Available online at www.sciencedirect.com
ScienceDirect
Journal of Algebra 313 (2007) 268–291
JOURNAL OF Algebra
www.elsevier.com/locate/jalgebra

Compression of finite group actions and covariant dimension ☆

Hanspeter Kraft [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*

Received 14 September 2006

Available online 25 January 2007

Communicated by Victor Kac, Ruth Kellerhals, Friedrich Knop, Peter Littelmann and Dmitri Panyushev

To Ernest Vinberg on the occasion of his 70th birthday

Abstract

Let G be a finite group and $\varphi : V \to W$ an equivariant morphism of 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 this paper we investigate covariant dimension and are able to determine it for abelian groups and to obtain estimates for the symmetric and alternating groups. We also classify groups of covariant dimension less than or equal to 2. A byproduct of our investigations is the existence of a purely transcendental field of definition of degree $n - 3$ for a generic field extension of degree $n \geqslant 5$.

Keywords: Compression; Essential dimension; Covariant; Covariant dimension

Contents

☆ The first author is partially supported by the Swiss National Science Foundation (Schweizerischer Nationalfonds), and the second author by NSA Grant H98230-04-1-0070.
* Corresponding author.
E-mail addresses: hanspeter.kraft@unibas.ch (H. Kraft), schwarz@brandeis.edu (G.W. Schwarz).

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2006.12.025

1. Introduction

Our base field is the field $\mathbb{C}$ of complex number. It could be replaced by any algebraically closed field of characteristic zero. Let G be a finite group. All G-modules that we consider will be finite-dimensional over $\mathbb{C}$.

Definition 1.1. A *covariant* of G is an equivariant morphism $\varphi : V \to W$ 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.

Here is a slightly different point of view [Rei04].

Definition 1.2. Let V be a G-module and X a faithful affine G-variety. A G-equivariant dominant morphism $\varphi : V \to X$ is called a *compression*.

Clearly, a faithful covariant $\varphi : V \to W$ defines a compression $\varphi : V \to X := \overline{\varphi(V)}$, and every compression arises in this way. We are interested in finding compressions (faithful covariants) with small dimension. This leads to the following definition.

Definition 1.3. The *covariant dimension* of G is defined to be the minimum of $\dim X$ where $\varphi : V \to X$ runs over all compressions of G. Equivalently,

$$\operatorname{covdim} G := \min\{\dim \varphi \mid \varphi : V \to W \text{ is a faithful covariant of } G\}.$$

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.

Definition 1.4. (See Buhler, Reichstein [BuR97].) The *essential dimension* $\operatorname{edim} G$ of G is the minimum dimension of all the faithful rational covariants of G.

The covariant dimension and essential dimension of G differ by at most 1 ([Rei04] and Proposition 2.2). Essential dimension and covariant dimension of G are related to cohomological invariants, generic polynomials and other topics, see [BuR97].

In this paper we study the notion of covariant dimension staying in the category of morphisms. A major role is played by covariants $\varphi : V \to W$ which are *homogeneous*. We are able to determine the covariant dimension of abelian groups and obtain estimates of the covariant dimension of the symmetric and alternating groups. Finally, we are able to classify the groups of covariant dimension less than or equal to 2. It turns out that these are exactly the finite subgroups of $\mathrm{GL}_2(\mathbb{C})$. We also obtain a new result about the "fields of definition" for generic extensions of degree n. Except for this and the classification above, most of our results could also be obtained from [BuR97] and [Rei04]. However, we think that our methods are of independent interest.

2. First properties

A covariant $\varphi : V \to W$ is called *minimal* if φ is faithful and $\dim \varphi = \operatorname{covdim} G$.

Lemma 2.1. *Let V, W be two G-modules and let $v \in V$, $w \in W$ be such that $G_v \subset G_w$. Then there is a covariant $\varphi : V \to W$ such that $\varphi(v) = w$.*

Proof. By assumption there is a G-equivariant map $\mu : Gv \to W$ which sends v to w. This map lifts to a morphism from V to W which we can average over G to obtain a covariant $\tilde{\mu}$ extending μ. □

Remark 2.1. Obviously, one can prescribe the images $w_1, w_2, \ldots, w_m \in W$ of a finite number of points $v_1, v_2, \ldots, v_m \in V$ from distinct orbits provided that $G_{v_i} \subset G_{w_i}$ for all i.

Proposition 2.1. *Let V, W be two faithful G-modules and let $v \in V$ and $w \in W$ be points with trivial stabilizer. Then there is a minimal covariant $\varphi : V \to W$ such that $\varphi(v) = w$.*

Proof. Let $\varphi_0 : V_0 \to W_0$ be a faithful covariant with $\dim \varphi_0 = \operatorname{covdim} G$. Then there is a $v_0 \in V_0$ such that $w_0 := \varphi_0(v_0) \in W_0$ has a trivial stabilizer. Thus v_0 has a trivial stabilizer, too. By the previous lemma we can find covariants $\varphi_1 : V \to V_0$ and $\varphi_2 : W_0 \to W$ and points $v \in V$ and $w \in W$ with trivial stabilizer such that $\varphi_1(v) = v_0$ and $\varphi_2(w_0) = w$. Then $\varphi := \varphi_2 \circ \varphi_0 \circ \varphi_1$ is faithful with $\dim \varphi \leqslant \operatorname{covdim} G$, hence we have equality. □

Here are some elementary properties of covariant dimension. We leave the proofs to the reader.

Remark 2.2.

(a) Let H be a subgroup of G. Then $\operatorname{covdim} H \leqslant \operatorname{covdim} G$.
(b) If G is a product $G_1 \times G_2$, then $\operatorname{covdim} G \leqslant \operatorname{covdim} G_1 + \operatorname{covdim} G_2$.
(c) If G is non-trivial cyclic, then $\operatorname{covdim} G = 1$.

Moreover, Remark 2.2 holds for essential dimension in place of covariant dimension. From [Rei04] we have

Proposition 2.2. *Let G be a finite group. Then* $\operatorname{edim} G \leqslant \operatorname{covdim} G \leqslant \operatorname{edim} G + 1$.

Proof. The first inequality is clear. Let $\varphi : V \to W$ be a rational faithful covariant of minimal dimension. Then there is a non-zero $f \in \mathbb{C}[V]^G$ such that $\Phi := f\varphi$ is a covariant. Now $\overline{\Phi(V)}$ is contained in the cone on $\overline{\operatorname{Im}\varphi}$, so $\operatorname{covdim} G \leqslant \operatorname{edim} G + 1$. □

3. Covariant dimension for abelian groups

Let G be a finite abelian group. We can write $G = G_1 \times G_2 \times \cdots \times G_n$ where G_i is cyclic of order d_i and $d_1|d_2|\cdots|d_n$. Then n is the *rank* of G. In this section we show that $\operatorname{covdim} G = n$. From Remark 2.2 we have $\operatorname{covdim} G \leqslant n$.

Lemma 3.1. *Let p be a prime number and let K be a field of characteristic 0 or p. Let $f_i \in K[x_1, x_2, \ldots, x_n]$, $i = 1, \ldots, n$ be polynomials of the form*

$$f_i = x_i^{j_i} h_i\bigl(x_1^p, x_2^p, \ldots, x_n^p\bigr), \quad 0 < j_i < p.$$

Then the Jacobian determinant $\det(\frac{\partial f_i}{\partial x_j})$ *is non-zero. In particular, $f_1, f_2, \ldots, f_n$ are algebraically independent.*

Proof. (a) If $\operatorname{char} K = p > 0$, then $(\frac{\partial f_i}{\partial x_j})$ is a diagonal matrix with non-zero entries $\frac{\partial f_i}{\partial x_i}$, and the lemma follows.

(b) If $\operatorname{char} K = 0$ we use a "reduction mod p" argument to reduce to case (a). Let $C \subset K$ be the set of coefficients of the polynomials h_i and set $L := \mathbb{Q}(C)$. We can find algebraically independent elements $a_1, \ldots a_m \in L$ such that the elements of C are algebraic over $\mathbb{Q}(a_1, \ldots, a_m)$. By multiplying the polynomials h_i with suitable elements from L we can assume that the elements of C are integral over $\mathbb{Z}[a_1, \ldots, a_m]$. Thus $R := \mathbb{Z}[a_1, \ldots, a_m][C]$ is a free $\mathbb{Z}$-module and $h_i \in R[x_1, \ldots, x_n]$. Then $pR \subsetneqq R$, and we can assume that $h_i \not\equiv 0 \bmod p$. Now it follows from (a) that $\det(\frac{\partial f_i}{\partial x_j}) \not\equiv 0 \bmod p$, hence the lemma. □

Remark 3.1. Lemma 3.1 does not hold if the characteristic of K is positive and prime to p. In fact, $\det(\frac{\partial f_i}{\partial x_j})$ vanishes for $p = 2$, $f_1 := x_1^3$, $f_2 := x_2^3 \in \mathbb{F}_3[x_1, x_2]$. Of course, f_1, f_2 are still algebraically independent, but we do not know if this holds in general.

Recall our decomposition $G = G_1 \times G_2 \times \cdots \times G_n$ where $d := d_1|d_2|\cdots|d_n$ and $d_i = |G_i|$. Fix embeddings $G_i \subset \mathbb{C}^*$. The homomorphism

$$g = (\zeta_1, \zeta_2, \ldots, \zeta_n) \mapsto \begin{bmatrix} \zeta_1 & & & \\ & \zeta_2 & & \\ & & \ddots & \\ & & & \zeta_n \end{bmatrix} \in \mathrm{GL}_n(\mathbb{C})$$

defines a faithful representation of G of dimension n.

Theorem 3.1. *Let G be a finite abelian group of rank n and V a faithful representation of dimension n. Then any faithful covariant $\varphi : V \to V$ is dominant. Hence* $\operatorname{covdim} G = n$.

Proof. It is enough to prove the theorem for the faithful representation defined above. Fix a prime divisor p of d. It suffices to show that the components φ_i of φ are of the form given in Lemma 3.1. Write $\varphi_1 = \sum_{k=0}^{m} h_k(x_2, \ldots, x_n)x_1^k$. Then the h_k's are invariants for the subgroup $G_2 \times \cdots \times G_n$, hence $h_k \in \mathbb{C}[x_2^p, \ldots, x_n^p]$. On the other hand, φ_1 is a covariant for G_1 and so $\varphi_1(\zeta_1 x_1, x_2, \ldots, x_n) = \zeta_1\varphi_1(x_1, x_2, \ldots, x_n)$ for $\zeta_1 \in \mathbb{C}$, which implies that $h_k = 0$ unless $k \equiv 1 \bmod p$. Hence we have that φ_1 is of the form $f_1(x_1^p, x_2^p, \ldots, x_n^p)x_1$, and similarly for $\varphi_2, \ldots, \varphi_n$. □

Remark 3.2. The theorem holds for $\operatorname{edim} G$ in place of $\operatorname{covdim} G$ [BuR97].

4. Faithful groups and irreducible covariants

We investigate conditions under which we may assume that $\operatorname{covdim} G$ is realized by an "irreducible" and homogeneous covariant. We start with the following easy lemma.

Lemma 4.1. *Let $W = \bigoplus_{i=1}^{r} W_i$ be faithful where the W_i are irreducible. Let $\varphi = (\varphi_1, \ldots, \varphi_r)$: $V \to W$ be a covariant. If $\varphi_i \neq 0$, $i = 1, \ldots, r$, then φ is faithful.*

Proof. If φ is not faithful, then $N := \operatorname{Ker}(G \to \operatorname{Aut}(\overline{\varphi(V)}))$ is a non-trivial normal subgroup of G. For some i we must have that $W_i^N = \{0\}$, so that $\varphi_i = 0$. □

Definition 4.1. We say that the covariant $\varphi : V \to W$ is *irreducible* if W is irreducible. We say that the group G is *faithful* if it has a faithful irreducible module.

Note that the symmetric group S_n is faithful as is any product of simple groups. Also, if G is faithful, then by Schur's lemma, the center of G must be a cyclic group. In general, there is the following useful criterion for a finite group G to be faithful, due to Gaschütz [Ga54]. Denote by $N_G \subset G$ the subgroup generated by the minimal elements (under set inclusion) among the non-trivial normal abelian subgroups of G.

Proposition 4.1. *(See [Ga54].) 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.*

Corollary 4.1. *Let G be a non-faithful group and $H \subset G$ a subgroup containing N_G. Then H is non-faithful, too.*

Proof. Since $N_G \subset N_H$ are both products of cyclic groups of prime order we can write $N_H = N_G \times M$ with a suitable normal subgroup $M \subset H$. By Proposition 4.1, N_G cannot be generated by the G-conjugacy class of a single element and so $N_G \times M$ cannot be generated by the H-conjugacy class of a single element. □

Let $\varphi = \sum_{j \leqslant n} \varphi_j : V \to W$ be a covariant where φ_j is homogeneous of degree j, $1 \leqslant j \leqslant n$. Assume that φ_n is not identically zero. We call φ_n the *maximal homogeneous component* and denote it by $\varphi_{\max}$.

Lemma 4.2. *Let $\varphi : V \to W$ be as above. Then* $\dim \varphi_{\max} \leqslant \dim \varphi$.

Proof. Let X denote $\overline{\varphi(V)}$, and let $\mathfrak{p}$ denote the (prime) ideal of X in $\mathcal{O}(W)$. If $f \in \mathfrak{p}$, let $\operatorname{gr} f$ denote the highest degree non-zero homogeneous part of f, and let $\operatorname{gr}\mathfrak{p}$ be the ideal generated by all the $\operatorname{gr} f$, $f \in \mathfrak{p}$. Then $\mathcal{C}X$, the associated cone of X, is the zero set of $\operatorname{gr}\mathfrak{p}$, and $\dim X = \dim \mathcal{C}X$ (see [Kr85]). We show that $\operatorname{Im}\varphi_{\max} \subset \mathcal{C}X$, which gives the lemma.

Let $f = \sum_{i=0}^{m} f_m$ be in $\mathfrak{p}$, where $\operatorname{gr} f = f_m \neq 0$. Then for $v \in V$, $0 \neq t \in \mathbb{C}$ we have $0 = f(\varphi(t^{-1}v))$ which implies that

$$f_m\big(\varphi\big(t^{-1}v\big)\big) = -\sum_{j=0}^{m-1} f_j\big(\varphi\big(t^{-1}v\big)\big).$$

Multiplying both sides by t^{nm}, where $n = \deg\varphi$, we obtain

$$f_m\big(t^n\varphi\big(t^{-1}v\big)\big) = -\sum_{j=0}^{m-1} t^{n(m-j)} f_j\big(t^n\varphi\big(t^{-1}v\big)\big).$$

Letting t go to zero we see that the left-hand side above converges to $f_m(\varphi_{\max}(v))$ and the right-hand side converges to zero. Thus f_m vanishes on $\operatorname{Im}\varphi_{\max}$, i.e., $\operatorname{Im}\varphi_{\max} \subset \mathcal{C}X$. □

If φ is faithful, it is not clear that $\varphi_{\max}$ is also. However, for faithful groups this is almost automatic. In fact, we have the following result which is an immediate consequence of Lemmas 4.1 and 4.2.

Proposition 4.2. *Let G be faithful with irreducible faithful G-module W and faithful G-module V. Then there is a homogeneous minimal covariant $\varphi : V \to W$.*

Remark 4.1. Starting with a faithful representation V we cannot always guarantee that there is a faithful homogeneous covariant $\varphi : V \to V$ with minimal dimension. Let $V = \mathbb{C}^2$ where $\mathbb{Z}/2$ (respectively $\mathbb{Z}/3$) acts by multiplication by roots of unity on the first (respectively second) copy of $\mathbb{C}$. Let x and y be coordinate functions on V. Then a faithful minimal covariant for $G := \mathbb{Z}/2 \times \mathbb{Z}/3$ is $\varphi(x, y) = (x^3y^3, x^4y^4)$. Suppose that we had a homogeneous faithful covariant ψ. Then for some $(x_0, y_0) \in V$, $\psi(x_0, y_0) = (x_1, y_1)$ where $x_1y_1 \neq 0$. By equivariance, $\psi(-x_0, y_0) = (-x_1, y_1)$. Thus the image of ψ, which is a cone, contains two linearly independent vectors. It follows that $\overline{\operatorname{Im}\psi} = V$ and so $\dim\psi = 2 > \operatorname{covdim} G = 1$.

Corollary 4.2. *Let G be a faithful group with trivial center. Then*

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

Proof. Let $\varphi : V \to V$ be a homogeneous minimal covariant. Then the rational covariant $\psi : V \to V \to \mathbb{P}(V)$ is faithful of dimension $\operatorname{covdim} G - 1$. □

The usefulness of the existence of *homogeneous* minimal covariants for calculating the covariant dimension is shown by Proposition 4.3 below. We first need a definition. For a set X, let $|X|$ denote its cardinality and let Id_X denote the identity map of X.

Definition 4.2. Let V be a G-module and $\rho_V : G \to \mathrm{GL}(V)$ the corresponding representation. Define

$$z_G(V) = z(V) := \left|\rho_V(G) \cap \mathbb{C}^* \operatorname{Id}_V\right|.$$

If V is irreducible and faithful, we have $z_G(V) = |Z(G)|$.

Proposition 4.3. *Assume that G has a homogeneous minimal covariant $\varphi : V \to V$. If $m > 0$ is coprime to $z_G(V)$, then* $\operatorname{covdim} G \times \mathbb{Z}/m = \operatorname{covdim} G$.

For the proof we will use the following result.

Lemma 4.3. *There is an integer $n_0 > 0$ and an open dense set $V' \subset V$ with the following property: for every $n \geqslant n_0$ there is a homogeneous invariant $h \in \mathcal{O}(V)^G$ of degree $n \cdot z_G(V)$ which has no zeroes on V'.*

Proof. Set $d := z_G(V)$. Let $M \subset \mathbb{N}$ be the monoid of degrees of homogeneous elements of $\mathcal{O}(V)^G$. By assumption, we have $M \subset d\mathbb{N}$, and so the subgroup $\langle M\rangle \subset \mathbb{Z}$ generated by M equals $d'\mathbb{Z}$ for some multiple d' of d. It follows that all G-invariants are also invariant under $\mu_{d'} \subset \mathbb{C}^*$, the d'th roots of unity. Thus $\mu_{d'} \subset \rho_V(G)$ and so $d' = d$.

Since $\langle M\rangle = d\mathbb{Z}$ we can find two homogeneous invariants $h_1, h_2 \in \mathcal{O}(V)^G$ with $\gcd(\deg h_1, \deg h_2) = d$. Therefore, for every n large enough there is a monomial $h_1^\alpha h_2^\beta$ of degree $n \cdot d$. The lemma now follows by setting V' to be the complement of the zero set of $h_1 h_2$. □

Proof of Proposition 4.3. Let $f \in \mathcal{O}(V)^G$ be a non-zero homogeneous invariant. Then $f \cdot \varphi : V \to V$ is again a homogeneous faithful covariant of minimal dimension. In fact, there is a $v \in V$ such that $f(v) \neq 0$ and such that $\varphi(v)$ has a trivial stabilizer. Then the same holds for any non-zero multiple $\lambda\varphi(v)$ and, in particular, for $f(v)\varphi(v)$. Thus $f \cdot \varphi$ is faithful. Since φ is homogeneous the image $\varphi(V)$ is a cone and so $(f \cdot \varphi)(V) \subset \varphi(V)$, hence $f \cdot \varphi$ is of minimal dimension.

The covariant $f \cdot \varphi$ has degree $\deg\varphi + \deg f$ which, by Lemma 4.3, can be any number of the form $\deg\varphi + n \cdot z_G(V)$ for $n \geqslant n_0$. Since m is coprime to $z_G(V)$ there is an $n \geqslant n_0$ such that $\deg\varphi + n \cdot z_G(V)$ is divisible by m. For the corresponding covariant $f \cdot \varphi$ this implies that it is also equivariant with respect to the scalar action of $\mathbb{Z}/m$ on V, and so $f \cdot \varphi$ is a covariant for $G \times \mathbb{Z}/m$. □

Corollary 4.3. *If G is faithful and $m > 0$ coprime to $|Z(G)|$, then* $\operatorname{covdim} G \times \mathbb{Z}/m = \operatorname{covdim} G$. *Moreover, $G \times \mathbb{Z}/m$ is faithful.*

Corollary 4.4. *Let $G = \mathbb{Z}/3^\ell \ltimes A$, $\ell \geqslant 1$, where A is a finite abelian 2-group of rank 2 and a generator a of $\mathbb{Z}/3^\ell$ acts non-trivially on A. Then* $\operatorname{covdim} G \geqslant 3$.

Proof. Denote by α the automorphism of A induced by a. We can assume that α is trivial on $2A$ since otherwise $2A$ has again rank 2 and we can replace G by the subgroup $\mathbb{Z}/3^\ell \ltimes 2A$. Then the

induced automorphism on $A/2A$ is non-trivial since the order of α is not a power of 2. It follows that the automorphism α is given by a matrix of the form

$$\begin{bmatrix} 2r & 1+2s \\ 1+2t & 1+2u \end{bmatrix}$$

with respect to suitable generators of A. Since α is the identity on $2A$ we get $2A = 0$ and so $A \simeq \mathbb{Z}/2 \oplus \mathbb{Z}/2$. It follows from Gaschütz's Criterion (Proposition 4.1) that G is faithful: $N_G = \langle a^3, (\mathbb{Z}/2)^2 \rangle$ and is generated by the conjugates of $a^3 \cdot (1,0)$. The center $Z(G)$ is generated by a^3 and so $\operatorname{covdim} G = \operatorname{covdim} G \times \mathbb{Z}/2 \geqslant \operatorname{covdim}(\mathbb{Z}/2)^3 = 3$. □

5. Existence of homogeneous covariants

If $v \in V$ is a *principal* point, i.e., the stabilizer of v equals the kernel of $\rho_V : G \to \mathrm{GL}(V)$, and $w \in V$ is arbitrary, we can always find a covariant $\varphi : V \to V$ such that $\varphi(v) = w$ (see Lemma 2.1). In order to find a *homogeneous* covariant with this property, we need an additional assumption.

Proposition 5.1. *Let V be a G-module and let $v \in V$ be a principal point such that the corresponding point $[v] \in \mathbb{P}(V)$ is also principal. Let w be another point of V. Then there is a homogeneous covariant $\varphi : V \to V$ such that $\varphi(v) = w$.*

For the proof we need the following result which is probably well known.

Lemma 5.1. *Let V be a vector space of dimension $\geqslant 2$ and $v_1, v_2, \ldots, v_s \in V$ pairwise linearly independent elements. If $r \geqslant s-1$, then $v_1^r, \ldots, v_s^r \in S^r V$ are linearly independent.*

Proof. (a) We first consider the case $\dim V = 2$. By choosing a suitable basis and multiplying the v_i's with scalars if necessary we can assume that $v_i = (1, b_i)$, $i = 1, \ldots, s$. Then $v_i^r = (1, b_i, b_i^2, \ldots, b_i^r) \in S^r(V) \simeq \mathbb{C}^{r+1}$ and linear independence follows from the non-singularity of the Vandermonde matrix (b_i^j).

(b) There is always a linear projection $\rho : V \to W$, $\dim W = 2$, such that the images $\rho(v_1), \ldots, \rho(v_s)$ are pairwise linearly independent. So the general case follows from part (a). □

Proof of Proposition 5.1. Define $H := \{g \in G \mid gv \text{ is a scalar multiple of } v\}$. By assumption, $H = \operatorname{Ker}(G \to \mathrm{PGL}(V))$. We have a character χ of H, where $h \cdot v' = \chi(h)v'$ for any $v' \in V$. Let $g_1 H, \ldots, g_s H$ be the set of left cosets of H where $g_1 = e$. Then, by Lemma 5.1, the elements $g_i \cdot v$ give rise to linearly independent elements $g_i \cdot v^r$ of $S^r V$, for $r \geqslant s-1$. Choose r to be congruent to 1 modulo $d := |H|$. Then the submodule $W := \operatorname{span}\{v^r, g_2 \cdot v^r, \ldots, g_s \cdot v^r\} \subset S^r V$ is isomorphic to the representation $\operatorname{Ind}_H^G \mathbb{C}_\chi$ induced from the character χ of H. Now there is a linear H-equivariant map $\mathbb{C}_\chi \to V$ such that $1 \mapsto w$, and so the induced map $W \xrightarrow{\sim} \operatorname{Ind}_H^G \mathbb{C}_\chi \to V$ is G-equivariant and sends v^r to w. It follows that the composition

$$V \xrightarrow{v \mapsto v^r} S^r V \xrightarrow{\mathrm{pr}} W \xrightarrow{\sim} \operatorname{Ind}_H^G \mathbb{C}_\chi \to V$$

is the required homogeneous covariant, where pr is equivariant projection onto W. □

Remark 5.1. One can establish a more general form of the proposition. For $v \in V$ let $\tilde{G}_v := \{g \in G \mid g \cdot v = \lambda v \text{ for some } \lambda\}$. There is the obvious character $\chi_v : \tilde{G}_v \to \mathbb{C}^*$. Let W be another G-module and $w \in W$. Then the following are equivalent:

(a) $\tilde{G}_v \subset \tilde{G}_w$ and $\chi_w(g) = \chi_v(g)^d$ for all $g \in \tilde{G}_v$ and for some $d \in \mathbb{N}$.
(b) There is a homogeneous covariant $\varphi : V \to W$ such that $\varphi(v) = w$.

Now we can prove the existence of a homogeneous minimal covariant under some additional assumption on the faithful representation V without assuming that V is irreducible. We first need a lemma about the degree of a covariant.

Lemma 5.2. *If $\varphi : V \to V$ is a covariant, then* $\deg \varphi \equiv 1 \bmod z_G(V)$.

Proof. Since every homogeneous component of φ is a covariant we can assume that φ is homogeneous, say of degree d. Then $\varphi(t \cdot v) = t^d \cdot \varphi(v)$ for all $t \in \mathbb{C}$, $v \in V$. Now choose $g \in G$ so that $\rho_V(g) = \zeta \operatorname{Id}_V$ where ζ is a primitive $z(V)$th root of unity. Then we have

$$\varphi(gv) = \varphi(\zeta \cdot v) = \zeta^d \cdot \varphi(v) \quad \text{and} \quad g\varphi(v) = \zeta \cdot \varphi(v)$$

for all $v \in V$. Hence, $\zeta^d = \zeta$ which implies that $d \equiv 1 \bmod z(V)$, as claimed. □

Proposition 5.2. *Let V be a faithful representation and let $V = \bigoplus_{i=1}^n V_i$ be a decomposition into irreducible submodules. Assume that $z(V_i) = z(V)$ for $i < n$ and that every prime divisor of $z(V_n)$ divides $z(V)$. Then there is a homogeneous minimal covariant $\varphi : V \to V$.*

Proof. We give the proof for $n = 2$ and leave the obvious generalization to the reader. Let $\varphi : V \to V$ be a faithful minimal covariant. We can clearly assume that the two components φ_1, φ_2 are both non-zero. If $\deg \varphi_1 = \deg \varphi_2$ then we are done: $\varphi_{\max}$ has two non-zero components $\varphi_{1\max}$ and $\varphi_{2\max}$, hence is faithful (Lemma 4.1), and $\dim \varphi_{\max} \leqslant \dim \varphi$ by Lemma 4.2.

We reduce to the case above by composing φ with a covariant ψ of the form

$$\psi(v_1, v_2) = \big(f_1(v_1)v_1,\, f_2(v_2)v_2\big) = \big(\psi_1(v_1), \psi_2(v_2)\big), \tag{1}$$

where $f_1 \in \mathcal{O}(V_1)^G$ and $f_2 \in \mathcal{O}(V_2)^G$ are homogeneous invariant functions, so that the two components of the composition $\varphi \circ \psi$ are both non-zero and have the same degree.

It follows from Lemma 4.3 applied to the two representations V_1 and V_2 that there are open dense subsets $V_1' \subset V_1$, $V_2' \subset V_2$ and an integer $n_0 > 0$ such that, for every $n \geqslant n_0$ there are homogeneous invariants $f_i \in \mathcal{O}(V_i)^G$ of degree $nz(V_i)$ which have no zeroes in V_i' $(i = 1, 2)$.

Since V_i is irreducible, the image of $\varphi_{i_{\max}} : V \to V_i$ contains a principal point v_i such that $[v_i] \in \mathbb{P}(V_i)$ is also principal. By Proposition 5.1, there is a homogeneous covariant $\mu_i : V_i \to V_i$ such that $\mu_i(v_i) \in V_i'$. Replacing φ_i by the composition $\mu_i \circ \varphi_i$ we can therefore assume that the image of $\varphi_{i_{\max}}$ meets V_i' $(i = 1, 2)$. Then the compositions $\psi_i \circ \varphi_{i_{\max}}$ are non-zero if the invariants f_i in Eq. (1) are chosen according to Lemma 4.3. Set $\tilde{\varphi}_i := \psi_i \circ \varphi_i$, $i = 1, 2$. We have

$$\deg \tilde{\varphi}_1 = \deg \varphi_1 \cdot (1 + \deg f_1) \quad \text{and} \quad \deg \tilde{\varphi}_2 = \deg \varphi_2 \cdot (1 + \deg f_2).$$

Now $\deg \varphi_i = 1 + a_i \cdot z(V)$ (Lemma 5.2), and so we have to solve the equation

$$\big(1 + xz(V_1)\big)\big(1 + a_1 z(V)\big) = \big(1 + yz(V_2)\big)\big(1 + a_2 z(V)\big)$$

with integers $x, y \geqslant n_0$ which is possible by the following lemma. □

Lemma 5.3. *Let $d, d_1, d_2, a_1, a_2 \in \mathbb{N}$. Assume that $d|d_1|d_2$ and that d_2 has the same prime divisors as d (i.e., $d_2|d^N$ for large N). Then the equation*

$$(1 + a_1 d)(1 + x d_1) = (1 + a_2 d)(1 + y d_2)$$

has a solution $x, y \in \mathbb{N}$ if and only if $a_1 \equiv a_2 \bmod d_1/d$. Moreover, x and y can be chosen to be arbitrarily large.

Proof. The equation implies that $a_1 d \equiv a_2 d \bmod d_1$, hence $a_1 \equiv a_2 \bmod d_1/d$. Conversely, assume that $a_1 d \equiv a_2 d \bmod d_1$. Then $1 + a_1 d \equiv 1 + a_2 d \bmod d_1$. Moreover, $1 + a_1 d$ is invertible mod d_2 and so there is an $m \in \mathbb{N}$ such that $(1 + a_1 d)m \equiv 1 \bmod d_2$. It follows that $(1 + a_2 d)m \equiv 1 \bmod d_1$, hence

$$(1 + a_1 d)m = 1 + y d_2 \quad \text{and} \quad (1 + a_2 d)m = 1 + x d_1$$

for some $x, y \in \mathbb{N}$, and so $(1 + a_1 d)(1 + x d_1) = (1 + a_2 d)(1 + y d_2)$. The last statement is clear. □

Corollary 5.1. *Let M be a finite abelian group of rank k whose order is odd, and let $G := \mathbb{Z}/2^s \ltimes M$, $s \geqslant 1$, be a semidirect product where a generator a of $\mathbb{Z}/2^s$ acts on M by sending each element to its inverse. Then* $\operatorname{covdim} G \geqslant k + 1$.

Proof. Replacing G by a suitable subgroup we can assume that $M = (\mathbb{Z}/p)^k$. The group $\bar{G} := \mathbb{Z}/2^s \ltimes \mathbb{Z}/p$ has a two-dimensional faithful irreducible representation. Using the k copies of $\mathbb{Z}/p$ we therefore obtain k irreducible representations $V_1, \ldots, V_k$ of G such that $V := \bigoplus_i V_i$ is faithful. The center $\bar{Z}$ of $\bar{G}$ is generated by a^2 and is isomorphic to $\mathbb{Z}/2^{s-1}$. Thus, the assumptions of Proposition 5.2 are satisfied with $z(V) = z(V_i) = 2^{s-1}$, and we can find a homogeneous minimal covariant $\varphi : V \to V$. Hence, by Corollary 4.3 and Theorem 3.1, $\operatorname{covdim} G = \operatorname{covdim} G \times \mathbb{Z}/p \geqslant \operatorname{covdim}(\mathbb{Z}/p)^{k+1} = k + 1$. □

6. Products with cyclic groups

We have seen in Section 4 that $\operatorname{covdim} G \times \mathbb{Z}/p = \operatorname{covdim} G$ if G is faithful and p is coprime to $|Z(G)|$. We will show now that $\operatorname{covdim} G \times \mathbb{Z}/p = \operatorname{covdim} G + 1$ if p is a divisor of $|Z(G)|$. More generally, we have the following.

Proposition 6.1. *Let $V = W \oplus \mathbb{C}_\chi$ be a faithful representation of G where W is irreducible and χ is a character of G. Assume that $z(W)$ and $|\chi(G)|$ have the same prime divisors as $z(V)$ and that either $z(W) = z(V)$ or $|\chi(G)| = z(V)$. If the kernel H of the action of G on W is non-trivial, then* $\operatorname{covdim} G = \operatorname{covdim} G/H + 1$.

Proof. By assumption, we have an embedding $G \hookrightarrow G/H \times \chi(G)$. Since $\chi(G)$ is cyclic we get $\operatorname{covdim} G \leqslant \operatorname{covdim}(G/H \times \chi(G)) \leqslant \operatorname{covdim} G/H + 1$.

For the reverse inequality, we consider a faithful covariant $\varphi : V \to V$ of minimal dimension. By Proposition 5.2 we can assume that φ is homogeneous. Set $m := |\chi(G)|$. We have $\varphi(w,t) = (F(w,t^m), t \cdot h(w,t^m))$ where h is a G-invariant function. If $F(w,0) = h(w,0) = 0$, then, because φ is homogeneous, we can divide it by t^m without changing its dimension or faithfulness. Thus we can assume that either $F(w,0) \neq 0$ or $h(w,0) \neq 0$. In the first case, $\varphi|_W : W \to W$ is non-zero, hence a faithful covariant of G/H. Since $\varphi(W) \subset \varphi(V)^H \subsetneq \varphi(V)$ we see that $\dim \overline{\varphi(V)} > \dim \overline{\varphi(W)} \geqslant \operatorname{covdim} G/H$, as desired.

If $h(w,0) \neq 0$ and $F(w,t^m) = t^{sm} F_0(w,t^m)$, $s \geqslant 1$, where $F_0(w,0) \neq 0$ we define

$$\psi(w,t) := \left(\frac{F(w,t)}{(t \cdot h(w,t^m))^{sm}}, t \cdot h\big(w,t^m\big) \right) = \left(\frac{F_0(w,t)}{h(w,t^m)^{sm}}, t \cdot h\big(w,t^m\big) \right).$$

The equivariant morphism $\psi = (\psi_1, \psi_2)$ is defined on the dense open set $V_h \subset V$ where h does not vanish. Moreover, $\dim \overline{\psi(V_h)} = \dim \overline{\varphi(V)} = \operatorname{covdim} G$, because ψ_1 and ψ_2 generate the same subfield of $\mathbb{C}(V)$ as the two components of φ. By definition, $\psi_1(w,0) \neq 0$, and $\psi(W_h) = \psi_1(W_h) = F_0(W_h)$ since ψ_1 is homogeneous of non-zero degree. Since $F_0|_W : W \to W$ is a non-zero (hence faithful) covariant for G/H, we get $\dim \overline{\psi(W_h)} \geqslant \operatorname{covdim} G/H$. Finally, $\overline{\psi(W_h)} \subset \overline{\psi(V_h)}^H \subsetneq \overline{\psi(V_h)}$, and so

$$\operatorname{covdim} G = \dim \overline{\psi(V_h)} > \dim \overline{\psi(W_h)} \geqslant \operatorname{covdim} G/H. \qquad \square$$

Remark 6.1. The proof above has two parts. First one shows that there is a homogeneous minimal covariant $\varphi : V \to V$ for $V = W \oplus \mathbb{C}_\chi$, and then one proves the inequality $\operatorname{covdim} G \geqslant \operatorname{covdim} G/H + 1$. The assumptions about $z_G(V)$, $z_G(W)$ and $|\chi(G)|$ are only used in the first part. Once the existence of a homogeneous minimal covariant φ is established, then the proof above applies if the action of G on W has a non-trivial kernel H.

Corollary 6.1. *Let G be a faithful group and p a prime divisor of $|Z(G)|$. Then* $\operatorname{covdim} G \times \mathbb{Z}/p = \operatorname{covdim} G + 1$.

Proof. This follows from the proposition above by choosing for W an irreducible faithful representation of G (with trivial action of $\mathbb{Z}/p$) and for χ the standard character $r \mapsto e^{2\pi i \frac{r}{p}}$ of $\mathbb{Z}/p$. $\square$

Corollary 6.2. *If H is a faithful group and q a prime which does not divide $|Z(H)|$, then* $\operatorname{covdim} H \times (\mathbb{Z}/q)^2 = \operatorname{covdim} H + 1$.

Proof. This is clear from Corollary 6.1: Take $G = H \times \mathbb{Z}/q$. Then G is faithful and $\operatorname{covdim} G = \operatorname{covdim} H$. $\square$

We finish this section with a result on the covariant dimension of the semi-direct product of two cyclic 2-groups. In the proof we will need a modification of the proof of Proposition 5.2 in order to reduce to a homogeneous minimal covariant.

Proposition 6.2. *Let $G = \mathbb{Z}/2^k \ltimes \mathbb{Z}/2^\ell$, $k, \ell \geqslant 1$. If G is commutative or $k = 1$, then* $\operatorname{covdim} G = 2$. *Otherwise,* $\operatorname{covdim} G \geqslant 3$.

Proof. (a) We can assume that G is not commutative and so $\ell \geqslant 2$. Let a be a generator of $\mathbb{Z}/2^k$, let b be a generator of $\mathbb{Z}/2^\ell$, and denote by α the (non-trivial) automorphism induced by a on $\mathbb{Z}/2^\ell$. If $k = 1$, then $\alpha(b) = b^{-1}$ if $l = 2$ and $\alpha(b) = b^{-1}$, $b^{2^{l-1}+1}$ or $b^{2^{l-1}-1}$ if $l > 2$, and one easily constructs a faithful representation on $\mathbb{C}^2$, see part (b). Thus we may assume that $k \geqslant 2$. We now show that $\operatorname{covdim} G \geqslant 3$.

(b) We may assume that α acts trivially on $2\mathbb{Z}/2^\ell$, and then it follows that α has order 2 and sends b to $b^{2^{l-1}+1}$. Let ξ be a primitive 2^ℓth root of unity and let τ be a primitive 2^kth root of unity, We have the irreducible representation ρ_W of G on $W := \mathbb{C}^2$ where b acts by the diagonal matrix $\left[\begin{smallmatrix} \xi & 0 \\ 0 & \xi^{2^{l-1}+1} \end{smallmatrix}\right]$ and a acts by the matrix $\left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right]$. We also have the character $\chi : G \to \mathbb{C}^*$ defined by $\chi(a) := \tau$ and $\chi(b) := 1$. The direct sum $V := W \oplus \mathbb{C}_\chi$ is a faithful representation ρ of G, so, clearly, $\operatorname{covdim} G \leqslant 3$. We have $z_G(W) = 2^{\ell-1}$ since $\rho_W(b^2)$ is a scalar matrix.

If $k \geqslant \ell$ we can assume that $\xi = \tau^{2^{k-\ell}}$. Then $\rho(b^2 a^{2^{k-\ell+1}}) = \xi^2 \operatorname{Id}_V$ and so $z_G(V) = 2^{\ell-1} = z_G(W)$. Thus we can apply Proposition 6.1 and find that $\operatorname{covdim} G = \operatorname{covdim} \rho_W(G) + 1 = 3$.

There remains the case where $k < l$. Then we set $\tau = \xi^{2^{\ell-k}}$ and find that the scalar matrices in $\rho(G)$ are generated by $\rho(a^2 b^{2^{\ell-k+1}})$. Thus $z_G(V) = 2^{k-1} < z_G(\mathbb{C}_\chi) = 2^k \leqslant z_G(W) = 2^{\ell-1}$ and we cannot apply Proposition 6.1 directly, but need a modification.

Let $\varphi = (F, h) : V \to V$ be a minimal covariant where $F : V \to W$ and $h : V \to \mathbb{C}_\chi$ are G-equivariant. If $\deg F = \deg h$, then $\varphi_{\max} = (F_{\max}, h_{\max})$ is again faithful and minimal, and we may proceed as in Proposition 6.1 (see Remark 6.1).

In general, $\deg F$ and $\deg h$ are both $\equiv 1 \bmod 2^{k-1}$, by Lemma 5.2. Consider the two homogeneous invariants $f_1(x, y) := xy^{2^{\ell-1}-1} + yx^{2^{\ell-1}-1} \in \mathcal{O}(W)^G$ and $f_2(t) := t^{2^k} \in \mathcal{O}(\mathbb{C}_\chi)^G$ of degree $2^{\ell-1}$ and 2^k, respectively, and the corresponding covariants

$$\psi = \left(f_1^u \operatorname{Id}_W, f_2^v \operatorname{Id}_{\mathbb{C}_\chi}\right) : V \to V$$

where $u, v \in \mathbb{N}$. Clearly, $h_{\max}$ and h are dominant, as are $F_{\max}$ and F (else we get that $\operatorname{covdim} \rho_W(G) \leqslant 1$). Thus the composition $\tilde{\varphi} := \psi \circ \varphi$ is faithful and the two components $\tilde{F} = f_1(F)^u \cdot F$ and $\tilde{h} = f_2(h)^v \cdot h$ have degrees

$$\deg \tilde{F} = \left(1 + u2^{\ell-1}\right) \deg F \quad \text{and} \quad \deg \tilde{h} = \left(1 + v2^k\right) \deg h.$$

Setting $\deg F = (1 + r2^{k-1})$ and $\deg h = (1 + s2^{k-1})$ it suffices to solve the equation

$$\left(1 + r2^{k-1}\right)\left(1 + u2^{\ell-1}\right) = \left(1 + s2^{k-1}\right)\left(1 + v2^{\ell-1}\right). \tag{2}$$

By Lemma 5.3 this is possible if and only if r and s have the same parity, i.e., if and only if $\deg F \equiv \deg h \bmod 2^k$. (In the notation of that lemma we have $d = 2^{k-1}$, $d_1 = 2^k$, $d_2 = 2^{\ell-1}$.)

If $\deg F \not\equiv \deg h \bmod 2^k$, consider the following G-invariant function on V:

$$f(x, y, t) := \left(xy^{2^{\ell-1}-1} - x^{2^{\ell-1}-1} y\right) t^{2^{k-1}}.$$

Then f is bihomogeneous of degree $(2^{\ell-1}, 2^{k-1})$. Since $h_{\max} \neq 0$ and $F_{\max}$ is dominant, $f(F_{\max}, h_{\max})$ is non-zero and $\tilde{F} := f(F, h) \cdot F : V \to W$ has degree

$$\deg \tilde{F} = \left(2^{\ell-1} + 1\right) \deg F + 2^{k-1} \deg h \equiv \left(1 + (r+1)2^{k-1}\right) \mod 2^k.$$

As a consequence, $\tilde{\varphi} := (\tilde{F}, h)$ is a minimal covariant and $\deg \tilde{F} \equiv \deg h \bmod 2^k$. Now we can apply Lemma 5.3 and solve Eq. (2). This finishes the proof. □

7. Covariant dimension and essential dimension for S_n and A_n

If we put together our results so far for the faithful groups S_n ($n \geqslant 3$) and A_n ($n \geqslant 4$) we have the following.

Theorem 7.1. *Let $n \geqslant 3$.*

(a) $\operatorname{covdim} S_n = \operatorname{edim} S_n + 1$;
(b) $\operatorname{covdim} S_n \times \mathbb{Z}/d = \operatorname{covdim} S_n$ *for* $d \geqslant 2$;
(c) $\operatorname{covdim} S_n \geqslant \lfloor n/2 \rfloor + 1$;
(d) $\operatorname{covdim} S_{n+2} \geqslant \operatorname{covdim} S_n + 1$.

Theorem 7.2. *Let $n \geqslant 4$.*

(a) $\operatorname{covdim} A_n = \operatorname{edim} A_n + 1$;
(b) $\operatorname{covdim} A_n \times \mathbb{Z}/d = \operatorname{covdim} A_n$ *for* $d \geqslant 2$;
(c) $\operatorname{covdim} A_n \geqslant 2\lfloor n/4 \rfloor + 1$;
(d) $\operatorname{covdim} A_{n+4} \geqslant \operatorname{covdim} A_n + 2$.

Proof of Theorems 7.1 and 7.2. Parts (a) and (b) follow from Corollaries 4.2 and 4.3. For part (c) we use (b) and Theorem 3.1. Since $S_{2m} \supset (\mathbb{Z}/2)^m$, we have $\operatorname{covdim} S_n = \operatorname{covdim} S_n \times \mathbb{Z}/2 \geqslant \operatorname{covdim}((\mathbb{Z}/2)^{\lfloor n/2 \rfloor + 1}) = \lfloor n/2 \rfloor + 1$. One proceeds similarly for A_n using that $A_{4m} \supset (\mathbb{Z}/2)^{2m}$.

Finally, for part (d) we have $\operatorname{covdim} S_{n+2} = \operatorname{covdim} S_{n+2} \times \mathbb{Z}/2 \geqslant \operatorname{covdim}(S_n \times (\mathbb{Z}/2)^2) \geqslant \operatorname{covdim}(S_n \times \mathbb{Z}/2) + 1 = (\operatorname{covdim} S_n) + 1$, by Corollary 6.1, and similarly for A_n. □

These results allow us to determine the covariant dimension for the small symmetric and alternating groups. Just recall that $\operatorname{covdim} A_n \leqslant \operatorname{covdim} S_n \leqslant n - 1$ since there is a faithful $(n-1)$-dimensional representation.

$$\operatorname{covdim} S_2 = \operatorname{covdim} A_3 = 1, \qquad \operatorname{covdim} S_3 = 2, \qquad \operatorname{covdim} A_4 = \operatorname{covdim} S_4 = 3.$$

We will see below that $\operatorname{covdim} S_n \leqslant n - 2$ for $n \geqslant 5$, hence

$$\operatorname{covdim} A_5 = \operatorname{covdim} S_5 = 3 \quad \text{and} \quad \operatorname{covdim} S_6 = 4.$$

The first unknown cases are $\operatorname{covdim} A_6$ which is either 3 or 4, and $\operatorname{covdim} S_7$ which is either 4 or 5:

n	2	3	4	5	6	7
$\operatorname{covdim} S_n$	1	2	3	3	4	4 or 5
$\operatorname{covdim} A_n$		1	3	3	3 or 4	

8. Upper bounds for the covariant dimension

Let G be finite group and V a G-module such that the G-action normalizes a reductive subgroup H of $\mathrm{GL}(V)$. Then we can form the *algebraic quotient*

$$\pi : V \to V/\!\!/H$$

which has coordinate ring $\mathcal{O}(V/\!\!/H) := \mathcal{O}(V)^H \subset \mathcal{O}(V)$ (see [Kr85]). Since G normalizes H the invariant ring is G-stable and the quotient morphism π is G-equivariant, hence a compression.

Lemma 8.1. *If the action of G on $V/\!\!/H$ is faithful, then*

$$\operatorname{covdim} G \leqslant \dim V/\!\!/H \leqslant \dim V - \max\{\dim Hv \mid v \in V\}.$$

Proof. We can find a finite-dimensional G-stable subspace W of $\mathcal{O}(V)^H$ which generates $\mathcal{O}(V)^H$. The associated morphism $\varphi : V \to W^*$ has image isomorphic to the quotient $V/\!\!/H$. Since φ maps V onto $V/\!\!/H$ and since G acts faithfully on $V/\!\!/H$, the covariant φ is faithful. The fibers of φ have dimension $\geqslant \max\{\dim Hv \mid v \in V\}$, so that $\operatorname{covdim} G \leqslant \dim V/\!\!/H \leqslant \dim V - \max\{\dim Hv \mid v \in V\}$. □

Proposition 8.1. *For $n \geqslant 5$ we have* $\operatorname{covdim} A_n \leqslant \operatorname{covdim} S_n \leqslant n-2$.

For the proof we use the following construction which will also play a central role in Section 9.

Start with the standard representation of SL_2 on $\mathbb{C}^2$, and let $T' \subset \mathrm{SL}_n$ be the group of diagonal matrices of determinant 1. Then $H := \mathrm{SL}_2 \times T'$ acts linearly on $V_n := \mathbb{C}^2 \otimes \mathbb{C}^n$. There is also the standard action of S_n by permutations on $\mathbb{C}^n$, hence on V_n which normalizes the action of T' and commutes with the action of SL_2.

We may regard an element of V_n as an n-tuple of elements in $\mathbb{C}^2$, so there is a canonical surjective morphism $\mu : V_n \to S^n(\mathbb{C}^2)$ given by multiplying the elements of $\mathbb{C}^2$. This morphism is the quotient by the group $S_n \cdot T'$, and is equivariant with respect to SL_2.

Consider the quotient $\pi : V_n \to X_n := V_n/\!\!/H$. Since S_n normalizes H it acts on the quotient X_n and π is S_n-equivariant. By construction, we have a canonical isomorphism $X_n/S_n \xrightarrow{\sim} S^n(\mathbb{C}^2)/\!\!/\mathrm{SL}_2$. Moreover, the quotient morphism π can be decomposed into $\eta : V_n \to Y_n := V_n/\!\!/\mathrm{SL}_2$, the quotient by SL_2, and $\rho : Y_n \to Y_n/\!\!/T' = X_n$, the quotient by T', so that we obtain the following commutative diagram:

$$\begin{array}{ccc}
V_n & \xrightarrow[\mu]{/\!\!/ S_n \cdot T'} & S^n(\mathbb{C}^2) \\
{\scriptstyle \eta}\downarrow{\scriptstyle /\!\!/ \mathrm{SL}_2} & & {\scriptstyle \pi''}\downarrow{\scriptstyle /\!\!/ \mathrm{SL}_2} \\
Y_n & \xrightarrow{/\!\!/ S_n \cdot T'} & S^n(\mathbb{C}^2)/\!\!/\mathrm{SL}_2 \\
{\scriptstyle \rho}\downarrow{\scriptstyle /\!\!/ T'} & & \| \\
X_n & \xrightarrow[\pi']{/S_n} & S^n(\mathbb{C}^2)/\!\!/\mathrm{SL}_2
\end{array}$$

The generic T'-orbit on V_n is closed with trivial stabilizer, and for $n \geqslant 3$ the generic SL_2-orbit on $S^n(\mathbb{C}^2)$ is closed with finite stabilizer. Thus, for $n \geqslant 3$, the generic H-orbit on V_n is closed and one easily sees that it has a trivial stabilizer. It follows that

$$\dim X_n = \dim V - \max\{\dim Hv \mid v \in V\} = 2n - (n-1+3) = n-2.$$

The following proposition collects properties of the morphisms and quotient maps above.

Proposition 8.2. *Consider the representation $V_n := \mathbb{C}^2 \otimes \mathbb{C}^n$ of $H := \mathrm{SL}_2 \times T'$ where $T' \subset \mathrm{SL}_n$ is the subgroup of diagonal matrices, and let $\pi : V_n \to X_n := V_n /\!\!/ H$ be the quotient.*

(a) *The natural action of S_n on V_n normalizes H, the quotient π is S_n-equivariant and* $\dim X_n = n-2$ *for $n \geqslant 3$.*
(b) *The quotient of V_n by SL_2 is given by the map $\eta : f_1 \otimes v_1 + f_2 \otimes v_2 \mapsto v_1 \wedge v_2 \in \bigwedge^2 \mathbb{C}^n$ with image $Y_n = \mathrm{GL}_n(e_1 \wedge e_2) \cup \{0\}$.*
(c) *(Kempe) The invariant ring $I_n := \mathcal{O}(Y_n)^{T'}$ is generated by the invariants of degree d where $d = n$ if n is odd and $d = n/2$ if n is even. Thus the quotient map $\rho : Y_n \to X_n$ is homogeneous of degree d.*
(d) *The action of S_n on X_n and on $\mathbb{P}(X_n)$ is faithful for $n \geqslant 5$.*

Proof of Proposition 8.1. The claim follows from Lemma 8.1 applied to the S_n-equivariant quotient $\pi : V_n \to X_n = V_n /\!\!/ H$, using Proposition 8.2(a) and (d). □

Remark 8.1. It is easy to analyze the cases $n = 2$, 3 and 4. For $n = 2$ the quotient $V_2 /\!\!/ H$ is $\mathbb{C}$ with a non-trivial action of S_2. For $n = 3$ the quotient $V_3 /\!\!/ H$ is also $\mathbb{C}$, but A_2 acts trivially. Finally, for $n = 4$ the quotient $V_4 /\!\!/ H$ is a hypersurface in $\mathbb{C}^3$ and the representation of S_4 on $\mathbb{C}^3$ has kernel the Klein 4-group and quotient group S_3 which acts on $\mathbb{C}^3$ in the standard way.

Proof of Proposition 8.2. Part (a) was already proved above. Part (b) is the classical First Fundamental Theorem for SL_2, see [How88, 5.2.1 Proposition and Remarks], and part (c) is due to Kempe. A proof can be found in [How88, 5.4.2.5 Theorem, p. 156ff].

For (d) it suffices to show that S_n acts faithfully on X_n since the only non-trivial normal subgroup of S_n is A_n for $n \geqslant 5$. But otherwise, the subgroup $A_n \subset S_n$ would act trivially on X_n. This means that a generic H-orbit on V_n is stable under A_n which implies that there is a non-trivial homomorphism $A_n \to H$, a contradiction. □

The idea behind the proof of the upper bounds above can be used to explicitly calculate compressions for the group S_n. We have seen in Proposition 8.2(b) that the algebraic quotient $\eta : \mathbb{C}^2 \otimes \mathbb{C}^n \to (\mathbb{C}^2 \otimes \mathbb{C}^n) /\!\!/ \mathrm{SL}_2$ is given by

$$\eta : f_1 \otimes v_1 + f_2 \otimes v_2 \mapsto v_1 \wedge v_2 \in \bigwedge^2 \mathbb{C}^n$$

and that $(\mathbb{C}^2 \otimes \mathbb{C}^n) /\!\!/ \mathrm{SL}_2 \subset \bigwedge^2 \mathbb{C}^n$ is $\{v_1 \wedge v_2 \mid v_1, v_2 \in \mathbb{C}^n\}$, the closure of the highest weight orbit in $\bigwedge^2(\mathbb{C}^n)$. Let $x_{ij} = (e_i \wedge e_j)^*$ be the usual dual basis of $\bigwedge^2 \mathbb{C}^n$. A monomial $\prod_{i<j} x_{ij}^{\alpha_{ij}}$ is T'-invariant if and only if each index i occurs the same number of times, i.e., for every fixed k the sum $\sum_{i<k} \alpha_{ik} + \sum_{i>k} \alpha_{ki}$ is independent of k. Choosing such a monomial f we obtain an S_n-equivariant and T'-invariant morphism $\Sigma_f : \bigwedge^2 \mathbb{C}^n \to \mathbb{C}[S_n]$ given by $\sum_{\sigma \in S_n} (\sigma f) \cdot \sigma$.

We can do slightly better by composing with the S_n-equivariant embedding $\iota : \mathbb{C}^n \subset \mathbb{C}^2 \otimes \mathbb{C}^n$, $a \mapsto f_1 \otimes a + f_2 \otimes (1, 1, \ldots, 1)$. Then $\eta \circ \iota(a_1, \ldots, a_n) = \sum_{i<j}(a_i - a_j)e_i \wedge e_j$. Now the next proposition follows immediately from what we have said so far.

Proposition 8.3. *Let $f \in \mathbb{C}[x_1, \ldots, x_n]$ be a monomial in the differences $x_i - x_j$, where $i < j$, such that each x_i occurs the same number of times. If $n \geqslant 5$ and f is not an S_n-invariant, then the morphism $\Sigma_f : \mathbb{C}^n \to \mathbb{C}[S_n]$ corresponding to $\sum_{\sigma \in S_n}(\sigma f) \cdot \sigma$ defines a compression of dimension $\leqslant n - 2$.*

Remark 8.2. If n is even, we can use $f := (x_1 - x_2)(x_3 - x_4) \cdots (x_{n-1} - x_n)$ and get a compression of dimension $\leqslant n - 2$ and of degree $n/2$. In general, we can always use $f := (x_1 - x_2)(x_2 - x_3) \cdots (x_{n-1} - x_n)(x_n - x_1)$ to obtain a compression of dimension $\leqslant n - 2$ and of degree n. As a consequence of Kempe's result (Proposition 8.2(c)) one shows that these compressions have dimension equal to $n - 2$.

It is an open problem if there exist other monomials f such that the corresponding covariant Σ_f has dimension strictly less than $n - 2$. So far, all our explicit calculations have only produced covariants of dimension $n - 2$.

9. Purely transcendental fields of definition for generic field extensions

In this section we shortly describe the relation between the essential dimension of a generic field extension of degree n and the essential dimension of S_n due to Buhler, Reichstein [BuR97], and then show that every such field extension is defined over a purely transcendental extension of degree $n - 3$.

In the following we assume that all fields contain the complex numbers $\mathbb{C}$. Let L/K be a finite field extension.

Definition 9.1. We say that L/K is *defined over a subfield* $K' \subset K$ if there is a finite field extension L'/K' of degree $[L' : K'] = [L : K]$ such that $L = L'K$. The minimal transcendence degree (over $\mathbb{C}$) of such a subfield K' is called the *essential dimension* of L/K:

$$\operatorname{edim}(L/K) := \min\{\operatorname{tdeg}_{\mathbb{C}} K' \mid L/K \text{ is defined over } K'\}.$$

Now assume that $\operatorname{tdeg}_{\mathbb{C}} K = \infty$ and consider the general field extension K_n/K of degree n defined by the equation

$$x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_{n-1}x + a_n = 0, \tag{3}$$

where the $a_i \in K$ are algebraically independent. The following result is due to Buhler, Reichstein, [BuR97, Corollary 4.2]. It was the starting point for studying compressions of group actions.

Theorem 9.1 *(Buhler–Reichstein).* $\operatorname{edim} K_n/K = \operatorname{edim} S_n$.

In order to prove the inequality $\operatorname{edim} K_n/K \leqslant \operatorname{edim} S_n$ one shows that every rational faithful S_n-covariant $\rho : \mathbb{C}^n \to W$ of dimension d determines a subfield $K' \subset K$ of $\operatorname{tdeg}_{\mathbb{C}} K' = d$ such that K_n/K is defined over K'. We will need this construction in a slightly different form which we are going to explain now.

Denote by $\widetilde{K}_n \supset K_n$ the splitting field of Eq. (3) so that $\widetilde{K}_n/K$ is a Galois extension with Galois group S_n. Clearly, $\widetilde{K}_n$ contains elements $x_1, x_2, \ldots, x_n$ which are permuted under S_n and generate $\widetilde{K}_n/K$. By assumption, the elements $x_1, \ldots, x_n$ are algebraically independent over $\mathbb{C}$. Define $V := \mathbb{C}x_1 + \cdots + \mathbb{C}x_n \subset \widetilde{K}_n$. By construction, V is the standard representation of S_n.

Now let $\varphi : V \to W$ be a homogeneous S_n-covariant of dimension d and consider the cone $X := \overline{\varphi(V)} \subset W$. The field $\mathbb{C}(X)$ of rational functions on X can be considered as a subfield of $\mathbb{C}(V) = \mathbb{C}(x_1, \ldots, x_n)$ and $\operatorname{tdeg}_{\mathbb{C}} \mathbb{C}(X) = d$. Moreover, the field $\mathbb{C}(X)$ contains the subfield $\mathbb{C}(\mathbb{P}(X))$ of rational functions on the projective variety $\mathbb{P}(X) := X \setminus \{0\}/\mathbb{C}^*$, i.e., the subfield generated by all quotients p/q where p, q are homogeneous regular functions on X of the same degree.

Assume now that the S_n-action on $\mathbb{P}(X)$ is faithful (which is always the case if φ is faithful and $n \geqslant 5$). Then $\mathbb{C}(\mathbb{P}(X))/\mathbb{C}(\mathbb{P}(X))^{S_n}$ is a Galois extension with Galois group S_n and so $K \cdot \mathbb{C}(\mathbb{P}(X))^{S_n} = \widetilde{K}_n$. This shows that the extension $\widetilde{K}_n/K$ is defined over $\mathbb{C}(\mathbb{P}(X))^{S_n}$ and the same holds for K_n/K. Thus we have proved the following result.

Proposition 9.1. *Let K_n/K be the field extension defined by the equation*

$$x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_{n-1} x + a_n = 0,$$

where the coefficients $a_1, a_2, \ldots, a_n \in K$ are algebraically independent over $\mathbb{C}$, and let $\varphi : \mathbb{C}^n \to W$ be a homogeneous covariant. Define $X := \overline{\varphi(\mathbb{C}^n)}$ and assume that S_n acts faithfully on $\mathbb{P}(X)$. Then K_n/K is defined over a subfield isomorphic to $\mathbb{C}(\mathbb{P}(X))^{S_n}$.

In order to apply this result we use the explicit construction of a faithful covariant for S_n given in Section 8, using the representation of $H := \mathrm{SL}_2 \times T'$ on $V_n := \mathbb{C}^2 \otimes \mathbb{C}^n$ together with the action of S_n on V_n by permutations normalizing H.

As before, we embed $\mathbb{C}^n$ into $V_n = \mathbb{C}^2 \otimes \mathbb{C}^n$ by $a \mapsto f_1 \otimes a + f_2 \otimes (1, 1, \ldots, 1)$, and obtain an S_n-equivariant linear map $\iota : \mathbb{C}^n \to V_n$. The composition $\eta \circ \iota$ is the linear map $a = (a_1, \ldots, a_n) \mapsto \sum_{i<j} (a_i - a_j)\, e_i \wedge e_j$ whose kernel is the trivial representation $\mathbb{C} \subset \mathbb{C}^n$.

Proposition 9.2.

(a) *The composition $\varphi := \rho \circ \eta \circ \iota : \mathbb{C}^n \to X_n$ is a homogeneous covariant of degree d where $d = n$ if n is odd and $d = n/2$ if n is even.*
(b) *$\varphi : \mathbb{C}^n \to X_n$ is surjective.*
(c) *For $n \geqslant 5$, the action of S_n on $\mathbb{P}(X_n)$ is faithful and* $\dim \mathbb{P}(X_n) = n - 3$.
(d) *The varieties $\mathbb{P}(X_n)$ and $\mathbb{P}(X_n)/S_n$ are both rational, for all n.*

Proof. Part (a) follows from Proposition 8.2(c). For (b) it suffices to show that $\pi' \circ \varphi : \mathbb{C}^n \to S^n(\mathbb{C}^2)/\!\!/ \mathrm{SL}_2$ is surjective since $\pi' : X_n \to S^n(\mathbb{C}^2)/\!\!/ \mathrm{SL}_2$ is the quotient by the finite group S_n. Now the composition $\gamma : \mathbb{C}^n \to V_n \to S^n(\mathbb{C}^2)$ is given by $a \mapsto \prod_i (a_i x + y)$, and so the image in $S^n(\mathbb{C}^2)$ meets every SL_2-orbit except $\{0\}$. Thus, $\pi' \circ \varphi = \pi'' \circ \gamma$ is surjective.

(c) This follows from Proposition 8.2(a) and (d).

(d) The field $\mathbb{C}(\mathbb{P}(X_n))^{S_n}$ is isomorphic to $\mathbb{C}(S^n(\mathbb{C}^2))^{\mathrm{SL}_2 \times \mathbb{C}^*}$ and $\mathbb{C}(\mathbb{P}(X_n))$ is isomorphic to $\mathbb{C}(V_n)^{\mathrm{SL}_2 \times T' \times \mathbb{C}^*}$, and the latter fields are both rational, due to a result of Katsylo [Kat84]. □

Combining this result with Proposition 9.1 we get the following consequence.

Theorem 9.2. *Let K_n/K be the field extension of degree $n \geqslant 5$ defined by the equation*

$$x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_{n-1} x + a_n = 0,$$

where the coefficients $a_1, a_2, \ldots, a_n \in K$ are algebraically independent over $\mathbb{C}$. Then K_n/K is defined over a purely transcendental extension K' of $\mathbb{C}$ of transcendence degree $n-3$. Moreover, if L'/K' is of degree n such that $L'K = K_n$ then $L'/\mathbb{C}$ is purely transcendental, too.

Remark 9.1. The two cases $n = 5$ and $n = 6$ are due to Hermite and Joubert, respectively. They showed that one can always find a generator of the field extension K_n/K whose equation has the form

$$t^5 + at^3 + bt + b = 0 \quad \text{or} \quad t^6 + at^4 + bt^2 + ct + c = 0,$$

see [Kr06]. It is unknown if similar results hold in degree $n > 6$.

10. Groups of low covariant dimension

In this section we describe the finite groups of covariant dimension $\leqslant 2$.

Theorem 10.1. *If G is a group of covariant dimension 1 then G is cyclic.*

Proof. Let $\varphi : V \to X$ be a one-dimensional compression. We can clearly assume that X is normal, hence a rational curve, by Lüroth's theorem. It follows that X must be isomorphic to $\mathbb{C}$ and so G is a subgroup of $\mathrm{Aut}(\mathbb{C})$ fixing the point $\varphi(0)$. Hence G is cyclic. □

Proposition 10.1. *If G is a faithful group of covariant dimension 2, then $Z(G)$ is cyclic and $G/Z(G)$ is isomorphic to D_{2n} $(n \geqslant 2)$, A_4, S_4 or A_5.*

Proof. Let $\varphi : V \to V$ be a homogeneous faithful covariant of dimension 2 where V is irreducible. Then $X := \overline{\varphi(V)} \subset V$ is a cone of dimension 2, and so $\mathbb{P}(X) \subset \mathbb{P}(V)$ is an irreducible rational curve. It follows that the kernel of the action of G on $\mathbb{P}(X)$ equals the center $Z(G)$ of G. The normalization of $\mathbb{P}(X)$ is the projective line $\mathbb{P}^1$ and so $G/Z(G)$ is isomorphic to a finite subgroup of PGL_2. Since G is not commutative the factor group $G/Z(G)$ is not cyclic and the proposition follows. □

Here is the main theorem of this section.

Theorem 10.2. *Let G be a group of covariant dimension 2. Then G is isomorphic to a subgroup of GL_2.*

We remark that a similar result does not hold for covariant dimension > 2 as shown by the group S_5 which has covariant dimension 3. There is a similarity of our theorem and the characterization by A. Ledet [Le06] of groups of essential dimension 1 over an infinite field: *The finite group G has essential dimension 1 if and only if it can be embedded into $\mathrm{GL}(2)$ such that the only scalar matrix in the image of G is the identity.*

First we show:

Theorem 10.3. *If G is a non-faithful finite group of covariant dimension 2, then G is abelian of rank 2.*

The proof needs some preparation.

Lemma 10.1. *Let G be a group of covariant dimension 2 and V a faithful representation. If $a, b \in G$ do not commute, then there is an irreducible subrepresentation $W \subset V$ such that the commutator (a, b) is non-trivial on W and such that the image $\bar{G}$ of G in $\mathrm{GL}(W)$ is a faithful group of covariant dimension 2. In particular, there is a surjective homomorphism from G to D_{2n} $(n \geqslant 2)$, A_4, S_4 or A_5.*

Proof. Let $\varphi : V \to V$ be a minimal covariant and $V = \bigoplus_i V_i$ the decomposition into irreducible subrepresentations. Then the commutator (a, b) acts non-trivially on the image $\varphi(V)$, hence non-trivially on $\varphi_i(V)$ for some component $\varphi_i : V \to V_i$ of φ. If $\bar{a}, \bar{b}$ denote the images of a, b in $\mathrm{GL}(V_i)$, then $(\bar{a}, \bar{b}) \neq 1$ and so $\bar{G} \subset \mathrm{GL}(V_i)$, the image of G in $\mathrm{GL}(V_i)$, is non-commutative. If $N \subset G$ is the kernel of $G \to \bar{G}$, then $\varphi_i(V^N) \neq (0)$, and so $\varphi_i : V^N \to V_i$ is a faithful covariant of $\bar{G} \simeq G/N$ of dimension $\leqslant \dim \varphi = 2$. Since $\bar{G}$ is not commutative, $\operatorname{covdim} \bar{G} = 2$. The last statement now follows from Proposition 10.1. □

Proof of Theorem 10.3. Assume that the assertion does not hold. Let G be a non-commutative non-faithful group of covariant dimension 2 and of minimal order with these properties. This implies that every strict subgroup H of G is either faithful or commutative. In particular, if H contains N_G then H is not faithful by Gaschütz's Criterion (Corollary 4.1), and so H is commutative. Since G is not faithful with $\operatorname{covdim} G = 2$, we have rank $N_G = 2$.

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

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 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. Then $\rho(N_G) \subset K$ and so 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 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.*

If a, b are two non-commuting elements of p-power order then, by Lemma 10.1, there is an irreducible representation W of G such that $\bar{a}$ and $\bar{b}$ do not commute in $\bar{G} \subset \mathrm{GL}(W)$, and $\bar{G}$ is faithful of covariant dimension 2. It follows from Proposition 10.1 and Claim 1 that $\bar{G}/Z(\bar{G}) \simeq D_{2n}$. Since $p > 2$, the images of $\bar{a}$ and $\bar{b}$ are in the cyclic subgroup $C_n \subset D_{2n}$ which leads to a

contradiction, since the inverse image of C_n in $\bar{G}$ is commutative. Hence pairs of elements of p-power order commute, and so the p-Sylow subgroup G_p is normal and commutative. It follows that $G' := \prod_{p>2} G_p$ is a normal commutative subgroup and that $G = G_2 \cdot G'$ is a semidirect product. This proves Claim 2.

Now we can finish the proof. The case that $G = G_2$ is handled in Lemma 10.2, so we can assume that G' is non-trivial. If G_2 commutes with G', then G_2 is not 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 covdim $H \geqslant 3$ by Corollary 6.2. So G' has rank 1. Then G' is cyclic, hence G is faithful (Corollary 4.3), 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 4.1) and the same holds for the subgroup $H := \langle g, N_2 \rangle \ltimes N'$ (Corollary 4.1). Thus H is neither faithful nor commutative, so that it must equal G by minimality.

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 6.2 has covariant dimension at least 3. If g acts by sending each element of $(\mathbb{Z}/p)^2$ to its inverse, then $\langle g \rangle \ltimes G_p$ has covariant dimension 3 by Corollary 5.1. 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. Moreover, 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 by Corollary 6.1. 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 6.2. This finishes the proof of the theorem, modulo the following lemma. □

Lemma 10.2. *Let G be a non-faithful 2-group of covariant dimension 2. Then G is commutative.*

Proof. Let G be a counterexample of minimal order and let $a, b \in G$ be two non-commuting elements. If $H := \langle a, b \rangle$ is a strict subgroup of G, then H is faithful and so $Z(H)$ has rank 1. Since $Z(G)$ has rank 2 this implies that G contains a subgroup of the form $H \times \mathbb{Z}/2$ which has covariant dimension 3 (Corollary 6.1).

Thus we can assume that every pair $a, b \in G$ of non-commuting elements generates G. From the minimality assumption it follows that $a^2, b^2, (ab)^2 \in Z(G)$. Denote by $d := (a, b)$ the commutator. Then $d = aba^{-1}b^{-1} = (ab)^2a^{-2}b^{-2} \in Z(G)$. Since $aba^{-1} = db$ we have $b^2 = ab^2a^{-1} = d^2b^2$ which implies that $d^2 = 1$. Hence $(G, G) = \{d, e\}$ and so $(a', b') = d$ for every pair a', b' of non-commuting elements. Since $G/\langle d \rangle$ is commutative, it follows that $Z(G) = \langle a^2, b^2, d \rangle = \langle a^2, b^2, (ab)^2 \rangle$.

If $a^2 = z^2$ for some $z \in Z(G)$, then $a' := az^{-1} \notin Z(G)$ and $a'^2 = 1$. Thus G contains a subgroup isomorphic to $Z(G) \times \mathbb{Z}/2$ which has covariant dimension 3. It follows that for every pair of non-commuting elements a, b the three elements a^2, b^2 and $(ab)^2$ are in $Z(G) \setminus Z(G)^2$. As a consequence, two of them generate $Z(G)$, i.e., there are generators a, b of G such that a^2, b^2 generate $Z(G)$. If $a^{2^p} = b^{2^q} \neq e$ where $p < q$ (and necessarily, $p, q \geqslant 2$), then the squares of $a' := ab^{-2^{q-p}}$ and b freely generate $Z(G)$. We make a similar modification if $p > q$. If $p = q$, then we replace a by $a' := ab^{-1}$. Then $(a')^{2^p} = a^{2^p}b^{-2^p} = e$. Thus we can assume that a and b

freely generate $Z(G)$. This implies that if a is of order 2^ℓ and b of order 2^k, then $\ell, k \geqslant 2$ and $|G| = 2^{\ell+k}$.

We have seen above that $d^2 = 1$ where $d = (a, b)$. Therefore we are in one of the following three cases: (1) $d = a^{2^{k-1}}$, (2) $d = b^{2^{\ell-1}}$ or (3) $d = a^{2^{k-1}} b^{2^{\ell-1}}$.

Case 1. $d = a^{2^{k-1}}$. Then $bab^{-1} = ad = a^{2^{k-1}+1}$ and so $G = \langle b \rangle \ltimes \langle a \rangle$ is a semidirect product. Then $\operatorname{covdim} G \geqslant 3$ by Proposition 6.2.

Case 2. $d = b^{2^{\ell-1}}$. As in the previous case $G = \langle a \rangle \ltimes \langle b \rangle$ is a semidirect product and so $\operatorname{covdim} G \geqslant 3$.

Case 3. $d = a^{2^{k-1}} b^{2^{\ell-1}}$. We can assume that $\ell \geqslant k$. If $\ell > k$ then $a' := ab^{2^{\ell-k}}$ and b generate G, a' has the same order as a and $d = a'^{2^{k-1}}$. Thus we are in Case 1 and so $\operatorname{covdim} G \geqslant 3$.

If $\ell = k > 2$, we have $(ab)^2 = da^2b^2$, and so $(ab)^{2^{\ell-1}} = d$. This implies that $G = \langle a \rangle \ltimes \langle ab \rangle$, hence $\operatorname{covdim} G \geqslant 3$.

Finally, for $\ell = k = 2$ we get $(ab)^2 = e$ and so $G \supset \langle a^2, b^2, ab \rangle \simeq (\mathbb{Z}/2)^3$, hence again $\operatorname{covdim} G \geqslant 3$. □

Now we prepare the proof of Theorem 10.2. We need only consider faithful groups, and we can employ Proposition 10.1. So, we have an exact sequence

$$1 \to \mathbb{Z}/m \to G \to K \to 1,$$

where K is D_{2n}, $n \geqslant 2$, A_4, S_4 or A_5. Thus we need to classify the cyclic central extensions of these groups. In terms of group cohomology, we need to calculate $\mathrm{H}^2(K, \mathbb{Z}/m)$. First we determine the *Schur multiplier* $\mathrm{M}(K) := \mathrm{H}^2(K, \mathbb{C}^*)$.

Lemma 10.3. *We have*

(a) $\mathrm{M}(A_5) \simeq \mathrm{M}(S_4) \simeq \mathrm{M}(A_4) \simeq \mathbb{Z}/2$.
(b) $\mathrm{M}(D_{2n}) \simeq \mathbb{Z}/2$ *if* n *is even and* $\mathrm{M}(D_{2n})$ *is trivial if* n *is odd.*

Proof. The first part is classical and goes back to Schur [Sch11]. The second part is surely also classical, but we do not know a reference, so we give a proof.

Suppose that

$$1 \to \mathbb{C}^* \to H \to D_{2n} \to 1$$

is exact. Then there are α, $\beta_1 \in H$ such that the image of α in $D_{2n} = \mathbb{Z}/2 \ltimes \mathbb{Z}/n$ generates $\mathbb{Z}/2$ and the image of β_1 generates $\mathbb{Z}/n$. It is easy to arrange that α has order 2 and that β_1 has order n. Then $\alpha\beta_1\alpha^{-1} = \lambda\beta_1^{-1}$ where $\lambda \in \mathbb{C}^*$ and $\lambda^n = 1$. Replacing β_1 by $\beta_2 := \lambda^{-1/2}\beta_1$ we have that $\alpha\beta_2\alpha^{-1} = \beta_2^{-1}$ where the order of β_2 is now n or $2n$. Suppose that the order is $2n$. If n is odd, then $\beta := \beta_2^2$ has order n and maps to a generator of $\mathbb{Z}/n$. Thus if β_2 has order n or n is odd, our exact sequence is split. If n is even, we see that there is a unique non-trivial extension, i.e., $\mathrm{M}(D_{2n}) \simeq \mathbb{Z}/2$. In fact, this extension is induced by the non-trivial extension

$$1 \to \{\pm 1\} \to D_{4n} \to D_{2n} \to 1. \qquad \square$$

Corollary 10.1. *We have*

(a) $\mathrm{H}^2(A_5, \mathbb{Z}/m) \simeq \mathbb{Z}/2$ *if* m *is even, else it is trivial.*
(b) $\mathrm{H}^2(S_4, \mathbb{Z}/m) \simeq (\mathbb{Z}/2)^2$ *if* m *is even, else it is trivial.*
(c) $\mathrm{H}^2(A_4, \mathbb{Z}/m) \simeq \mathbb{Z}/d$ *where* $d = \mathrm{GCD}(6, m)$.
(d) $H := \mathrm{H}^2(D_{2n}, \mathbb{Z}/m) \simeq (\mathbb{Z}/2)^3$ *if* m *and* n *are even,* $H \simeq \mathbb{Z}/2$ *if* n *is odd and* m *is even and* H *is trivial if* m *is odd.*

Proof. We just give the proof of (c). The other proofs follow the same reasoning. From the short exact sequence

$$1 \to \mathbb{Z}/m \to \mathbb{C}^* \xrightarrow{m} \mathbb{C}^* \to 1$$

we obtain a long exact sequence of cohomology

$$\cdots \to \mathrm{Hom}(A_4, \mathbb{C}^*) \xrightarrow{m} \mathrm{Hom}(A_4, \mathbb{C}^*) \to \mathrm{H}^2(A_4, \mathbb{Z}/m) \to \mathrm{M}(A_4) \xrightarrow{m} \mathrm{M}(A_4) \to \cdots,$$

where we use the fact that, since $\mathbb{C}^*$ is a trivial A_4-module, we have

$$\mathrm{H}^1(A_4, \mathbb{C}^*) \simeq \mathrm{Hom}(A_4, \mathbb{C}^*) \simeq \mathbb{Z}/3.$$

Now (c) follows from the exact sequence and Lemma 10.3. □

Proof of Theorem 10.2. We can assume that G is faithful. Proposition 10.1 gives us the possibilities for $G/Z(G)$. Suppose that $G/Z(G) \simeq A_4$. If $\mathrm{GCD}(6, m) = 1$, then we have a product extension of A_4 which has covariant dimension at least $\mathrm{covdim}\, A_4 = 3$. Suppose that we have a non-zero element of $\mathrm{H}^2(A_4, \mathbb{Z}/m)$ which has order 3. Then $3|m$ and we have the semidirect product $\mathbb{Z}/3m \ltimes (\mathbb{Z}/2)^2$ where the generator α of $\mathbb{Z}/3m$ permutes the non-zero elements of $(\mathbb{Z}/2)^2$ cyclically. If $2|m$, then G contains a copy of $(\mathbb{Z}/2)^3$, otherwise $G \times \mathbb{Z}/2$ has the same covariant dimension as G and contains a copy of $(\mathbb{Z}/2)^3$. Hence $\mathrm{covdim}\, G \geqslant 3$. Now suppose that we have an element of $\mathrm{H}^2(A_4, \mathbb{Z}/m)$ of order 2. Then we have the extension

$$1 \to \mathbb{Z}/m \to \widetilde{A_4} \to A_4 \to 1,$$

where $\widetilde{A_4} \subset \mathrm{GL}_2$ is the binary tetrahedral group BA_4 multiplied by the $2m$th roots of 1 (as scalar matrices). So $\mathrm{covdim}\, G = 2$. Finally, suppose that we have an element of order 6. Here we need to be specific about the binary tetrahedral group. If we identify SU_2 with the unit quaternions, then BA_4 is generated by the subgroup $BK := \{\pm i, \pm j, \pm k\}$ (the inverse image of the Klein 4-group) and the element $\alpha := 1/2(-1 + i + j + k)$ which has order 3, so that $BA_4 \simeq \mathbb{Z}/3 \ltimes BK$. To get the extension of order 6 we need to take the group generated by BK and the product of α by a primitive $3m$th root of unity. But this is still a subgroup of GL_2. This completes the proof for A_4.

Now suppose that $G/Z(G) = S_4$. We can think of S_4 as the semidirect product $\mathbb{Z}/2 \ltimes A_4 \simeq \mathbb{Z}/2 \ltimes (\mathbb{Z}/3 \ltimes (\mathbb{Z}/2)^2)$. If we have a trivial extension of S_4 by $\mathbb{Z}/m$, then we have a group of covariant dimension at least 3. If m is even, then $\mathrm{H}^2(S_4, \mathbb{Z}/m)$ has order 4, where the three non-zero elements correspond to the following three groups:

(a) $\mathbb{Z}/2m \ltimes A_4$ where $\mathbb{Z}/2m$ has a generator which acts by an automorphism of order 2. This group contains A_4, hence has covariant dimension at least 3.
(b) $(\mathbb{Z}/2m \ltimes BA_4)/(\mathbb{Z}/2)$ where the generator $\alpha \in \mathbb{Z}/2m$ acts by order 2 on BA_4 and we identify α^m with $-1 \in BA_4$. This is easily seen to be isomorphic to a subgroup of GL_2. If $m = 2$ it is the binary octahedral group BS_4.
(c) $(\mathbb{Z}/m \times BS_4)/(\mathbb{Z}/2)$ where if α generates $\mathbb{Z}/m$ (acting as scalar matrices), then we identify $\alpha^{m/2}$ with $-1 \in BS_4$. This is again a subgroup of GL_2.

We now consider the case of $K := D_{2n}$. If the class in $\mathrm{H}^2(K, \mathbb{Z}/m)$ is trivial, then we have $G = D_{2n} \times \mathbb{Z}/m$. If n is odd then D_{2n} has trivial center, so that $\operatorname{covdim} G = \operatorname{covdim} D_{2n} = 2$ and G is isomorphic to a subgroup of GL_2. If n is even, then we have center $\mathbb{Z}/2$ which means that we have covariant dimension 3 if m is even and covariant dimension 2 (and G is a subgroup of GL_2) if m is odd. From now on we can suppose that m is even.

Suppose that n is odd and that we have a non-trivial extension of D_{2n}. Then the only candidate is $(\mathbb{Z}/m \times D_{4n})/\mathbb{Z}/2$ where we identify the $(m/2)$nd power of the generator of $\mathbb{Z}/m$ with the central element in D_{4n}. This is clearly a subgroup of GL_2. From now on we can assume that n is even.

Choose $\alpha \in G$ whose image generates $\mathbb{Z}/2 \subset D_{2n}$ and $\beta \in G$ whose image generates $\mathbb{Z}/n \subset D_{2n}$ where $D_{2n} = \mathbb{Z}/2 \ltimes \mathbb{Z}/n$. Then $\alpha^2 \in \mathbb{Z}/m$ and $\beta^n \in \mathbb{Z}/m$. We have that $\alpha\beta\alpha^{-1} = z\beta^{-1}$ where $z \in \mathbb{Z}/m$. Replacing β by a product $\beta z'$ for $z' \in \mathbb{Z}/m$ we can reduce to the case that $z = e$ or that z is a (fixed) generator of $\mathbb{Z}/m$. Similarly, we can assume that $\alpha^2 = w$ where $w = e$ or w is the same fixed generator of $\mathbb{Z}/m$ as above. Now $\alpha\beta^n\alpha^{-1} = z^n(\beta^{-1})^n = \beta^n$, so that $\beta^{2n} = z^n$ and $\beta^n = \pm z^{n/2}$ (where we think of -1 as $n/2 \in \mathbb{Z}/n$). If $\beta^n = z^{n/2}$, then it follows that α fixes $\beta^{n/2}$, hence that $\beta^{n/2} \in \mathbb{Z}/m$ which would imply that the image of β in $\mathbb{Z}/n$ would have order $n/2$, a contradiction. Hence $\beta^n = -z^{n/2}$.

Case 1. $\alpha^2 = e$. If $z = e$, then β has order n so that our exact sequence is split, a case that we have already handled. So we can assume that $\beta^n = -z^{n/2}$ where z generates $\mathbb{Z}/m$. Now we see that $G \subset \mathrm{GL}_2$. Represent α by the matrix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ and represent β as the matrix $\left(\begin{smallmatrix} \xi\eta & 0 \\ 0 & \xi^{-1}\eta \end{smallmatrix}\right)$ where ξ is a primitive $2n$th root of 1 and η is a primitive $2m$th root of 1. Then β^n is central and we have that $\alpha\beta\alpha^{-1} = z\beta^{-1}$ where $z = \left(\begin{smallmatrix} \eta^2 & 0 \\ 0 & \eta^2 \end{smallmatrix}\right)$ generates a central copy of $\mathbb{Z}/m$ and $\beta^n = -z^{n/2}$.

Case 2. $\alpha^2 = w$ generates $\mathbb{Z}/m$. If $z = e$, then our group is isomorphic to the group generated by the matrices $\left(\begin{smallmatrix} 0 & \eta \\ \eta & 0 \end{smallmatrix}\right)$ where η is a primitive $2m$th root of 1 and $\left(\begin{smallmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{smallmatrix}\right)$ where ξ is a primitive $2n$th root of 1. If $z = w$ generates $\mathbb{Z}/m$, then we use α as above and $\beta = \left(\begin{smallmatrix} \xi\eta & 0 \\ 0 & \xi^{-1}\eta \end{smallmatrix}\right)$ where ξ is a primitive $2n$th root of 1. Then α and β generate a subgroup of GL_2 isomorphic to G. □

Acknowledgments

The authors thank Zinovy Reichstein for introducing us to the notions of essential dimension and covariant dimension. We thank Daniel Goldstein for informing us about [Ga54] and his help with the cohomology groups in the last section. We thank the referee for useful remarks and corrections.

References

[BuR97] J. Buhler, Z. Reichstein, On the essential dimension of a finite group, Compos. Math. 106 (1997) 159–179.
[Ga54] W. Gaschütz, Endliche Gruppen mit treuen absolut-irreduziblen Darstellungen, Math. Nachr. 12 (1954) 253–255.
[How88] R. Howe, The Classical Groups and Invariants of Binary Forms, Proc. Sympos. Pure Math., vol. 48, Amer. Math. Soc., Providence, RI, 1988.
[Kat84] P.I. Katsylo, Rationality of the orbit spaces of irreducible representations of the group SL_2, Math. USSR-Izv. 22 (1984) 23–32.
[Kr85] H. Kraft, Geometrische Methoden in der Invariantentheorie, Aspekte der Mathematik, vol. D1, Vieweg, Braunschweig/Wiesbaden, 1985.
[Kr06] H. Kraft, Equations of degree 5 and 6 and a result of Hermite, J. Algebra 297 (2006) 234–253.
[Le06] A. Ledet, On groups with essential dimension one, in press.
[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.
[Sch11] I. Schur, Über die Darstellung der symmetrischen und der alternierenden Gruppe durch gebrochene lineare Substitutionen, J. Reine Angew. Math. 139 (1911) 155–250.