Transformation Groups, Vol. 15, No. 3, 2010, pp. 611–623

APPLICATION OF MULTIHOMOGENEOUS COVARIANTS TO THE ESSENTIAL DIMENSION OF FINITE GROUPS

ROLAND LÖTSCHER*

Institute of Mathematics
University of Basel
Rheinsprung 21
CH-4051 Basel, Switzerland

rolandlo@gmail.com

Abstract. We investigate the essential dimension of finite groups using the multihomogenization technique introduced in [KLS09], for which we provide new applications in a more general setting. We generalize the central extension theorem of Buhler and Reichstein [BR97, Theorem 5.3] and use multihomogenization as a substitute to the stack-involved part of the theorem of Karpenko and Merkurjev [KM08] about the essential dimension of p-groups.

1. Introduction

Throughout this paper we work over an arbitrary base field k. Sometimes we extend scalars to a larger base field, which will be denoted by K. All vector spaces and representations in consideration are finite dimensional over the base field. A geometrically integral separated scheme of finite type defined over the base field will be called a variety. We denote by G a finite group. A G-variety is then a variety with a regular algebraic G-action $G \times X \to X$ on it.

The *essential dimension of* G was introduced by Buhler and Reichstein [BR97] in terms of *compressions*: A *compression* of a faithful G-variety Y is a dominant G-equivariant rational map $\varphi\colon Y \dashrightarrow X$, where X is another faithful G-variety.

For a vector space V we denote by $\mathbb{A}(V)$ the affine variety representing the functor $A \mapsto V \otimes_k A$ from the category of commutative k-algebras to the category of sets.

Definition 1. The *essential dimension of* G is the minimal value of $\dim X$ taken over all compressions $\varphi\colon \mathbb{A}(V) \dashrightarrow X$ of a faithful representation V of G.

The notion of essential dimension is related to Galois algebras, torsors, generic polynomials, cohomological invariants and other topics, see [BR97], [BF03].

We take a slightly different point of view, which was used in [KS07] and [KLS09]: A *covariant* of G (over k) is a G-equivariant (k-)rational map $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$,

---

DOI: 10.1007/s00031-010-9092-7

*The author gratefully acknowledges support from the Swiss National Science Foundation (Schweizerischer Nationalfonds).

Received November 9, 2009. Accepted December 11, 2009. Published online April 20, 2010.

where V and W are representations of G (over k). A covariant φ is called *faithful* if the closure of the image $\overline{\operatorname{im}\varphi}$ of φ is a faithful G-variety. Equivalently, there exists a $\bar{k}$-rational point in the image of φ with trivial stabilizer. We denote by $\dim\varphi$ the dimension of $\overline{\operatorname{im}\varphi}$.

Definition 2. The *essential dimension of* G, denoted by $\operatorname{edim}_k G$, is the minimum of $\dim\varphi$ where φ runs over all faithful covariants over k.

The second definition of essential dimension is in fact equivalent to the first definition. This follows, e.g., from (an obvious variant of) [Fl08, Prop. 2.5]. Moreover, in Definition 2 one may work with covariants between his favorite faithful G-modules. In fact, the argument shows that for any faithful G-modules V and W there exists a faithful covariant $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ with $\dim\varphi = \operatorname{edim}_k G$. We will exploit this to work with completely reducible faithful representations whenever such representations of G exist.

In Section 2 we recall the multihomogenization technique for covariants from [KLS09], generalizing some of the results of [KLS09] and, in particular, extending them to arbitrary base fields. Given G-stable gradings $V = \bigoplus_{i=1}^m V_i$ and $W = \bigoplus_{j=1}^n W_j$ a covariant $\varphi = (\varphi_1, \ldots, \varphi_n)\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ is called *multihomogeneous* if the identities

$$\varphi_j(v_1, \ldots, v_{i-1}, sv_i, v_{i+1}, \ldots, v_m) = s^{m_{ij}}\varphi_j(v_1, \ldots, v_m)$$

hold true for all i, j and suitable m_{ij}. Here s is an indeterminate and the m_{ij} are integers, forming a matrix $M_\varphi \in \operatorname{Mat}_{m\times n}(\mathbb{Z})$. Thus multihomogeneous covariants generalize homogeneous covariants. A whole matrix of integers takes the role of a single integer, the degree of a homogeneous covariant. It will be shown that the degree matrix M_φ and especially its rank have a deeper meaning with regards to the essential dimension of G. Theorem 5 states that if each V_i and W_j is irreducible then the rank of the matrix M is bounded from below by the rank of a certain central subgroup $Z(G,k)$ (the k-center, see Definition 5). Moreover, if the rank of M_φ exceeds the rank of $Z(G,k)$ by $\Delta \in \mathbb{N}$, then $\operatorname{edim}_k G \le \dim\varphi - \Delta$. This observation will be useful for several applications, in particular, for proving lower bounds for $\operatorname{edim}_k G$.

A generalization of a theorem from [BR97] about the essential dimension of central extensions is obtained in Section 3 where the following situation is investigated: G is a (finite) group and H a central subgroup which intersects the commutator subgroup of G trivially. Buhler and Reichstein deduced the relation

$$\operatorname{edim}_k G = \operatorname{edim}_k G/H + 1$$

(over a field k of characteristic 0) for the case that H is a maximal cyclic subgroup of the k-center $Z(G,k)$ and has prime order p and that there exists a character of G which is faithful on H, see [BR97, Theorem 5.3]. In this paper we give a generalization which reads like

$$\operatorname{edim}_k G = \operatorname{edim}_k G/H + \operatorname{rk} Z(G,k) - \operatorname{rk} Z(G/H,k),$$

where we only assume that G has no nontrivial normal p-subgroups if $\operatorname{char} k = p > 0$ and that k contains a primitive root of unity of high enough order. For details see Theorem 9.

Section 4 contains a result about direct products, obtained easily with the use of multihomogeneous covariants.

In Section 5 we shall use multihomogeneous covariants to generalize Florence's twisting construction [Fl08]. The generalization gives a substitute to the use of algebraic stacks in the proof of a recent theorem of Karpenko and Merkurjev about the essential dimension of p-groups, which says that the essential dimension of a p-group G equals the least dimension of a faithful representation of G, provided that the base field contains a primitive pth root of unity. Our main result in this section is Theorem 14 which gives a lower bound of the essential dimension of any group G that admits a completely reducible faithful representation over k.

Acknowledgments. I am grateful to my PhD adviser Hanspeter Kraft for many fruitful discussions about covariant and essential dimension and for helpful remarks on this paper. Moreover, I wish to thank the anonymous referees who made valuable comments on this and on an earlier version of this paper.

2. The multihomogenization technique

2.1. Multihomogeneous maps and multihomogenization

In [KLS09] multihomogenization has originally been introduced for regular covariants over the field $\mathbb{C}$ of complex numbers. We give a more direct and general approach here and refer to [KLS09] for proofs if the corresponding facts can easily be generalized to our setting.

Let $T = \mathbb{G}_m^m$ and $T' = \mathbb{G}_m^n$ be tori split over k. The homomorphisms $D \in \operatorname{Hom}(T, T')$ defined over k correspond bijectively to matrices $M = (m_{ij}) \in \operatorname{Mat}_{m\times n}(\mathbb{Z})$ by

$$D(t_1, \dots, t_m) = (t'_1, \dots, t'_n) \qquad \text{where} \quad t'_j = \prod_{i=1}^{m} t_i^{m_{ij}}.$$

Let V be a graded vector space $V = \bigoplus_{i=1}^m V_i$. We associate with V the torus $T_V \subseteq \mathrm{GL}(V)$ consisting of those linear automorphisms which act by multiplication by scalars on each $\mathbb{A}(V_i)$. We identify T_V with $\mathbb{G}_m^m$ acting on $\mathbb{A}(V)$ by

$$(t_1, \dots, t_m)(v_1, \dots, v_m) = (t_1 v_1, \dots, t_m v_m).$$

Let $W = \bigoplus_{j=1}^n W_j$ be another graded vector space and $T_W \subseteq \mathrm{GL}(W)$ its associated torus.

Definition 3. A rational map $\varphi = (\varphi_1, \dots, \varphi_n)\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ is called *multihomogeneous* (with respect to the given gradings $V = \bigoplus_{i=1}^m V_i$ and $W = \bigoplus_{j=1}^n W_j$) of degree $M = (m_{ij}) \in \operatorname{Mat}_{m,n}(\mathbb{Z})$ if

$$\varphi_j(v_1, \dots, s v_i, \dots, v_m) = s^{m_{ij}} \varphi_j(v_1, \dots, v_m) \tag{1}$$

for all i and j.

In terms of the associated homomorphism $D \in \mathrm{Hom}(T_V, T_W)$ this means that

$$\begin{tikzcd} T_V \times \mathbb{A}(V) \arrow[r, "(t,v)\mapsto tv"] \arrow[d, dashed, "D\times\varphi"'] & \mathbb{A}(V) \arrow[d, dashed, "\varphi"] \\ T_W \times \mathbb{A}(W) \arrow[r, "(t',w)\mapsto t'w"] & \mathbb{A}(W) \end{tikzcd} \tag{2}$$

commutes.

Example 1. Let $V = \bigoplus_{i=1}^m V_i$ be a graded vector space. If $h_{ij} \in k(V_i)^*$, for $1 \leq i, j \leq m$, are homogeneous rational functions of degree $r_{ij} \in \mathbb{Z}$ then the map

$$\psi_h \colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(V), \qquad v \mapsto (h_{11}(v_1) \cdots h_{m1}(v_m)v_1, \ldots, h_{1m}(v_1) \cdots h_{mm}(v_m)v_m),$$

is multihomogeneous with degree matrix $M = (r_{ij} + \delta_{ij})_{1 \leq i,j \leq m}$.

Let $\varphi \colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ be a multihomogeneous rational map. If the projections φ_j of φ to $\mathbb{A}(W_j)$ are nonzero for all j, then the homomorphism $D \in \mathrm{Hom}(T_V, T_W)$ is uniquely determined by condition (2). We shall write D_φ and M_φ for D and M_D, respectively. If $\varphi_j = 0$ for some j then the matrix entries m_{ij} of M_φ, for $i = 1, \ldots, m$, can be chosen arbitrarily. Fixing the choice $m_{ij} = 0$ for such j makes M_φ with property (1) and the corresponding D_φ with property (2) unique again. This convention that we shall use in the sequel has the advantage that adding or removing of some zero-components of the map φ does not change the rank of the matrix M_φ.

Given an arbitrary rational map $\varphi \colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ we construct a multihomogeneous map $H_\lambda(\varphi) \colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ which depends only on φ and the choice of a suitable one-parameter subgroup $\lambda \in \mathrm{Hom}(\mathbb{G}_m, T_V)$. Our construction is similar to the one given in [KLS09].

Let $\nu \colon k(V \times k) = k(s)(V) \to \mathbb{Z} \cup \{\infty\}$ be the discrete valuation belonging to the hyperplane $\mathbb{A}(V) \times \{0\} \subset \mathbb{A}(V) \times \mathbb{A}^1$. So $\nu(0) = \infty$ and for $f \in k(V \times k) \setminus \{0\}$ the value of $\nu(f)$ is the exponent of the coordinate function s in a primary decomposition of f. Let $O_s \subset k(V \times k)$ denote the valuation ring corresponding to ν. Every $f \in O_s$ can be written as $f = p/q$ with polynomials p, q where $s \nmid q$. For such f we define $\lim f \in k(V)$ by $(\lim f)(v) = p(v, 0)/q(v, 0)$. It is nonzero if and only if $\nu(f) = 0$. Moreover, $\nu(f - \lim f) > 0$ since $\lim(f - \lim f) = 0$, where $\lim f \in k(V)$ is considered as an element of $k(V \times k)$. This construction can easily be generalized to rational maps $\psi \colon \mathbb{A}(V) \times \mathbb{A}^1 \dashrightarrow \mathbb{A}(W)$ by choosing coordinates on W. So for $\psi = (f_1, \ldots, f_d)$ where $d = \dim W$ and $f_1, \ldots, f_d \in O_s$, we shall write $\lim \psi$ for the rational map $(\lim f_1, \ldots, \lim f_d) \colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$.

Let $\lambda \in \mathrm{Hom}(\mathbb{G}_m, T_V)$ be a one-parameter subgroup of T_V. Consider

$$\widetilde{\varphi} = (\widetilde{\varphi}_1, \ldots, \widetilde{\varphi}_n) \colon \mathbb{A}(V) \times \mathbb{G}_m \dashrightarrow \mathbb{A}(W), \qquad (v, s) \mapsto \varphi(\lambda(s)v),$$

as a rational map on $\mathbb{A}(V) \times \mathbb{A}^1$. For $j = 1 \ldots n$ let α_j be the smallest integer d such that all coordinate functions in $s^d \widetilde{\varphi}_j$ are elements of O_s (if $\widetilde{\varphi}_j = 0$ we choose $\alpha_j = 0$). Let $\lambda' \in \mathrm{Hom}(\mathbb{G}_m, T_W)$ be the one-parameter subgroup defined by $\lambda'(s) = (s^{\alpha_1}, \ldots, s^{\alpha_n})$. Then $H_\lambda(\varphi)$ is the limit

$$H_\lambda(\varphi) = \lim((v,s) \mapsto \lambda'(s)\varphi(\lambda(s)v))\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W).$$

Now recall from [KLS09, Sect. 2] the following facts.

Lemma 1.

- *For any one-parameter subgroup* $\lambda \in \mathrm{Hom}(\mathbb{G}_m, T_V)$,

$$\dim H_\lambda(\varphi) \le \dim \varphi.$$

- *There exists a one-parameter subgroup* $\lambda \in \mathrm{Hom}(\mathbb{G}_m, T_V)$ *such that* $H_\lambda(\varphi)$ *is multihomogeneous.*
- *If* $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ *is a covariant and all* V_i, W_j *are* G*-stable then* $H_\lambda(\varphi)$ *is a covariant too.*

From now on let $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ denote a covariant of G where $V = \bigoplus_{i=1}^m V_i$ and $W = \bigoplus_{j=1}^n W_j$ are G-stably graded representations. In general, the covariant $H_\lambda(\varphi)$ does not have to be faithful if the covariant φ is. However, recall the following easy consequence of [KS07, Lemma 4.1].

Lemma 2. *If the representations* $W_1, \ldots, W_n$ *are all irreducible, then* $H_\lambda(\varphi)$ *is faithful as well.*

A faithful covariant $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ of G is called *minimal* if $\dim \varphi = \mathrm{edim}_k G$. Assume we are given a completely reducible representation $W = \bigoplus_{j=1}^n W_j$ (each W_j irreducible) and another representation $V = \bigoplus_{i=1}^m V_i$ of G. Then we can replace a minimal covariant $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ by the multihomogeneous covariant $H_\lambda(\varphi)$ (for a suitable one-parameter subgroup λ of T_V as in Lemma 1) without loosing faithfulness or minimality.

Note however that in contrast to the case $k = \mathbb{C}$ from [KLS09] a completely reducible faithful representation W does not need to exist. For example, if $k = \bar{k}$ and the center of G has an element g of prime order p, then g acts by multiplication by a primitive pth root of unity on some of the irreducible components of W. That is only possible if $\mathrm{char}\, k \neq p$.

Definition 4. G is called *semifaithful* (over k) if it admits a completely reducible faithful representation (over k).

By a result of Nakayama [Na47, Theorem 1] a finite group G is semifaithful over a field of $\mathrm{char}\, k = p > 0$ if and only if it has no nontrivial normal p-subgroups.

Corollary 3. *If* G *is semifaithful or, equivalently, if either* $\mathrm{char}\, k = 0$ *or* $\mathrm{char}\, k = p > 0$ *and* G *has no nontrivial normal* p*-subgroup, there exists a multihomogeneous minimal faithful covariant for* G.

2.2. Degree matrix and k-center

The following subgroup of G will play an important role in the sequel.

Definition 5. The central subgroup

$$Z(G,k) := \{g \in Z(G) \mid k \text{ contains primitive } (\operatorname{ord} g)\text{th roots of unity}\}$$

of G is called the *k-center* of G. In the sequel, as usual, $\zeta_n \in \bar{k}$ denotes a primitive nth root of unity when either $\operatorname{char} k = 0$ or $(\operatorname{char} k, n) = 1$.

The k-center of G is the largest central subgroup Z which is diagonalizable as a constant algebraic group over k. The elements of $Z(G,k)$ are precisely the elements of G which act as scalars on every irreducible representation of G over k.

Lemma 4. *Let $V = \bigoplus_{i=1}^m V_i$ be a faithful representation of G with all V_i irreducible. Then $\rho_V(Z(G,k)) = T_V \cap \rho_V(G)$.*

Proof. Since both sides are abelian groups it suffices to prove equality for their Sylow subgroups. Let p be a prime ($p \neq \operatorname{char} k$) and let $g \in Z(G)$ be an element of order p^l for some $l \in \mathbb{N}_0$. We must show that the following conditions are equivalent:

(A) g acts as a scalar on every V_i; and
(B) $\zeta_{p^l} \in k$.

Since V is faithful the order of g equals the order of $\rho(g) \in \mathrm{GL}(V)$, hence the first condition implies the second one. Conversely, let $\rho'' \colon G \to \mathrm{GL}(V'')$ be any irreducible representation of G. Then the minimal polynomial of $\rho''(g)$ has a root in k since it divides $T^{p^l} - 1 \in k[T]$ which factors over k assuming the second condition. Hence $\rho''(g)$ is a multiple of the identity on V''. In particular this holds for all $G \to \mathrm{GL}(V_i)$, proving the claim. $\square$

Let G be semifaithful and let $V = \bigoplus_{i=1}^m V_i, W = \bigoplus_{j=1}^n W_j$ be two faithful representations of G. For a faithful multihomogeneous covariant $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ we will prove the following inequality relating the rank of M_φ and the rank of $Z(G,k)$.

Theorem 5. *Let $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ be a faithful multihomogeneous covariant between representations $V = \bigoplus_{i=1}^m V_i$, $W = \bigoplus_{j=1}^n W_j$ with all V_i and W_j irreducible. Then*

$$\operatorname{edim}_k G - \operatorname{rk} Z(G,k) \leq \dim \varphi - \operatorname{rk} M_\varphi.$$

Moreover,

$$\operatorname{rk} M_\varphi \geq \operatorname{rk} Z(G,k)$$

with equality in case that φ is minimal.

Remark 1. The case when G has trivial center (and $k = \mathbb{C}$) is [KLS09, Prop. 3.4].

Proof of Theorem 5. Let $\rho_V \colon G \to \mathrm{GL}(V)$ and $\rho_W \colon G \to \mathrm{GL}(W)$ denote the representation homomorphisms. We first prove the second inequality. By Lemma 4 we have $\rho_V(Z(G,k)) \subseteq T_V$. Since φ is equivariant with respect to both tori- and G-actions, $\rho_W(g)\varphi(v) = \varphi(\rho_V(g)v) = D_\varphi(\rho_V(g))\varphi(v)$ for $g \in Z(G,k)$. Thus $\rho_W(Z(G,k)) = D_\varphi(\rho_V(Z(G,k))) \subseteq D_\varphi(T_V)$, whence $\operatorname{rk} M_\varphi = \operatorname{rk} D_\varphi(T_V) \geq \operatorname{rk} \rho_W(Z(G,k)) = \operatorname{rk} Z(G,k)$.

The first inequality follows from the following Proposition 6, which yields a compression $\mathbb{A}(V) \dashrightarrow X'/S$ of $\mathbb{A}(V)$ to the geometric quotient of a dense open subset X' of $\overline{\operatorname{im}\varphi}$ by a free action of a torus S of dimension $\operatorname{rk} M_\varphi - \operatorname{rk} Z(G,k)$. $\square$

Proposition 6. *Under the assumptions of Theorem 5 there exists a subtorus $S \subseteq D_\varphi(T_V)$ of dimension $\operatorname{rk} M_\varphi - \operatorname{rk} Z(G,k)$ and a G-invariant open subset $W' \subseteq \mathbb{A}(W)$ on which $D_\varphi(T_V)$ acts freely such that the geometric quotient $(\overline{\operatorname{im}\varphi} \cap W')/S$ exists as a variety and its induced G-action is faithful.*

For the proof of Proposition 6 we need the following result which is an obvious generalization of Lemma 3.3 from [KLS09].

Lemma 7. *Let $\varphi = (\varphi_1, \dots, \varphi_n)\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ be a faithful multihomogeneous covariant with W_j irreducible and $\varphi_j \neq 0$ for all j. Let $\pi_W\colon \mathbb{A}(W) \dashrightarrow \mathbb{PP}(W) := \prod_j \mathbb{P}(W_j)$ be the obvious G-equivariant rational map. Then the kernel of the action of G on $\pi_W(\overline{\operatorname{im}\varphi})$ equals $Z(G,k)$.*

Proof of Proposition 6. Removing zero-components of φ we may assume that $\varphi_j \neq 0$ for all j. Let $Z := \rho_W(Z(G,k))$. The torus $D_\varphi(T_V)$ contains Z and has dimension $d := \operatorname{rk} M_\varphi \geq r := \operatorname{rk} Z$. By the elementary divisor theorem there exist integers $c_1, \dots, c_r > 1$ and a basis $\chi_1, \dots, \chi_d$ of $X(D_\varphi(T_V))$ such that

$$Z = \bigcap_{i=1}^{r} \ker \chi_i^{c_i} \cap \bigcap_{j=r+1}^{d} \ker \chi_j.$$

Set $S := \bigcap_{i=1}^{r} \ker \chi_i$. This is a subtorus of $D_\varphi(T_V)$ of rank $d - r = \operatorname{rk} M_\varphi - \operatorname{rk} Z$ with $S \cap Z = \{1\}$.

Let $W' := \prod_{j=1}^{n} (\mathbb{A}(W_j) \setminus \{0\})$. Since φ is multihomogeneous the closed subgroup $S \subseteq D_\varphi(T_V)$ preserves $X := \overline{\operatorname{im}\varphi}$ and also the open subset $X' := X \cap W'$ of X. The S-action on X' is free in the sense of [MFK94, Def. 0.8] and in particular seperated. In the notation of [MFK94] X' coincides with $(X')^s(\mathrm{Pre})$. By [MFK94, Prop. 1.9] a geometric quotient X'/S of X' by the action of the reductive algebraic group S exists as a scheme of finite type over k. By [MFK94, Chap. 0, §2, Remark (2) and Lemma 0.6] X'/S is a variety. Moreover X'/S is a categorical quotient. Since the G-action on X' commutes with the S-action it passes to X'/S. The kernel of the G-action on X'/S is contained in $Z(G,k)$ by Lemma 7. Since $Z \cap S = \{e\}$ it is trivial. $\square$

To illustrate the usefulness of the existence of minimal faithful multihomogeneous covariants and Lemma 7 we give a simple corollary.

Corollary 8. *Let G be a semifaithful group.*

- *If $\operatorname{edim}_k G \leq \operatorname{rk} Z(G,k)$, then $G = Z(G,k)$, hence G is abelian and $\zeta_{\exp G} \in k$.*
- *If $\operatorname{edim}_k G \leq \operatorname{rk} Z(G,k) + 1$, then G is an extension of a subgroup of $\mathrm{PGL}_2(k)$ by $Z(G,k)$.*

Proof. Let $V = \bigoplus_{j=1}^n V_j$ be a completely reducible faithful representation of G and let $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(V)$ be a minimal faithful multihomogeneous covariant of G. We may assume that $\varphi_j \neq 0$ for all j. Let $X := \overline{\operatorname{im}\varphi}$. By Lemma 7 the group $G/Z(G,k)$ acts faithfully on $Y := \overline{\pi_V(X)} \subseteq \mathbb{PP}(V)$. The nonempty fibers of the restriction $X \dashrightarrow Y, x \mapsto \pi_V(x)$ of π_V have dimension $\geq \dim D_\varphi(T_V) = \operatorname{rk} M_\varphi$, which is equal to $\operatorname{rk} Z(G,k)$ by Theorem 5. Hence, $\dim Y \leq \dim X - \dim D_\varphi(T_V) = \dim\varphi - \operatorname{rk} Z(G,k) = \operatorname{edim}_k G - \operatorname{rk} Z(G,k)$.

In the first case, when $\operatorname{edim}_k G \leq \operatorname{rk} Z(G,k)$, the variety Y must be a single point, whence $G = Z(G,k)$. In the second case, when $\operatorname{edim}_k G \leq \operatorname{rk} Z(G,k) + 1$, the variety Y is unirational and has dimension ≤ 1 and it follows by Lüroth's theorem that $G/Z(G,k)$ embeds into $\mathrm{PGL}_2(k)$. $\square$

Remark 2. Corollary 8 can be used to classify semifaithful groups with $\operatorname{edim}_k G - \operatorname{rk} Z(G,k) \leq 1$. We conjecture that any semifaithful group G of $\operatorname{edim}_k G \leq 2$ with nontrivial k-center $Z(G,k)$ embeds into $\mathrm{GL}_2(k)$. In the case of $k = \mathbb{C}$ this follows from [KS07, Theorem 10.2] combined with [KLS09, Theorem 3.1].

3. The central extension theorem

As announced in the Introduction we shall prove a generalization of the theorem about the essential dimension of central extensions from [BR97].

Theorem 9. *Let G be a semifaithful group. Let H be a central subgroup of G with $H \cap [G,G] = \{e\}$. Let H' be a direct factor of $G/[G,G]$ containing the image of H under the embedding $H \hookrightarrow G/[G,G]$ and assume that k contains primitive roots of unity of order* $\exp H'$. *Then*

$$\operatorname{edim}_k G - \operatorname{rk} Z(G,k) = \operatorname{edim}_k G/H - \operatorname{rk} Z(G/H,k).$$

Remark 3. Theorem 9 generalizes the following results about central extensions: [BR97, Theorem 5.3], [Ka08, Theorem 4.5], [KLS09, Cors. 3.7 and 4.7], [Le04, Theorem 8.2.11] as well as [BRV08, Theorem 7.1 and Cor. 7.2] and [BRV07, Lemma 11.2].

If G is a p-group then Theorem 9 can be deduced from the theorem of Karpenko and Merkurjev about the essential dimension of p-groups.

Proof of Theorem 9. It is straightforward to reduce to the case where H is cyclic. We leave this to the reader. The assumptions on G and H imply the existence of a faithful representation of G of the form $V \oplus k_\chi$ where χ is faithful on H and $V = \bigoplus_{i=1}^n V_i$ is a completely reducible representation with kernel H. We prove the two inequalities of the equation $\operatorname{edim}_k G - \operatorname{edim}_k G/H = \operatorname{rk} Z(G,k) - \operatorname{rk} Z(G/H,k)$ separately.

"$\leq$": Let $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(V)$ be a minimal faithful multihomogeneous covariant of G/H. Define a faithful covariant of G via

$$\Phi\colon \mathbb{A}(V \oplus k_\chi) \dashrightarrow \mathbb{A}(V \oplus k_\chi), \qquad (v,t) \mapsto (\varphi(v), t).$$

Clearly Φ is multihomogeneous again of rank $\operatorname{rk} M_\Phi = \operatorname{rk} M_\varphi + 1 = \operatorname{rk} Z(G/H,k) + 1$, where the last equality comes from Theorem 5. Moreover, by the same theorem,

$$\operatorname{edim}_k G \leq \dim\Phi - (\operatorname{rk} M_\Phi - \operatorname{rk} Z(G,k)) = \operatorname{edim}_k G/H - \operatorname{rk} Z(G/H,k) + \operatorname{rk} Z(G,k).$$

"$\geq$": Let $\varphi\colon \mathbb{A}(V \oplus k_\chi) \dashrightarrow \mathbb{A}(V \oplus k_\chi)$ be a minimal faithful multihomogeneous covariant of G. Let $m := |H|$ and consider the G-equivariant regular map

$$\pi\colon \mathbb{A}(V \oplus k_\chi) \to \mathbb{A}(V \oplus k_{\chi^m})$$

defined by $(v,t) \mapsto (v, t^m)$. It is a geometric quotient of $\mathbb{A}(V \oplus k_\chi)$ by the action of H. The composition $\varphi' := \pi \circ \varphi\colon \mathbb{A}(V \oplus k_\chi) \dashrightarrow \mathbb{A}(V \oplus k_{\chi^m})$ is H-invariant, hence we get a commutative diagram:

$$\begin{tikzcd}
\mathbb{A}(V \oplus k_\chi) \arrow[r, dashed, "\varphi"] \arrow[d, "\pi"'] \arrow[dr, dashed, "\varphi'"] & \mathbb{A}(V \oplus k_\chi) \arrow[d, "\pi"] \\
\mathbb{A}(V \oplus k_{\chi^m}) \arrow[r, dashed, "\bar\varphi"] & \mathbb{A}(V \oplus k_{\chi^m}),
\end{tikzcd}$$

where $\bar\varphi\colon \mathbb{A}(V \oplus k_{\chi^m}) \dashrightarrow \mathbb{A}(V \oplus k_{\chi^m})$ is a faithful G/H-covariant. Since π is finite the rational maps φ, φ' and $\bar\varphi$ all have the same dimension $\operatorname{edim}_k G$. Moreover, φ' and $\bar\varphi$ are multihomogeneous as well. The degree matrix $M_{\varphi'}$ is obtained from M_φ by multiplying its last column by m and from $M_{\bar\varphi}$ by multiplying its last row by m. Hence $\operatorname{rk} M_\varphi = \operatorname{rk} M_{\varphi'} = \operatorname{rk} M_{\bar\varphi}$. Application of Theorem 5 yields $\operatorname{edim}_k G/H - \operatorname{rk} Z(G/H,k) \leq \dim \bar\varphi - \operatorname{rk} M_{\bar\varphi} = \operatorname{edim}_k G - \operatorname{rk} Z(G,k)$. This finishes the proof. $\square$

Corollary 10. *Let G and A be groups, where G is semifaithful and A is abelian. Assume that k contains a primitive root of unity of order* $\exp A$. *Then*

$$\operatorname{edim}_k(G \times A) - \operatorname{rk}(Z(G,k) \times A) = \operatorname{edim}_k G - \operatorname{rk} Z(G,k).$$

Proof. Apply Theorem 9 to the central subgroup $\{e\} \times A \subseteq G \times A$. $\square$

4. Direct products

Proposition 11. *Let G_1 and G_2 be semifaithful groups. Then*

$$\operatorname{edim}_k G_1 \times G_2 - \operatorname{rk} Z(G_1 \times G_2, k) \leq \operatorname{edim}_k G_1 - \operatorname{rk} Z(G_1,k) + \operatorname{edim}_k G_2 - \operatorname{rk} Z(G_2,k).$$

Proof. Let $V = \bigoplus_{i=1}^m V_i$ and $W = \bigoplus_{j=1}^n W_j$ be faithful representations of G_1 and G_2, respectively, where each V_i and W_j is irreducible. Let $\varphi_1\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(V)$ and $\varphi_2\colon \mathbb{A}(W) \dashrightarrow \mathbb{A}(W)$ be minimal faithful multihomogeneous covariants for G_1 and G_2. Then $\operatorname{rk} M_{\varphi_1} = \operatorname{rk} Z(G_1,k)$ and $\operatorname{rk} M_{\varphi_2} = \operatorname{rk} Z(G_2,k)$ by Theorem 5. The covariant $\varphi_1 \times \varphi_2\colon \mathbb{A}(V \oplus W) \dashrightarrow \mathbb{A}(V \oplus W)$ for $G_1 \times G_2$ is again faithful and multihomogeneous with $\operatorname{rk} M_\varphi = \operatorname{rk} M_{\varphi_1} + \operatorname{rk} M_{\varphi_2} = \operatorname{rk} Z(G_1,k) + \operatorname{rk} Z(G_2,k)$. Thus, by Theorem 5,

$$\begin{aligned}
\operatorname{edim}_k G_1 \times G_2 - \operatorname{rk} Z(G_1 \times G_2, k) &\leq \dim \varphi - \operatorname{rk} M_\varphi \\
&= \dim \varphi_1 + \dim \varphi_2 - \operatorname{rk} Z(G_1,k) - \operatorname{rk} Z(G_2,k).
\end{aligned}$$

Since $\dim \varphi_1 = \operatorname{edim}_k G_1$ and $\dim \varphi_2 = \operatorname{edim}_k G_2$, this implies the claim. $\square$

Remark 4. We do not know of an example where the inequality in Proposition 11 is strict.

5. Twisting by torsors

In the sequel we use the following notation.

Definition 6. Let $V = \bigoplus_{i=1}^m V_i$ be a graded vector space. Define the variety $\mathbb{PP}(V)$ by

$$\mathbb{PP}(V) := \mathbb{P}(V_1) \times \cdots \times \mathbb{P}(V_m).$$

It is the geometric quotient of the natural free T_V action on the open subset $(\mathbb{A}(V_1) \setminus \{0\}) \times \cdots \times (\mathbb{A}(V_m) \setminus \{0\}) \subset \mathbb{A}(V)$. We write $\pi_V : \mathbb{A}(V) \dashrightarrow \mathbb{PP}(V)$ for the corresponding rational quotient map.

Now assume that $V = \bigoplus_{i=1}^m V_i$ is a faithful representation of G where each V_i is irreducible and let $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(V)$ be a multihomogeneous covariant of G with $\varphi_j \neq 0$ for all j. Since φ is multihomogeneous the composition $\pi_V \circ \varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{PP}(V)$ is T_V-invariant. Hence there exists a rational map $\psi\colon \mathbb{PP}(V) \dashrightarrow \mathbb{PP}(V)$ making the diagram

$$\begin{tikzcd} \mathbb{A}(V) \arrow[r, dashed, "\varphi"] \arrow[d, dashed, "\pi_V"] & \mathbb{A}(V) \arrow[d, dashed, "\pi_V"] \\ \mathbb{PP}(V) \arrow[r, dashed, "\psi"] & \mathbb{PP}(V) \end{tikzcd}$$

commute. Let $Z := Z(G,k)$ which acts trivially on $\mathbb{PP}(V)$ and let $C \subseteq Z$ be any subgroup. We view ψ as an $H := G/C$-equivariant rational map. Let K/k be a field extension and let E be an H-torsor over K. We will twist the map ψ by the H-torsor E to get a rational map ${}^E\psi_K\colon {}^E\mathbb{PP}(V_K) \dashrightarrow {}^E\mathbb{PP}(V_K)$. For the construction and basic properties of the twist construction we refer to [Fl08, Sect. 2]. The twisted variety is described in the following lemma.

Lemma 12. ${}^E\mathbb{PP}(V_K) \simeq \prod_{i=1}^m \mathrm{SB}(A_i)$. *Here* $\mathrm{SB}(A_i)$ *denotes the Severi–Brauer variety of the twist* A_i *of* $\mathrm{End}_K(V_i \otimes K)$ *by the* H*-torsor* E*. Moreover, the class of* A_i *in the Brauer group* $\mathrm{Br}(K)$ *coincides with the image* $\beta^E(\chi)$ *of* E *under the map*

$$H^1(K,H) \to H^2(K,C) \xrightarrow{\chi_*} H^2(K,\mathbb{G}_m) = \mathrm{Br}(K),$$

where $\chi \in C^*$ *is the character defined by* $gv = \chi(g)v$ *for* $g \in C$ *and* $v \in V_i$*.*

Proof. The first claim follows from [Fl08, Lemma 3.1]. For the second claim see [KM08, Lemma 4.3]. $\square$

For a smooth projective variety X the number $e(X)$ is defined as the least dimension of the closure of the image of a rational map $X \dashrightarrow X$. This number is expressed in terms of generic splitting fields in the following Lemma 13.

Definition 7. Let X be a K-variety and let $D \subseteq \mathrm{Br}(K)$ be a subgroup of the Brauer group of K. The *canonical dimension of* X (resp. D) is defined as the least transcendence degree (over K) of a generic splitting field (in the sense of [KM08, Sect. 1.4]) of X (resp. D). It is denoted by $\mathrm{cd}(X)$ (resp. $\mathrm{cd}(D)$).

Lemma 13 ([KM06, Cor. 4.6]). *Let $X = \prod_{i=1}^{n} \mathrm{SB}(A_i)$ be a product of Severi–Brauer varieties of central simple K-algebras $A_1, \ldots, A_n$. Then $e(X) = \mathrm{cd}(X) = \mathrm{cd}(D)$, where $D \subseteq \mathrm{Br}(K)$ is the subgroup generated by the classes of $A_1, \ldots, A_n$.*

Our main result in this section is the following theorem, which is a generalization of a result of Karpenko and Merkurjev [KM08, Theorems 4.2 and 3.1].

Theorem 14. *Let G be a semifaithful group and let $V = \bigoplus_{i=1}^{m} V_i$ be a faithful representation of G with each V_i irreducible. Let E be a G/C-torsor over an extension K of k where C is any subgroup of $Z(G,k)$. Then*

$$\mathrm{edim}_k\, G - \mathrm{rk}\, Z(G,k) \geq e({}^{E}\mathbb{PP}(V_K)) = \mathrm{cd}(\mathrm{im}\, \beta^{E}).$$

Proof. Let $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(V)$ and $\psi\colon \mathbb{PP}(V) \dashrightarrow \mathbb{PP}(V)$ be as at the beginning of this section and assume that φ is minimal, i.e. $\dim \varphi = \mathrm{edim}_k\, G$. By functoriality we have $\dim {}^{E}\psi_K \leq \dim \psi_K$. Hence

$$e({}^{E}\mathbb{PP}(V_K)) \leq \dim {}^{E}\psi_K \leq \dim \psi_K = \dim \psi.$$

We now show that $\dim \psi \leq \dim \varphi - \mathrm{rk}\, Z(G,k)$. Let $X := \overline{\mathrm{im}\, \varphi} \subseteq \mathbb{A}(V)$. The fibers of $\pi_V|_X\colon X \to \mathbb{PP}(V)$ are stable under the torus $D_\varphi(T_V) \subseteq T_V$. The dimension of $D_\varphi(T_V)$ is greater than or equal to $\mathrm{rk}\, Z(G,k)$, since it contains the image of $Z(G,k)$ under the representation $G \hookrightarrow \mathrm{GL}(V)$. Moreover, $D_\varphi(T_V)$ acts generically freely on X. Hence the claim follows by the fiber dimension theorem. Since the restriction of V to C is faithful, the characters $\chi_1, \ldots, \chi_m$ generate C^*. Lemmas 13 and 12 imply $e({}^{E}\mathbb{PP}(V_K)) = \mathrm{cd}({}^{E}\mathbb{PP}(V_K)) = \mathrm{cd}\,\mathrm{im}\, \beta^{E}$, hence the claim. $\square$

We now go further to prove a generalization of [KM08, Theorem 4.1]. Our generalization however involves two key results from their work.

Theorem 15 ([KM08, Theorem 2.1 and Remark 2.9]). *Let p be a prime, K be a field and let $D \subseteq \mathrm{Br}(K)$ be a finite p-subgroup of rank $r \in \mathbb{N}$. Then $\mathrm{cd}\, D = \min\{ \sum_{i=1}^{r} (\mathrm{Ind}\, a_i - 1)\}$ taken over all generating sets $a_1, \ldots, a_r$ of D. Here $\mathrm{Ind}\, a_i$ denotes the index of a_i.*

For a central diagonalizable subgroup C of an algebraic group G and $\chi \in C^*$ we denote by $\mathrm{rep}^{(\chi)}(G)$ the class of irreducible representations of G on which C acts through scalar multiplication by χ.

Theorem 16 ([KM08, Theorem 4.4 and Remark 4.5]). *Let $1 \to C \to G \to H \to 1$ be an exact sequence of algebraic groups over some field k with C central and diagonalizable. Then there exists an H-torsor E over some field extension K/k such that, for all $\chi \in C^*$,*

$$\mathrm{Ind}\, \beta^{E}(\chi) = \gcd\{\dim V \mid V \in \mathrm{rep}^{(\chi)}(G)\}.$$

We have the following result.

Corollary 17 (cf. [KM08, Theorem 4.1]). *Let G be an arbitrary group whose socle C is a central p-subgroup for some prime p and let k be a field containing a primitive pth root of unity. Assume that for all $\chi \in C^*$ the equality*

$$\gcd\{\dim V \mid V \in \mathrm{rep}^{(\chi)}(G)\} = \min\{\dim V \mid V \in \mathrm{rep}^{(\chi)}(G)\}$$

holds. Then $\mathrm{edim}_k\, G$ is equal to the least dimension of a faithful representation of G.

Proof. Let d denote the least dimension of a faithful representation of G. The upper bound $\operatorname{edim}_k G \le d$ is clear. By the assumption on k we have $\operatorname{rk} C = \operatorname{rk} Z(G,k) = \operatorname{rk} Z(G)$. Hence, by Theorem 14, it suffices to show $\operatorname{cd}(\operatorname{im}\beta^E) = d - \operatorname{rk} C$ for some $H := G/C$-torsor E over a field extension K of k.

By Theorem 15 there exists a basis $a_1, \dots, a_s$ of $\operatorname{im}\beta^E$ such that $\operatorname{cd}(\operatorname{im}\beta^E) = \sum_{i=1}^s (\operatorname{Ind} a_i - 1)$. Choose a basis $\chi_1, \dots, \chi_r$ of C^* such that $a_i = \beta^E(\chi_i)$ for $i = 1, \dots, s$ and $\beta^E(\chi_i) = 1$ for $i > s$ and choose $V_i \in \operatorname{rep}^{(\chi_i)}(G)$ of minimal dimension. By assumption $\dim V_i = \gcd\left\{\dim V \mid V \in \operatorname{rep}^{(\chi_i)}(G)\right\}$, which is equal to the index of $\beta^E(\chi_i)$ for the H-torsor E of Theorem 16.

Set $V = V_1 \oplus \cdots \oplus V_r$. This is a faithful representation of G since every normal subgroup of G intersects $C = \operatorname{soc} G$ nontrivially. Then $\operatorname{cd}(\operatorname{im}\beta^E) = \sum_{i=1}^s (\operatorname{Ind} a_i - 1) = \sum_{i=1}^r \operatorname{Ind}\beta^E(\chi_i) - \operatorname{rk} C = \sum_{i=1}^r \dim V_i - \operatorname{rk} C = \dim V - \operatorname{rk} C \ge d - \operatorname{rk} C$. The claim follows. $\square$

We conclude this section with the following conjecture, which is based on Theorem 14 and the formula

$$\operatorname{cd}(D) = \sum_p \operatorname{cd}(D(p)) \tag{3}$$

for any finite subgroup $D \subseteq \operatorname{Br}(K)$ with p-Sylow subgroups $D(p)$. This formula was conjectured in [CKM07] (in case D is cyclic) and discussed in [BRV07, Sect. 7].

Conjecture 18. *Let G be nilpotent. Assume that k contains a primitive pth root of unity for every prime p dividing $|G|$. Let d_p denote the least dimension of a faithful representation of a p-Sylow subgroup of G, and let $C(p)$ denote a p-Sylow subgroup of $C := \operatorname{soc}(G)$. Then*

$$\operatorname{edim}_k G = \sum_p (d_p - \operatorname{rk} C(p)) + \operatorname{rk} C.$$

Remark 5. Formula (3) was proved in [CKM07] in the special case where D is cyclic of order 6 and k contains $\mathbb{Q}(\zeta_3)$. In particular, let $G = G_2 \times G_3$ where G_p is a p-group of essential dimension p for $p = 2, 3$. Then $\operatorname{edim}_k G = 4$ for any field k containing $\mathbb{Q}(\zeta_3)$.

References

[BF03] G. Berhuy, G. Favi, *Essential dimension: A functorial point of view (after A. Merkurjev)*, Doc. Math. **8** (2003), 279–330.

[BR97] J. Buhler, Z. Reichstein, *On the essential dimension of a finite group*, Compositio Math. **106** (1997), 159–179.

[BRV07] P. Brosnan, Z. Reichstein, A. Vistoli, *Essential dimension and algebraic stacks*, `http://www.math.ubc.ca/~reichst/pub.html` (2007).

[BRV08] P. Brosnan, Z. Reichstein, A. Vistoli, *Essential dimension and algebraic stacks I*, Linear Algebraic Groups and Related Structures Preprint Server, `http://www.math.uni-bielefeld.de/LAG/man/275.pdf` (2008).

[CKM07] Ж.-Л. Кольо-Телен, Н. Карпенко, А. Меркурьев, *Рациональные поверхности и каноническая размерность* PGL_6, Алгебра и анализ **19** (2007), no. 5, 159–178. Engl. transl.: J.-L. Colliot-Thélène, N. Karpenko, A. Merkurjev, *Rational surfaces and canonical dimension of* PGL_6, St. Petersburg Math. J. **19** (2008), no. 5, 793–804.

[Fl08] M. Florence, *On the essential dimension of cyclic p-groups*, Invent. Math. **171** (2008), 175–189.

[Ka08] M. C. Kang, *A central extension theorem for essential dimensions*, Proc. Amer. Math. Soc. **136** (2008), 809–813.

[KM06] N. Karpenko, A. Merkurjev, *Canonical p-dimension of algebraic groups*, Adv. Math. **205**, no. 2 (2006), 410–433.

[KM08] N. Karpenko, A. Merkurjev, *Essential dimension of finite p-groups*, Invent. Math., **172** (2008), 491–508.

[KLS09] H. Kraft, R. Lötscher, G. Schwarz, *Compression of finite group actions and covariant dimension* II, J. Algebra **322** (2009), no. 1, 94–107.

[KS07] H. Kraft, G. Schwarz, *Compression of finite group actions and covariant dimension*, J. Algebra **313** (2007), 268–291.

[Le04] A. Ledet, *On the essential dimension of p-groups*, in: *Galois Theory and Geometry with Applications*, Springer, New York, 2004, pp. 159–172.

[MFK94] D. Mumford, J. Fogarty, F. Kirwan, *Geometric Invariant Theory*, 3rd ed., Ergebnisse der Mathematik und ihrer Grenzgebiete (2), Vol. 34, Springer-Verlag, Berlin, 1994.

[Na47] T. Nakayama, *Finite groups with faithful irreducible and directly indecomposable modular representations*, Proc. Japan Acad. Ser. A Math. Sci. **23** (1947), 22–25.

[Re04] Z. Reichstein, *Compressions of group actions*, in: *Invariant Theory in all Characteristics*, CRM Proc. Lecture Notes, Vol. 35, Amer. Math. Soc., Providence, RI, 2004, pp. 199–202.