*n}$ and $Z(G) = G \cap \mathbb{C}^{*m}$.

(1) The first inequality is clear because X is stable under S. For the second we remark that $Z(G) \subset S$ since φ is G-equivariant and so $T(A)z = z$ for all $z \in Z(G)$.

(2) Let $g \in G$ act trivially on $\mathbb{P}(X)$. Then every $x \in X_j := \mathrm{pr}_{W_j}(X)$ is an eigenvector of $g|_{Wj}$. But X_j is irreducible and therefore contained in a fixed eigenspace of g on W_j. Since W_j is a simple G-module this implies that $g|_{W_j}$ is a scalar. □

Proposition 3.4. *Let $\varphi: V \to W$ be a multihomogeneous faithful covariant of degree $A = (\alpha_{ji})$ where all components φ_j are non-zero. Assume that G has a trivial center. Then*

$$\operatorname{edim} G \leqslant \dim \varphi - \operatorname{rank} A \quad \textit{and} \quad \operatorname{covdim} G \leqslant \dim \varphi - \operatorname{rank} A + 1.$$

In particular, if φ is a minimal regular covariant, then $\operatorname{rank} A = 1$, *and if φ is a minimal rational covariant, then $A = 0$.*

Proof. Let $X := \overline{\varphi(V)}$, let $\mathbb{P}(X) \subset \prod_{j=1}^m \mathbb{P}(W_j)$ denote the image of X and set $X' := X \cap W'$. Finally, let S denote the image of $T(A): \mathbb{C}^{*n} \to \mathbb{C}^{*m}$. The torus S has dimension $\operatorname{rank} A$ and acts generically freely on $X := \overline{\varphi(V)}$ since all components of φ are non-zero. Composing φ with the projection $p: W \to \mathbb{P}(W_1) \times \cdots \times \mathbb{P}(W_m)$ we obtain a rational G-equivariant map $\varphi': V \to \mathbb{P}(W_1) \times \cdots \times \mathbb{P}(W_m)$ such that $\overline{\varphi'(V)} = \mathbb{P}(X)$. Since $Z(G)$ is trivial, G acts faithfully on $\mathbb{P}(X)$, and $\dim \mathbb{P}(X) \leqslant \dim X - \dim S$, by Lemma 3.3. Thus $p \circ \varphi'$ is a rational faithful covariant of dimension $\leqslant \dim X - \operatorname{rank} A$, proving the first claim. The second follows since $\operatorname{covdim} G \leqslant \operatorname{edim} G + 1$. □

Corollary 3.5. *If G is a (non-trivial) group with trivial center, then*

$$\operatorname{covdim} G = \operatorname{edim} G + 1.$$

Proof. Let $\varphi: V \to V$ be a minimal multihomogeneous regular covariant of degree A. By Proposition 3.4, $\operatorname{rank} A = 1$ and φ is not minimal as a multihomogeneous rational covariant. Hence $\operatorname{edim} G < \dim \varphi = \operatorname{covdim} G$ and the claim follows. □

Proposition 3.6. *If G has a non-trivial center, then* $\operatorname{covdim} G = \operatorname{edim} G$.

Proof. Let $\psi: V \to V$ be a multihomogeneous minimal rational covariant of degree $A = (\alpha_{ji})$ which is of the form $h^{-1}\varphi$ where $h \in \mathcal{O}(V)^G$ is a multihomogeneous invariant and $\varphi: V \to V$ a multihomogeneous regular minimal covariant (Theorem 2.6).

(a) If there is a $\beta \in \mathbb{Z}^n$ such that all entries of $\gamma := A\beta$ are > 0, then the covariant $\varphi := (h^{\gamma_1}\psi_1, \ldots, h^{\gamma_n}\psi_n): V \to V$ is regular and faithful. Moreover, $\overline{\varphi(V)} \subset \overline{\psi(V)}$ because the latter is stable under $T(A)(\mathbb{C}^{*n})$. Hence $\operatorname{covdim} G \leqslant \dim \varphi \leqslant \dim \psi = \operatorname{edim} G$ and we are done.

(b) In general, $A \neq 0$, since otherwise the center of G would act trivially on the image $\psi(V)$. If $\alpha_{j_0 i_0} \neq 0$, choose a homogeneous invariant $f \in \mathcal{O}(V_{j_0}) \subset \mathcal{O}(V)$ which does not vanish on $\psi(V)$. For any $r \in \mathbb{Z}$ the composition $\psi' := (f^r \cdot \mathrm{Id}) \circ \psi$ is still faithful and rational, and $\dim \psi' \leqslant \dim \psi$. Moreover, we get $\psi'_j(v) = f^r(\psi_{j_0}(v)) \cdot \psi_j(v)$. Therefore the degree of ψ'_j in V_{i_0} is $r \cdot \deg f \cdot \alpha_{j_0 i_0} + \alpha_{j i_0}$ for $j = 1, \ldots, n$. Hence, for a suitable r, all these degrees are > 0, and we are in case (a) with $\beta := e_{i_0}$. □

In some of our applications we will need the following result.

Corollary 3.7. *Assume that the center $Z(G)$ is cyclic (and non-trivial) and that $Z(G) \cap (G,G) = \{e\}$. If $G/Z(G)$ is faithful, then G is faithful, too, and*

$$\operatorname{edim} G = \operatorname{covdim} G = \operatorname{covdim} G/Z(G) = \operatorname{edim} G/Z(G) + 1.$$

Proof. It easily follows from the assumption $Z(G) \cap (G,G) = \{e\}$ that the center of $G/Z(G)$ is trivial and that every character of $Z(G)$ can be lifted to a character of G. Now let V be an irreducible faithful $G/Z(G)$-module and let $\varphi: V \to V$ be a homogeneous minimal covariant. Since $G/Z(G)$ has a trivial center we may assume that the degree of φ is $\equiv 1 \mod |Z(G)|$ (see Remark 3.2). If $\chi: G \to \mathbb{C}^*$ is a character which is faithful on $Z(G)$ then $V \otimes \chi$ is an irreducible faithful G-module and $\varphi: V \otimes \chi \to V \otimes \chi$ is G-equivariant and faithful. Hence $\operatorname{covdim} G = \operatorname{covdim} G/Z(G)$. The other two equalities follow from Proposition 3.6 and Corollary 3.5. □

4. The image of a covariant

In certain cases one can get a handle on the ideal of $\operatorname{Im}\varphi$.

Proposition 4.1. *Let $V := \bigoplus_{i=1}^n V_i$ and let $\varphi = (\varphi_1, \dots, \varphi_n): V \to V$ be a multihomogeneous morphism of degree $A = (\alpha_{ji})$. Assume that* $\det A \neq 0$. *Then the ideal $\mathcal{I}(\varphi(V))$ of the image of φ is generated by multihomogeneous polynomials.*

Proof. For $v = (v_1, \dots, v_n) \in V$ we have

$$\varphi(s_1 v_1, \dots, s_n v_n) = \left(s^{\alpha_1}\varphi_1, \dots, s^{\alpha_n}\varphi_n\right)(v)$$

where $s^{\alpha_j} = s_1^{\alpha_{j1}} \cdots s_n^{\alpha_{jn}}$. Choose coordinates in each V_i and let M be a monomial in these coordinates. Let $\beta = \beta(M)$ denote the multidegree of M, so we have $M(s_1 v_1, \dots, s_n v_n) = s^\beta M(v_1, \dots, v_n)$. Then $M(\varphi(s_1 v_1, \dots, s_n v_n))$ is $M(\varphi(v))$ multiplied by

$$\left(s^{\alpha_1}, \dots, s^{\alpha_n}\right)^\beta = s_1^{\beta_1\alpha_{11}+\dots+\beta_n\alpha_{n1}} \cdots s_n^{\beta_1\alpha_{1n}+\dots+\beta_n\alpha_{nn}} = s^{\beta A}$$

where βA is the matrix product of β and A. If $F \in \mathcal{I}(\varphi(V))$, we may write $F = \sum_M c_M M$ where the c_M are constants and M varies over all monomials in the coordinates of the V_i. We have $F(\varphi(s_1 v_1, \dots, s_n v_n)) = \sum_M c_M s^{\beta(M)A} M(\varphi(v))$. Hence, for any $\gamma \in \mathbb{N}^n$, we obtain

$$\sum_{\beta(M)A=\gamma} c_M M \in \mathcal{I}\big(\varphi(V)\big).$$

Since $\det A \neq 0$, for any γ there is at most one β such that $\beta A = \gamma$. It follows that every sum of the form $\sum_{\beta(M)=\beta} c_M M$ belongs to $\mathcal{I}(\varphi(V))$. Thus $\mathcal{I}(\varphi(V))$ is generated by multihomogeneous polynomials. □

Corollary 4.2. *Suppose that φ is as above and that there is a k, $1 \leqslant k < n$, such that* $\dim V_{k+1} = \dots = \dim V_n = 1$. *Then* $\dim \varphi = \dim(\varphi_1, \dots, \varphi_k) + (n-k)$.

Proof. Since the degree matrix $A = (\alpha_{ji})$ exists, no φ_j is zero. Let $m = \dim V_1 + \dots + \dim V_k$. By Proposition 4.1 the ideal of $\overline{\varphi(V)}$ is generated by functions of the form $F(y_1, \dots, y_m) t_{k+1}^{r_{k+1}} \cdots t_n^{r_n}$ where F is multihomogeneous. Such a function vanishes on $\operatorname{Im}\varphi$ if and only if $F(y_1, \dots, y_m)$ vanishes on the image of $(\varphi_1, \dots, \varphi_k)$. Thus the ideal $\mathcal{I}(\varphi(V))$ is generated by functions not involving $t_{k+1}, \dots, t_n$. As a consequence, $\overline{\varphi(V)} = \overline{(\varphi_1, \dots, \varphi_k)(V)} \times V_{k+1} \times \dots \times V_n$. □

In order to apply Proposition 4.1 and Corollary 4.2 we need a version of [KS07, Lemma 5.2].

Corollary 4.3. *Let $G = G_1 \times \cdots \times G_n$ and $V = V_1 \oplus \cdots \oplus V_n$ where each V_i is an irreducible G_i-module, $i = 1, \ldots, n$. Let $\varphi : V \to V$ be a multihomogeneous covariant of degree A and suppose that the prime p divides $|Z(G_i)|$ for all i. Then* $\det A \neq 0$*, and the ideal $\mathcal{I}(\varphi(V))$ is generated by multihomogeneous elements.*

Proof. Let ξ be a primitive pth root of unity. Then we have $\varphi_j(v_1, \ldots, \xi v_i, \ldots, v_n) = \xi^{\alpha_{ji}} \varphi_j(v_1, \ldots, v_n)$. There is an element of G_j which acts as ξ on V_j and trivially on V_i if $i \neq j$. Hence $\xi^{\alpha_{ji}} = 1$ for $i \neq j$. If $i = j$, one similarly shows that $\xi^{\alpha_{jj}} = \xi$ by equivariance relative to G_j. This implies that

$$\alpha_{ji} \equiv \begin{cases} 1 \bmod p & \text{for } i = j, \\ 0 \bmod p & \text{otherwise,} \end{cases}$$

and so $\det(\alpha_{ij}) \neq 0$. Now apply Proposition 4.1. □

We say that G is *faithful* if it admits a faithful irreducible representation. We now get the following result which extends Corollaries 6.1 and 6.2 of [KS07].

Corollary 4.4. *Let $G = G_1 \times \cdots \times G_n$ be a product of non-trivial faithful groups and let p be a prime.*

(1) *If p is coprime to $|Z(G)|$, then* $\operatorname{covdim}(G \times \mathbb{Z}/p) = \operatorname{covdim} G$.
(2) *If p divides all $|Z(G_i)|$, then* $\operatorname{covdim}(G \times (\mathbb{Z}/p)^m) = \operatorname{covdim} G + m$.

In particular, if H is a non-trivial faithful group and $m \geqslant 1$, then

$$\operatorname{covdim}\bigl(H \times (\mathbb{Z}/p)^m\bigr) = \begin{cases} \operatorname{covdim} H + m & \text{if } p \text{ divides } |Z(H)|, \\ \operatorname{covdim} H + (m-1) & \text{otherwise.} \end{cases}$$

Proof. Let V_i be a faithful irreducible G_i-module. Then $V := V_1 \oplus \cdots \oplus V_n$ is a faithful G-module. By Corollary 2.5 there is a minimal multihomogeneous faithful covariant $\varphi = (\varphi_1, \ldots, \varphi_k) : V \to V$ of degree A. For any $\delta = (\delta_1, \ldots, \delta_n) \in \mathbb{Z}^n$ there is a linear action of $\mathbb{Z}/p$ on V where the generator $\bar{1} \in \mathbb{Z}/p$ acts by

$$v = (v_1, \ldots, v_n) \mapsto \bigl(\zeta^{\delta_1} v_1, \ldots, \zeta^{\delta_n} v_n\bigr), \quad \zeta := e^{\frac{2\pi i}{p}}.$$

This action commutes with the G-action and defines a $(G \times \mathbb{Z}/p)$-module structure on V which will be denoted by V_δ. It follows that for $\mu = A\delta$ the multihomogeneous map φ is a $(G \times \mathbb{Z}/p)$-equivariant morphism from V_δ to V_μ. If p is coprime to $|Z(G)|$ we can assume that $A \not\equiv 0 \bmod p$ (Remark 3.2). Then there is a δ such that $\mu = A\delta \not\equiv 0 \bmod p$ and so φ is a faithful covariant for the group $G \times \mathbb{Z}/p$, proving (1).

Assume now that p divides all $|Z(G_i)|$. There is a minimal multihomogeneous covariant $\psi : V \oplus \mathbb{C}^m \to V \oplus \mathbb{C}^m$ for $G \times (\mathbb{Z}/p)^m$ where $(\mathbb{Z}/p)^m$ acts in the obvious way on $\mathbb{C}^m$. Clearly, no entry of ψ is zero and by Corollaries 4.3 and 4.2, we get $\dim \psi = \dim \varphi + m$ where $\varphi : V \oplus \mathbb{C}^m \to V$ is ψ followed by projection to V. Since each component of φ is non-zero, φ is faithful for G [KS07, Lemma 4.1]. Thus $\dim \varphi \geqslant \operatorname{covdim} G$. But clearly, $\operatorname{covdim}(G \times (\mathbb{Z}/p)^m) \leqslant \operatorname{covdim} G + m$, hence we have equality, proving (2). □

As an immediate consequence we get the following result.

Corollary 4.5. *Let G be abelian of rank r. Then* $\operatorname{covdim} G = r$.

Remark 4.6. The corollary is Theorem 3.1 of [KS07]. The proof in [KS07] uses a lemma whose proof is incorrect. The problem is that the quotient ring R/pR constructed there may have zero divisors. However, one can give a correct proof of the lemma by paying attention to the powers of the variables that occur in the determinant $\det(\partial f_i/\partial x_j)$. We omit this proof since the lemma is no longer needed.

The following strengthens [KS07, Proposition 6.1], which in turn then simplifies other proofs in the paper, e.g., the proof of Proposition 6.2.

Corollary 4.7. *Let $V = W \oplus \mathbb{C}_\chi$ be a faithful G-module where W is irreducible and χ is a character of G. Let H denote the kernel of $G \to \mathrm{GL}(W)$. Assume that there is a prime p which divides the order of H and such that the following two equivalent conditions hold*:

(i) *There is a subgroup of* $\ker\chi$ *acting as scalar multiplication by $\mathbb{Z}/p$ on W*;
(ii) *There is a subgroup of G acting as scalar multiplication by $\mathbb{Z}/p$ on V.*

Then $\operatorname{covdim} G = \operatorname{covdim} G/H + 1$.

Proof. It is easy to see that the two conditions are equivalent, because $\chi|_H : H \to \mathbb{C}^*$ is injective. Since G embeds into $G/H \times \chi(G)$, we have $\operatorname{covdim} G \leqslant \operatorname{covdim} G/H + 1$.

To prove the reverse inequality let $(\varphi, h) : W \oplus \mathbb{C}_\chi \to W \oplus \mathbb{C}_\chi$ be a minimal faithful multihomogeneous covariant of degree (α_{ji}). Since H is non-trivial, h cannot be zero. By assumption, H contains a subgroup of order p which is mapped injectively into $\mathbb{C}^*$ by χ. Thus the subgroup acts trivially on W and by scalar multiplication on $\mathbb{C}_\chi$. Therefore,

$$\alpha_{22} \equiv 1 \quad \text{and} \quad \alpha_{12} \equiv 0 \mod p.$$

Similarly, condition (i) implies that

$$\alpha_{11} \equiv 1 \quad \text{and} \quad \alpha_{21} \equiv 0 \mod p.$$

Thus $\det(\alpha_{ij}) \neq 0$, and so $\dim(\varphi, h) = \dim\varphi + 1$ by Corollary 4.2. The equivariant morphism $\varphi : W \oplus \mathbb{C}_\chi \to W$ factors through the quotient $(W \oplus \mathbb{C}_\chi)/H$ which is isomorphic to the G/H-module $W \oplus \mathbb{C}$, and defines a faithful G/H-covariant $\bar{\varphi} : W \oplus \mathbb{C} \to W$. Hence, $\dim\varphi \geqslant \operatorname{covdim} G/H$, and our result follows. □

Now consider the following commutative diagram with exact rows where $\ell > m \geqslant 0$, $\mu_N \subset \mathbb{C}^*$ denotes the Nth roots of unity and π is the canonical homomorphism $\xi \mapsto \xi^{p^{\ell-m}}$:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & K & \longrightarrow & G & \xrightarrow{\chi} & \mu_{p^\ell} & \longrightarrow & 1 \\
 & & \| & & \downarrow & & \downarrow{\scriptstyle \pi} & & \\
1 & \longrightarrow & K & \longrightarrow & G' & \xrightarrow{\chi'} & \mu_{p^m} & \longrightarrow & 1.
\end{array}$$

Corollary 4.8. *In the diagram above assume that G' is faithful and that the prime p divides $|Z(G') \cap K|$. Then* $\operatorname{covdim} G = \operatorname{covdim} G' + 1$.

Proof. Let $\rho : G' \to \mathrm{GL}(W)$ be a faithful irreducible G'-module. Then $V := W \oplus \mathbb{C}_\chi$ is a faithful G-module. Fix a pth root of unity $\zeta \in \mathbb{C}^*$ and let $z' \in Z(G') \cap K$ be such that $\rho(z') = \zeta \cdot \mathrm{Id}$. We have

$$G = \left\{ (g', \xi) \in G' \times \mu_{p^\ell} \;\middle|\; \chi'(g') = \pi(\xi) \right\}$$

and so $z := (z', \zeta) \in Z(G)$ acts as scalar multiplication with ζ on V. Now the claim follows from Corollary 4.7. □

5. Some examples

We consider the covariant dimension of some products and semidirect products of groups. We denote by C_n a cyclic group of order n.

Example 5.1. Consider the group $G := C_3 \rtimes C_4$ where a generator of C_4 acts on C_3 by sending each element to its inverse. Then $Z(G) \subset C_4$ is of order 2, $(G, G) = C_3$ and $G/Z(G) \simeq S_3$. Hence $\operatorname{edim} G = \operatorname{covdim} G = \operatorname{covdim} S_3 = 2$, by Corollary 3.7.

Example 5.2. Let $H := S_3 \times S_3$. Since $\operatorname{covdim} S_3 = 2 = \operatorname{edim} S_3 + 1$, we have $\operatorname{covdim} H = \operatorname{edim} H + 1 \leqslant 2\operatorname{edim} S_3 + 1 \leqslant 3$. We claim that $\operatorname{covdim} H = 3$. Let G denote $H \times (\mathbb{Z}/2\mathbb{Z})^2$. By Corollary 4.4, $\operatorname{covdim} G = \operatorname{covdim} H + 1$. Since G contains a copy of $(\mathbb{Z}/2\mathbb{Z})^4$, its covariant dimension is at least 4, hence it is 4, and so the covariant dimension of H is 3. The same reasoning shows that $\operatorname{covdim} S_3 \times S_4 = 4$ and $\operatorname{covdim} S_4 \times S_4 = 5$.

Example 5.3. Let $G := A_4 \rtimes C_4$ where a generator x of C_4 acts on A_4 by conjugation with a 4-cycle $\sigma \in S_4$. We get

$$Z(G) = \langle x^2\sigma^2 \rangle \simeq C_2, \qquad (G, G) = A_4, \qquad G/Z(G) \simeq S_4.$$

Thus $\operatorname{edim} G = \operatorname{covdim} G = \operatorname{covdim} S_4 = 3$, by Corollary 3.7. Moreover, G has a 3-dimensional faithful representation—the standard representation of A_4 lifts to a faithful representation of G—and G contains a subgroup isomorphic to $C_2 \times C_2 \times C_2$.

Example 5.4. Let $\sigma \in S_n \setminus A_n$ be of (even) order m where $n \geqslant 4$, and consider the group $G := A_n \rtimes C_m$ where a generator of C_m acts on A_n by conjugation with σ. Again, we can apply Corollary 3.7 and get $\operatorname{edim} G = \operatorname{covdim} G = \operatorname{covdim} S_n$.

Example 5.5. Let $G := (C_3 \times C_3) \rtimes (C_4 \times C_8)$ where a generator x of C_4 acts on $C_3 \times C_3$ by sending each element to its inverse, and a generator y of C_8 acts by sending the first component to its inverse and leaving the second component invariant. Then $Z(G) = \langle x^2, y^2 \rangle \simeq C_2 \times C_4$, $(G, G) = C_3 \times C_3$ and $G/Z(G) \simeq S_3 \times S_3$. Since the center is not cyclic we cannot apply Corollary 3.7 directly, but have to pass through the intermediate group $\bar{G} := G/\langle x^2 \rangle$ which has a cyclic center, namely $\langle y^2 \rangle$. Thus we obtain $\operatorname{edim} \bar{G} = \operatorname{covdim} \bar{G} = \operatorname{covdim} \bar{G}/Z(\bar{G}) = \operatorname{covdim} S_3 \times S_3 = 3$ by Example 5.2. Since $\bar{G}$ is faithful we can apply Corollary 4.7: Take $H := \langle x^2 \rangle$ and choose for χ a lift of the character $\bar{\chi}$ on $Z(G) = \langle x^2, y^2 \rangle$ given by $\bar{\chi}(x^2) = -1$ and $\bar{\chi}(y^2) = 1$. We finally get $\operatorname{edim} G = \operatorname{covdim} G = \operatorname{covdim} \bar{G} + 1 = 4$.

Example 5.6. A recent general theorem due to Karpenko and Merkurjev [KM08] is the following. *For any finite p-group G the essential dimension* $\operatorname{edim} G$ *equals the minimal dimension of a faithful representation of G.* Using this, Meyer and Reichstein [MR08] have found formulas for the essential dimension of all p-groups. Here we give a simple formula for the essential dimension of semidirect products $G_p(k, \ell, \alpha) := \mathbb{Z}/p^k \ltimes \mathbb{Z}/p^\ell$ where the generator $\bar{1}$ of $\mathbb{Z}/p^k$ induces the automorphism α on $A := \mathbb{Z}/p^\ell$. Our results generalize [KS07, Proposition 6.2]. We have

$$\operatorname{covdim} G_p(k, \ell, \alpha) = \begin{cases} p^k & \text{if } \alpha \text{ has order } p^k, \\ p^d + 1 & \text{if } \alpha \text{ has order } p^d,\ d < k. \end{cases}$$

Note that $C := p^{\ell-1}A$ lies in the center of $G := G_p(k, \ell, \alpha)$, so that the covariant dimension and essential dimension are the same.

The second case follows from the first using Corollary 4.8. So we assume that α has order p^k. Let V be a faithful G-module. Then the (cyclic) center of G acts faithfully on an irreducible component W of V, and $\mathrm{Ker}(G \to \mathrm{GL}(W))$ is trivial since any non-trivial normal subgroup of G intersects the center. Thus G is faithful. (One could also use Proposition 6.1 below.)

Let V be an irreducible faithful G-module. Then, since G is supersolvable, V is induced by a character of a proper subgroup H. We claim that H is abelian. If not, then $(H,H) \subset (G,G) \subset A$ contains C, so C acts trivially on V, a contradiction. If H is an abelian subgroup, we may consider a character of H which is faithful on H intersected with the (cyclic) center. Then the induced representation is faithful of dimension $[G:H]$. Thus we only need to show that any abelian subgroup H of G has order at most p^ℓ.

Let γ generate the canonical projection of H to $\mathbb{Z}/p^k$ and let y generate $H \cap A$. We may assume that $\gamma \neq e$ and that $y \neq e$. Now H is generated by x and y where $x \in H$ has image γ in $\mathbb{Z}/p^k$. Choose a generator z of A such that $y = z^{p^r}$ for some r where $1 \leqslant r < l$. We have $\gamma(z) = z^{s+1}$ where $0 < s < p^l - 1$. Since H is abelian, the commutator $(x,y) = (x, z^{p^r})$ is trivial. It follows that $\gamma(z)^{p^r} = z^{p^r} = z^{sp^r + p^r}$, so that p^ℓ divides sp^r and $p^{\ell - r}$ divides s. Hence γ has order at most p^r. It follows that H has order at most p^ℓ.

6. Faithful groups

Let $N_G \subset G$ denote the subgroup generated by the minimal subgroups (under set inclusion) among the non-trivial normal abelian subgroups of G. Our work in [KS07] used the following criterion of Gaschütz.

Proposition 6.1. *(See [Gas54].) Let G be a finite group. Then G is faithful if and only if N_G is generated by the conjugacy class of one of its elements.*

We have the following corollary [KS07, Corollary 4.1], which we need in the next section.

Corollary 6.2. *Let G be a non-faithful group and $H \subset G$ a subgroup containing N_G. Then H is non-faithful, too.*

The proof given in [KS07] claims that $N_G \subset N_H$. But this is false. For example, let $G = S_4 \supset D_4$. Then N_G is the Klein 4-group, while $N_H = Z(D_4) \simeq \mathbb{Z}/2\mathbb{Z}$. Here is a correct proof.

Lemma 6.3. *Let $N_1, \ldots, N_k$ be the minimal non-trivial normal abelian subgroups of a finite group G. Then*:

(1) *Each N_i is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^n$ for some $n \in \mathbb{N}$ and prime p.*
(2) *Let L be a G-normal subgroup of N_G. There is a direct product M of a subset of $\{N_1, \ldots, N_k\}$ such that N_G is the direct product LM.*

Proof. By minimality, for any prime p and i, pN_i is zero or N_i. Thus $N_i \simeq (\mathbb{Z}/p\mathbb{Z})^n$ for some p and n giving (1). For (2), inductively assume that we have found a G-normal subgroup M_j of N_G which is a direct product of a subset of $\{N_1, \ldots, N_j\}$ such that LM_j is a direct product containing $N_1, \ldots, N_j$. We start the induction with $M_0 = \{e\}$. If LM_j contains N_{j+1}, then set $M_{j+1} = M_j$. If not, then $N_{j+1} \cap LM_j$ must be trivial, so that the products $M_{j+1} := M_j N_{j+1}$ and LM_{j+1} are direct where $N_{j+1} \subset LM_{j+1}$. Set $M = M_k$. Then LM is a direct product containing all the generators of N_G, hence equals N_G. □

Corollary 6.4. *N_G is a direct product of a subset of $\{N_1, \ldots, N_k\}$, hence N_G is abelian.*

Proof of Corollary 6.2. The subgroup $N_G \cap N_H \subset N_H$ is normal in H. By Lemma 6.3 it has a complement M. Now assume that H is faithful. Then by Proposition 6.1 there exists an element $(c,d) \in N_H = (N_G \cap N_H) \times M$ whose H-conjugacy class generates N_H. Then the H-conjugacy class of c generates $N_G \cap N_H$. Now let N_i be one of the minimal non-trivial normal abelian subgroups of G.

By hypothesis, $N_i \subset H$, hence N_i contains a minimal non-trivial H-submodule N'. Then $N' \subset N_G \cap N_H$. The smallest G-stable subspace of N_G containing N' is N_i, hence N_i lies in the G-submodule of N_G generated by the conjugacy class of c. Since N_i is arbitrary, we see that G is faithful. □

Remark 6.5. Let $G_1, G_2, \dots, G_m$ be faithful groups. *Then the product $G_1 \times \cdots \times G_m$ is faithful if and only if the orders of the centers $Z(G_i)$ are pairwise coprime.* In fact, the center of the product is cyclic if and only if the orders $|Z(G_i)|$ are pairwise coprime, and in this case the tensor product of irreducible faithful representations V_i of G_i is irreducible and faithful.

7. Groups of covariant dimension 2

In [Led07] it is shown that G has essential dimension one if and only if admits an embedding into GL_2 such that the only scalar matrix in the image is the identity. In [KS07] we showed that a finite group of covariant dimension 2 is a subgroup of GL_2 and thus admits a faithful 2-dimensional representation. In particular, we have the following result (cf. [KS07, Theorem 10.3]).

Theorem 7.1. *If G is a non-faithful finite group of covariant dimension 2, then G is abelian of rank 2.*

Unfortunately, there is a gap in the proof of Lemma 10.3 in [KS07] which is used in the proof of the theorem. So we give a new proof here which avoids this lemma. We start with the following result.

Lemma 7.2. *If G is a non-commutative finite group of covariant dimension 2, then $G/Z(G)$ is isomorphic to a subgroup of PGL_2.*

Proof. We use the notation of Section 3. Let $\varphi : V \to W$ be a multihomogeneous minimal covariant of degree A. Set $X := \overline{\varphi(V)} \subset W$ and let S denote the image of the homomorphism $T(A) : \mathbb{C}^{*n} \to \mathbb{C}^{*m}$. Since S is non-trivial, Lemma 3.3 shows that $\dim \mathbb{P}(X) \leqslant 1$ and that $G/Z(G)$ acts faithfully on $\mathbb{P}(X)$. Thus $\dim \mathbb{P}(X) = 1$ and $G/Z(G)$ acts faithfully on the normalization $\mathbb{P}^1$ of $\mathbb{P}(X)$. The lemma follows. □

Proof of Theorem 7.1. Let G be a minimal counterexample, i.e., G is non-faithful and non-commutative of covariant dimension 2, and every strict subgroup is either commutative or faithful. By the lemma above, $G/Z(G)$ is isomorphic to A_5, S_4, A_4, or D_{2n}, and the image of N_G in $G/Z(G)$ is a normal abelian subgroup.

Claim 1. *There are no surjective homomorphisms from G to A_5, S_4, or A_4.*

If ρ is a surjective homomorphism from G to A_5 then $\rho(N_G)$ is trivial. If ρ is a surjective homomorphism from G to S_4 then $\rho(N_G) \subset K$ where $K \subset S_4$ is the Klein 4-group. In both cases $\rho^{-1}(A_4) \subsetneq G$ is neither faithful (by Corollary 6.2) nor commutative, contradicting the minimality assumption.

Now assume that there is a surjective homomorphism $\rho : G \to A_4$, and let $g_3 \in G$ be the preimage of an element of A_4 of order 3. We may assume that the order of g_3 is a power 3^ℓ. Since $\rho(N_G) \subset K$, the strict subgroup $S := \rho^{-1}(K) \subsetneq G$ is commutative. Denote by S_2 the 2-torsion of S. Since $\rho(S_2) = K$ we see that S_2 has rank 2. Moreover, S_2 is normalized by g_3, but not centralized, and so $\operatorname{covdim}\langle g_3, S_2\rangle \geqslant 3$ by [KS07, Corollary 4.4]. This contradiction proves Claim 1.

Claim 2. *For every prime $p > 2$ the p-Sylow-subgroup $G_p \subset G$ is normal and commutative of rank $\leqslant 2$. Hence G is a semidirect product $G_2 \ltimes G'$ where $G' := \prod_{p>2} G_p$ and G_2 is a 2-Sylow subgroup.*

From Claim 1 we know that $G/Z(G) \simeq D_{2n}$. Then Claim 2 follows, because every p-Sylow-subgroup of D_{2n} for $p \neq 2$ is normal and cyclic.

Now we can finish the proof. The case that $G = G_2$ is handled in [KS07, Lemma 10.2], so we can assume that G' is non-trivial. If G_2 commutes with G', then G_2 is non-commutative and faithful. Moreover, no G_p can be of rank 2, else we have a subgroup which is a product $H := G_2 \times (\mathbb{Z}/p)^2$, and we have $\operatorname{covdim} H \geqslant 3$ by Corollary 4.4. So G' has rank 1. Then G' is cyclic, hence G is faithful by Remark 6.5, which is a contradiction. Hence we may assume that G_2 acts non-trivially on G'.

It is clear that $N_G = N_2 \times N'$ where $N_2 = N_G \cap G_2$ and $N' := N_G \cap G'$. Since G_2 acts non-trivially on G', there is a $g \in G_2$ which induces an order 2 automorphism of some $G_p \neq \{e\}$. Then one can see that g acts non-trivially on N_{G_p}. Since G is not faithful, N_G is not generated by a conjugacy class (Proposition 6.1) and the same holds for the subgroup $H := \langle g, N_2\rangle \ltimes N'$ (Corollary 6.2). Thus H is neither faithful nor commutative, so that it must equal G by minimality. It follows that each non-trivial G_p, for $p \neq 2$, is isomorphic to either $\mathbb{Z}/p$ or $(\mathbb{Z}/p)^2$.

Suppose that $G_p = (\mathbb{Z}/p)^2$ for some p. If g acts trivially on G_p, then it must act non-trivially on some G_q, and then we have the subgroup $(\langle g\rangle \ltimes G_q) \times (\mathbb{Z}/p)^2$ which by Corollary 4.4(2) has covariant dimension at least 3. If g acts by sending each element of G_p to its inverse, then, by Corollary 4.4(1) and Corollary 4.5,

$$\operatorname{covdim}\langle g\rangle \ltimes G_p = \operatorname{covdim}\big(\langle g\rangle \ltimes G_p\big) \times \mathbb{Z}/p \geqslant \operatorname{covdim}(\mathbb{Z}/p)^3 = 3.$$

So we can assume that g acts on G_p fixing one generator and sending the other to its inverse for every G_p of rank 2. Thus G' is generated by the conjugacy class of a single element. It follows that N_2 must have rank 2 and g must commute with N_2, else $N_2 \times G'$ is generated by the conjugacy class of a single element. Suppose that $\langle g\rangle \cap N_2 \simeq \mathbb{Z}/2$. If g acts non-trivially on $\mathbb{Z}/p \subset G'$, then $\langle g, N_2\rangle \ltimes \mathbb{Z}/p$ contains a subgroup $(\langle g\rangle \ltimes \mathbb{Z}/p) \times \mathbb{Z}/2$ which has covariant dimension 3, again by Corollary 4.4(2). If $\langle g\rangle \cap N_2 = \{e\}$, then we have the subgroup $(\langle g\rangle \ltimes \mathbb{Z}/p) \times (\mathbb{Z}/2)^2$ which has covariant dimension three by Corollary 4.4(1). This finishes the proof of the theorem. □

8. Errata to [KS07]

First sentence after Definition 4.1. Replace “simple groups.” by “non-abelian simple groups.”

Proof of Proposition 4.3, second paragraph. Replace “is divisible by m” with “is congruent to 1 mod m.”

Proof of Corollary 5.1 last sentence. Replace “Corollary 4.3” by “Proposition 4.3.”

Proof of Proposition 6.1 second paragraph. Change “$\varphi|_W$” to $F|_W$.”

Proof of Proposition 6.1 first displayed formula. Replace “$F(w,t)$” and “$F_0(w,t)$” by “$F(w,t^m)$” and “$F_0(w,t^m)$.”

Top of page 282. Change “trivial stabilizer” to “trivial stabilizer or stabilizer $\pm I$.”

Acknowledgment

We thank the referee for helpful comments.

References

[BR97] J. Buhler, Z. Reichstein, On the essential dimension of a finite group, Compos. Math. 106 (2) (1997) 159–179.
[CLO07] David Cox, John Little, Donal O'Shea, Ideals, Varieties, and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra, third ed., Undergrad. Texts Math., Springer, New York, 2007.
[Flo08] Mathieu Florence, On the essential dimension of cyclic p-groups, Invent. Math. 171 (1) (2008) 175–189.
[Gas54] Wolfgang Gaschütz, Endliche Gruppen mit treuen absolut-irreduziblen Darstellungen, Math. Nachr. 12 (1954) 253–255.
[JLY02] Christian U. Jensen, Arne Ledet, Noriko Yui, Generic Polynomials. Constructive Aspects of the Inverse Galois Problem, Math. Sci. Res. Inst. Publ., vol. 45, Cambridge Univ. Press, Cambridge, 2002.
[KM08] Nikita A. Karpenko, Alexander S. Merkurjev, Essential dimension of finite p-groups, Invent. Math. 172 (3) (2008) 491–508.
[KS07] Hanspeter Kraft, Gerald W. Schwarz, Compression of finite group actions and covariant dimension, J. Algebra 313 (1) (2007) 268–291.
[Led07] Arne Ledet, Finite groups of essential dimension one, J. Algebra 311 (1) (2007) 31–37.

[Löt08] Roland Lötscher, Application of multihomogeneous covariants to the essential dimension of finite groups, http://arxiv.org/abs/0811.3852.

[MR08] Aurel Meyer, Zinovy Reichstein, Some consequences of the Karpenko–Merkurjev theorem, http://arxiv.org/abs/0811.2517v1.

[Pop94] Vladimir Popov, Sections in invariant theory, in: The Sophus Lie Memorial Conference, Oslo, 1992, Scand. Univ. Press, Oslo, 1994, pp. 315–361.

[Rei04] Z. Reichstein, Compressions of group actions, in: Invariant Theory in all Characteristics, in: CRM Proc. Lecture Notes, vol. 35, Amer. Math. Soc., Providence, RI, 2004, pp. 199–202.

[Stu96] Bernd Sturmfels, Gröbner Bases and Convex Polytopes, Univ. Lecture Ser., vol. 8, Amer. Math. Soc., Providence, RI, 1996.